# *SYSTEM ENGINEERING BULLETIN*

| | |
|---|---|
| **NUMBER:** | SEB-02-10-001 |
| **VER.ISS:** | 4.4.0 |
| **DATE:** | March 12, 2004 |
| **SUBJECT:** | Packet Trunking-IP (PT-IP) Engineering Rules |
| **DESCRIPTION:** | This document provides engineering guidelines for deploying, and configuring to the engineering limits of the network elements that make up the PT-IP solution. |
| **CONTACT:** | Forward questions and/or comments concerning this document to the author or any Nortel Networks System Capacity Engineer. |
| **MARKET:** | All Markets |


Randy Tuttle
Sr. System Engineer
Succession System Engineering

Ian Scales
Manager
Succession System Engineering


**NORTEL NETWORKS PROPRIETARY**

# SN06 Engineering Rules

## Packet Trunking IP

Document Status: Released
Release: 4.4.0
Publication Date: March 12, 2004
Security Status: Nortel Networks Proprietary
Document Owner: Randy Tuttle
Document Prime(s): Randy Tuttle

**NO NORTEL NETWORKS LIABILITY FOR CERTAIN USES OF ITS PRODUCTS**

The information contained in this release relates to certain Nortel Networks products that have been designed by or on behalf of Nortel Networks to conform to applicable Nortel Networks and third party specifications and requirements, including, for example, NEBS compliance. In addition, such Nortel Networks products are designed to be used for its intended purpose as specified in this documentation. In the event, and to the extent, that such Nortel Networks products are used by the user for a purpose other that its intended purpose, or used with third party products that do not conform to any such applicable Nortel Networks and third party specifications and requirements, including, for example, NEBS compliance, Nortel Networks shall have no liability of any kind to the user for any problems which may arise, including, without limitation, any related failure of the Nortel Networks product to perform in accordance with its specification.

© 2002 Nortel Networks
All rights reserved
Published in the United States

**NORTEL NETWORKS PROPRIETARY**: The information contained in this document is the property of Nortel Networks. Except as specifically authorized in writing by Nortel Networks, the holder of the information contained herein confidential and shall protect same in whole or in part from disclosure and dissemination to third parties and use same for evaluation, operation, and maintenance purposes only.

Information subject to change without notice.

# Document History

| Issue No.<br>Rel Date | Reason(s) for Reissue | Author and Department |
|---|---|---|
| 4.1.0<br>Dec. 20, 2002 | Pre-IT5 release for SN06 | Succession System Engineering — JB20 |
| 4.2.0 | IT+6 release for SN06 | Succession System Engineering — JB20 |
| 4.3.0 | SN06 FCS Release | Succession System Engineering — JB20 |
| 4.3.1 | Update to include final data in Trunk Gateway sections | Succession System Engineering — JB20 |
| 4.3.3 | Updates to align version number of document with SEB version number, remove the information on Destination Protection, clarify IP addressing for compact, and make minor security changes. | Succession System Engineering — JB20 |
| 4.4.0 | SN06.2 Release | Succession System Engineering — JB20 |

# About this Document

**Purpose**
The purpose of this document is to provide configuration and engineering guidelines for deploying Succession Packet Trunking-IP (PT-IP).

**Audience**
This document is intended for Nortel Networks internal and external customer use only. The audience for this document consists of the following individuals or groups:

- **Network Planners/Engineers and Sales Engineers** who have the responsibility of implementing the guidelines described in this document.
- **System Verification** who have the responsibility of verifying that the implementation matches the design.
- **Field Engineering Groups** who have the responsibility of implementing the final customer networks using these guidelines.

**Support and feedback**

The prime for this document is:
Randy Tuttle
external : (919) 991-4570
internal : ESN 351-4570
E-mail : rmtuttle@nortelnetworks.com

**Terminology**
The term “CS LAN” used in this document refers to the components that provide packet connectivity for CS2000 network devices, traditionally located in the Central Office (CO). The CS LAN also provides network connectivity to the core packet network, either IP or ATM, as well as to other external networks, typically Operations Support Systems (OSS) or other OAM&P networks.

Words or phrases used interchangeably in this document to refer to the **CS-LAN** include:

- CS LAN
- CO-LAN
- CS LAN components (or devices)
- Components (or devices) that comprise/comprising the CS LAN
- CS2000 CS LAN

Throughout this document the term “Media Gateway” is referred to all voice gateways. These are:

- Trunk Gateways (i.e., PVGs).
- Line Gateways (Cable Modems E-MTA, IAD).
- IP Phones and soft-clients (i.e., i2004 and i2050).

In this document, a trunk gateway is referred to as:

- A PVG representing a combination of a VSP FP and its assigned ATM/TDM FP cards.
- A PVG7000 representing a number of VSP FPs and ATM/TDM FPs housed in a Passport 7000 shelf.

- A PVG15000 representing a number of VSP FPs and ATM/TDM FPs housed in a Passport 15000 shelf.
- A Fully populated PVG15000 represents a shelf that maximizes the capacity, i.e. number of trunks of a PVG with regards to the interconnecting IP network.
- PVG - the terms PVG15000, PVG7000, and PVG may be used interchangeably unless noted specifically.

Words or phrases used interchangeably in this document to refer to the **CS2K Management Tools Server** include:

- SSPFS
- Packet Telephony Manager (PTM)
- Succession Element and Subnetwork Manager (SESM)

# 1.0 Introduction

## 1.1 Succession Objective

The Succession Network Solutions were developed to support shared use by voice, signaling, OAM and data traffic. The objective of this document is to describe the engineering required to ensure that the Packet Trunking (PT-IP) solution is highly scalable and will maintain optimal network performance and reliability, as the customer's network requirements change to meet its growing number of subscribers.

## 1.2 Packet Trunking (PT) Network

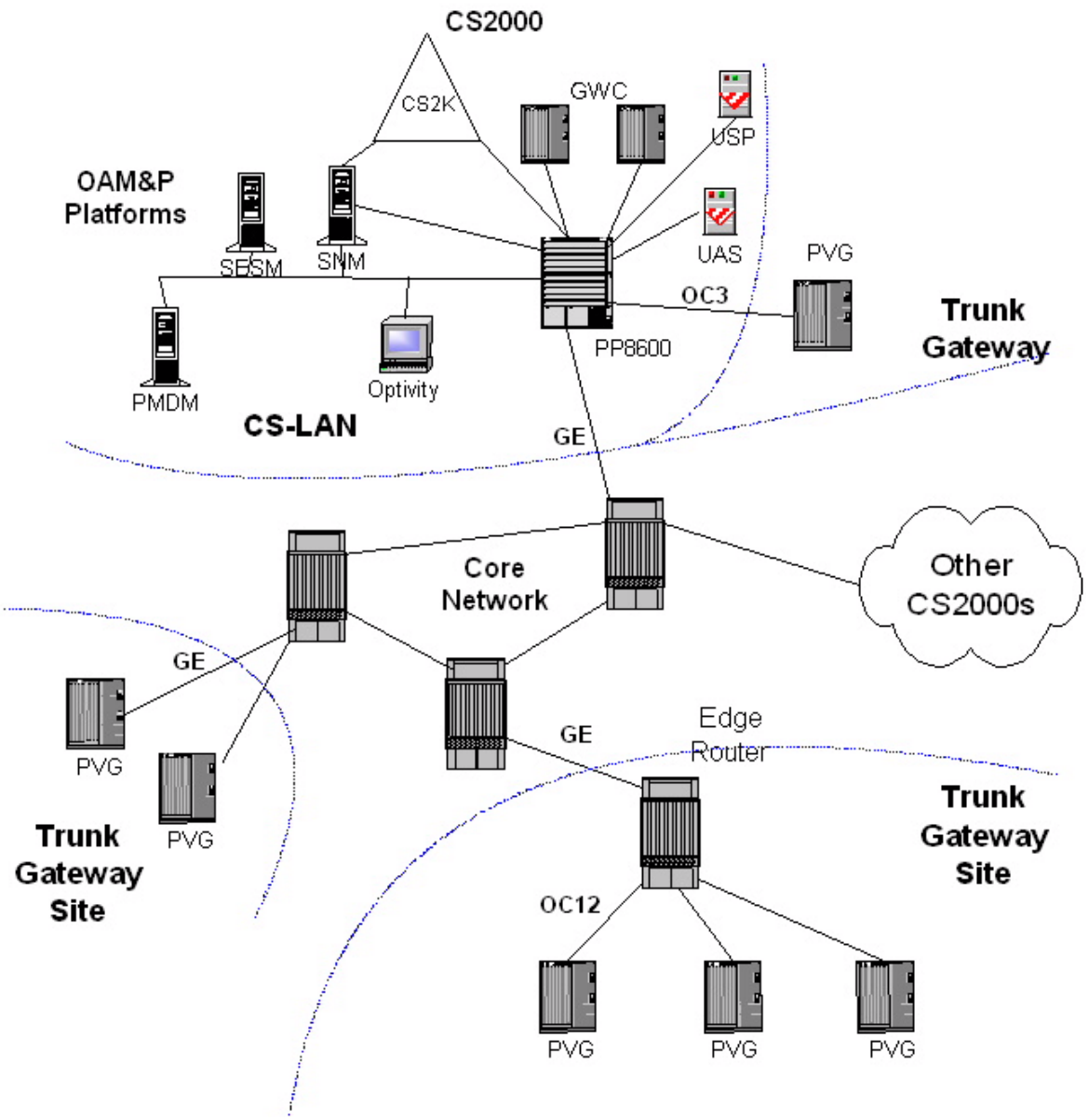
The Succession PT-IP network will provide a packet alternative to carrier network customers while maintaining existing ISUP and PRI features. The PT-IP network will carry packetized voice, call control signaling, inter-office signaling and OAM traffic. These packets will contend for network resources as they are transported through the network. The efficient sharing of network resources by multiple traffic streams is a fundamental economic premise for packet switched networks.

