Avaya System Connectivity and Cisco Network Configuration Guide

May 2008

Version 1.6

Contents

1 Introduction

This document is written specifically for network engineers who will be responsible for providing the necessary network support and connectivity for a new Avaya system or an existing Avaya system that is to be migrated to IP. This document only details relevant Avaya system configuration relating to network connectivity and does not provide reference for more general Avaya system configuration.

Key Avaya system design and Cisco switch/router configuration details are discussed here. This relates to logical Avaya system design, network design and physical connectivity specifically for typical central and remote location solutions. This document outlines **example** network configurations. Port, QoS and general design/configuration can take many forms. As a result, the exact syntax or values chosen for any particular network environment may vary from the configurations shown here.

Distinct Cisco hardware platforms using various IOS and/or CatOS revisions may implement certain features using a variety of different commands. This document attempts to incorporate most of these differences but may not include all. Please refer to the specific Cisco documentation for further information. Diagrams illustrating Avaya device connectivity show the recommended connection methods.

This document does not discuss Cisco AutoQoS. The Cisco AutoQoS feature is a mechanism allowing the automation of QoS configuration across LAN switches (not WAN routers) and can be used to configure the environment successfully for use with the Avaya system. This document details a ‘manual’ approach to QoS implementation in order to provide a greater level of understanding for those wishing to deploy the necessary elements of Cisco QoS configuration. Please refer to the relevant Cisco AutoQoS documentation.

2 Pre-Statement for QoS, Port and PoE Configuration

2.1 QoS

QoS markings will require agreement by all parties and used consistently throughout the network. The customer will need to determine whether to use CoS (802.1p) tags in the LAN and DiffServ (DSCP) in the WAN or DSCP throughout LAN and WAN. The example below will instruct the Avaya system to mark signalling, audio and video traffic with the values shown, as configured in the **network-region** form. Upon registration, IP Phones, IP Softphone and H.248 gateways will tag signalling, audio and video with these values. In order to ensure IP Phones receive 802.1p values, the Avaya **ip-network-map** form must also be populated with the destination VLAN IDs associated to each group of IP Phones.

CoS/802.1p for signalling traffic = 3 (default 7)
CoS/802.1p for audio traffic = 5 (default 6)
CoS/802.1p for video traffic = 4 (default 7)
DSCP for signalling traffic = 24 (default 34)
DSCP for bearer (audio) traffic = 46 (default 46)
DSCP for video traffic = 34 (default 34)

NB: QoS parameters for 802.1p and DSCP must be consistent between the Avaya system (network-region) and the configuration implemented across the network. Inconsistent QoS classification, marking and/or scheduling policies between network and Avaya system may impact voice quality and/or system stability.

NB: Please see section 3.4.1.1 for QoS recommendations for S87xx to/from IPSI traffic.

2.2 Power to IP Phones

Power over Ethernet (PoE) provided by LAN switches for IP Phones **must** be 802.3af compliant. Avaya cannot guarantee successful operation with any proprietory inline power mechanism. Correct power calculations must be made to ensure sufficient power is available for **all** IP Phones connected to each individual LAN switch or line module.

2.3 Port Speed/Duplex

Avaya recommends Cisco ports connected to CLAN, MedPro, IPSI, S8xxx, G700, G450, G350 and G250 are **fixed at 100Mb/s full-duplex**. Cisco LAN switch ports connecting IP Phones should be configured for **auto-negotiation**. PCs connecting to IP Phones' secondary Ethernet ports should also be auto-negotiation. To avoid duplex mismatch, fixed or auto values must be identically configured ***at both ends of the Ethernet link***. A value of 'auto' at one end and 'fixed' at the other will result in duplex mismatch.

2.4 IP Phone Local Connection

LAN switch ports connecting IP Phones are configured as **trunk** ports. CoS (802.1p) and DSCP values can be marked by the Avaya IP Phone (see section 2.1) or alternatively, marked by the network. If marked by the Avaya IP Phone (recommended), the corresponding Cisco switch port will trust the incoming CoS or DSCP value ('trust dscp' is recommended).

<u>NB:</u> Whether connections to IP Phones use the ‘traditional 802.1Q method’ or make use of Cisco’s proprietory ‘voice vlan’ (IOS) or ‘auxiliaryvlan’ (CatOS) method, the link to the IP Phone uses a VLAN trunk. With ‘voice vlan’ and ‘auxiliaryvlan’ more Cisco features are available (eg. bpdu-guard, 802.1X). Please see section 3.1 in this document and the relevant Cisco documentation.

2.5 MedPro, CLAN, IPSI, S87xx, G700, G450, G350, G250 Local Connections

LAN switch ports connecting MedPro, CLAN, G700, G450, G350, G250, S8xxx and IPSI are configured as **access** ports. Ingress traffic from MedPro, CLAN, G700, G450, G350 & G250 will be marked at the corresponding Cisco switch ports with a default port priority (cos) value or will be configured to trust incoming DSCP values (trust-dscp is recommended) depending on which method is chosen. Assuming S8xxx and IPSI traffic stay within the LAN environment (ie. do not pass over a WAN) and exist in dedicated VLANs, QoS parameters may not be required for IPSI and corresponding S8xxx interfaces. This will be dependent on the network topology and may require further discussion to confirm. If S8xxx to/from IPSI traffic passes over a WAN (eg. in ESS or remote G650 deployments) this traffic *must be given priority* over the network. Avaya strongly recommend using a minimum of AF42 (DSCP36) but, ideally, EF (DSCP46) for this traffic.

<u>NB:</u> Please note that 802.1p is a component of the 802.1Q header. If there is no 802.1Q header (ie. the link is not a trunk), 802.1p values will not be present. In the case above, the ports are configured as access ports (not trunk ports). Therefore, no 802.1Q/802.1p header exists. In this case, either set the default priority of the LAN switch port to use cos (802.1p) 5 or trust the DSCP header (recommended) which exists regardless of whether the port is a trunk or access.

3 Connectivity

3.1 Summary Review of Avaya Components

G650 gateway is the high density gateway that can be stacked. In Avaya parlance a collection of stacked G650s is known as a 'Port Network' (PN). The key network facing boards in the PN are IPSI (IP Server Interface), CLAN (Control LAN), MedPro (Media Processor). IPSI allows communication between the server (S8xxx) and the PN (there are 2x IPSI boards, A & B, per PN for redundancy). The CLAN handles signalling traffic to IP Phones & smaller gateways such as G700/G450/G350/G250 and other PNs, and MedPro which handles audio RTP streams to IP Phones, smaller gateways and other PNs. Access to CLAN and MedPro resource is load balanced. See Figure A.

The S8xxx series server is the processor controlling all call processing. S87xx are installed in pairs for redundancy. S85xx are installed as single servers. S8400 can be installed directly in G650 PNs and S8300 are Local Survivable Processors (LSP) designed for G700, G450, G350 & G250 only. In typical, redundant deployments the S8300 is used to provide local PBX processing should the primary (S87xx or S85xx) server become unavailable. S8xxx series servers are analogous to a supervisor module in a Cisco Catalyst 6500 switch. They provide all call processing function (IP, non-IP, incoming/outgoing, Softphone, video etc) as a primary or redundant server in the same way that Catalyst supervisor modules provide all processing relating to Ethernet switching. The S87xx & S85xx series servers reside externally from the gateways (G650 PNs). S8400 & S8300 series servers are installed as a blade inside their corresponding gateways. External S87xx & S85xx servers communicate with the G650s (PNs) via TCP connections to IPSI boards inside the PN chassis. Hence, the S87xx & S85xx to/from IPSI communication must be up and functioning at all times. See Figure A.

The smaller gateways G700, G450, G350, G250 do not connect to the primary server directly via IPSI. They register via a CLAN (H.248) located inside a G650 PN, providing access to the server. As a result, these are sometimes referred to as 'H.248 gateways'. For smaller installations, H.248 gateways can provide call processing functionality (S8300) without the need of central S87xx servers and PNs. See Figure A.

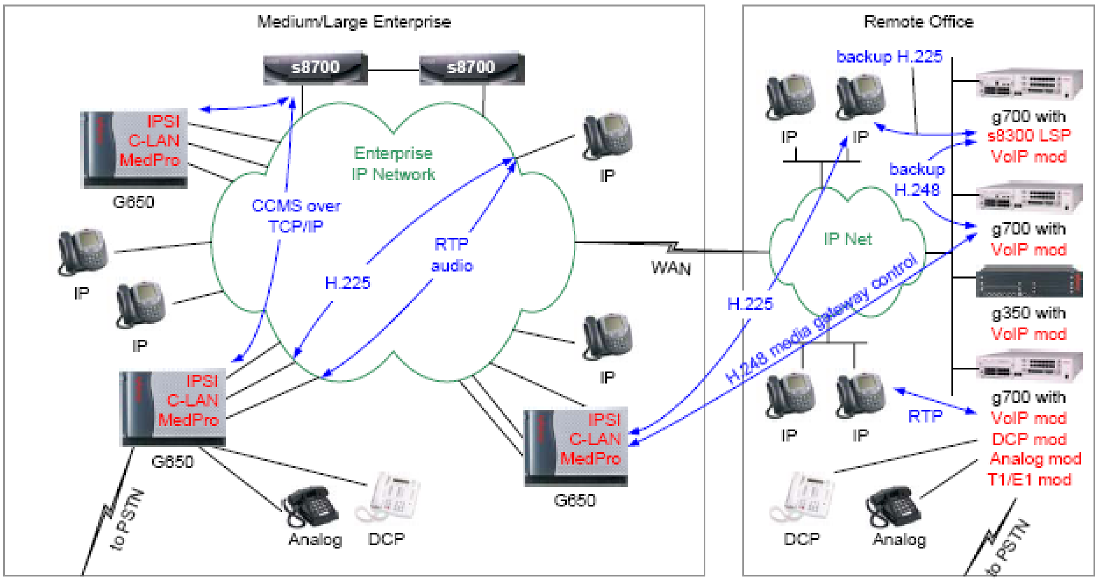


Figure A – S8xxx, G650, G700, G350 Overview

ESS (Enterprise Survivable Server). This is a collection of S87xx and/or S85xx servers connected to the network which can control some or all of the PNs and smaller gateways in the event that the primary server pair or network fails. One server pair will control all PNs and H.248 gateways in normal operation. IPSI traffic will pass over WAN links for the remote PNs. If a PN were to lose contact with its primary server it can search for another. This is a service affecting event so it is important to make sure IPSI networks (known as Control Networks) are up and functioning at all times. The G700, G450, G350 and G250 gateways function differently. They may have an on-board server (S8300) known as 'LSP', which can assume the role of local call processing in the event of a failure to contact targeted CLAN boards located in a PN, or if the primary server is no longer available. S87xx, S85xx, S8300 are regularly updated from the primary server pair with incremental changes in the configuration database, known as 'save translations'. This traffic does not require anything other than best effort treatment (similar to FTP). See Figure B.

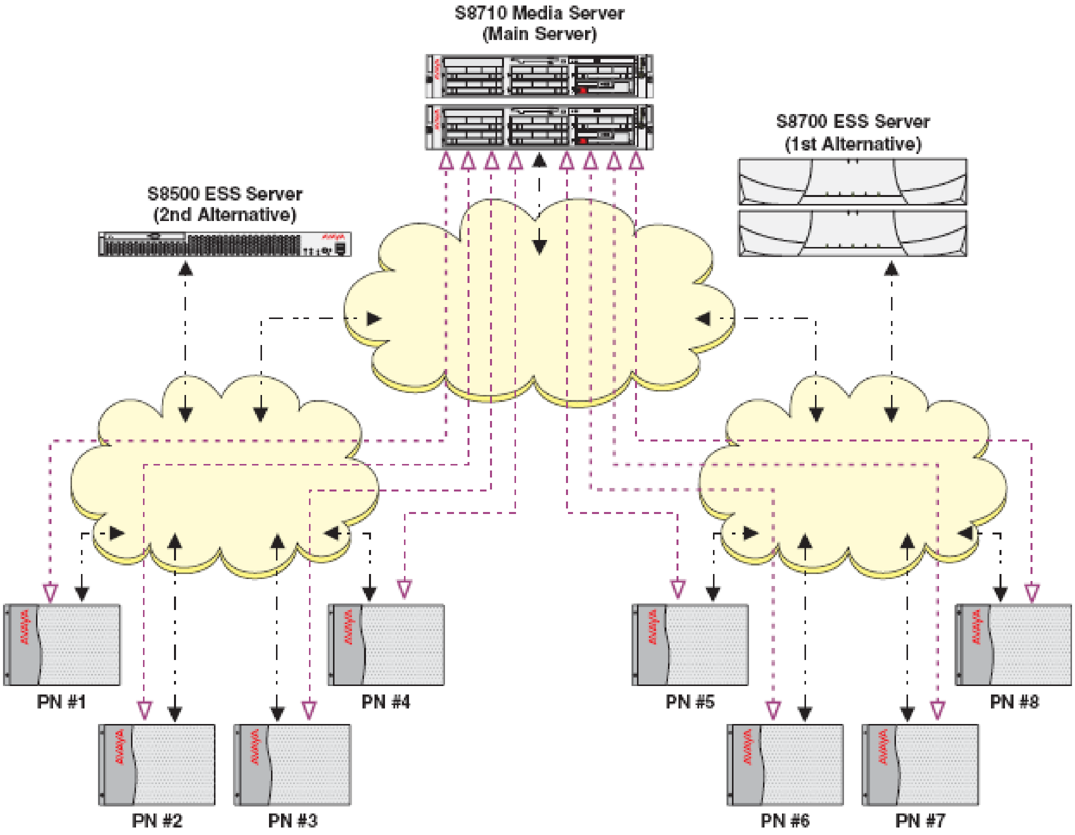


Figure B – ESS Overview

3.2 Connecting Avaya Components To The Network

Figure 1 summarises the details of the LAN switch configuration. Coloured numbers shown in the diagram relate to the points throughout this document. Please note that the diagram is for illustration purposes only and does not demonstrate redundancy features or network design detail. For detailed S8xxx, IPSI, MedPro, CLAN, G700, G450, G350 & G250 connectivity see Section 3.4.