The initial Succession PT-IP networks will support connection of multiple Succession CS2000 nodes using Dynamic Packet Trunks, allowing direct voice over packet connections between gateways on different nodes.

Figure 1 on page 22 shows the basic IP network design for the PT-IP solution. This network can be conceptually divided into three zones:

- Communication Server LAN (CS-LAN),
- Core Network, and
- Trunk Gateway Site

**Figure 1 Basic IP Network Design For PT-IP Solution**




### 1.2.1 CS-LAN

The CS-LAN comprises the Passport 8600 Routing Switch, the CS2K, the Gateway Controllers (GWC), the Universal Signaling Point, and the Universal Audio Server. The OAM network management platforms can be located anywhere within the network; however, the SDM must be located in the CS-LAN. In Figure 1 on page 22, they are shown located at the CS-LAN.

Throughout this document, CS-LAN refers to the CS-LAN Call Processing subnet unless otherwise specified.

### 1.2.2 Core Network

This version of the Packet Trunking IP Network Engineering Guidelines deals with VoIP, that is, where bearer is carried strictly in IP packets. Voice over AAL2 is considered in a separate document.

The IP core network in its basic form is comprised of one or more routers, such as the Juniper M40, which serves to interconnect the CS-LAN to the Trunk Gateway sites and other PT nodes within the customer's network. It is possible that the Core Network will be carrying significant additional data traffic beyond the Succession IP traffic.

### 1.2.3 Trunk Gateway Site

Passport Voice Gateway 15K (PVG15K) or PVG7K Media Gateways (MG) make up a Trunk Gateway Site offering ISUP and ISDN PRI trunking services.

Remotely located from the CS-LAN, the PVG MG interconnects either with a Juniper router to aggregate the traffic to the core network, or directly to the core network router which may be a Passport 15000 Virtual Router (VR), Juniper M-Series or other vendor prior to connecting to the managed IP core network. The guidelines in this document have been verified for the PVG interconnect with the Passport 15000 VR and with the Juniper M-Series routers.

The following table shows the delays introduced based on the cable miles that a PVG may be remotely located from the CS2000. Although these distances may be exceeded, Nortel Networks currently does not recommend exceeding 2000 miles as a practical limit. Beyond this, perceived voice quality may degrade [with CS-LAN to Trunk Gateway Media Gateways], and speech clipping may also result.

**Table 1 Cross-office Delay (IAM incoming to IAM outgoing) to MG Distance[1]**

| Mileage | 0 miles | 1000 miles | 2000 miles | 3000 miles |
|---|---|---|---|---|
| Delay | 170-ms | 210-ms | 250-ms | 290-ms |

## 1.3 Traffic Flows

Call-control signaling routes between any gateway through to the GWC and the CS2000.

Voice traffic, in the form of Real Time Protocol (RTP) packets flows between:

- PVG and PVG located in the same Trunk Gateway site. The RTP stream is switched in the Hub router (i.e. Juniper M40)
- PVG and PVG located at different Trunk Gateway site. In this instance the RTP voice flows are routed through Juniper M40s and the core router(s)
- PVG and the UAS routed through the core router to the CS-LAN.

OAM traffic will route from each network element to its associated network management platform.

It can be observed that the different transport links will carry a different mix of voice, signaling, and

1. Based on XACore Atlas 3+1.

OAM traffic.

The traffic engineering rules are designed to optimize network performance for each traffic flow, while making effective and economic use of shared network resources.

## 1.4 IP Network Planning and Traffic Engineering Process

This document details the rules to be followed as well as limiting factors on capacity and performance. Itemized below are the main steps involved in planning and engineering a Succession Packet Trunking IP network solution:

**1.** Network Planning

- Identify the geographic source, and amount of the voice traffic: i.e. number of trunks and estimated ccs/trunk. This step will identify the number of Trunk Gateways and points of interconnection with the PSTN. This is not covered in this document.
- Determine the IP addressing scheme and subnet configurations.

**2.** Trunk Gateway Traffic Engineering

- Size the PSTN trunk gateways
- Size the router at the trunk gateway site.

**3.** CS LAN Traffic Engineering and Configuration

- Size the Central Office equipment, capacity required in the CS2000, number of GWCs, and number of UASs.

**4.** Network Loss Planning.

**5.** Core Network Engineering.

- Specify the Quality-of-Service (QoS) objectives.
- Size the transport links interconnecting the Trunk Gateway sites, CS-LAN and core router based on the forecast amount of voice, signaling or OAM traffic.
- Verify signaling and voice transport latency objectives will be met.
- Identify the traffic control mechanisms that will be used to control congestion and assist in meeting QoS objectives.
- Consider centralized versus decentralized PVG15Ks

**6.** Size the network management platforms required.

**7.** Ensure appropriate equipment redundancy is in place to meet network reliability objectives.

**8.** Network Qualification

# 2.0 CS-LAN Common Components and Subnet Configuration

Succession Communication Server 2000 (CS2K) network elements require connectivity for Call Processing, OAM&P messaging and, optionally, bearer path. The Communication Server LAN (CS LAN) provides this connectivity as required for those elements that are co-located with the CS2000 complex. These different message flows are separated into the following subnets on the CS-LAN redundant routers:

- CallP - for Call Processing (or Call Signaling) traffic flows
- Bearer - for RTP bearer traffic flows
- MLT - intra-Passport 8600 traffic flows
- SP-OAM - Service Provider OAM traffic flows (Optional)
- OAM - for OAM&P traffic flows
- OOB - Out of Band OAM traffic flows

In addition to the above subnets, the following subnets are created in the CS LAN

- WAN - 2 subnets per PP8600 Chassis for connectivity to IP or ATM Backbone Network. This assumes a fully meshed connectivity between CS LAN and core network, see section 2.4.1.1 for more details.
- NOC-OSS - one (1) subnet per PP8600 Chassis for connectivity to Corporate Network

***Note:*** The subnets discussed in this document should be the only subnets created in the CS-LAN. In addition, only Succession network elements and OAM Clients should be connected directly to the CS LAN.

The devices that are configured in the Call Processing subnet are:

- XA-Core and/or cCS2K
- SAM21 (GWC and SC)
- SDM Call Processing interface
- SAM16 (UAS) Call Processing interface
- USP Call Processing interface
- USP-Compact

The devices that are configured in the Bearer subnet are:

- UAS
- PVGs/APGs
- IW-SPM

The devices that are configured in the OAM&P subnet are:

- CS2000 Management Tools
- SDM Management interfaces
- USP Management interfaces
- USP Manager
- Preside MDM server

The devices that are configured in the SP-OAM subnet are:

- OAM clients

***Note:*** Only OAM clients should be connected to the SP-OAM subnet

***Note:*** If security is a concern, then OAM Clients should be placed in the Corporate NOC which should be connected through its own router to the CS-LAN.“12.0 Security” on page 271

Further details on IP addressing requirements and element membership for these subnets are discussed later in this chapter and a summary table is provided in chapter “38.0 Appendix: IP Addressing and Port Setting Requirements Summary” on page 699

## 2.1 CS-LAN CallP, Bearer, MLT, and CorpNet Subnets

The CS-LAN contains several devices of fundamental importance. It is therefore essential to address these network elements correctly so that optimum connectivity and redundancy schemes are in place.