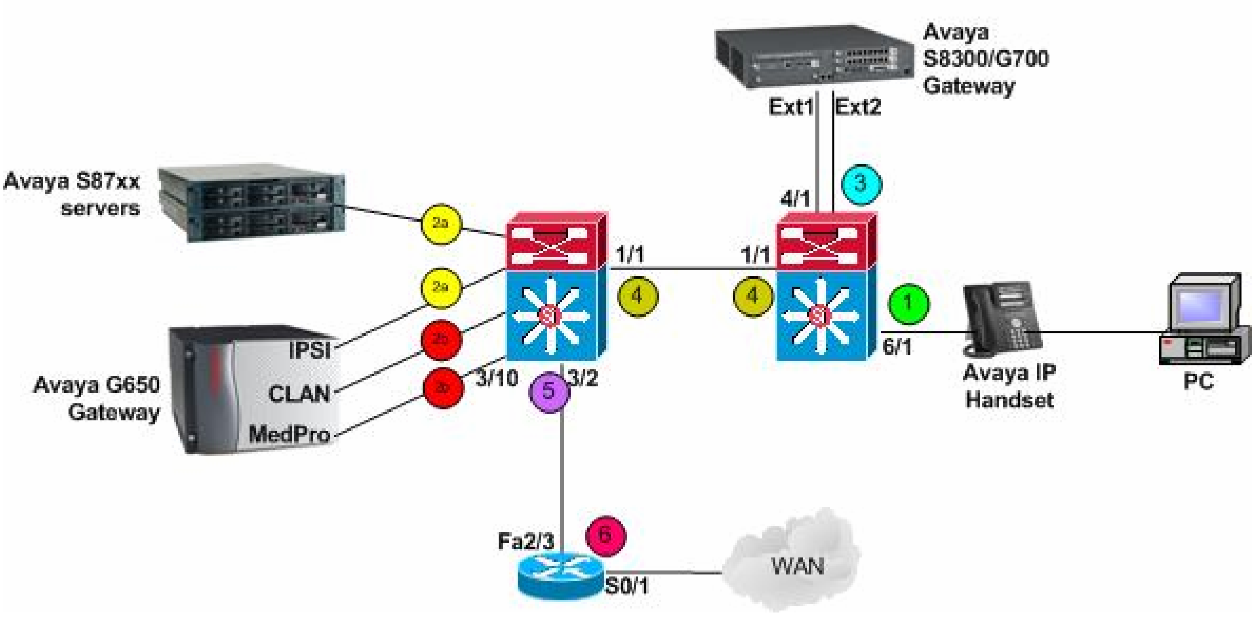


Figure 1 – Reference Diagram

3.3 Connecting an IP Phone with PC Connected to Its Secondary Ethernet Port

1

First enable QoS on the LAN switches. For all LAN switches through which IP Telephony traffic will pass, the cos-dscp-map should be configured as the example below. This is to ensure that the DSCP value of 46 (and others used by the Avaya system if configured) is/are not overwritten by any Cisco switch device in the traffic path:

CatOS

`Console>(enable)set qos enable` **<-enable QoS**
`Console>(enable)set qos cos-dscp-map 0 8 16 24 34 46 48 56` **<-In this example, ingress CoS value of 5 will map to DSCP 46 (default 40) for the internal passage across the switch backplane. Ingress CoS value of 3 will be mapped to 24. 46 & 24 will be preserved on egress from the switch.**

IOS

`switch(config)#mls qos` **<-enable QoS**
`switch(config)#mls qos map cos-dscp 0 8 16 24 34 46 48 56`

<u>NB:</u> Some workgroup switches (eg. 2950, 3550) have mechanisms to restrict DSCP overwriting by the switch. In cases where this command is available please use the second command below:
`switch(config)# qos map cos 5 to dscp 46` **<-map cos values to DSCP values**
`switch(config)# no qos rewrite ip dscp` **<-don't allow switch to overwrite incoming dscp values**

<u>NB:</u> Other versions of IOS, typically for chassis based switches (eg. 65xx, 45xx) may not prefix commands with 'mls'.

There are two key methods for LAN switch port configurations connecting Avaya IP Phones. The traditional 802.1Q method can be used and may well be the only option for non-Cisco

LAN switches. Section 3.3.1 details this option. The “voice vlan” (or “auxiliaryvlan” for CatOS) option is Cisco proprietory. This option also creates a two-VLAN trunk using 802.1Q but allows additional features to be applied to the port that would otherwise not be available (eg. bpdu-guard, 802.1X). Section 3.3.2 details this option.

3.3.1 Traditional 802.1Q Method

For a CatOS Cisco port that connects to an IP Phone with a PC connected to the IP Phone’s secondary Ethernet port use the following configuration (assumes voice/data VLANs already created and that Phone is connected to port 6/1):

```
Console>(enable)set vlan 10 6/1 <-this sets the native VLAN for the trunk port and should be the data VLAN the PC needs to connect to. In this case the data VLAN is VLAN 10
Console>(enable)set port qos 6/1 trust trust-cos|trust-dscp <-trust the incoming cos or dscp value from the phone
Console>(enable)set trunk 6/1 nonegotiate dot1q <-std 802.1q with DTP turned off
Console>(enable)clear trunk 6/1 <-remove all VLANs except voice and data eg. 2-9,11-24,26-1005
Console>(enable)set port inlinepower 6/1 auto <-ports set to auto by default
Console>(enable)set cdp disable 6/1
Console>(enable)set spantree portfast 6/1 enable trunk
```

For any IOS based Cisco port that will connect to the Avaya IP Phone with PC connected to the secondary Ethernet port, use the following:

```
interface FastEthernet6/1
 description IP Phone connection
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 10 <- this will be the data VLAN the PC needs to connect to. By default native VLAN is not tagged. Default native VLAN is 1.
 switchport mode trunk
 switchport nonegotiate <-turns off DTP
 switchport trunk allowed 1,10,25 <-where 10 is the data VLAN and 25 is the voice VLAN
 priority-queue out <-enables outbound priority queue (depends on Cisco switch hardware)
 no cdp enable
 mls qos trust cos|dscp <-trust the incoming cos or dscp value from the phone
 power inline auto <-this is on by default (use with consumption default statement if available/required)
 spanning-tree portfast trunk
```

3.3.2 ‘Voice VLAN’ & ‘Auxiliary VLAN’ Method

The following configurations use Cisco proprietory techniques for connecting IP Phones to LAN switch ports.

For a CatOS Cisco port that connects to an IP Phone with a PC connected to the IP Phone’s secondary Ethernet port use the following configuration (assumes voice/data VLANs already created and that Phone is connected to port 6/1):

```
Console>(enable)set vlan 10 6/1 <-this sets the native VLAN for the trunk port and should be the data VLAN the PC needs to connect to. In this case the data VLAN is VLAN 10
Console>(enable)set port qos 6/1 trust trust-cos|trust-dscp <-trust the incoming cos or dscp value from the phone
Console>(enable)set port auxiliaryvlan 6/1 25 <-set auxiliary vlan to 25 (the voiceVLAN). No ‘clear trunk’ is required – this port only carries VLAN 10 & 25. This port is an 802.1Q port although not explicitly configured
Console>(enable)set port inlinepower 6/1 auto <-port is set to auto by default
Console>(enable)set cdp disable 6/1
Console>(enable)set spantree portfast 6/1 enable
```

For any IOS based Cisco port that will connect to the Avaya IP Phone with PC connected to the secondary Ethernet port, use the following:

```
interface FastEthernet6/1
 description IP Phone connection
 switchport access vlan 10 <- this will be the data VLAN the PC needs to connect to. By default
native VLAN is not tagged. Default native VLAN is 1.
 switchport mode access
 switchport voice vlan 25 <- set the voice vlan to 25. No ‘clear trunk’ is required – this port only
carries vlans 10 & 25. This port is an 802.1Q port although not explicitly configured
 priority-queue out <-enables outbound priority queue (depends on Cisco switch hardware)
 no cdp enable
 mls qos trust cos|dscp <-trust the incoming cos or dscp value from the phone
 power inline auto <-this is on by default (use with consumption default statement if
available/required)
 spanning-tree portfast
```

NB. For Cisco 6500 switches using **1q4t** ports (except Gigabit Ethernet) the trust-cos keyword on its own will NOT trust incoming cos values. For these ports it is necessary to configure a trust-cos ACL to activate the port trust state to trust-cos. Use the **show port capabilities** command to confirm port types. Please see the relevant Cisco Catalyst 6500 QoS Guide for more information.

NB: The inline power statement may require review based on the power requirements (no. of IP Phones and 802.3af Class) and maximum power available in any Cisco switch (see Section 3.11). It *may* be possible to restrict the 802.3af power delivery (consumption default) for some Cisco switches to less than the class defaults (7W for Class 2 and 15.4W for Class 3). See PoE section later in this document.

NB: Catalyst 6500 switch ports with priority queue hardware are shown as 1p3q2t, 1p1q2t or similar, where the ‘1p’ component represents the priority queue. If there is no inclusion of a ‘p’ queue, then the port hardware will only support class based queues eg. 2q2t. In this case the voice traffic should be placed in the ‘high’ queue. At the time of writing all priority queue hardware placed cos 5 in the priority queue or high queue by default. In this case a DSCP value of 46 will also be placed in the priority queue (assuming the port is set to trust DSCP) as the default dscp-cos-map (dscp40-47=cos5) will be used to determine the internal cos value for correct egress queue mapping. Priority queues for ports with priority hardware use the following method to determine the priority queue number: 1p1q2t – 2 queues with priority queue=Q2; 1p2q2t – 3 queues with priority queue=Q3; 1p4q2t – 5 queues with priority queue=Q5 and so on. For default queue mappings, please review the Cisco 6500 series Configuration Guide>Configuring [PFC] QoS>[PFC] QoS Default Configuration.

NB: The IOS command “priority-queue out” tends to be used on some Cisco workgroup switches. For chassis based switches running IOS (eg. 45xx), this command varies. For example, in the Catalyst 4507 running IOS 12.1 and above use the following command:

```
Switch(config)# interface FastEthernet6/1
Switch(config-if)# tx-queue 3
Switch(config-if-tx-queue)# priority high
```

This will convert Q3 into a priority queue (rather than standard class based queue). CoS 5 and DSCP 46 are placed into Q3 by default. Catalyst 6500 switches automatically enable priority queues if the hardware supports them.

NB: For smaller workgroup switches such as 2950, 3550 it may be necessary to map cos values into the correct queues. For example, if CoS 5 is used for audio and/or signalling use the following command to ensure CoS 5 is placed in queue 4 (default is queue 3). When the **priority-queue out** statement is used, **queue 4** becomes the high priority queue. For all switches it is recommended that cos 5 & DSCP 46 are placed into the correct priority queue (or the 'high' queue if a priority queue is not supported). If this is not the switch default behaviour, the priority queue should be remapped to include the desired priority markings:

```
Switch(config-if)#wrr-queue cos-map 4 5 6 7 <-Place CoS values 5, 6 & 7 into Q4
```

For the 2950 series switches to enable the priority queue (Q4), the **priority-queue out** statement is NOT used. Instead use:

```
Switch(config-if)#wrr-queue bandwidth 25 25 25 0 <-Configure Q4 as the priority queue
by configuring zero as the bandwidth percentage for the queue
```

Turn off DSCP values overwritten on passage through the switch using:

```
Switch(config-if)#mls qos trust cos pass-through dscp <-trust state of port set to
"trust cos" in pass-thru mode
```

It may also be possible to use the global command to turn off DSCP overwriting but will depend on the switch hardware and software revision:

```
Switch(config)# no qos rewrite ip dscp <-turn off dscp overwriting
```

3.4 Connecting MedPro, CLAN, S87xx/S85xx, IPSI, G700, G450, G350, G250

3.4.1 IPSI and S87xx Connectivity

IPSI and S87xx/S85xx connections will be connected to the core LAN switches or to dedicated LAN switches. S87xx/S85xx default NIC connections are shown in Figure 2 and detailed below (for Avaya ‘IP Connect’ installations). The Avaya installation engineer and on-site network engineer should confirm the interfaces to be used before installation. It is possible to use eth4 as the management interface freeing up eth0 for connection to Control Network A only. The management interface (eth0 or eth4) is used to ‘save translations’ between the central, active S87xx pair and remote backup servers: S8300 (LSP) and/or S8500/S87xx (ESS). This interface is also used for system administration and management. For this reason, the management interface needs access to the customer network in order to reach the remote S8xxx servers and administrator PCs.

Communication between the S87xx servers and G650 PNs uses redundant control networks as shown in Figure 2 (the S85xx server uses a single Control Network). In steady-state operation Server A is active with Control Network A. Failure of Server A will cause a server interchange. Failure of Control Network A will cause a control network interchange. Both are non-service affecting.

eth0 – Control Network A & Management Access – Connection to VLAN A
eth1 – Services laptop
eth2 – Arbiter – Direct connection between S87xxA&B
eth3 – Control Network B – Connection to VLAN B
eth4 – Management/file transfer interface if not used through eth0

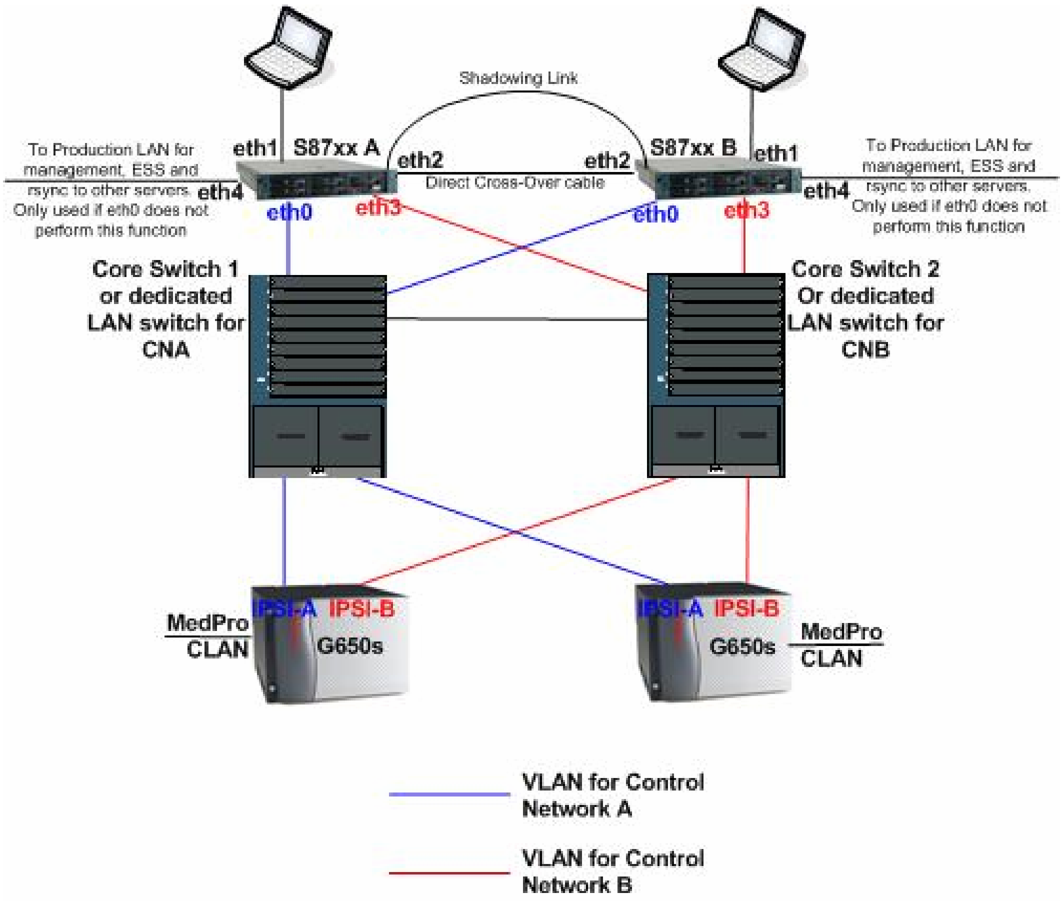

Shadowing Link
To Production LAN for management, ESS and rsync to other servers. Only used if eth0 does not perform this function
eth1
S87xx A
eth2
eth4
eth0
eth3
Direct Cross-Over cable
eth2
S87xx B
eth1
eth4
eth0
eth3
To Production LAN for management, ESS and rsync to other servers. Only used if eth0 does not perform this function
Core Switch 1 or dedicated LAN switch for CNA
Core Switch 2 Or dedicated LAN switch for CNB
MedPro
CLAN
IPSI-A
IPSI-B
G650s
IPSI-A
IPSI-B
G650s
MedPro
CLAN
VLAN for Control Network A
VLAN for Control Network B

Figure 2 – S87xx & IPSI Control Networks A&B (CNA & CNB)

S87xx and IPSI traffic should be configured in two VLANs across the LAN switches as shown in figure 2. One VLAN for Control Network A (CNA) and a second VLAN for Control Network B (CNB) are required. If dedicated LAN switches are provided for CNA & CNB, VLANs may not be required.