**Figure 2 Simplified CS-LAN**

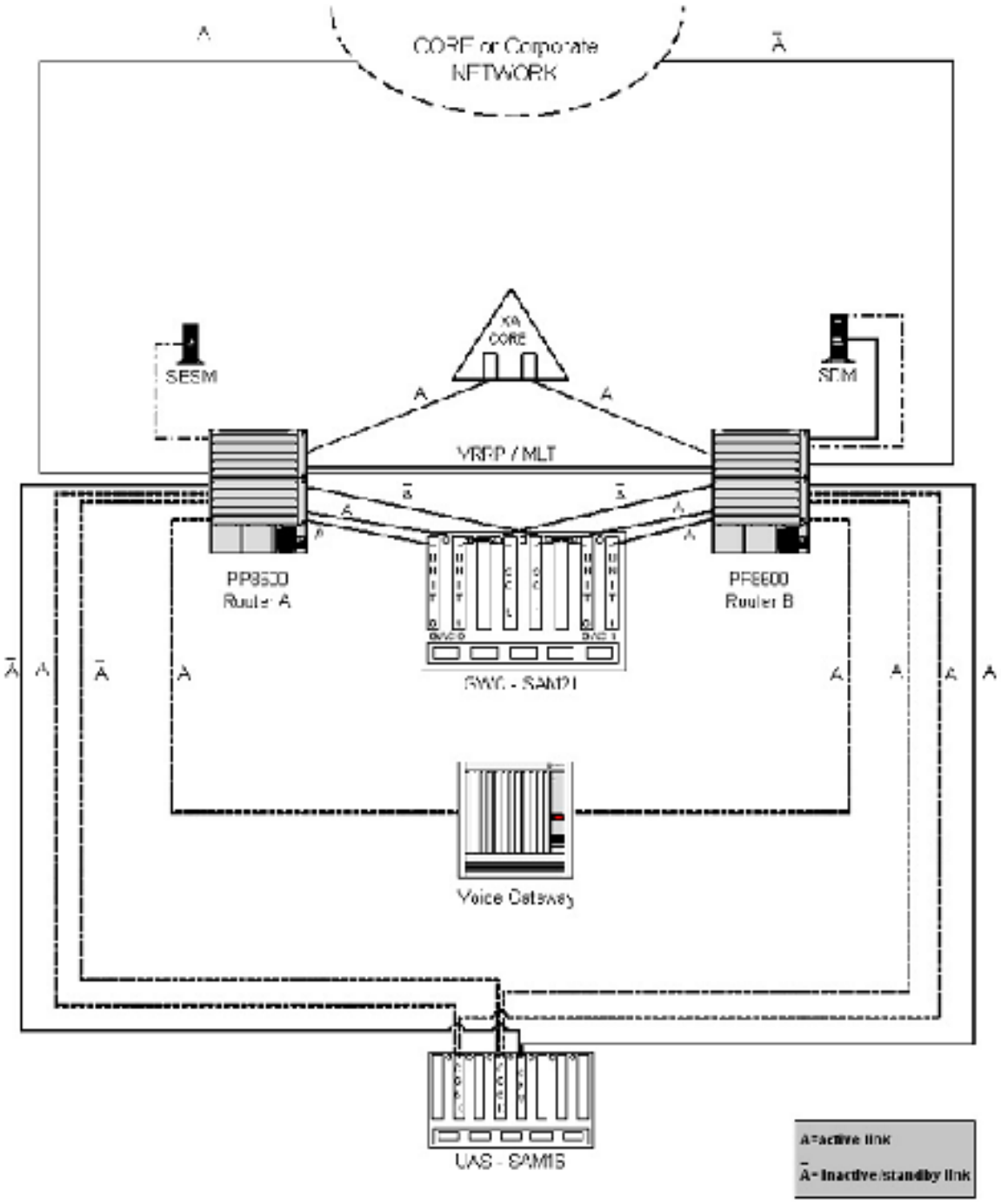
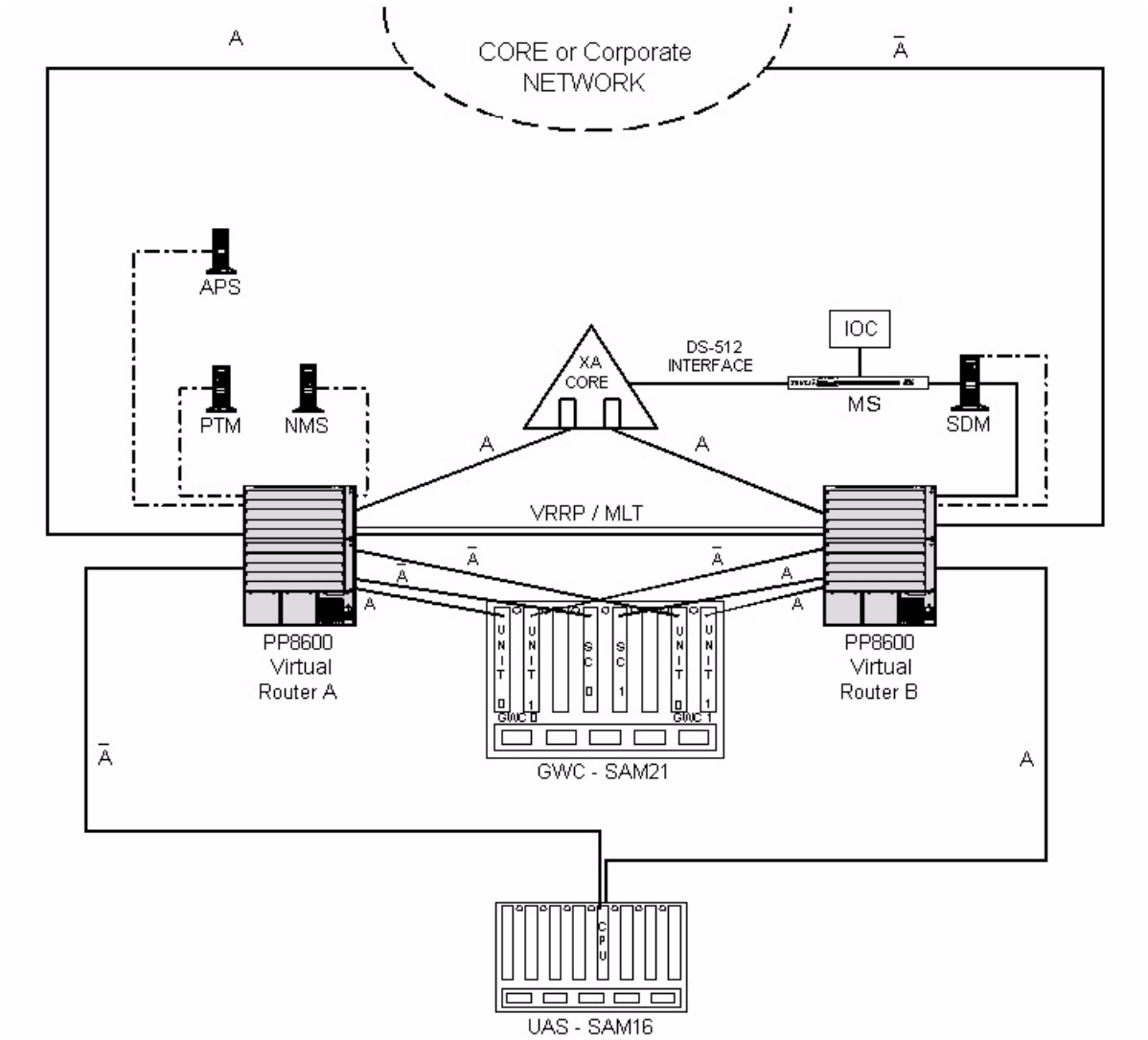


**Figure 3 Simplified CS-LAN**




## 2.1.1 Passport 8600

The central components of the CS-LAN are two (2) Passport 8600 10-slot NEBS chassis (Model Passport 8010co) which are provided for high reliability. The Passport 8600 Routing Switch is a modular product that offers Layer 2 switching along with wire-speed, IP-based Layer 3 switching functionality in a single chassis. The Passport 8600 has no single point of failure, all system components are hot swappable and redundant. For load sharing, the redundant Passport 8600s should be provisioned in dual-active mode (i.e. enable backup-master) versus active-standby mode. This will facilitate sharing the network traffic load across both devices instead of fully utilizing one and not utilizing the other one.

**Figure 4 CS-LAN Redundant Passport 8600 Configuration**

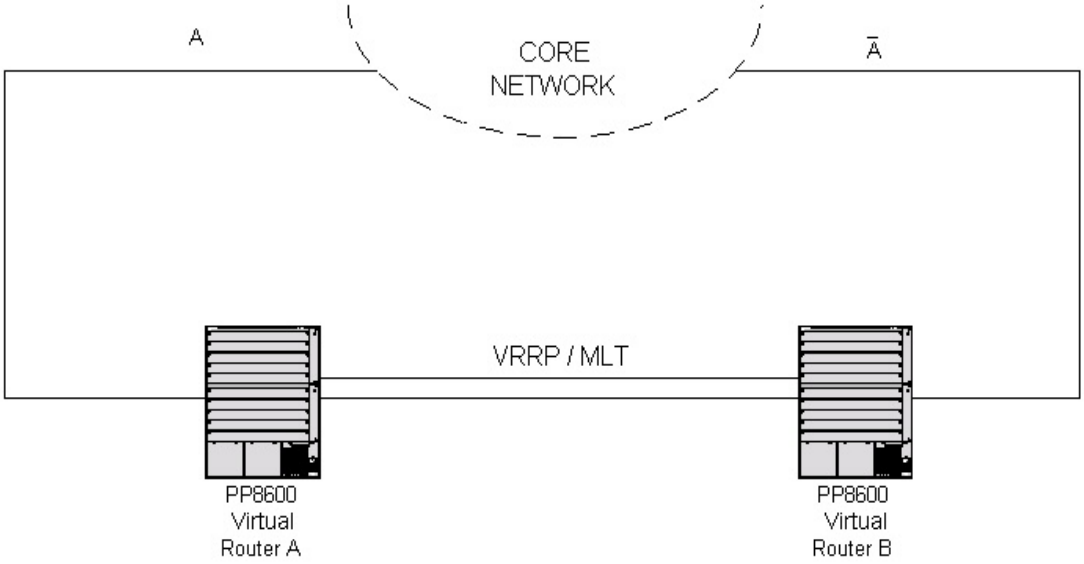
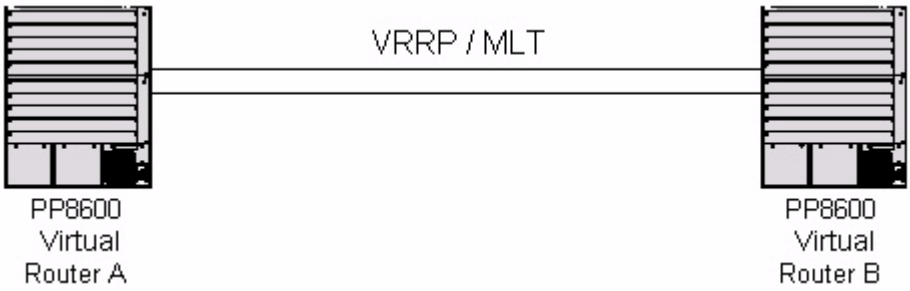



**Figure 5 CS-LAN Redundant Passport 8600 Configuration**




In Figure 5, the Passport 8600 configuration is shown. Currently, as a hardware baseline, each 8010co chassis must be configured with ONLY one (1) 8691SF/CPU module, along with a minimum of two (2) 8632TXE modules. See the Traffic Engineering Section for more details.