See the VLAN assignments section later in this document. Corresponding Cisco switch ports for IPSI and S87xx interface connections are configured as **access** ports.

3.4.1.1 S87xx to/from IPSI over WAN (ESS)

For ESS implementations traffic between IPSI and S87xx servers will, most likely, pass over a WAN. The recommended network performance required for S87xx to IPSI traffic over a WAN is detailed here. Network performance at or below the figures shown **must** be maintained **at all times**:

- Maximum one-way delay 100ms
- Maximum packet loss 1%*

*Maximum packet loss percentage will be dependent on the proportion of IPSI traffic compared to overall traffic passing over any WAN link. For this reason, this value may vary up or down for specific customer installations. 1% packet loss is estimated for general guidance only.

Avaya recommend the use of redundant WAN circuits as shown in the example detailed in Figure 2a. For optimum Avaya system performance and reliability, Control Network A and B should be diversely routed end-to-end. In the example shown in Figure 2a, Control Network A is diversely routed over WAN circuit 1 (blue) and Control Network B over WAN circuit 2 (red). In this example CNA would never be routed over circuit 2 and CNB would never be routed over circuit 1 (even if one or other of the circuits were to fail completely). In the event of a complete circuit failure or WAN performance degradation across either WAN circuit, a Control Network interchange would occur in the normal way. In this instance the Avaya network failure recovery mechanism (Control Network interchange) is preferred over the implicit network recovery mechanism (IGP/BGP re-convergence).

In environments where both CNA and CNB are routed over a single (but redundant) WAN connection, network routing (re-convergence) would be used in favour of the Avaya Control Network interchange following a network failure. In this case Avaya system stability may be impacted if network re-convergence time is too long. This may cause service interruption at the remote site(s). Please also bear in mind that if CNA and CNB are routed over the same single WAN connection which suffers performance degradation (ie. the link does not fail, but performance across it worsens) network re-convergence may not occur (error rates on the link increase but routes remain up). Increased error rates are likely to impact communications between the S87xx and remote IPSIs as both Control Networks would be affected. For these reasons the example topology detailed in Figure 2a is recommended.

NB: QoS for the S87xx to IPSI traffic is recommended for WAN connections and, depending on the network topology, may be a requirement where S87xx to IPSI traffic passes over a LAN. If the network is to trust DSCP or 802.1p then S87xx and IPSI interfaces must be configured to mark packets in the appropriate way. S87xx and IPSI QoS is not configured in the network-region form. In order to enable packet marking at the IPSI board, the IPSI CLI is used. For the S87xx Ethernet NICs the **ipserver-interface** form (or web interface: **Server Configuration and Upgrade>Configure Server**) is used. Alternatively, use the network to classify and mark traffic between S87xx and IPSI. S87xx connections passing traffic to/from IPSIs across a WAN must provide better than 'best effort' transmission. Avaya recommend using strict priority similar to IP audio traffic. The use of LLQ or similar QoS mechanism is recommended. Server to IPSI traffic QoS marking is recommended at a minimum of AF42 but, ideally, at EF.

NB: 'Save translations' files (TCP21874) from the primary S87xx pair to remote S8300 (LSP) and/or S8500/S87xx (ESS) servers should be kept out of the priority queues that may be set up for S87xx to IPSI traffic. Translations files can be serviced in the best effort queue.

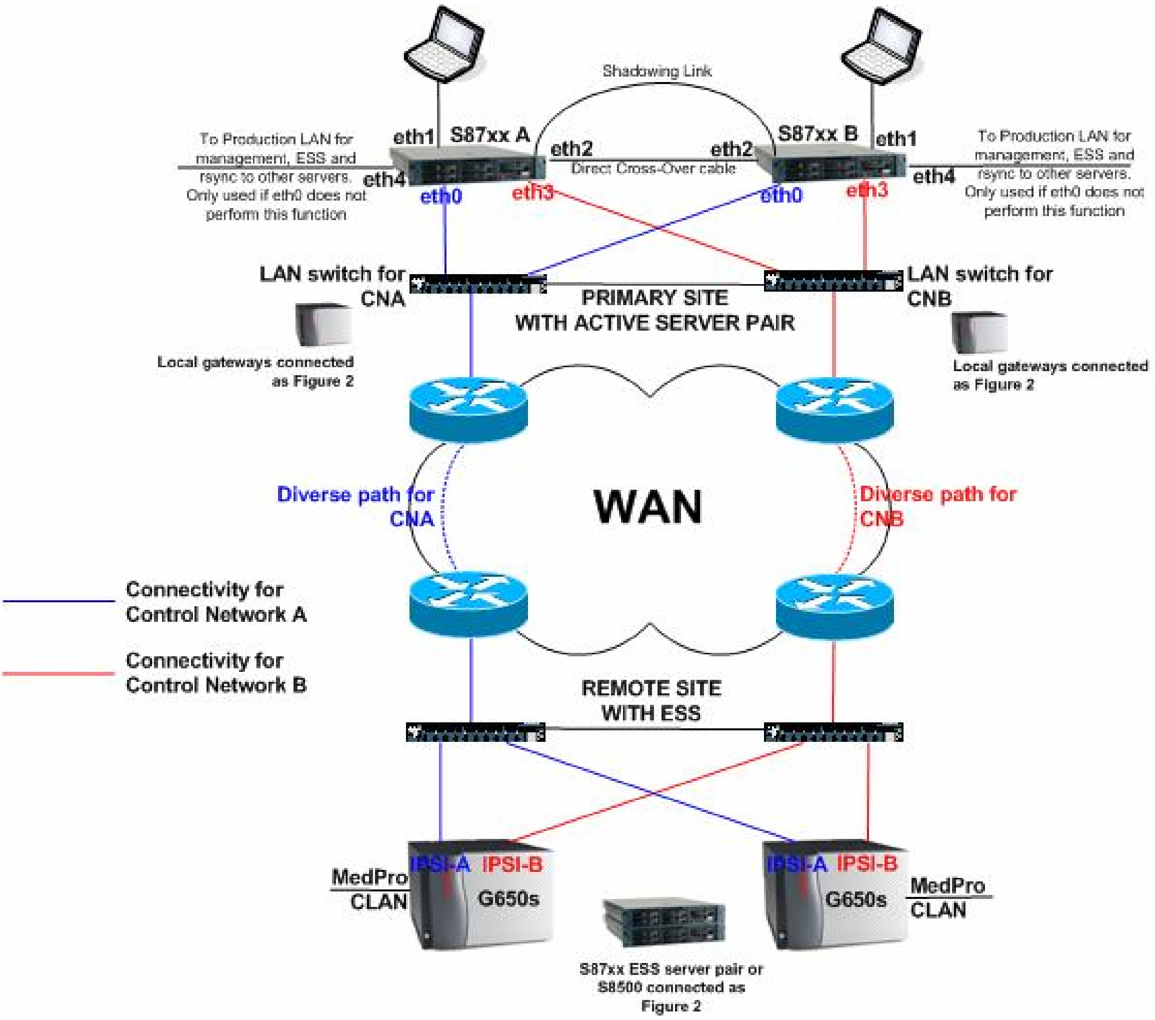

Shadowing Link
To Production LAN for management, ESS and rsync to other servers. Only used if eth0 does not perform this function
eth1
S87xx A
eth2
eth2
Direct Cross-Over cable
S87xx B
eth1
To Production LAN for management, ESS and rsync to other servers. Only used if eth0 does not perform this function
eth4
eth0
eth3
eth0
eth3
eth4
LAN switch for CNA
PRIMARY SITE WITH ACTIVE SERVER PAIR
LAN switch for CNB
Local gateways connected as Figure 2
Local gateways connected as Figure 2
Diverse path for CNA
WAN
Diverse path for CNB
Connectivity for Control Network A
Connectivity for Control Network B
REMOTE SITE WITH ESS
MedPro
CLAN
IPSI-A
IPSI-B
G650s
IPSI-A
IPSI-B
G650s
MedPro
CLAN
S87xx ESS server pair or S8500 connected as Figure 2

Figure 2a – S87xx & IPSI Control Networks A&B over WAN (ESS)

3.4.2 IPSI and ESS Timers

When designing topologies with S87xx and remote IPSIs (for ESS and remote Port Network designs), it is important to understand the basic function of IPSI timers and various failure scenarios. This section describes basic timer function.

S87xx/S85xx to IPSI keepalives are sent every second. A sanity count is incremented for each missed keepalive. If 3 consecutive keepalives are missed the TCP socket is torn down*. The system attempts to setup a new socket to the IPSI(s) affected. Active calls will remain up but new calls through the affected Port Network (PN) will be blocked. If the socket is brought back up in <60 seconds, the G650 PN will go through a 'warm' restart. All phones connected to the affected PN will behave as follows:

- All non-IP stable and held calls are preserved;
- IP Phones re-register: active calls are preserved (from CM v4.0 IP Phones no longer need to re-register);
- IP Agents are logged off and must manually re-login. Active calls remain connected but CMS stops tracking;

- IP trunks reset and links re-initialise (from CM v4.0 IP trunks do not need to reset – using IP Trunk Resiliency);

If the socket is brought back up in >60 seconds but less than the ESS start time (minimum 3 minutes), a cold restart of the PN will occur. All phones connected to the affected PN will behave as follows:

- All ports reset causing all calls passing through the PN to drop

If the primary server is not able to open a socket to the PN, ESS will take over in the configured time (minimum 3 minutes).

When discussing the impact of S87xx/S85xx to IPSI communication loss, it is important to distinguish IP Phone to IP Phone calls as opposed to IP Phone to non-IP Phone/TDM/external calls. After call setup, IP Phone to IP Phone calls are shuffled (direct VoIP, Phone to Phone) and subsequently the calls do not use PN resource or pass through the PN. These calls may not be affected in the same way as IP Phone to non-IP Phone/TDM/external calls which pass through the PN.

*From CM v3.1.3 and above this value can be adjusted to allow increased missed keepalives before the socket is torn down. Changing IPSI timers in this way will impact the Avaya system globally. To avoid negatively impacting the system, any planned changes to global IPSI timers must be discussed with your Avaya support representative.

3.4.3 CLAN and MedPro Connectivity

The recommended connections for CLAN and MedPro resource for individual PNs (G650s) is to connect CLAN and MedPro resources for each PN into two or more redundant core LAN switches (see figure 3). For example, if two LAN switches are provided for these connections, approximately half of the MedPro and CLAN resource for each PN should be connected to each LAN switch. VLANs must be created to segregate the production (data) traffic from the CLAN & MedPro traffic.

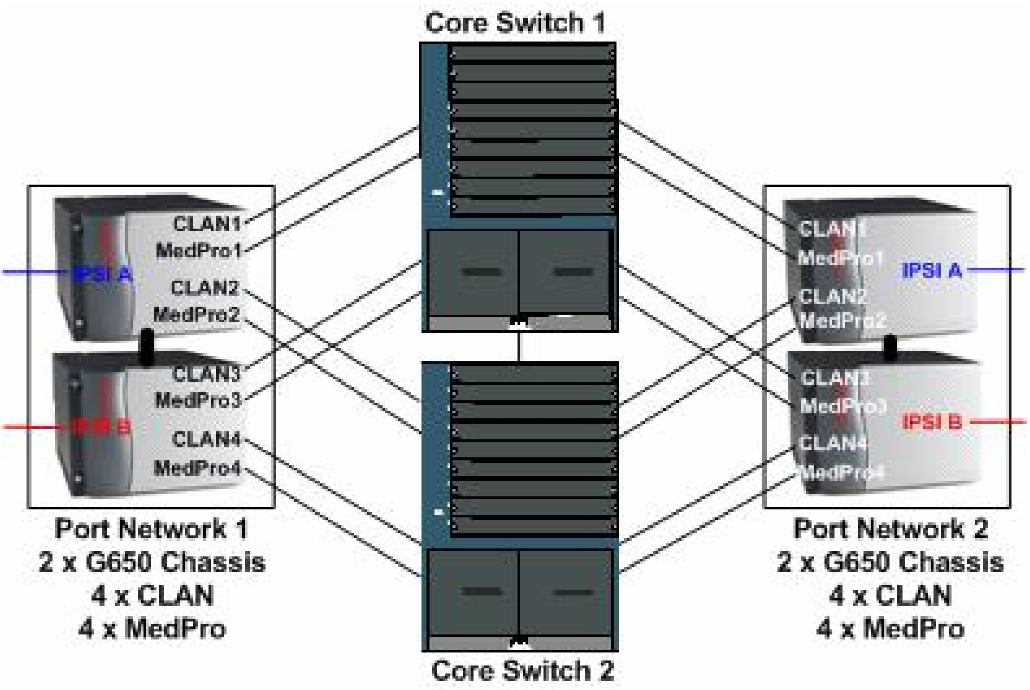


Figure 3 – Redundant CLAN & MedPro Connections

Figure 3a illustrates a combined example solution showing a primary active location, an ESS location and a S8300/G700 providing local survivability.

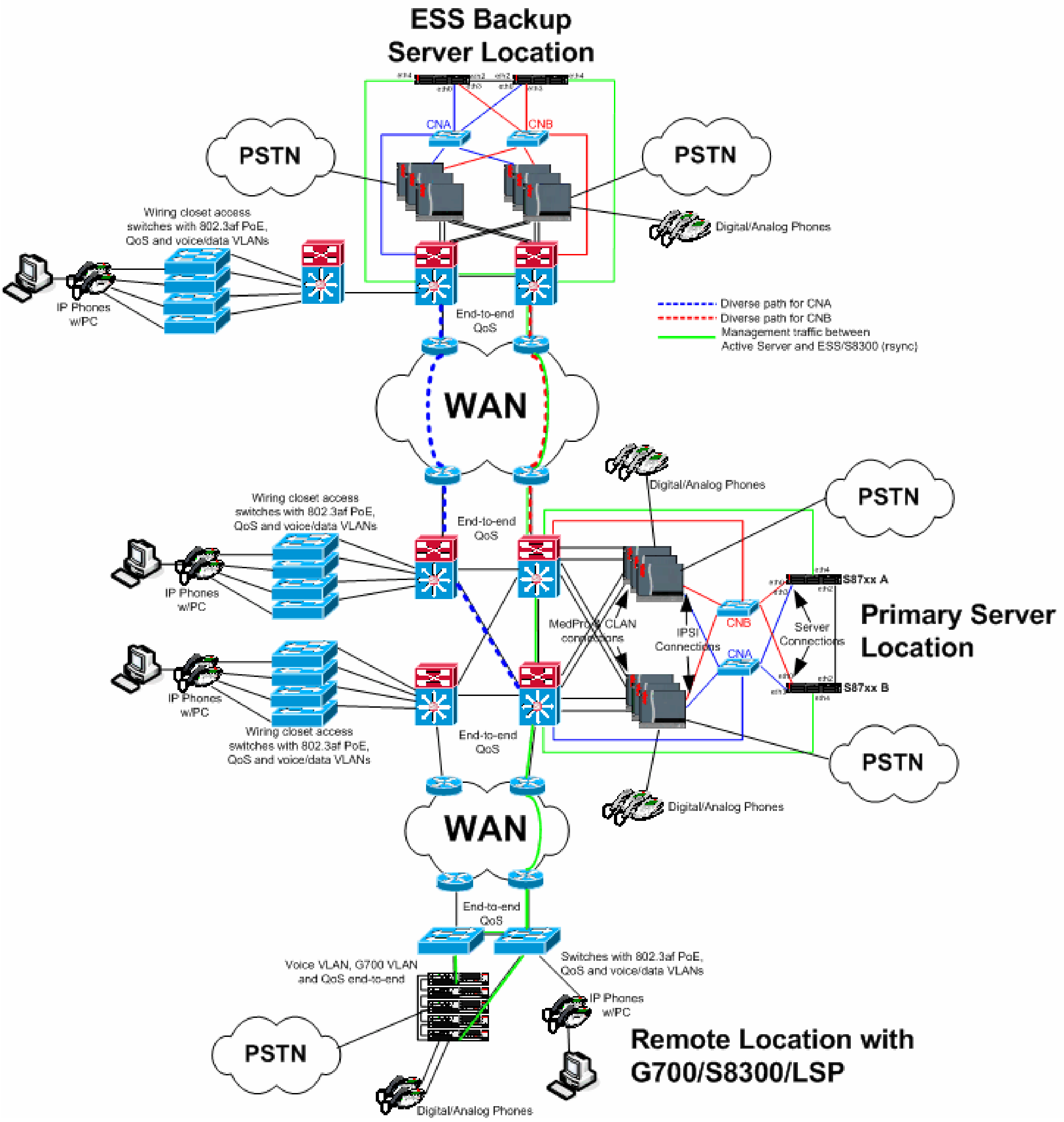

ESS Backup Server Location
CNA
CNB
PSTN
PSTN
Wiring closet access switches with 802.3af PoE, QoS and voice/data VLANs
IP Phones w/PC
Digital/Analog Phones
End-to-end QoS
Diverse path for CNA
Diverse path for CNB
Management traffic between Active Server and ESS/S8300 (rsync)
WAN
Digital/Analog Phones
PSTN
Wiring closet access switches with 802.3af PoE, QoS and voice/data VLANs
IP Phones w/PC
End-to-end QoS
S87xx A
CNB
MedPro/CLAN connections
IPSI Connections
CNA
Server Connections
Primary Server Location
S87xx B
IP Phones w/PC
Wiring closet access switches with 802.3af PoE, QoS and voice/data VLANs
End-to-end QoS
PSTN
Digital/Analog Phones
WAN
End-to-end QoS
Voice VLAN, G700 VLAN and QoS end-to-end
Switches with 802.3af PoE, QoS and voice/data VLANs
IP Phones w/PC
PSTN
Remote Location with G700/S8300/LSP
Digital/Analog Phones

Figure 3a – Example Enterprise Installation with Primary Server, ESS and G700/S8300/LSP

3.4.4 S87xx/S85xx and IPSI LAN Switch Port Configuration

2a

These connections are configured as **access** ports. For a CatOS port connecting S87xx/S85xx & IPSI, perform the following:

`Console>(enable)set vlan 50 4/3` **<-this sets the relevant VLAN for CNA/CNB**

`Console>(enable)set port qos 3/10 cos 5` **<-sets default port priority to cos 5 use this if using 802.1p tagging in the LAN. For the default cos port priority to mark packets accordingly, you will also need** `set port qos 3/10 trust trust-cos`**. Use** `set port qos 3/10 trust trust-dscp` **to trust DSCP in the LAN (recommended)**

```
Console>(enable)set port speed 4/3 100
Console>(enable)set port duplex 4/3 full
Console>(enable)set cdp disable 4/3
```

`Console>(enable)set spantree portfast 4/3 enable` **<-disable spanning tree**

IOS:

```
interface FastEthernet4/3
 description S87xx/S85xx/IPSI connection
```

` switchport access vlan 50` **<- this sets the relevant VLAN for CNA/CNB**

```
 duplex full
 speed 100
```

` mls qos cos 5` **<-sets default port priority to cos 5 use this if using 802.1p tagging in the LAN. For the default cos port priority to mark packets accordingly, you will also need** `mls qos trust cos`**. Use** `mls qos trust dscp` **to trust DSCP in the LAN (recommended).**

```
 no cdp enable
```

` spanning-tree portfast` **<-disable spanning tree**

<u>NB:</u> If using trust-dscp (recommended) in the network, ensure packets are marked with the correct DSCP value, configured at the IPSI CLI and S87xx/S85xx ipserver-interface form.

3.4.5 MedPro and CLAN LAN Switch Port Configuration

2b

These connections are configured as **access** ports. For a CatOS port connecting MedPro, & CLAN perform the following:

`Console>(enable)set vlan 110 3/10` **<-this sets the relevant VLAN for the access port**

`Console>(enable)set port qos 3/10 cos 5` **<-sets default port priority to cos 5 use this if using 802.1p tagging in the LAN. For the default cos port priority to mark packets accordingly, you will also need** `set port qos 3/10 trust trust-cos`**. Use** `set port qos 3/10 trust trust-dscp` **to trust DSCP in the LAN (recommended)**

```
Console>(enable)set port speed 3/10 100
Console>(enable)set port duplex 3/10 full
Console>(enable)set cdp disable 3/10
```

`Console>(enable)set spantree portfast 3/10 enable` **<-disable spanning tree**

IOS:

```
interface FastEthernet3/10
 description MedPro/CLAN connection
```

` switchport access vlan 110` **<- this sets the relevant VLAN for the access port**

```
 duplex full
 speed 100
 no cdp enable
```

` mls qos cos 5` **<-sets default port priority to cos 5 use this if using 802.1p tagging in the LAN. For the default cos port priority to mark packets accordingly, you will also need** `mls qos trust cos`**. Use** `mls qos trust dscp` **to trust DSCP in the LAN (recommended)**

` spanning-tree portfast` **<-disable spanning tree**

NB: Be sure to place the Cisco switch port that connects to the CLAN/MedPro into the correct VLAN. The VLAN number configured in the Avaya Communications Manager **ip-interfaces** form should be left to ‘n’. Setting a value in the in this field would convert this interface to an 802.1Q trunk.

3.4.6 Avaya G700/G450/G350/G250 Connectivity & Switch Port Configuration

3

These connections are configured as **access** ports. The G700 has two LAN switch ports located on the front panel marked as ‘Ext1’ and ‘Ext2’. The G700 chassis is based on LAN switch architecture. As a result the G700 can be connected to the LAN infrastructure as if it was ‘just another’ LAN switch. Spanning tree or rapid spanning tree can be used between the two LAN switch ports for redundant connections into the existing LAN. In this case, `portfast` must **NOT** be enabled on the connecting Cisco LAN switch ports. Alternatively, ‘port redundancy’ can be configured on the G700. Port redundancy is a layer 1 fast switch-over mechanism that does not require spanning tree and requires no additional configuration on the Cisco LAN switches. This method is recommended. See Figure 4.

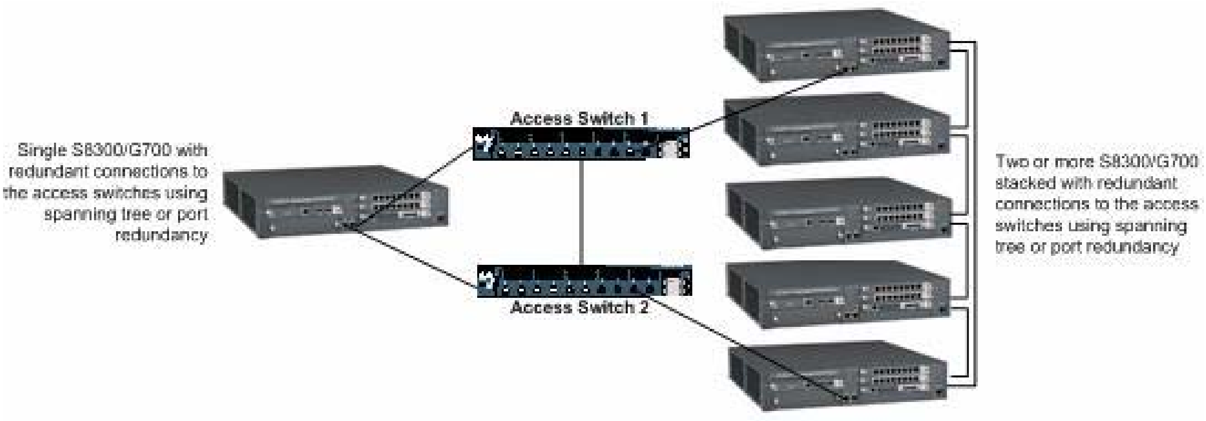

Single S8300/G700 with redundant connections to the access switches using spanning tree or port redundancy
Access Switch 1
Access Switch 2
Two or more S8300/G700 stacked with redundant connections to the access switches using spanning tree or port redundancy

Figure 4 – G700 Redundant Connections

The G700 has a Cajun CLI interface to configure the LAN switch features such as spanning tree, port redundancy and port speed/duplex. To disable spanning tree and enable port redundancy perform the following:

`G700(super)# set port spantree enable|disable <mod/port>` **<-turn on|off spanning tree for the G700 ports connecting to the Cisco LAN switch. Do not disable spanning tree if port redundancy is not used. If port redundancy is enabled, disable spanning tree and set ‘portfast’ on the corresponding Cisco LAN switch ports.**
`G700(super)# set port redundancy <primary mod/port> <secondary mod/port> on|off <port_redundancy_name>` **<-place port redundancy entry in port redundancy table (use ‘on’ to place it in the table and ‘off’ to remove it).**
`G700(super)# set port redundancy enable` **<-enable port redundancy entry stored in port redundancy table**
`G700(super)# show port redundancy`

Use **`set intermodule port redundancy`** when configuring port redundancy on stacked G700 installations.

The G450/G350/G250 is similar to the G700 with the following caveats:

1. The G450 has dual fixed Ethernet ports on the chassis, similar to the G700. G450 supports spanning tree and port redundancy;
2. The G350 has a single Ethernet port on the chassis. In order to have redundant connections, an additional Ethernet switch port module would be required. G350 supports spanning tree and port redundancy;
3. G250 does not support spanning tree or port redundancy. As a result, only a single LAN switch connection is possible;
4. G450, G350 and G250 cannot be stacked as shown in figure 4.

For a CatOS port that connects to G700/G450/G350/G250 perform the following:

`Console>(enable)set vlan 230 4/1` **<-this sets the relevant VLAN for the access port**

`Console>(enable)set port qos 4/1 cos 5` **<-sets default port priority to cos 5 use this if using 802.1p tagging in the LAN. For the default cos port priority to mark packets accordingly, you will also need** `set port qos 4/1 trust trust-cos`**. Use** `set port qos 4/1 trust trust-dscp` **to trust DSCP in the LAN (recommended)**

```
Console>(enable)set port speed 4/1 100
Console>(enable)set port duplex 4/1 full
Console>(enable)set cdp disable 4/1
```

`Console>(enable)set spantree portfast 4/1 enable` **<-disable spanning tree only if a single connection or port redundancy is used**

IOS:

```
interface FastEthernet4/1
 description G700/G350 connection
```

` switchport access vlan 230` **<- this sets the relevant VLAN for the access port**

```
 duplex full
 speed 100
 no cdp enable
```

` mls qos cos 5` **<-sets default port priority to cos 5 use this if using 802.1p tagging in the LAN. For the default cos port priority to mark packets accordingly, you will also need** `mls qos trust cos`**. Use** `mls qos trust dscp` **to trust DSCP in the LAN (recommended)**

` spanning-tree portfast` **<-disable spanning tree only if a single connection or port redundancy is used**

NB: Be sure to place the Cisco switch port connecting the G700/G450/G350/G250 in the correct VLAN. The VLAN number configured internally on the G700/G450/G350/G250 can be left at the default. All IP addresses configured in the G700/G450/G350/G250 (minimum 3) must be on the same subnet and VLAN (configured inside the chassis). These would be configured by the Avaya installation engineer. It is recommended that the on-site network engineer and Avaya installation engineer agree the configuration to be adopted.

NB: Trunk ports can be configured between the G700/G450/G350/G250 and local LAN switch. Use this option if 802.1p is required in the LAN and different 802.1p values are configured for signalling and audio traffic. By configuring this connection as an 802.1Q trunk, the different 802.1p values are maintained for audio and signalling traffic passing over the trunk. Use similar configurations to connecting an IP Phone using the 802.1Q method (with trust cos) as described earlier in this document (trunk ports are not required if trust DSCP is used here). Please also note that using this option will require the gateway VLAN ID configured to the same value as configured on the local LAN switch (802.1Q tags must use the same VLAN ID at both ends of the trunk). Avaya recommend the preferred, simple access port configuration as detailed above using trust-dscp. Only use the 802.1Q method when special circumstances exist.

NB: The G700/G450/G350/G250 should not assume the spanning tree root. Manipulate bridge priorities to avoid this as appropriate.

NB: The G700/G450/G350/G250 can directly connect to WANs. Please refer to the appropriate Avaya documentation for more information.

3.5 Inter-switch Uplink LAN Switch Port Configuration

4

For a CatOS uplink port for inter-switch links use the following configuration:

```
Console>(enable)set port qos 1/1 trust trust-cos <-trust the incoming cos value from
the other switch if using 802.1p in the LAN otherwise use: set port qos 1/1 trust trust-dscp
for DSCP in the LAN (recommended)
Console>(enable)set trunk 1/1 dot1q <-std 802.1q trunk
Console>(enable)clear trunk 1/1 <-remove VLANs as required
```

For an IOS uplink port for inter-switch links use the following configuration:

```
interface GigabitEthernet1/1
 description Switch Uplink
 switchport trunk encapsulation dot1q
 switchport mode trunk
 mls qos trust cos <-trust the incoming cos value from the other switch  if using 802.1p tagging in
the LAN otherwise use: mls qos trust dscp  for DSCP in the LAN (recommended)
 switchport trunk allowed <-allow VLANs as required
```

NB: Remember to ensure that the correct cos-dscp-map statements are added for **all switches** in the path of IP Telephony traffic. Alternatively, be sure to disable dscp overwriting on all Cisco switches in the traffic path.