***Note:*** Dual 8691SF/CPU modules per 8010co chassis are not supported in SN06.2.

### 2.1.1.1 Software Configuration

Each Passport 8600 chassis should be running Release 3.2.2 (or later 3.x) software based on the Succession Release Management Load Line-up Matrix.

Once powered up, the Passport 8600, boots to a factory default configuration in which it operates as a Layer 2 only device. Therefore, in order to configure the 8600 to perform Layer 3 as well, some configuration modifications are required. For step-by-step Command Line Interface (CLI) instructions on basic Layer 3 functionality, refer to section “18.0 Appendix: Configuring the Passport 8600” on page 337

***Note:*** By default, it is a requirement to enable Spanning Tree Protocol (STP) on the box level and disable STP on all the Passport 8600 interfaces unless these guidelines explicitly state otherwise. (Since these are end devices, no forwarding loops are created.) For step-by-step instructions on disabling STP on the 8600 interfaces, refer to section “18.0 Appendix: Configuring the Passport 8600” on page 337. Failure to follow this guideline may result in a CallP outage since the GWC will stop communicating with the CS2K for 1.5 minutes whenever STP converges.

***Note:*** An issue exists on some of the Revision 5 of the TX-E modules where the Ethernet port may operate in a full duplex mode when configured in half duplex causing message loss. To verify the hardware version of the 8648TX-E module, the following command can be typed “show sys info card”. The Passport GNPS team can identify if a potential issue can exist based on the serial number of the card.

#### 2.1.1.2 CS-LAN IP Addresses - Common

Number of IP addresses used on the pair of Passport 8600s:

- one (1) per chassis for Management Interface [out-of-band (OOB) OAM Subnet]
- one (1) per chassis (physical) for each of configured VLANs [CS-LAN CallP, CS-LAN OAM, Bearer (RTP), intra-Passport 8600 (MLT)]
- one (1) for each VRRP logical IP address per VLAN pair [CS-LAN CallP, CS-LAN OAM, Bearer (RTP)]

Therefore, at least 13 IP addresses (OOB - 2, CALLP - 3, OAM - 3, Bearer - 3, MLT - 2) are required for the suggested configuration.

***Note:*** Since the Passport 8600 management interface is routable, it should be configured with an OOB IP address from a subnet that is not in the Passport 8600’s routing table.

#### 2.1.1.3 CS-LAN IP Addresses - Optional

As an option, for dedicated connectivity to the Service Provider OAM network, the IP addressing is slightly different. Additional VLANs (each of which will require two (2) IP addresses) might be needed to interconnect with the Service Provider OAM network.

***Note:*** For further details on configuring the Passport 8600, refer to the Passport 8600 documentation.

### 2.1.2 Call Server 2000 (XA-Core or CS2K)

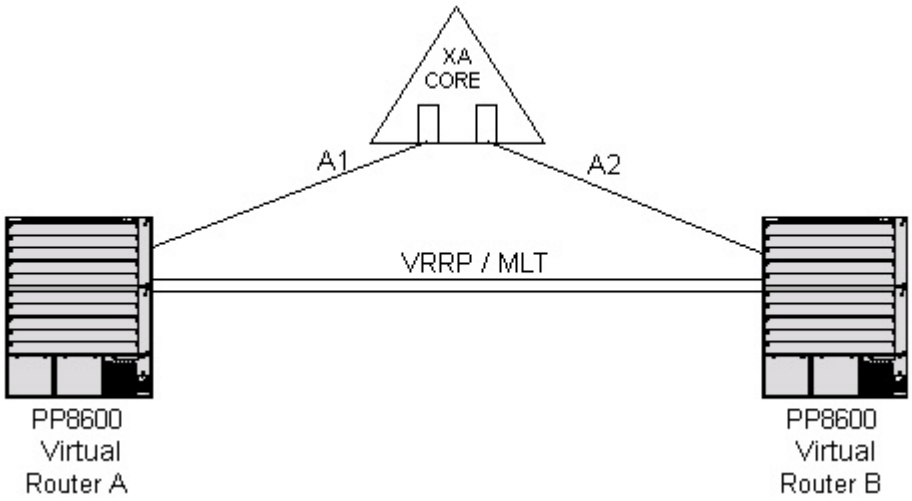
**EIOP/HIOP Heartbeat Guidelines**

Table CMIPADDR in the Core, has a field that is used by the HIOP/EIOP for heartbeat. This should be populated with the physical IP address of the CallP VLAN/subnet of its connected Passport 8600.

#### 2.1.2.1 High-Capacity Input/Output Processor (HIOP)

The recommended baseline for XA-Core is to configure it with two HIOPs. The HIOPs are the high capacity IOP cards designed to replace the EIOP cards. During normal operation, both HIOPs are active and operate in load-balancing mode.

**Figure 6 CS-LAN XA-Core with HIOPs**




The IP addresses required for the HIOPs are assigned on the CS-LAN Call Processing subnet as follows:

- two (2) floating addresses for the active interfaces
- one (1) address for the maintenance interface on each HIOP
- one (1) address for the physical interface on each HIOP

Number of IP addresses used on XA-Core:

- six (6) IP addresses are used for the HIOPs.

XA-Core will use one (1) port per Passport 8600.

**Example of table CMIPADDR:**

```
GATEWAY 0 GW (172 16 0 1) 0
CMHOST 0 HOST (172 16 14 108) 20 0
CMHOST 1 HOST (172 16 14 109) 20 0
ETHRLNK 1 ETHR 12 REAR NONE (172 16 14 104) 20 (172 16 14 110) 20 (172 16 0 2)   0
ETHRLNK 2 ETHR 6 REAR NONE (172 16 14 106) 20 (172 16 14 112) 20 (172 16 0 3)   0
```

***Note:*** The last Etherlink IP address (i.e. 172.16.0.2 and 172.16.0.3) MUST be set to the physical IP address of the CallP VLAN/subnet on the Passport 8600 that each HIOP subtends.

***Note:*** In order for the HIOP units to communicate reliably, auto-negotiation MUST be enabled on ports of the remote end device (Passport 8600) to which they are connected. This will cause both ends to automatically negotiate to 100 BaseT full duplex.

***Note:*** Disable Spanning Tree Protocol on each of the Passport 8600 ports to which the HIOP units are connected. (Since these are end devices, no loops will be created.) For more details on configuring STP on the Passport 8600 refer to section “18.0 Appendix: Configuring the Passport 8600” on page 337.

### 2.1.2.2 EIOP

This is an optional solution to the HIOP solution described above that is only supported for existing sites upgrading to SN06, however, new sites MUST use the HIOP baseline.

XA-Core has four (4) Ethernet I/O Packlet (EIOP) cards. Each Ethernet packlet has a single Ethernet connection. A minimum of two (2) units is required with two (2) standby units.

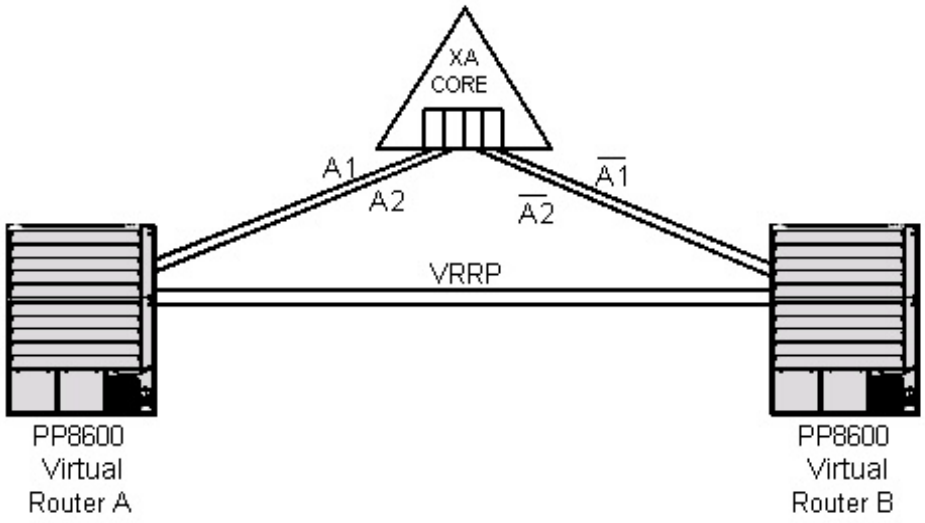
Of the four (4) EIOP packlets, two EIOP units are active and the other two (considered for redundancy) are inactive. In the event the active link/unit fails the software will switch the IP address over to a standby EIOP and make it active.

For connectivity to the CS-LAN CallP subnet, each active/inactive pair of EIOP devices should be split across each Passport 8600.

***Note:*** In order for the EIOP units to communicate reliably, auto-negotiation MUST be enabled on ports of the remote end device (Passport 8600) to which they are connected. This will cause both ends to automatically negotiate to 100 BaseT full duplex.

***Note:*** Disable Spanning Tree Protocol on each of the Passport 8600 ports to which the EIOP units are connected. (Since these are end devices, no loops will be created.) For more details on configuring STP on the Passport 8600 refer to section “18.0 Appendix: Configuring the Passport 8600” on page 337.

**Figure 7 CS-LAN XA-Core with EIOPs**




In Figure 7, the connectivity from XA-Core to the redundant Passport 8600s is shown. Four EIOPs are required and will interconnect with the Passport 8600 via 100 BaseT full duplex links (see note above on auto-negotiation) During normal operation, there are two active EIOPs and two inactive (for sparing).

The IP addresses required for the EIOPs are assigned on the CS-LAN CallP subnet as follows:

- 2 floating addresses for the active interfaces

- 1 address for the maintenance interface on each EIOP
- 1 address for the physical interface on each EIOP

Number of IP addresses used on XA-Core:

- 10 for the EIOPs.

XA-Core will use two (2) ports per Passport 8600.

### 2.1.3 Compact CS2K

The Compact CS2K (cCS2K) solution meets new demands for a smaller foot print, easy commissioning and maintainability, lower cost product that supports the same feature set as the full size CS2000 and scales easily. It incorporates the functionality of CS2K into the Call Agent cards. Compact CS2K is comprised of a Storm blade for NFS access to a dot bill disk array, a cCS2K processor blade, and a USP-Compact blade (or full USP depending on the SS7 requirements).

The minimum configuration of a cCS2K is comprised of two SAM21 chassis, and can house up to 14 pairs of GWCs in a split shelf configuration across the two SAM21 chassis. Beginning with the SN06 release, all new cCS2K installation must have all GWCs configured in a split shelf configuration. For more details on GWC split shelf configuration refer to Section 2.1.4.3

Ten IP addresses on the CS-LAN CallP subnet are required. The last octet of the active call processing IP address must be divisible by 8. An example of the IP address assignment is as follows:

**Table 2 Compact CS2K IP Addressing Example**

| Internal Name | IP Address | Description |
|---|---|---|
| localptp | 192.168.1.1 | |
| localport0 | 172.16.15.9 | Physical Passport 8600-0 |
| localport1 | 172.16.15.10 | Physical Passport 8600-1 |
| localblade | 172.16.15.11 | |
| activeirm | 172.16.15.16 | Logical Active |
| inactiveirm | 172.16.15.15 | Logical Inactive |
| mateptp | 192.168.1.2 | |
| mateport0 | 172.16.15.12 | Physical Passport 8600-0 |
| mateport1 | 172.16.15.13 | Physical Passport 8600-1 |
| mateblade | 172.16.15.14 | |

***Note:*** The IP addresses for localptp and mateptp have to be datafilled for internal purposes, but they are not visible externally.

Table IPNETWRK --- Provision the active IRM IP address. (This replaces table CMIPADDR used for HIOPs).

KEYREF CMIPADDR SUBNET OPTION PARMAREA

0 **172 16 15 16** 5 $(SCRNFLAG N) $

***Note:*** Due to a code design requirement, the IP subnet used for the block of 10 IP addresses must meet certain rules, see section “2.1.3.1 IPNETWRK Subnet restrictions” for a summary of these restrictions. Reference the Compact CS2K documentation for more information.

***Note:*** In order for the cCS2K cards to communicate reliably, auto-negotiation MUST be enabled on ports of the remote end device (Passport 8600) to which they are connected. This will cause both ends to automatically negotiate to 100 BaseT full duplex.

***Note:*** Disable Spanning Tree Protocol on each of the Passport 8600 ports to which the cCS2K cards are connected. (Since these are end devices, no loops will be created.) For more details on configuring STP on the Passport 8600 refer to section “18.0 Appendix: Configuring the Passport 8600” on page 337.

### 2.1.3.1 IPNETWRK Subnet restrictions

The following rules must be met for a subnet and an IP address from the subnet to be usable for CMIPADDR field in table IPNETWRK:

- Subnet bits cannot be 0
- Host bits overlapping the subnet bits can not be all 1's or all 0's - As can be seen from the example below, you always have to have at least two subnet bits, for the subnet to be usable
- IP address assigned to CMIPADDR (i.e. IRM active address) must be divisible by 8

**Example:**

This is just an example and does not imply that only a class C address wil work. To the contrary, it is much easier to meet the restrictions with a class A or B subnet.

With a class C and a /24 subnet: [nnnn nnnn] [nnnn nnnn] [nnnn nnnn] [hhhh hhhh] - subnet bit is 0, therefore subnet can not be used.

With a class C and a /25 subnet: [nnnn nnnn] [nnnn nnnn] [nnnn nnnn] [shhh hhhh] - subnet bit is 1, however, any IP address you pick will fail the 2nd test, since ther is only 1 subnet bit to overlap, so it always be overlapped with either 1 or 0.

With a class C and a /26 subnet: [nnnn nnnn] [nnnn nnnn] [nnnn nnnn] [sshh hhhh] - subnet bits is 11, now one can use addresses in the range of 64 -191 for host address. This range ensures the overlapping subnet bits are either 01 or 10

**Workaround:**

These restrictions apply only to the SOS application. Since SOS does not make any routing decisions and relies on the 3PC Linux OS for all routing decisions, one can apply the restriction when assigning the IP address to CMIPADDR field in table IPNETWRK, but then use a /25 or /24 subnet evrywhere else, as long as the larger subnet encompasses the smaller subnet used in table IPNETWRK.

### 2.1.3.2 CS2Kc Storage Manager (STORM)

STORM provides a highly reliable storage solution for applications running in the SAM21 shelf, such as the 3PC application. CS2Kc platform utilizes a couple of different hardware platforms for the STORM application.

#### 2.1.3.2.1 Storm-DotHill

In this configuration, 2 MCPN750 cards (STORM blades) and a DotHill 7128 storage box are deployed.

Each of the STORM blades requires an IP address from the CallP subnet, these IP addresses are referred to as STORM0 and STORM1 IP addresses.

For connectivity to the CS-LAN CallP subnet, one STORM blade should be connected to one Passport 8600, while the other STORM blade should be connected to the other PP8600.

***Note:*** In order for the STORM blades to communicate reliably, auto-negotiation MUST be enabled on ports of the remote end device (Passport 8600) to which they are connected. This will cause both ends to automatically negotiate to 100 BaseT full duplex.

***Note:*** Disable Spanning Tree Protocol on each of the Passport 8600 ports to which the STORM Blades are connected. (Since these are end devices, no loops will be created.) For more details on configuring STP on the Passport 8600 refer to section “18.0 Appendix: Configuring the Passport 8600” on page 337.

#### 2.1.3.2.2 SAM-XTS

In this configuration, 2 SAM-XTS Linux based boxes are deployed in an active/active configuration. Each SAM-XTS box has 4 10/100/1000 ethernet interfaces, labeled as ports A,B,1 and 2.

The 2 SAM-XTS boxes are interconnected using interfaces A and 2 on each box. The other ports, B and 1, are used for connectivity to the Passport 8600s. Each box requires an IP address from the CallP subnet.

The SAM-XTS boxes are configured with an MLT on the 2 ports connected to the Passport 8600s.

#### 2.1.3.2.3 Split Multi-Link Trunking (SMLT)

For optimal reliability of the connectivity between the PP8600s and the SAM-XTS’, a Split Multi-Link Trunking (SMLT) is configured on each PP8600 for each SAM-XTS box. This configuration ensures availability of both logical drive partitions in case of one PP8600 fails.

***Note:*** Configuring SMLT requires that IST be enabled on the MLT interconnecting the two (2) PP8600s. See section 2.5.1.2.1 for IST details

The following rules must be used in creating the SMLTs:

- Two (2) SMLTs (one SMLT per SAM-XTS box) need to be created on each of the two PP8600s and added to the CallP VLAN.
- The same SMLT ID must be used on both PP8600s for each SMLT.
- To provide optimal redundancy, each SAM-XTS box should have one of its network interfaces connected to each CS-LAN Passport 8600.

It is recommended that cp-limit and broadcast and multicast rate-limit be enabled and set to 1000

on the SMLT ports to safeguard against undesirable network loops created by hardware failure on the SAM-XTS boxes.

***Note:*** In order for the SAM-XTS' to communicate reliably, auto-negotiation MUST be enabled on ports of the remote end device (Passport 8600) to which they are connected. This will cause both ends to automatically negotiate to 100 BaseT full duplex.