3.5.1 Connecting Local Cisco LAN switch to Gateway WAN router

5

It is important to ensure that the correct QoS processing occurs in both directions at the point at which the voice packets leave the LAN to pass over the WAN and leave the WAN to pass over the LAN. WAN routers use DSCP or IP Precedence whereas the LAN switches ***may*** be configured to use 802.1p. CoS or 802.1p only exists in Ethernet networks and, by implication, cannot be used or passed over the WAN. This section looks at the LAN switch port configuration only. The next section looks at the WAN router QoS configuration and interface application.

Voice traffic passing from the WAN toward the LAN will have no 802.1p value. The incoming packet will have DSCP value (eg. 46 for audio) as per the example configuration at the beginning of this document. Voice traffic from the LAN switch to the WAN router must arrive at the router with the correct DSCP value. To ensure the DSCP value is consistently maintained from switch to switch and passed onto the WAN router, the outgoing map (or the disabling of DSCP overwriting) between 802.1p and DSCP must be set on the LAN switches as described throughout this document.

A CatOS switch port connecting the WAN router would be as follows:

```
Console>(enable)set port qos 3/2 trust trust-dscp <-trust the incoming DSCP value
from the WAN router (example: 46 for audio)
Console>(enable)set trunk 3/2 nonegotiate dot1q <-std 802.1q with DTP turned off
Console>(enable)clear trunk 3/2 <-remove all except relevant VLANs
Console>(enable)set port speed 3/2 100
Console>(enable)set port duplex 3/2 full
Console>(enable)set spantree portfast 3/2 enable trunk
```

IOS:

```
interface FastEthernet3/2
 description WAN Router connection
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport nonegotiate <-turn off DTP
 switchport trunk allowed <- allow permitted VLANs
 priority-queue out <-enables outbound priority queue (depends on Cisco switch hardware)
 duplex full
 speed 100
 mls qos trust dscp <-trust the incoming dscp value from the router  (example: 46 for audio)
 spanning-tree portfast trunk
```

NB: The trunk configuration statements can be left out if the LAN switch connection to the WAN router is a non-trunk (access) port.

NB: The incoming DSCP value from the WAN router to the LAN switch port will be mapped to the correct 802.1p value only if the DSCP to CoS mappings are configured correctly (left at default) at the LAN switch (DSCP 40-47 is mapped to CoS 5). This is only relevant if 802.1p is used in the LAN. Alternatively and if available, switch off DSCP overwriting.

3.6 WAN Router

6

Low Latency Queuing (LLQ) is used to provide strict priority for voice traffic over the WAN. It is also used to ensure traffic from the WAN router towards the local LAN is prioritised over the router Ethernet interface. The following configuration details a simple, example LLQ implementation.

```
class-map match-any|all bearer <-choose to match based on AND/OR
       match ip dscp 46 <-match incoming (from the LAN or WAN) traffic
       match access-group name voice-subnets <-match by source address from relevant
voice subnets
class-map match-any|all signalling
       match ip dscp 24 <-match incoming (from the LAN or WAN) traffic
       match access-group name voice-subnets <-match by source address from relevant
voice subnets

policy-map voip_audio_control
       class bearer
              priority 2000 <-set required bandwidth for concurrent calls with strict priority.
              Please note: this is the bandwidth including the IP header only. It does not include the
              layer 2 header
       class signalling
              bandwidth 512 <-choose signalling bandwidth for class based treatment
       class class-default
              fair-queue <- all other traffic by WFQ
```

The router WAN and LAN interfaces are configured as follows:

```
interface serial 0/1 <-interface connecting WAN
       service-policy output voip_audio_control

interface fastethernet 2/3 <-interface connecting local LAN switch
       service-policy output voip_audio_control
```

NB: A policy map is a grouping of queue classifications. Audio and Signalling traffic bandwidth calculations must be carried out on a per site basis to derive the correct priority bandwidth configuration. Assigning insufficient priority WAN bandwidth for the number of concurrent calls will affect voice quality *on all calls* passing over it.

NB: The bandwidth configured in the 'priority' command is the bandwidth consumed including the IP header only. The bandwidth allocation is not calculated based on the full frame size including the layer 2 header. Please bear this in mind when calculating the priority bandwidth to be allocated.

NB: If ATM interfaces are used to pass VoIP traffic ensure that the **tx-ring-limit** parameter is configured to ensure the ATM egress logic does not impose increased delay and/or jitter through the output buffer process when QoS (LLQ) is switched on. The numeric value of this parameter will depend on the specific network environment and may need to be adjusted on a 'trial and error' basis. Avaya always recommend discussing tx-ring-limit parameter changes with an appropriate Cisco technical resource.

NB: Other possible LLQ 'match' parameters are as follows:

- Match IP Precedence
- Match protocol RTP
- Match ACL

Be sure to configure the match criteria required and to configure either **match-all** or **match-any** in the **class-map** statement depending on the classification requirement.

3.7 RED & WRED

Random Early Detection (RED) and Weighted Random Early Detection (WRED) are queue management (congestion avoidance) techniques. They work by randomly discarding packets (WRED works by using IP Precedence/DSCP to determine which lower priority packets should be discarded first). Both make use of the congestion control mechanism of TCP. As packets are discarded, TCP throttles back the transmission rate, so reducing the bandwidth consumption during periods of high utilisation (congestion). RED and WRED are useful tools for managing data traffic, but should not be used for voice. IP Telephony traffic is UDP-based which provides no retransmission function, nor does it provide a throttling function to decrease transmission rates. For voice streams, RED and WRED will only add packet loss resulting in poor voice quality.

3.8 Traffic Shaping & Policing

Traffic shaping is a mechanism to reduce the rate at which data is transmitted over an interface. Traffic shaping is often confused with traffic policing. Policing works by altering the priority of traffic exceeding bandwidth thresholds or dropping traffic. As with RED, discarding TCP traffic has the effect of throttling the stream by forcing the window size to shrink. Because RTP is a fixed bandwidth application, discarding RTP packets reduces voice quality and has no effect on the transmission rate. Altering (downgrading) the priority of RTP traffic removes the necessary protection for reducing latency and jitter. As a result traffic shaping and policing should only be used for voice traffic with extreme caution. Correct bandwidth sizing for maximum concurrent call rates should be calculated to ensure voice traffic is not discarded or downgraded over the network.

3.9 Frame Relay Shaping and LLQ

Traffic shaping is important in technologies that implement virtual circuits (VCs) such as Frame Relay or ATM where the Committed Information Rate (CIR) may be less than the physical speed of the interface. In these scenarios it is possible for traffic to burst above the CIR. A provider may mark excess traffic as Discard Eligible (DE) and either delay or discard it if congestion occurs within the provider network. This is unacceptable for voice traffic. There is a popular misconception that voice traffic can be confined to the CIR, while data traffic can be allowed to burst. There is no such QoS mechanism for Frame Relay that is negotiated between service providers and customers. Service providers view all traffic equally even if the packet is high priority voice. The only way to ensure optimal performance for voice traffic is to restrict the traffic rate to the CIR and enable LLQ. Points to note:

1. Disable Frame Relay Adaptive Shaping. This reduces the CIR in response to Backward Explicit Congestion Notification (BECN) messages from the Service Provider. Traffic will be transmitted only as fast as the CIR so there is no need to throttle it.
2. Set CIR and MINCIR to the negotiated CIR. If FRF.12 is used reduce the CIR and MINCIR values a little to account for the fragment headers.
3. Set BE, the excess burst rate, to 0.
4. Set BC, the committed burst rate, to CIR/100. This accounts for, at most, a 10-ms serialization delay (generally good for voice streams).
5. Apply the map-class to an interface, sub-interface or VC.
6. In order to activate LLQ on Frame Relay interfaces, Frame Relay Traffic Shaping (FRTS) must be enabled on the physical interface (not to be confused with Frame Relay Adaptive Shaping as described in (1.) above).

An example recommended Frame Relay configuration with LLQ for voice would be as follows:

```
class-map match-all bearer
       match ip dscp 46
       match access-group name voice-subnets
class-map match-all signalling
       match ip dscp 24
       match access-group name voice-subnets

policy-map voip_audio_control
       class bearer
              priority 2000
       class signalling
              bandwidth 512
       class class-default
              fair-queue

interface serial2
       encapsulation frame-relay
       frame-relay traffic-shaping

interface serial2.100
       frame-relay interface-dlci 100
       frame-relay class NoBurst&LLQ

map-class frame-relay NoBurst&LLQ
       no frame-relay adaptive shaping
       frame-relay cir 6000000 (for a 6Mb/s CIR)
       frame-relay mincir 6000000
       frame-relay be 0
       frame-relay bc 60000
       service-policy output voip_audio_control
```

3.10 Network Performance Parameters

The definition of network performance for the support of VoIP is given as follows:

One-Way Delay

80ms one-way delay or less can, but may not, yield ‘Toll Quality’ voice.

80ms to 180ms one-way delay can give ‘Business Communication Quality’ voice. This is much better than mobile phone quality and in fact is well suited for the majority of businesses.

Delays **exceeding 180ms** may still be quite acceptable depending on customer expectations, analogue trunks used, codec type, etc.

Packet Loss

1% or less can yield ‘Toll Quality’ voice depending on a number of factors.

3% or less should give ‘Business Communications Quality’ voice. Again, this quality is much better than mobile phone quality but not as good as Toll Quality

More than 3% may or may not be acceptable for voice and may interfere with signalling.

Jitter

‘Toll Quality’ suggests average jitter be **less than 20ms** or less than the packet payload (which, in the case of default Communication Manager configuration, is 20ms). This value has some latitude depending on the type of service the jitter buffer has in relationship to other router buffers, packet size used, etc.

MOS

In voice communications, particularly IP Telephony, the Mean Opinion Score (MOS) provides a numerical measure of the quality of human speech at the destination end of the circuit. The scheme uses subjective tests (opinionated scores) that are mathematically averaged to obtain a quantitative indicator of the system performance. To determine MOS, a number of listeners rate the quality of test sentences read aloud over the communications circuit by male and female speakers. MOS is calculated during voice simulation assessment, as an overall measure for the one-way delay, packet loss and jitter recorded effectively ‘simulating’ the voice quality as users might rate it. Scores are rated: 1(bad), 2(poor), 3(fair), 4(good), 5(excellent). A score no lower than 3.6 should be targeted, however, a score of 4.0 or above should be achievable in most cases.

3.11 Avaya System Configuration

In order for the Avaya voice traffic to be correctly handled with regard to the network QoS configuration, the Avaya system needs to be configured as described in this section.

The Avaya installation engineer should configure an ‘n’ for VLAN number for the MedPros, CLANs, IPSIs and S87xx **ip-interfaces** form.

If 802.1p values will be used in the LAN and the **ip-network-map** form is populated, the destination VLAN IDs for IP Phones connected to the network must be entered. This is to ensure the IP Phones receive the correct 802.1p values to use on registering with the Avaya system. If DSCP is used in the LAN, this does not apply (the DSCP values will still reach the IP Phones regardless of the entries in the ip-network-map form).

Continuing with the example QoS parameters used in this document, the installation engineer would configure a value of **5** for the 802.1p parameters for audio and **3** for signalling. For DSCP the values would be **46** for audio and **24** for signalling. This should be configured for each **network-region** present on the system.

The Avaya installation engineer must configure all interfaces (CLAN, MedPro, G700, G450, G350, G250, IPSI & S8xxx) to (fixed) 100Mb/s full-duplex. All corresponding Cisco switch ports for these interfaces **must also** be fixed at 100Mb/s full-duplex. All Cisco switch ports connecting IP Phones should be configured to auto-negotiate (default). All PCs connected to IP Phones secondary Ethernet ports should also be configured to auto-negotiate (default).

In all cases, the customer network engineering personnel should confirm this requirement to the Avaya installation engineer during implementation. Port error and discard information should be gathered from the Cisco switch ports to ensure duplex mismatch has not occurred. As a general rule there should be **no errors or discards reported on any LAN switch port connecting any Avaya equipment or through which Avaya traffic passes**. Errors or discards such as these may impact voice quality and/or system stability.

3.12 DHCP Configuration

Assuming PCs will be connected into the secondary Ethernet ports of 46xx/96xx series IP Phones, the DHCP configuration serving the IP Phones needs to be configured to include the **Option176** parameter also known as **SSON176.** For 96xx series IP Phones, **Option242** or **SSON242** is used. All other Avaya equipment (except IP Phones) will use static IP addressing.

3.12.1 4600 Series IP Phones

SSON176 is detailed as follows and assumes the port configuration, as described earlier in this document, has been used for the IP Phone connections. The SSON176 would be placed in the *data* scope. A similar SSON176 string is also placed in the voice scope. However, the L2QVLAN statement can be removed from the voice scope entry as it is assumed the IP Phone must already be in the correct (voice) VLAN in order to receive an appropriate IP address in the voice scope.

The IP Phone first boot sequence is as follows:

1. DHCP request sent from Phone for a 'native' VLAN (ie. data VLAN) data address from the DHCP server;
2. DHCP server responds with address but is also configured with 'SSON176' string (see below). SSON176 exists in the data scope as well as the voice scope.
3. From SSON176 Phone learns where to register (Avaya CLAN address), which RAS UDP port to use, where the TFTP or HTTP server is (for firmware download and additional parameters) and which (voice) VLAN to use.
4. IP Phone releases address from the data scope and re-starts using 802.1Q tag in voice VLAN. DHCP issues voice scope address.
5. Phone registers with CLAN and normal registration process continues.

The following SSON176 ***example*** for 4600 series IP Phones would look as follows:

```
MCIPADD=10.1.1.1,10.1.1.2,10.1.1.3,MCPORT=1719,TFTPSRVR=10.200.1.100,L2QVLAN=220,VLANTEST=0
```

MCIPADD is the CLAN IP addresses -- list up to six (no spaces; commas between each address)
MCPORT is the UDP port used by the phone (must be 1719) for RAS registration and port signalling.
TFTPSRVR is the address for the TFTP server. If more than one TFTP server exists, include all addresses with commas between each (no spaces). Use HTTPSRVR if using HTTP
L2QVLAN is the voice VLAN number assigned for the Phone and must match the corresponding voice VLAN number configured at the LAN switch
VLANTEST=0 configures the phone never to lose its assigned voice VLAN number following a failure to receive a DHCP offer in the voice VLAN (please see the important note below).

3.12.2 9600 Series IP Phones

SSON242 follows a similar boot process as described for SSON176 and 4600 series IP Phones. The SSON242 would be placed in the data scope. A similar SSON242 string is also placed in the voice scope. However, the L2QVLAN statement can be removed from the voice scope entry as it is assumed the IP Phone must already be in the correct (voice) VLAN in order to receive an appropriate IP address in the voice scope.

The following SSON242 ***example*** for 9600 series IP Phones would look as follows:

```
MCIPADD=10.1.1.1,10.1.1.2,10.1.1.3,MCPORT=1719,HTTPSRVR=10.200.1.100,L2QVLAN=220,VLANTEST=0
```

NB: Avaya strongly recommend DHCP server compliance with RFC2131 to ensure lease time, lease renewal time and rebinding time values (Options 51, 58 & 59) are in accordance with the appropriate standards. Deviation from DHCP standards may cause unexpected behaviour.