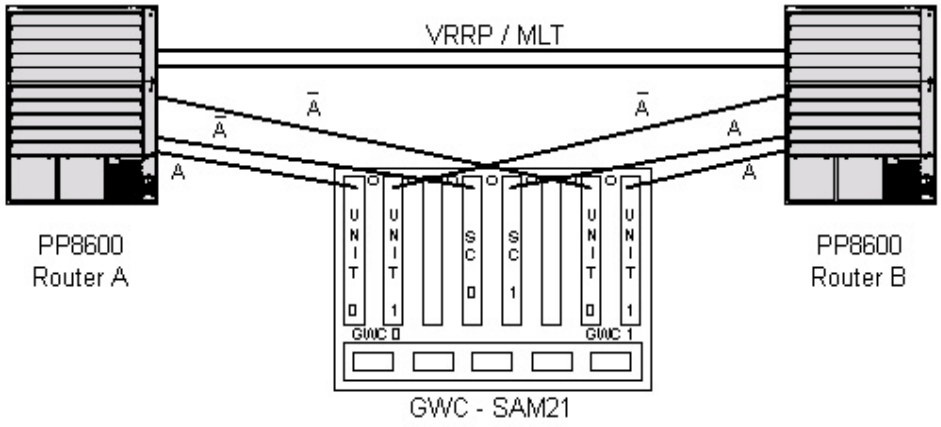
***Note:*** Disable Spanning Tree Protocol on each of the Passport 8600 ports that are in the STORM SMLTs. For more details on configuring STP on the Passport 8600 refer to section "18.0 Appendix: Configuring the Passport 8600" on page 337.

### 2.1.4 Gateway Controllers and the SAM21 Shelf

The SAM21 hardware platform consists of a 21-slot chassis with at least two instances of critical field replaceable units in order to provide redundancy (99.999%) in the case of a failure.

Figure 8 shows the connectivity between a SAM21 shelf (which contains the GWC cards and the SC cards) and the redundant Passport 8600s. Each SAM21 can have up to sixteen (16) GWC units and up to two (2) Shelf Controllers (SC).

**Figure 8 CS-LAN SAM21 with Two Gateway Controller Pairs and One Shelf Controller Pair**




Number of IP addresses used on one SAM21:

- four (4) per SC pair (refer to Section 2.1.4.1)
- four (4) per GWC pair (refer to Section 2.1.4.2)

A fully configured SAM21 will need 36 IP addresses (4 x 8 + 4 x 1), and will require nine (9) ports per redundant Passport 8600.

***Note:*** Disable Spanning Tree Protocol on each of the Passport 8600 ports to which the GWC and SC units are connected in order to prevent unstable CallP recovery during certain failover conditions. (Since these are end devices, no loops will be created.) For more details on STP for the Passport 8600, refer to section"18.0 Appendix: Configuring the Passport 8600" on page 337.

### 2.1.4.1 SAM21 Shelf Controllers

The Shelf Controller (SC) cards are running in an active/warm standby mode. To connect the shelf controllers into the CS-LAN CallP subnet, each one should be connected to a different 10/100 BaseT I/O port module residing in separate Passport 8600 chassis.

Each SC pair is composed of two units (one is active and one is inactive) and needs four (4) consecutive IP addresses, assigned as follows:

- one (1) address for the active interface
- one (1) address for the inactive interface
- one (1) address for the physical interface of unit 0
- one (1) address for the physical interface of unit 1

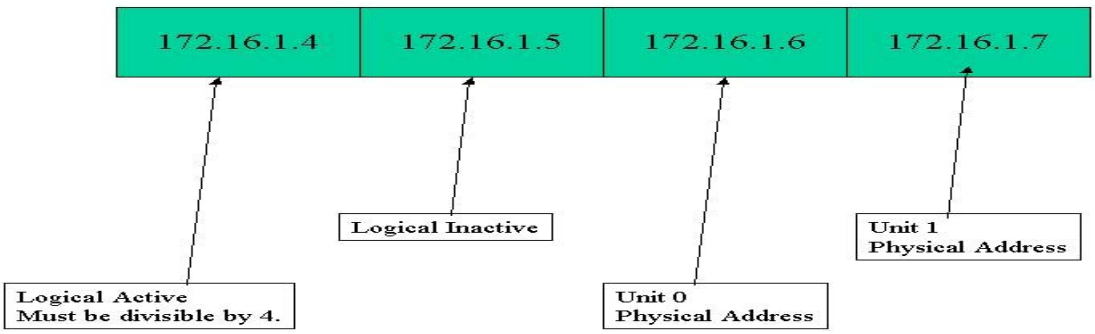
***Note:*** The last byte of the IP address for the active interface must be a number divisible by four (4) due to a code design requirement. Additionally, the SCs must be in the same subnet as the GWCs.

Number of IP addresses used on one SAM21:

- four (4) per SC pair

***Note:*** The SC units ports must be configured at the CS-LAN routers as auto-negotiate Enable and STP must be disabled. This will cause both ends of the connections to automatically negotiate to 100 BaseT Full duplex.

**Figure 9 SAM21 Shelf Controller IP Address Example**




### 2.1.4.2 Gateway Controllers

The remaining slots in the chassis will be populated with intelligent CPU boards. The first of these intelligent boards is a Gateway Controller that provides the call processing functionality.

Pairs of GWCs are deployed in a 1+1 active/inactive redundancy arrangement. Both units should be deployed in the same shelf, but can also function across shelves (refer to Section 2.1.4.3). Both units must be deployed in the same shelf.

Each GWC card has only one (1) network interface (NI). Each unit's NI should be connected to a different 10/100 BaseT I/O port module residing in separate Passport 8600 chassis on the CS-LAN CallP subnet.

Similar to the SC configuration, each GWC pair is composed of two units (one is active and one is inactive) and needs four (4) consecutive IP addresses, assigned as followed:

- one (1) address for the active interface
- one (1) address for the inactive interface
- one (1) address for the physical interface of unit 0
- one (1) address for the physical interface of unit 1

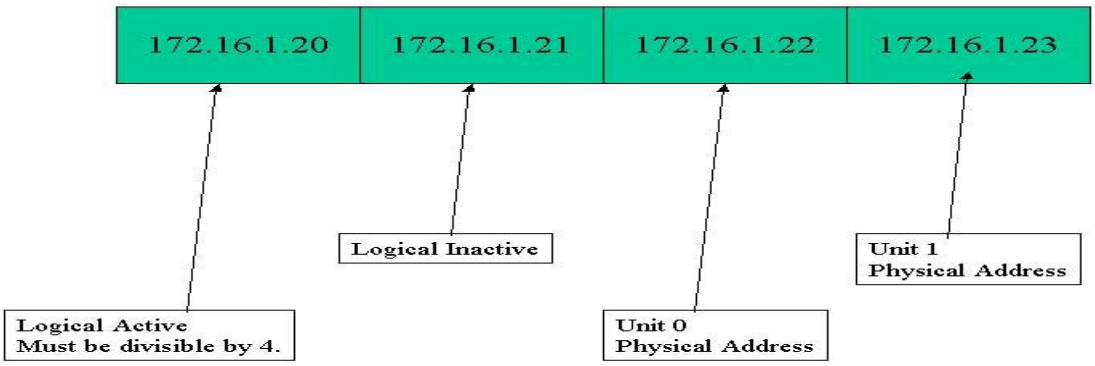
***Note:*** The last byte of the IP address for the active interface must be a number divisible by four (4) due to a code design requirement. Additionally, the GWCs must be in the same subnet as the SCs.

Number of IP addresses used on one SAM21:

- four (4) per GWC pair

***Note:*** The GWC units ports must be configured at the CS-LAN routers as auto-negotiate Enable and STP must be disabled. This will cause both ends of the connections to automatically negotiate to 100 BaseT Half duplex.

**Figure 10 SAM21 Gateway Controller IP Address Example**

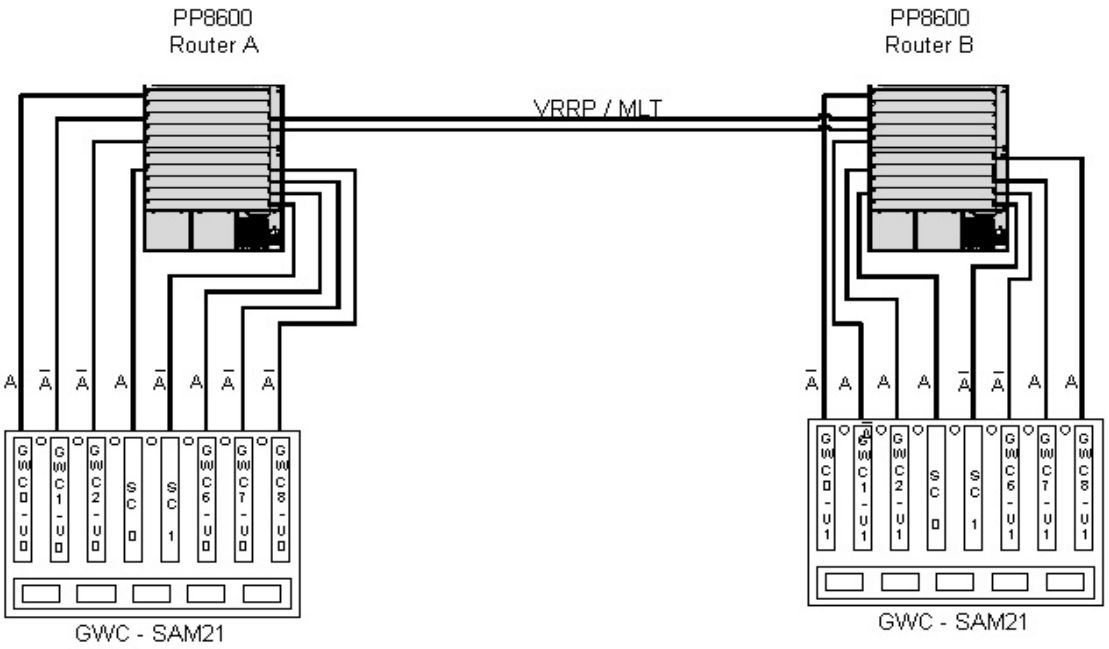



### 2.1.4.3 Gateway Controllers Split-shelf Configuration

Figure 11 shows the connectivity between 2 SAM21 shelves (which contain the GWC cards and the SC cards) and the redundant Passport 8600s.

Pairs of GWCs are deployed in a 1+1 active/inactive redundancy arrangement. Each unit is deployed in a different shelf and each unit's NI should be connected to a different 10/100 BaseT I/O port module residing in separate Passport 8600 chassis on the CS-LAN CallP subnet. This configuration offers additional protection against shelf failure.

**Figure 11 CS-LAN Gateway Controller Split Shelf Configuration**




This configuration does not affect the total number of Shelf Controllers and Gateway Controller pairs supported on the two shelves, or the number of IP addresses required for the Shelf controllers and Gateway Controller pairs.

So two fully configured Sam21 shelves will support sixteen (16) GWC pairs and two (2) SC pairs, require 72 IP addresses (4x16 + 4x2), and will require 18 ports per redundant Passport 8600.

It is important to note that the operational status of one GWC unit in a shelf is independent of the status of other GWC units in the same shelf.

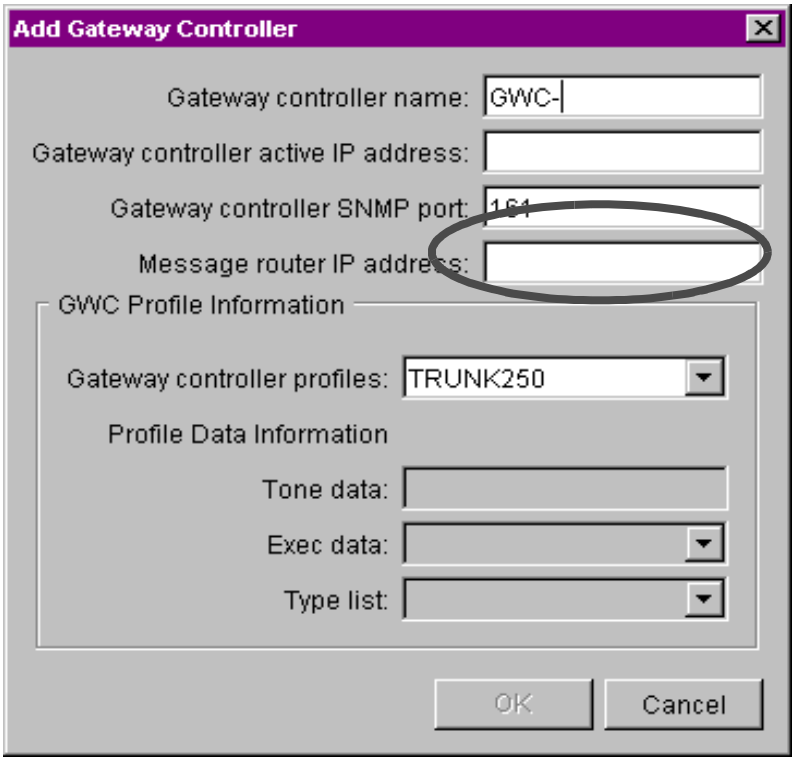
***Note:*** The pair of SCs in a shelf are configured to control the one shelf they are deployed in and are not affected by the split shelf configuration of GWCs.

***Note:*** The GWC units ports must be configured at the CS-LAN routers as auto-negotiate Enable and STP must be disabled. This will cause both ends of the connections to automatically negotiate to 100 BaseT Half duplex

### 2.1.4.4 Distributing Gateway Controllers across CS2K and Compact CS2K

When provisioning the Gateway Controllers from within the CMT (Gateway Controller Element Manager), ensure that there is an equitable balance of Gateway Controllers across the IP addresses assigned to the CS2K. This is the "*Message router IP address*" field shown in the following figure. This helps to balance the messaging traffic across the links during normal traffic conditions.

**Figure 12 Provisioning a Gateway Controller**




### 2.1.5 Inter-working SPM (not applicable to Compact CS2K solutions)

The primary role of IP Inter-working SPM (IW-SPM) is to transcode voice between the traditional PSTN network and the IP network. IP IW-SPM is an ENET-hosted SPM which has four C-side DS512 links connecting the CEM to the ENET.

The Gigabit Ethernet Module (GEM) is a new Spectrum RM which is currently being developed to provide Voice over IP (VoIP) capability for the Spectrum Platform. Each IP RM supports 2016 DS0-to-IP channels and a Gigabit Ethernet interface, which is physically connected to the CS-LAN Passport 8600.

Two GEMs are configured in the same protection group to support 1+1 protection switching in the event of failures, and they must be seated in the adjacent high-speed slots in lower shelf of the SPM frame. Also, no circuit packs should be put directly on top of the GEMs in the upper shelf for the thermal considerations.

The IP address assignments on the CS-LAN are as follows:

- One IP address on GEM 0 for management purposes (activated when the card is inactive).
- One IP address on GEM 1 for management purposes (activated when the card is inactive)
- One IP address on the Bearer (RTP) subnet for the VoIP interface (this address must be the same for both GEM cards in the 1+1 protection switching) that carries the bearer.

***Note:*** In order for the GEM cards to communicate reliably, auto-negotiation MUST be enabled on ports of the remote end device (Passport 8600) to which they are connected. (Since these are L3

routable interfaces, no loops will be created.) This will cause both ends to automatically negotiate to 1-Gbps full duplex.

***Note:*** Disable Spanning Tree Protocol on each of the Passport 8600 ports to which the GEM cards are connected. For more details on configuring STP on the Passport 8600 refer to section “18.0 Appendix: Configuring the Passport 8600” on page 337.

***Note:*** In order for the GEM cards to communicate with all Succession devices outside the CS-LAN, they must be connected to a pair of Layer 3 switches. Connectivity to routers is **not** supported because the GEM cards behave like a standard Ethernet-based host.

### 2.1.6 Universal Signaling Point (USP)

The Universal Signaling Point (USP) provides the CS2K IP network an interface to the Signaling System Number 7 (SS7) network. Each signaling interface handles all the SS7 functions that must be carried out on a per-message basis. Examples include Message Transfer Part (MTP), Signaling Connection Control Part (SCCP) routing, Global Title Translation (GTT) and Gateway.

The USP is composed of the following principle System Nodes:

- RTC System Node - One IP Link per node, up to two nodes per USP
- M3UA IP Link System Node - one IP Link per node, up to six nodes per USP
- CC System Node - One node per USP, no connectivity required.
- SS7 V.35 Link System Node - Four SS7 signaling links per card
- SS7 DS0A Link System Node - Four SS7 signaling links per card
- SS7 Channelized T1/E1 Links - Eight SS7 signaling link channels per card

The SS7 Link System Nodes (V.35, DS0A and Channelized T1/E1) provide the interface to the SS7 network, while the M3UA IP Link System Node provides the interface to the IP network (CS-LAN).

The IP address assignments on the CS-LAN are as follows:

- RTC System Node - One for each node for a total of two (2) IP addresses on the **OAM&P subnet**.
- IP Link System Node - One for each node in the system not to exceed a total of six (6) IP addresses[1] on the **CallP subnet**. See the Traffic Engineering section for guidelines on determining the number of required IP Link Gateway nodes.

A fully configured USP will use a maximum of eight (8) IP addresses and 16 ports on both Passport 8600s.

***Note:*** In order for the USP nodes to communicate reliably, auto-negotiation MUST be enabled on ports of the remote end device (Passport 8600) to which they are connected. This will cause both ends to automatically negotiate to 100 BaseT Full duplex.

***Note:*** Disable Spanning Tree Protocol on each of the Passport 8600 ports to which the USP nodes are connected. (Since these are end devices, no loops will be created.) For more details on

1. The maximum number of M3UA IP links is four (4) in SN04.

configuring STP on the Passport 8600 refer to section “18.0 Appendix: Configuring the Passport 8600” on page 337.

#### 2.1.6.1 Dual Application Server Process Paths

The USP uses Application Server Process (ASP) Paths to monitor connectivity between the SS7 IP link card and an Application Server Process, which, in the case of UA-AAL1, is the XA-Core. When connectivity between all IP link cards and their corresponding ASPs is lost, SS7 “routesets” are taken out of service.

To increase reliability and survivability in the presence of IP network failures, the USP should be provisioned with dual ASP Paths for each IP Link card. The Application Server Process IP addresses used in the paths should be the CMHOST addresses provisioned in the XA-Core table CMIPADDR. The ASP Paths are provisioned via the USP OAM GUI. Figure 13 shows an example USP OAM GUI screen after provisioning of dual ASP Paths.