NB: Please see the ‘Avaya 46xx LAN Admin Guide’ for detail on additional parameter syntax for DHCP and TFTP/HTTP/HTTPS and other general information for the 4600 series IP Phones.

NB: Please see the ‘Avaya 96xx Administrator Guide’ for detail on additional parameter syntax for DHCP and HTTP/HTTPS and other general information for the 9600 series IP Phones. The 96xx series IP Phones do not support TFTP.

NB: 96xx IP Phone support is provided in CM v3.0 and above. CM v3.1 provides G.722 wideband codec support. For CM3.x installations 96xx IP Phone support is provided using 46xx series alias configurations. From CM v4.0 native 96xx support is provided.

NB: Subsequent IP Phone boot sequences will not use the data (native) VLAN. Once learnt, the voice VLAN number remains in NVRAM. If the IP Phone is moved to another voice VLAN, NVRAM must be flushed. See the VLANTEST note below.

NB: We have noticed that some DHCP software versions need the SSON176 string in quotes whilst others do not. It is recommended that testing takes place to ensure the DHCP server software operates successfully with the Avaya IP Phones.

NB: Be sure to place `ip helper-address a.b.c.d` where a..b.c.d is the address of the DHCP server, on router interfaces providing default gateway service for IP Phones and PCs.

NB: It is good practice to **rotate the order of MCIPADD CLAN addresses** in the SSON176/242 string for each different voice scope configured on the DHCP server. By default the IP Phone will use the first address in the list to attempt registration. The receiving CLAN will then off-load (implicit load balance) to an alternative CLAN to continue the registration process for any individual IP Phone. To ensure the initial CLAN is not oversubscribed (eg. following major power failure recovery, where a large number of IP Phones attempt to re-register simultaneously), the order of the MCIPADD list should be cycled to ensure the same CLAN IP address is not used as the first registration point for all DHCP Option176/242 scopes.

NB: For 46xx firmware before v2.6 and 96xx firmware before v2.0 (H.323) and v1.0 (SIP), if DHCPOFFER is not received by the IP Phone in the voice VLAN, the IP Phone will continue to request an offer for a limited period of time. As the period of time expires, the IP Phone will attempt connectivity over the data VLAN. By setting VLANTEST=60 (default), the IP Phone would wait to receive a DHCPOFFER for 60 seconds then fall back to the data VLAN. Voice quality may become degraded using the data VLAN. As a result there is a trade-off between no phone function at all and phone function with the possibility of unpredictable voice quality for the period of the failure. In order to revert to the voice VLAN, the IP Phones will require a reset.

Setting VLANTEST=0 ensures that the IP Phone will never attempt to receive a DHCPOFFER in the data VLAN following a failure of this kind in the voice VLAN. If VLANTEST=0 and it is required that the IP Phone be moved to a different voice VLAN, the IP Phone will require a reset to flush the current voice VLAN number held in NVRAM. A reset can be completed by depressing **HOLD** followed by typing **RESET#** using the phone keypad (do not press HOLD and RESET# simultaneously – HOLD first then RESET#). Please see the '4600/9600 Series LAN Admin Guide' for more details.

For 46xx firmware v2.6 and 96xx firmware v2.0 (H.323), v1.0 (SIP) and later, there is a change to the IP Phone behaviour using VLANTEST. Following a 60 second [default] period where no voice VLAN DHCPOFFER has been received, the IP Phone will request a DHCPOFFER over the data VLAN but will continue to try to receive DHCPOFFER over the voice VLAN. IP Phones will automatically revert to the voice VLAN when the request is successful.

3.13 VLAN Requirements

The Avaya system will require VLAN segregation for all Avaya devices connecting to the LAN infrastructure. The Avaya recommendations are as follows:

1. *Multiple VLANs for IP Phones*. VLANs configured for **IP Phones** should follow the same data VLAN design in each wiring closet. This is described as a dedicated voice VLAN in addition to each dedicated data VLAN.

2. *Single VLAN for the Avaya Gateway interfaces*. These interfaces are part of the G650 install. All **CLAN** and **MedPro** interfaces need to be connected into a dedicated VLAN or VLANs on the local LAN switches.

3. *S87xx and IPSI connections*. For **S87xx** and **IPSI** traffic two VLANs should be configured. The first for Control Network A, the second for Control Network B.

4. *Single VLAN for connected G250/G350/G450/G700*. A separate VLAN should be configured for connections to Avaya G250/G350/G450/G700 gateways.

NB: Adjuncts to the Avaya system (eg. CMS, Modular Messaging, Meeting Exchange, Voice Recording etc) requiring IP connectivity to CLAN boards for normal operation should be assigned to the most appropriate VLAN based on the customer infrastructure topology. Adjuncts can be placed in the same VLAN (inside the CLAN/MedPro VLAN) or they can be placed in a 'server farm' (data) VLAN or a dedicated 'voice server' VLAN. Avaya recommend the use of a dedicated voice server VLAN. The necessary CLAN resource (required for registering adjuncts servers) should be dedicated (ie. not used for IP Phone or gateway registration but dedicated to adjuncts only) and located inside the voice server VLAN. Customer network personnel should agree with the Avaya installation engineer how the adjunct CLAN resource and adjunct VLAN(s) are to be configured and installed.

3.13.1 IP Phones per VLAN

General recommendations for the number of IP Phones per VLAN are as follows:

- A VLAN containing IP Phones where there are no PCs connected to the secondary Ethernet ports of Phones, should have no more than ~500 hosts;
- A voice VLAN containing IP Phones and a data VLAN for PCs connected to the secondary Ethernet port of Phones, should have no more than ~250 hosts per VLAN (ie. 250 PCs in the data VLAN and 250 IP Phones in the voice VLAN);
- General maximum broadcasts per second should be no more than 500, with peaks of no more than 1000.

The DHCP Option176/242 should be configured to "round-robin" between initial CLANs. No more than 400 IP Phones should attempt to connect to a CLAN following an outage. Initial CLAN registration is carried out on a VLAN basis. This suggests that general good practice would be to restrict the number of IP Phones per VLAN to ~250 regardless of whether PCs were connected to them or not.

3.14 IP Address Requirements

IP Subnets will need to be assigned in accordance with the VLAN configurations detailed in the earlier section.

1. Sufficient dynamically assigned IP addresses for all IP Phones in the IP Phone VLANs throughout the network.

2. Sufficient static IP addresses for the Avaya Gateway interfaces VLAN (CLAN and MedPro). One IP address per MedPro or CLAN (and other boards such as VAL) in the system with sufficient spare addresses for future expansion.

3. Sufficient static IP addresses for the Avaya Control Networks to include all interfaces on both S87xx/S85xx servers. One IP address for each physical Ethernet interface on each S87xx/S85xx and relevant VIP addresses. One IP address for each IPSI board in each Control Network VLAN.

4. Sufficient static IP addresses for the Avaya G250/G350/G450/G700 VLAN (Single VLAN for connected G250/G350/G450/G700). Each chassis (assuming standby S8300 processor LSP) will typically require 4 or more (internal) IP addresses. This will depend on the configuration.

NB. Subnet mask and gateway address (local router HSRP address) must also be supplied with each set of host IP addresses.

NB: Sufficient adjunct and associated dedicated CLAN IP addressing should be provided. Please see the note in ‘VLAN Requirements’ section.

NB: Additional VIP addresses may be required for pairs of MedPro boards. This will depend on the hardware and configuration chosen.

3.15 Power over Ethernet Calculations for LAN Switches

The Power over Ethernet (PoE) capabilities for LAN switches and/or switch line cards connecting Avaya IP Phones must ensure the following:

- The Cisco PoE cards/switches are 802.3af compliant
- Sufficient power is available for all phones in a single switch or attached to a single line card

The following table details the power requirements for Avaya 46xx IP Phones:

Power Consumption - Watts (IEEE 802.3af -2003@ 48V)

	4601, 4602 Class 2	4602SW Class 2	4606/12/24 Class 0	4610SW Class 2	4620 Class 3	4620SW Class 3	4620SW Class 2	4621SW 4622SW Class 2	4625SW Class 3	4630SW Class 3
Typical	3.5	4.1	5	4	7.7	5.9	4.6	4.9	7.8	11.8
Worst Case	4.6	5.0	6.4	6	9.9	8.0	5.75	6.45	9.42	12.9

- Class 1 devices draw max 4W
- Class 2 devices draw max 7W
- Class 3 devices draw max 15.4W

NB: 9610 IP Phones are Class 1 devices. All other 96xx series IP Phones (9620/30/40/50) are Class 2 devices, however, adding one or more SBM modules will uplift to Class 3. 96xx series with GigE adapters are Class 3.

Power efficiency
There is an approximate 11% power loss when using the IEEE 802.3af method of powering Powered Devices (PDs). Please review the appropriate Cisco documentation. As a result, more power is required to compensate for the natural loss in the power supply conversion process. This means power transport through the Cisco 6500 series switch is only 89% efficient. The approximate 11% loss occurs between the power supplies, along the back-plane and through the PoE switch card of this chassis-based system and is mostly lost in the form of heat. As a result, a class-3 non-Cisco PD will have 17.3Watts logically reserved to yield 15.4Watts to the Ethernet cable.

3.15.1 Example 1

Power consumption calculations should be made to ensure sufficient power is available. Total power consumption calculations for a 6500 series switch, with the following line modules, is as follows:

1. Power consumption for Cisco line modules (single Cisco 6509 worst case):
   - WS-Sup720 x2 = 787.5W
   - WS-C6k-9SLOT-FAN2 x1 = 160W
   - WS-X6704-10GE x1 = 329.70W
   - WS-X6548-GE-45AF x5 = 829.50W

Grand total for Cisco line modules in example 6509 = **2276.40W** leaving **1723.60W** for IP Phones

2. Power consumption for 80x 4620 class 3 IP Phones (worst case):
   - 15.4W x 80 = **1232W**

All calculations are based on worst case. Please contact your Cisco provider to confirm power calculations for specific switch hardware.

3.15.2 Example 2

Cisco 3750 48-port wiring closet switches have a maximum of 370W. This would provide sufficient power for 24 class 3 devices (15.4W) or 48 class 2 devices (7W). Later releases of IOS allow restriction of the maximum power allocated as described earlier in this document. The availability of this command is dependent on switch hardware and software.

The Power Consumption table above outlines the power allocation and actual maximum power required for Avaya IP Phones (these values will always be less than the 802.3af class reservations, however, the 802.3af standard will reserve the maximum for the class regardless of whether the IP Phones need it or not).

3.15.3 Configuration Details For Cisco Switch Hardware

Auto is an automatic mode that senses the PoE class and then delivers the maximum power of the particular class range (7W or 15.4W) if enough power is available. When all available power is allocated, no remaining ports can be powered.

Never is used to disable power and power sensing on that port (interface). Non-PDs (Powered Device) such as desktop PCs are good candidates for this command.

Static is used to pre-allocate power to a port even before the switch senses a valid PD. This is a priority scheme to make sure the most important PDs always receive power.

The **`max`** ***`max-wattage`*** option for the Auto and Static states is used to restrict the use of higher power PDs. One example may be a 24-hour call centre where the agents use a class-2 IP phone and the supervisor uses a class-3 display phone. If an agent “borrowed” the display phone, and connected in place of the class-2 phone, the fixed switch would shutdown power to that port. There are two occasions where fixed switches will remove power from a port:

1) A PD requires more power than the Max option is set to provide
2) The Max option is set lower than the PoE class maximum value

You can determine if one of the two conditions listed above has occurred by using the **`show power inline`** command. If **`power-deny`** is listed instead of **`on`**, in the ‘oper’ column, either the PD requested too much power or the max value was lower than the class maximum value.

NB: You cannot use the **`max`** ***`max-wattage`*** option to save logical power in the hopes of increasing the maximum number of PDs that can be powered from a single switch.

More recently, the Catalyst 3750 (and possibly others) have a command that allows the reclaim of logical power beginning with IOS 12.2(25)SEC. This command sets a power ceiling that is more than the device will draw, but less than the max value of the PoE class range. The command is **`power inline consumption default`** `[`*`wattage value`*`].` This command can be applied in global configuration mode for the entire switch or individual values for each interface (port). A global setting of 6 watts for every port would be:

```
        Switch (config)# power inline consumption default 6000
```

An individual port setting for Gig port 1/0/2 at 11 watts would be:

```
Switch (config)# interface gigabitethernet 1/0/2
Switch (config-if)# power inline consumption default 11000
```

This command is extremely useful if you are deploying class 3 PDs. The value is greatly diminished when deploying class 2 or class 1 PDs because the difference between the actual power-draw and the class maximum value is much smaller.

3.16 TFTP/HTTP Server Requirements

TFTP or HTTP (or HTTPS) server can be used for firmware and configuration downloads to 4600 series IP Phones as they progress through the boot sequence. 9600 series IP Phones do not support TFTP. TFTP/HTTP server software purchased should be able to support simultaneous downloads that match the maximum number of IP Phones served by the TFTP/HTTP server (in the event that all phones require TFTP/HTTP services simultaneously). There is no specific recommendation for specific TFTP/HTTP application software, however, if TFTP is used, Avaya recommend the use of UNIX or Linux based application for the best results. HTTP server is preferred over TFTP.

3.16.1 Central or Local TFTP/HTTP Servers

For medium to large enterprise customers, the question of whether to deploy central TFTP/HTTP servers or have them reside locally at remote sites is often asked. Avaya have no explicit recommendation concerning the location and spread of TFTP/HTTP servers. The points raised below should be considered when discussing proposals for deploying TFTP/HTTP servers (these points also apply to the deployment of DHCP servers).

Centralising TFTP/HTTP servers:

- Will reduce cost and management overhead;
- May cause problems when downloading files to many endpoints simultaneously (WAN bandwidth consumption) and is entirely reliant on network (WAN) availability.

Customers often choose to deploy using either:

- Central TFTP/HTTP only;
- Remote (local) TFTP/HTTP only;
- Hybrid (distributed) service: TFTP/HTTP servers are located a key sites throughout the network. Each server provides services for a small number of remote sites and the site where it is located. Servers back-up one another.

NB: The TFTP server supplied with the IP Phone firmware at http://support.avaya.com will only support a very small number of simultaneous downloads.

NB: Firmware files are of the order of 2-3MB in size. This should be taken into account if the TFTP/HTTP server is centralised and a large number of IP Phones require firmware update over a WAN link.

3.17 Access Control Lists and/or Firewall

The Avaya system uses a range of TCP and UDP ports in normal operation. If firewalls and/or Access Control Lists (ACLs) are to be used, the “Avaya IP Telephony Implementation Guide - Appendix D” should be referenced for port allocations for firewall and/or ACL configurations. If firewalls have Network Address Translation (NAT) configuration this may impact Avaya system operation.

IP Telephony may not work through devices performing NAT because the NAT device is unable to convert IP addresses held in the packet payload (eg. an alternative CLAN IP address for IP Phone registration).

The problem is not encountered in all VoIP scenarios. For example, problems with NAT do not generally occur in VPN-based remote access for IP Softphone or Hardphone with VPN client.

Ideally, enterprise firewalls should not perform a NAT function between Avaya devices. If NAT must be implemented, Avaya strongly recommend testing all areas of the solution to confirm successful operation.

3.18 802.1X and LLDP

From firmware version 2.6 for the 4600 series and version 1.0 for the 9600 series IP Phones, 802.1X is supported. Link Layer Discovery Protocol (LLDP) is supported from version 2.6 for the 4600 series and version 1.2 for the 9600 series IP Phones. LLDP is designated as IEEE 802.1ab and is analogous to Cisco Discovery Protocol (CDP) or Nortel Discovery Protocol (NDP). At the time of writing LLDP is supported on an increasing number of Cisco switch hardware (eg. 3750 & 3560). Testing should take place to determine the level of LLDP support available between Avaya IP Phone and Cisco switch as certain features may not be available.

3.18.1 802.1X

802.1X is divided into 3 key elements:

- Supplicant (the PC and/or IP Phone)
- Authenticator (the Ethernet switch the PC/IP Phone is connected to)
- Authentication server (RADIUS server holding valid user/device credentials)

As a supplicant the Avaya IP Phone provides the following:

- Supports only MD5-Challenge, EAP method (Extensible Authentication Protocol)
- During the initial boot up, the IP Phone display prompts for an EAP ID and Password (not repeated on subsequent boot-ups)
- Default EAP ID is the MAC address (minus the separating colons). The EAP ID may be changed but this is not recommended
- EAP password is a maximum of 12 numeric characters. The EAP password uses numbers only; no alphabetic/special characters are permitted
- After initial provisioning, the EAP ID and Password are stored in flash
- The EAP ID and Password are submitted automatically to 802.1X authentication/re-authentication requests

The 4600 & 9600 series IP Phones support several modes of 802.1X operation. These include supplicant operation for authentication of the phone (IP Phone authenticates), pass-through of 802.1X messages for authentication of an attached PC (PC authenticates), and a multi-supplicant mode in which both the IP Phone and the PC can authenticate concurrently.

In order for both the IP Phone and PC to be authenticated, the local LAN switch hardware must support ‘multi-supplicant’ 802.1X (mac-based). At the time of writing, multi-supplicant support for Cisco switch hardware is expanding. Customers are advised to contact their LAN switch vendor to determine the latest support for multi-supplicant and whether this is supported on ports with multiple VLANs assigned. In order to have either the PC or IP Phone authenticate (but not both) the LAN switch port must support ‘multi-host’ (single-supplicant) 802.1X (port-based) configuration. Proxy-logoff is supported to alert the network if an authenticated PC is disconnected from the IP Phone.

There are three 802.1X states adopted by the IP Phone. Extensible Authentication Protocol Over LAN (EAPOL) is the protocol used between authenticator and supplicant using multicast:

1. DOT1X=0 (default). The Ethernet switch in the IP Phone forwards multicast 802.1X frames from authenticator to the attached PC. Proxy Logoff* function is disabled.
2. DOT1X=1. As above but with Proxy Logoff enabled.
3. DOT1X=2. The Ethernet switch in the IP Phone forwards multicast 802.1X frames only to the IP Phone and ignores multicast 802.1X frames from the PC. Proxy Logoff is disabled.

*Proxy Logoff allows the IP Phone to inform the network if an authenticated PC has been disconnected.
**DOT1X is the configuration parameter used to configure 802.1X support for the IP Phone through DHCP Option176/242 or the optional 46xxsettings.txt file in TFTP/HTTP.

Possible combinations are as follows:

- Phone authenticates (no PC attached), use option (3.) above;
- Phone authenticates (PC attached), use option (3.) above;
- PC authenticates (attached to IP Phone), use option (1.) or (2.) above;
- PC and Phone authenticate (assumes Ethernet switch supports multi-supplicant, mac-based, mode), use option (1.) or (2.)

Example IOS Configuration using Cisco ‘Multi-Domain’ (both PC and Phone authenticate) configuration

```
aaa new-model
aaa authentication dot1x default group radius
aaa authorization network default group radius
!
dot1x system-auth-control
dot1x guest-vlan supplicant
!
radius-server host 172.20.5.6 auth-port 1645 acct-port 1646
radius-server source-ports 1645-1646
radius-server key 7 15031C09163E32
!
!
interface GigabitEthernet1/0/11
 switchport access vlan 21
 switchport mode access
 switchport voice vlan 30
 priority-queue out
 power inline auto
 dot1x mac-auth-bypass
 dot1x pae authenticator
 dot1x port-control auto <-port in unauthorized state. Process starts when EAP frames received
from client or port transitions from down to up
 dot1x host-mode multi-domain <-multi-supplicant if supported on hardware otherwise use
'dot1x host-mode multi-host' for Phone or PC authentication (not both).
 dot1x timeout reauth-period 30
 dot1x reauthentication <-enables periodic reauthentication of the supplicant
 dot1x auth-fail max-attempts 2
 dot1x guest-vlan 20       ) The guest VLAN and restricted VLAN
 dot1x auth-fail vlan 20         ) features only apply to the data devices
 mls qos trust dscp
 no cdp enable
 spanning-tree portfast
```

Useful CatOS commands:

```
 set port dot1x port-control auto <-port in unauthorized state. Process starts when EAP
frames received from client or port transitions from down to up
 set port dot1x multi-host enable <-enables multiple hosts per port
 set port dot1x reauthentication enable <-enables periodic reauthentication of the
supplicant
```

Use the following command for CatOS switches supporting multi-supplicant:

```
 set port dot1x multiple-authentication enable <-enables multiple supplicants per port
and should be used instead of set port dot1x multi-host enable
```

Configuration Notes:

You must configure the voice VLAN for the IP phone when the host mode is set to multi-domain (multi-supplicant). If you use a dynamic VLAN in order to assign a voice VLAN on an MDA-enabled (multi-domain) switch port, the voice device fails authorization.

NB: 802.1X cannot be configured on a trunk port. Hence, for IP Phone connections the 'voice vlan' or 'auxiliary vlan' method should be used. See the relevant section in this document.

NB: Please see the 46xx Series and/or 96xx Series LAN Administrator Guide for more information.

3.18.2 Link Layer Discovery Protocol (LLDP)

LLDP is supported on 46xx IP Phones with release v2.6 or later and v1.2 for 9600 series IP Phones. LLDP is enabled by default and requires no additional configuration for the IP Phone. The IP Phone will transmit LLDP frames only after it has received an initial LLDP packet from the Ethernet switch. Thereafter, it will continue to send LLDP packets every 30 seconds. LLDP frames received from the LAN switch are not forwarded to a PC connected to the IP Phone's secondary Ethernet port. LLDP frames are not generated for the secondary Ethernet port at all.

LLDP TLVs are used to pass information between endpoints such as IP Phones and LAN switches. LLDP-MED TLVs (Media Endpoint Discovery) are a subset of LLDP TLVs, specifically related to VoIP. These handle capability discovery, network policy, Power over Ethernet (PoE), inventory management and location information. Testing is recommended to confirm LLDP-MED implementations between Avaya IP Phone and LAN switch operate successfully. By default, LLDP-MED function is enabled on Cisco LAN switch ports supporting LLDP. Avaya IP Phone LLDP is fully supported on all Extreme switches.

The following IP Phone parameters are passed between IP Phone and LAN switch via LLDP-MED (will depend on switch vendor compatibility, testing recommended):

1. PHY2VLAN (802.1Q encapsulated VLAN ID for the IP Phone's secondary Ethernet port attaching the PC)
2. L2QVLAN (the voice VLAN the IP Phone is a member of)
3. MCIPADD (IP address of registration gateway, CLAN)
4. TFTPSRVR, HTTPSRVR, TLSSRVR (IP addresses of either the TFTP, HTTP or HTTPS servers to be used)
5. L2Q (802.1Q state: on, off, auto)
6. PoE power conservation mode (enabled/disabled)

Items 1, 2 & 5 delivered by LLDP take precedence over the DHCP delivered parameters.

3.19 Bandwidth Consumption

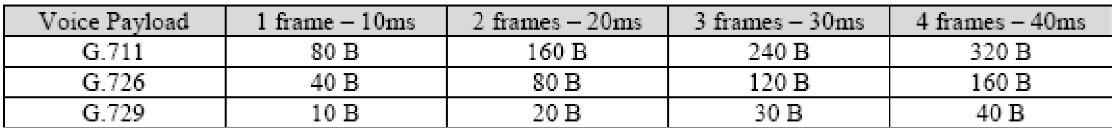
Bandwidth consumption for bearer (audio) and signalling traffic can be calculated in order to provide information to enable correct bandwidth sizing.

3.19.1 Bearer Traffic

When calculating bandwidth consumption for bearer traffic, the following points must be known in order to size individual calls correctly:

- The codec used (typically, either G.711 uncompressed or G.729 compressed)
- The voice sample size per packet (default is 20ms but can be configured 10-60ms)
- The voice sample size determines the packet throughput (pps). For example, a voice sample size of 20ms would require throughput of 50pps. 50 packets will provide 1 second of voice
- The layer 2 encapsulation type (Ethernet, PPP, frame-relay, ATM etc)
- Whether VPN (IPSec) or GRE tunnels are use to encapsulate VoIP calls. These add considerably to the packet overhead
- Whether RTP compression is used

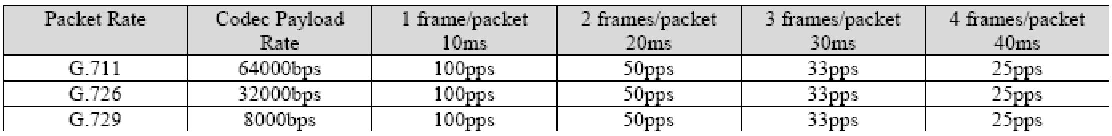
Table 1 details the payload size in Bytes for the different codec types and voice sample sizes.



Voice Payload	1 frame – 10ms	2 frames – 20ms	3 frames – 30ms	4 frames – 40ms
G.711	80 B	160 B	240 B	320 B
G.726	40 B	80 B	120 B	160 B
G.729	10 B	20 B	30 B	40 B

Table 1 – Sample Size vs Payload

Table 2 details the throughput depending on the voice sample size used but does not include the frame/packet overhead.



Packet Rate	Codec Payload Rate	1 frame/packet 10ms	2 frames/packet 20ms	3 frames/packet 30ms	4 frames/packet 40ms
G.711	64000bps	100pps	50pps	33pps	25pps
G.726	32000bps	100pps	50pps	33pps	25pps
G.729	8000bps	100pps	50pps	33pps	25pps

Table 2 – Sample Size vs Packet Throughput (pps)

The following example bandwidth calculations use the default 20ms voice sample (payload) size.

An example bandwidth calculation for a single G.711 call over Ethernet would be as follows:

Ethernet overhead inc preamble:	26-bytes
Optional 802.1Q header:	4-bytes
IP overhead including UDP & RTP hdrs:	40-bytes
Voice payload:	160-bytes (20ms)
Throughput:	50pps (20ms sample requires 50 packets for 1 second of voice)

(26+4+40+160)*8 = 1840-bits
1840*50 = **92Kb/s**

An example bandwidth calculation for a single G.729 call over PPP would be as follows:

PPP overhead inc CRC:	10-bytes
IP overhead including UDP & RTP hdrs:	40-bytes
Voice payload:	20-bytes (20ms)
Throughput:	50pps (20ms sample requires 50 packets for 1 second of voice)

(10+40+20)*8 = 560-bits
560*50 = **28Kb/s**

An example bandwidth calculation for a single G.729 call over ATM would be as follows:

AAL5 overhead	8-bytes
IP overhead including UDP & RTP hdrs:	40-bytes
Voice payload:	20-bytes (20ms)
Throughput:	50pps (20ms sample requires 50 packets for 1 second of voice)

The information above suggests that 2x ATM cells would be required to encapsulate the 68-byte (8+40+20) payload. Each cell is 53-bytes with 48-bytes available for payload. As a result, the second cell would be padded with 28-bytes. This is commonly referred to as 'cell-tax'.

2x 53-bytes = 106-bytes
106*8 = 848-bits
848*50 = **42.4Kb/s***

***NB:** If passing VoIP bearer (audio) over ATM circuits (eg. ATM tail circuits into an MPLS network) with the G.729 codec, consider adjusting the voice sample size per packet to 30ms or 40ms in order to conserve bandwidth. Cell tax (overhead) occurring in ATM networks can add considerable additional per-call bandwidth consumption when using the default 20ms voice sample size. In the example above, 30ms payload over ATM would give 28.3Kb/s and 40ms payload, 21.2Kb/s.

NB: When sizing the priority and class based queues for Cisco LLQ configuration, the 'priority', 'police' and 'bandwidth' statements use bandwidth calculations without the layer 2 overhead. When sizing for concurrent calls remove the layer 2 header (& MPLS label) bytes when totalling likely bandwidth consumption for LLQ.

NB: AES 128-bit bearer encryption does not add overhead to the audio (RTP) traffic stream. All key exchange and other overheads are established during call set up.

3.19.2 Signalling Traffic

Signalling bandwidth is calculated based on the specific Avaya installation. It uses information based on the number of IP Phones and/or number of gateways, number of Busy Hour Calls (BHC) and Grade of Service (GoS). GoS is conceptual and is an assurance that that a user will get a response (eg. hear dial tone) within a 350ms period 98% of the time.

Signalling traffic is divided into 2 areas:

- Calculate actual bandwidth signalling traffic will use
- Calculate bandwidth required to ensure GoS is met

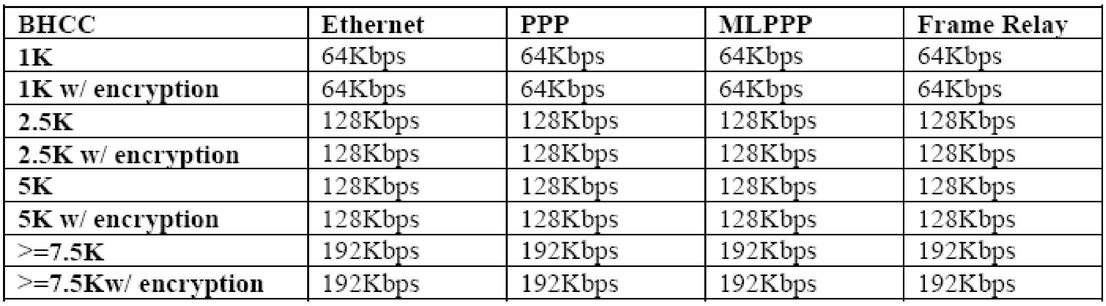
GoS bandwidth estimates tend to ‘require’ more bandwidth for signalling than actual signalling bandwidth consumption.

Bandwidth consumption for signalling traffic is very small by comparison to audio traffic and is calculated (estimated) using a number of variables specific to the installation as described above. Formulas are available from Avaya to assist in calculating the likely bandwidth consumption for signalling traffic.

Alternatively, signalling bandwidth can be *very roughly* estimated. For example, if there are 50 simultaneous G711 calls over a link, adding a 51st call would most likely cover the additional bandwidth consumption for the associated signalling traffic. This is a rough estimate and may not be an appropriate sizing tool for all Avaya installations. Avaya recommend using the appropriate formulas available for signalling bandwidth sizing.

3.19.3 S87xx/S85xx To/From IPSI: Bandwidth & QoS

The bandwidth consumption for traffic between the primary server (S87xx/S85xx) to remote IPSI boards in G650, is also small compared to audio traffic. This is calculated based on the number of Busy Hour Calls Completed (BHCC) for each remote Port Network (PN) the S87xx/S85xx server is controlling. Table 3 details the bandwidth consumption for S87xx to/from IPSI traffic for Ethernet and other layer 2 WAN protocols in 64Kb/s increments.



BHCC	Ethernet	PPP	MLPPP	Frame Relay
1K	64Kbps	64Kbps	64Kbps	64Kbps
1K w/ encryption	64Kbps	64Kbps	64Kbps	64Kbps
2.5K	128Kbps	128Kbps	128Kbps	128Kbps
2.5K w/ encryption	128Kbps	128Kbps	128Kbps	128Kbps
5K	128Kbps	128Kbps	128Kbps	128Kbps
5K w/ encryption	128Kbps	128Kbps	128Kbps	128Kbps
>=7.5K	192Kbps	192Kbps	192Kbps	192Kbps
>=7.5Kw/ encryption	192Kbps	192Kbps	192Kbps	192Kbps

Table 3 – S87xx to IPSI Bandwidth Consumption per Port Network

S87xx to IPSI traffic is TCP based and intolerant of packet loss. Avaya recommend marking this traffic with DSCP46 (EF, similar to bearer traffic) or at least, DSCP36 (AF42, loss intolerant). Both the IPSI boards and S87xx/S85xx Ethernet interfaces can be configured to mark traffic with DSCP values. Use the **ipserver-interface** form to configure the S87xx server interfaces to mark outgoing server to IPSI traffic. The IPSI boards require **set diffserv** command configured at the IPSI CLI to mark traffic from IPSI to server. Please see the latest IP Telephony Implementation Guide, Appendix H for further information.

3.19.4 File Transfer Traffic between S8xxx Servers

The primary S87xx server in any system will be responsible for updating remote backup servers (S87xx/S85xx ESS & S8300) and is known as ‘save translations’ in Avaya parlance. This is an rsync transfer and is analogous to FTP. Estimating bandwidth consumption for traffic such as rsync is difficult as it depends largely on the size of the installation, number of moves/adds/changes, number of phones, gateways and so on.

System databases are of the order of 15MB in size for typical enterprise installations. After the initial rsync with the other servers in the network (where the entire database is sent), only incremental changes are transferred. Rsync traffic can be passed as best effort (DSCP0) and requires no special treatment. This traffic will pass from the management interface (eth0 or eth4) on the active S87xx server pair to the management interface for ESS S87xx or S8500 servers and to the S8300 in H.248 gateways such as G250, G350, G450 and G700.

3.20 Video Conferencing

Avaya video conferencing is provided from IP Softphone release 5 and later, and CM version 3.0.1 and later. Video conferencing can be point-to-point or via a Polycom MGC video bridge for larger conferences.

Video conferencing operates in either ‘Shared Control’ or ‘Road Warrier’ IP Softphone modes. Shared control is a version of Telecommuter mode with one key restriction. Shared control allows the use of an external Phone for the audio path but only if the Phone is registered directly to the Avaya system where the IP Softphone/Video client is registered. This can be a DCP or IP Phone. Non-Avaya registered phones, such as a home phone, cannot be used with video conferencing. In this case Road Warrier mode would be required. Road Warrier mode provides the audio path to the PC via a USB headset.

During a video conferencing call, whether in Shared Control or Road Warrier, the system would establish a separate RTP stream for audio and another for video. This allows the network to prioritise the audio and video streams independently from one another.

3.20.1 Video Bandwidth

Video call bandwidth can vary from 128Kb/s to 4Mb/s and will fluctuate during the life of a video call based on the picture content and movement. It is advisable to restrict the maximum ceiling for video call bandwidth consumption in Avaya CM. Typical maximum ‘per call’ values offering acceptable quality are of the order of 384Kb/s. It should be noted that this figure includes payload only (no layer 2 or 3 header) and also includes 64Kb/s for the audio component, regardless of whether G.729 or G.711 is used. For the purposes of sizing QoS queues in the network (WAN LLQ) a value derived from the maximum video bandwidth per call, in this case 384Kb/s, less the audio component of 64Kb/s (giving 320Kb/s), should be used. Remember to add approximately 20% for the layer 3 overhead. QoS queue sizing for the audio stream per video call will behave in the normal way as described earlier in this document.

3.20.2 QoS For Video Calls

As the video and audio RTP streams are separated for each video call, QoS can be applied separately. For IP Softphone, DSCP values for signalling, audio and video will be downloaded to the client on registration with the appropriate network-region in CM. In certain circumstances video and audio can be prioritised using the same LLQ priority queue, but for most applications this may not be appropriate. The network-region form allows DSCP values to be configured for audio, signalling and video. DSCP markings for audio and signalling have been discussed throughout this document. General 'industry standard' best practices indicate DSCP marking for video at AF41 (DSCP34) and 802.1p value at 4. Using LLQ, a priority queue would be configured for the audio streams, and a class based (bandwidth) queue for the video streams with queue sizes based on the information described above. Placing video and audio in the priority queue runs the risk of negatively impacting the audio streams. As video streams will use larger packets, there may be contention in the priority queue resulting in smaller audio packets suffering increased jitter and/or delay. As the number of video streams increase, the effect on the audio streams is likely to become significantly worse. As a general rule of thumb, if audio and video streams use the same priority queue, this should be no more than 35% of the link capacity. Please remember that this figure is a 'general' guideline and may vary depending on the traffic flows present over any particular network. Placing video and audio in the same priority queue but maintaining different DSCP values will allow different drop thresholds to be applied for voice and video. This can be used to fine-tune priority queue sharing.

The following example configuration shows audio placed in the priority queue and signalling and video in a class-based 'bandwidth' queue:

```
class-map match-all bearer <-choose to match based on AND/OR
        match ip dscp 46 <-match incoming audio (from the LAN or WAN)
        match access-group name voice-subnets <-match by source address from relevant
voice subnets
class-map match-all signalling
        match ip dscp 24 <-match incoming signalling (from the LAN or WAN)
        match access-group name voice-subnets <-match by source address from relevant
voice subnets
class-map match-all video
        match ip dscp 34 <-match incoming video (from the LAN or WAN)
        match access-group name video-subnets <-match by source address from relevant
video subnets


policy-map audio_control_video
        class bearer
                priority 2000 <-set required bandwidth for concurrent calls with strict priority.
                Please note: this is the bandwidth including the IP header only. It does not include the
                layer 2 header
        class signalling
                bandwidth 512 <-choose signalling bandwidth for class based treatment
        class video
                bandwidth 4000 <-choose video bandwidth for class based treatment
        class class-default
                fair-queue <- all other traffic by WFQ
```

The router WAN and LAN interfaces are configured as follows:

```
interface serial 0/1
        service-policy output audio_control_video

interface fastethernet 2/3 <-interface connecting local LAN switch
        service-policy output audio_control_video
```

3.20.3 Network Performance For Video

Network performance requirements for video conferencing are very similar to that of audio. Recommended performance parameters are:

Delay: no worse than 150ms one-way (toll quality audio: 80ms)
Loss: no worse than 1% (toll quality audio: 1%)
Jitter: no worse than 30ms (audio should be the same as the configured voice sample size per packet – default 20ms)

NB: The performance thresholds detailed above are for (interactive) video conferencing. These should not be confused with video streaming where performance parameters are less strict. For example, industry standard recommendations for video streaming are: one-way delay - 5 seconds or less; loss - 5% or less; jitter – recommended threshold not specified.

3.20.4 Restricting Video & Audio Calls

In CM it is possible to restrict the number of concurrent video calls between network-regions. It is also possible to restrict audio calls between network-regions using the Call Admission Control (CAC) feature. This should be considered when passing video or audio calls over limited bandwidth links to operate alongside the configured QoS queues in the network. In the event that a limit has been reached, successive video calls would be connected with audio only (assuming an audio CAC limit has not been reached). Priority users can be configured for video and audio only calls, to ensure certain VIP clients can always make calls by prioritising their access to available bandwidth configured in CM.

3.20.5 Testing IP Softphone

Whether IP Softphone is used for video or audio only calls, Softphone application testing is always recommended. This section has discussed the Avaya CM and network requirements for IP Softphone with specific regard to video, but has not included the PC environment onto which the Softphone application will be installed. As a result, testing must always take place before any implementation of IP Softphone, with or without video, to ensure successful operation. Testing should:

1. Confirm successful operation with PC hardware;
2. Confirm operation with PC OS and standard image;
3. Confirm operation with USB headset (Road Warrier mode) and/or USB camera;
4. Confirm Windows QoS Packet Scheduler installation and NIC support for 802.1p marking (if used);
5. Baseline IP Softphone call performance and confirm acceptance.

4 Network Readiness & Performance Monitoring

The recommended strategy to ensure network readiness before the implementation of an IP Telephony solution is outlined here. Avaya Network Consulting Services (NCS) provide assessment and consulting services relating to network readiness for all IP Telephony implementations. The recommended strategy is as follows:

(i) Develop a Network Design and QoS strategy for VoIP (use Avaya guideline documentation and/or design workshops):

- Ensure Network Design meets the voice SLAs required and that sufficient capacity exists in the network to support the IP Telephony solution
- Ensure QoS strategy meets business objectives
- Classify/prioritize voice, signalling, video and data (eg. Citrix) traffic based on the proposed converged solution design
- Allocate network resource to take ownership for voice related network design/configuration
- Create the converged network. Implement necessary design and configuration changes in accordance with the recommendations detailed in this document

(ii) Assess & fine tune the converged network

- Perform Basic Assessment (CIRS) and/or Detailed Assessment (NANO) to assess network performance to ensure IP Telephony readiness
- Baseline network
- Review network design & configuration
- Make necessary changes as appropriate and re-assess
- Implement the Avaya solution

(iii) Monitor network performance following implementation of Avaya solution

- Review and implement changes to converged network configuration/design as required (if any)
- Implement monitoring solution (Converged Network Analyser – CNA)
- Implement Avaya Integrated Management Suite (IMS) providing network and Avaya system management
- Enhance network resilience using CNA Adaptive Path Control (APC)
- Ensure network design/redundancy meets business SLA for voice on an ongoing basis

4.1 Network Assessment

There are two network assessment consulting offers available from Avaya NCS. These are Basic Assessment (CIRS) or Detailed Assessment (NANO)

4.1.1 Basic Assessment

This service provides a high-level evaluation of a customer's network infrastructure. Working remotely, Avaya NCS Consultants use questionnaires and customer topology information to gather data regarding the customer's LAN and WAN. The NCS Consultant uses this information to identify network devices to be monitored and the optimum position of the data collection tool. The non-intrusive, network data collection tool is used to record delay, packet loss, jitter and Mean Opinion Score (MOS) statistics from the target devices.

Basic Assessment provides:

- High level review
- Calculates delay, packet loss, jitter using UDP ping and/or basic voice simulation to nominated targets
- Low cost
- Low impact on the network
- Simple to run and generate basic report
- Basic SNMP analysis*
- Basic identification of performance faults
- Basic summaries

4.1.2 Detailed Assessment

This service provides a detailed evaluation of a customer's network infrastructure. Working on-site and remotely, Avaya NCS Consultants use questionnaires, interviews with customer data teams and customer topology information to gather data regarding the customer's LAN and WAN. The NCS Consultant uses this information to identify devices to be monitored on the client's network and the optimum position of the voice simulation endpoints (babels). These allow complex voice call simulations across the customer network in a many-to-many relationship. This provides QoS and capacity analysis and records delay, packet loss, jitter and Mean Opinion Score (MOS) while network baseline is measured using SNMP*. Additional information is gathered (eg ‘show tech’ output** for router and switch devices, call analysis, and others) in order to prove network performance and configuration (QoS, 802.3af, VLAN design etc) is in accordance with Avaya recommended guidelines.

Detailed Assessment provides:

- Detailed review
- A thorough understanding of problem areas, root causes, and recommendations on how to fix them
- Call synthesis simulates no. of calls, port range, paths, codec, voice sample size and DSCP values in a many-to-many relationship
- Detailed performance assessment
- Detailed SNMP analysis*
- Network design and configuration review**
- Vital network information and functional requirements needed for IP Telephony implementation

*Requires SNMP read-only access to all switches/routers carrying Avaya related traffic
**Requires switch/router configuration output using 'show tech' and other commands

4.2 Converged Network Analyser (CNA)

Converged Network Analyzer (CNA) is the flagship product in the Application Assurance Networking (AAN) product line. CNA software delivers two key value propositions for Avaya customers:

- Detailed visibility into the performance of paths through the converged IP network for both IP Telephony and data applications

- ‘Path performance’ based re-routing over diverse WAN connections between locations, known as Adaptive Path Control (APC). APC provides real time optimisation that can significantly enhance the reliability of business-critical applications including VoIP.

CNA provides key information concerning the performance of network paths and how this relates to specific classes of traffic. It provides on-going end-to-end performance statistics implicitly measuring 3rd party service providers for performance compliance for real-time and non real-time applications. CNA can be configured to act when performance falls below thresholds and is used to complement traditional Network Management tools that cannot identify which applications and users are affected by problems with individual links and/or network devices.

4.2.1 Server Based Measurement

A CNA server targets statically configured or dynamically discovered targets with streams of measurement traffic to discover raw latency, loss, and jitter characteristics for paths from the server to the targets. Measurement traffic is configured to carry certain DSCP values and to pass over some or all links between locations. Performance over paths through the network is expressed by converting raw network measurements into an application performance rating, comparable to ‘star’ ratings. A four or five star path means the application performance is good or excellent, while paths below three stars indicate application outages. These relate to network performance problems severe enough to affect users. These scores are used to derive performance from the point of view of application availability based on the ‘five nines’ construct.

4.2.2 Agent Based Measurement

A CNA server can also monitor paths through the IP network using a collection of CNA agents embedded in Avaya IP Telephony equipment, such as IP Phones, media gateways or Extreme LAN switches. Standalone CNA Agent Devices are also available for locations where no IP Telephony equipment resides. Agents register with the CNA server and are scheduled by the CNA to conduct simulated RTP calls between pairs of agents in a many-to-many arrangement. This functionality is known as ‘Chatter’.

4.2.3 Path Optimisation

CNA enables administrators to monitor the general health of their IP network and its ability to support real-time applications such as voice, video, and non real-time business critical applications. CNA also uses Adaptive Path Control (APC) for automatic path optimisation. APC can add a “9”to the overall application availability in a way that no other network management tool can. APC can re-route traffic based on the performance (or lack of performance) over a particular network path when compared to an alternative path. Constant comparison between paths can be used to determine the path with the best possible performance and does not rely solely on network re-convergence following a link or interface failure (up/down state). This is especially beneficial over single or dual provider links where a network path suffers performance degradation but where routes remain up. Traditional CE routers are not equipped to deal with performance problems in this way. CE routers make decisions based only on whether the interface is up and available for traffic forwarding. If CNA detects an application outage on the current path chosen by standard IP routing, APC intervenes in real time to move the traffic to a better performing path.