In addition to the ASP path provisioning at the USP OAM GUI, the paths must be opened at the XA-Core using the M3UA Path Setup Tool (M3UATOOL). Figure 14 shows the XA-Core path provisioning that corresponds to the USP OAM GUI path provisioning from Figure 13

**Figure 13 Dual Application Server Process Path Provisioning**

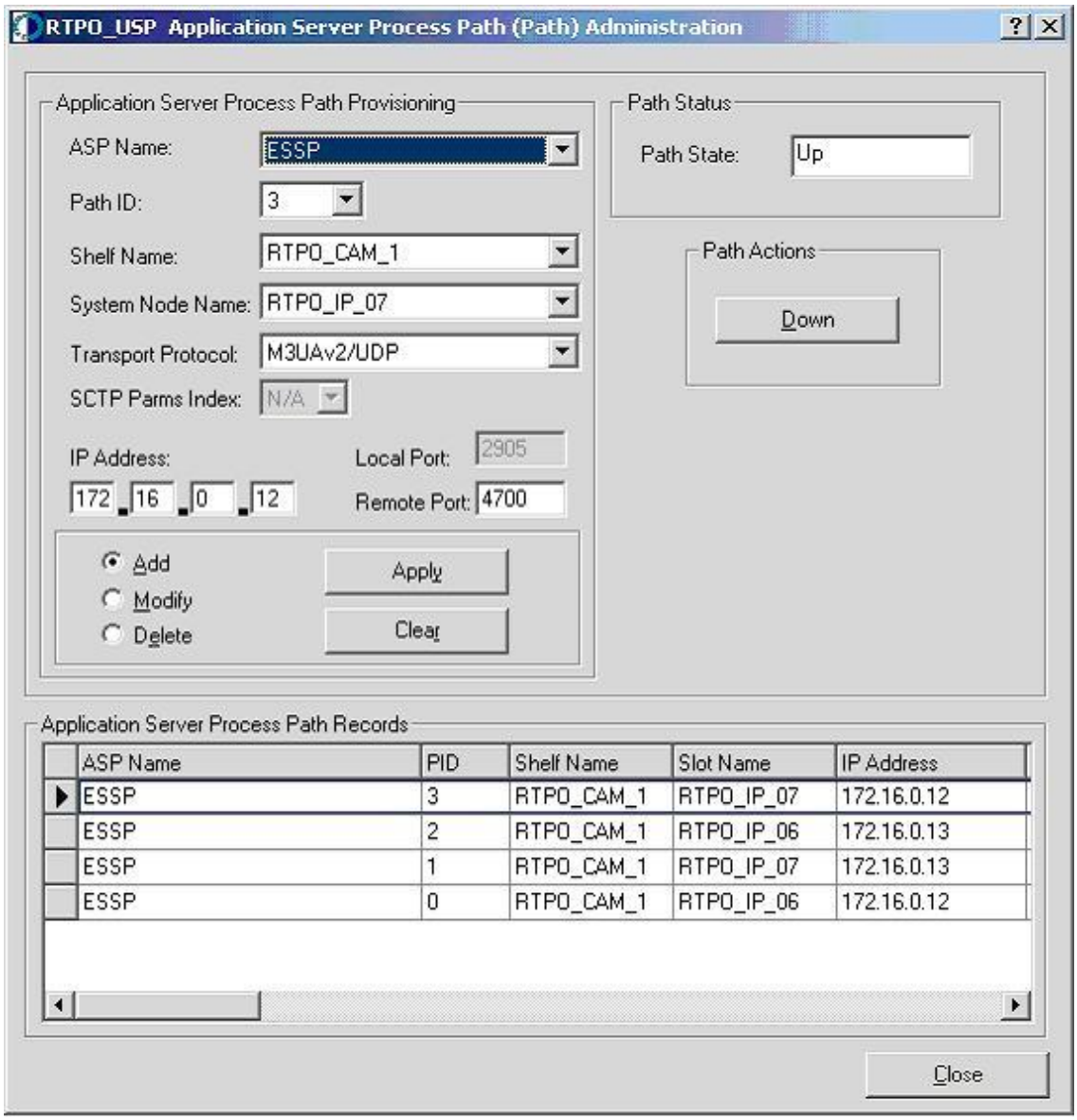
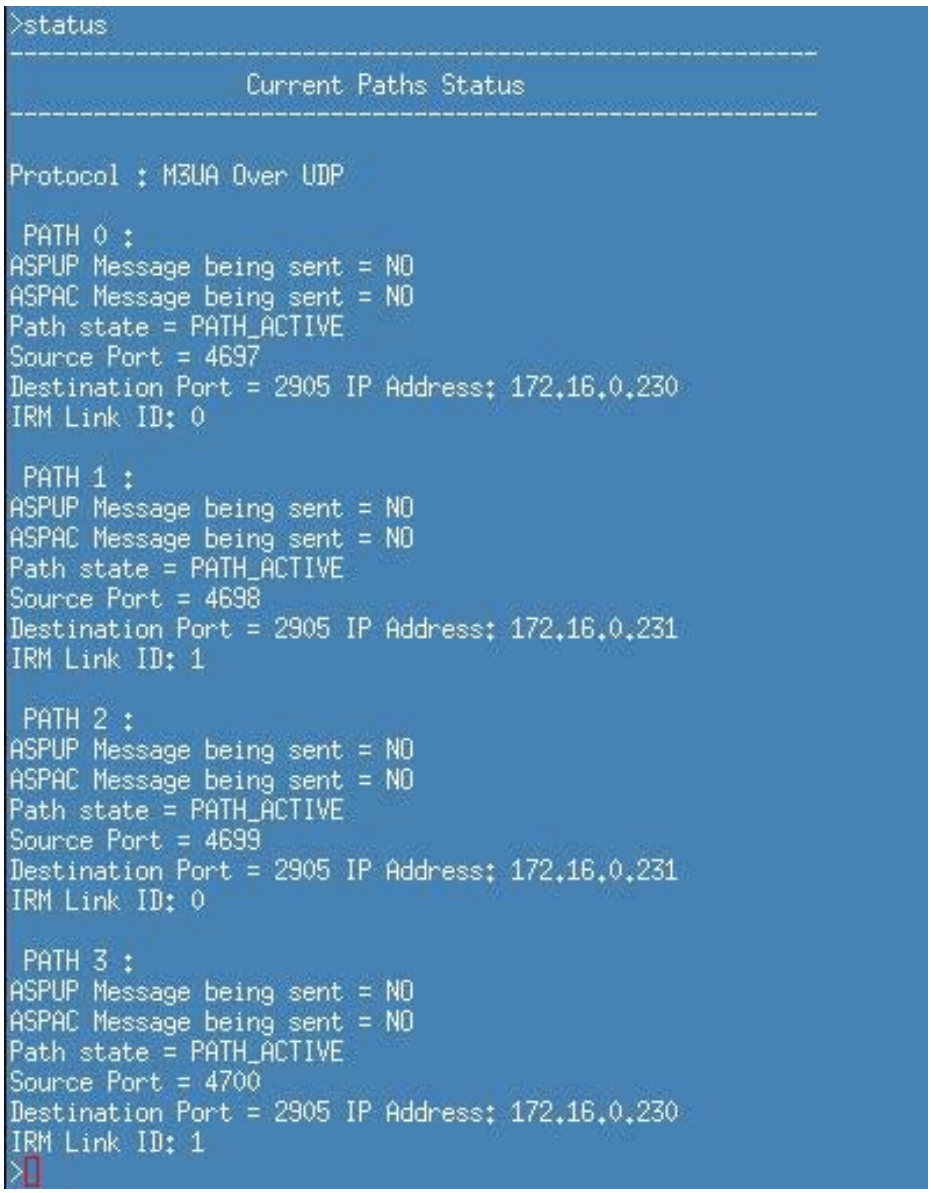


**Figure 14 M3UA Path Provisioning**




### 2.1.7 Universal Signaling Point Compact (USP-Compact)

Depending on the SS7 requirements, the USP-Compact (instead of the full USP) may be used in the Compact CS2K configuration only to provide the signalling gateway function. The USP compact is based on a Motorola cPCI blade and is installed in the Compact Call Controller shelves in the SAM21 chassis.

***Note:*** For more information, refer to the USP-Compact documentation.

For reliability, two USP-Compact blades should be provisioned. When the USP-Compact blades are provisioned with the SAM21 EM, the USP-Compact blades must be supplied four (4) consecutive IP addresses on the CallP subnet. It is a requirement that the provisioned IP addresses be different by two (2). That is, the first address be divisible by four (4), and the other blade's address be two (2) greater, for example, 192.168.1.132 for the first blade, and 192.168.1.134 by the second blade. The total IP address range requirement would then be 192.168.1.132 - 192.168.1.135.

***Note:*** In order for the USP-Compact cards to communicate reliably, auto-negotiation MUST be disabled on ports of the remote end device (Passport 8600) to which they are connected. The administrative status should be set to 100 BaseT half duplex.

***Note:*** Disable Spanning Tree Protocol on each of the Passport 8600 ports to which the USP-Compact cards are connected. (Since these are end devices, no loops will be created.) For more details on configuring STP on the Passport 8600 refer to section "18.0 Appendix: Configuring the Passport 8600" on page 337.

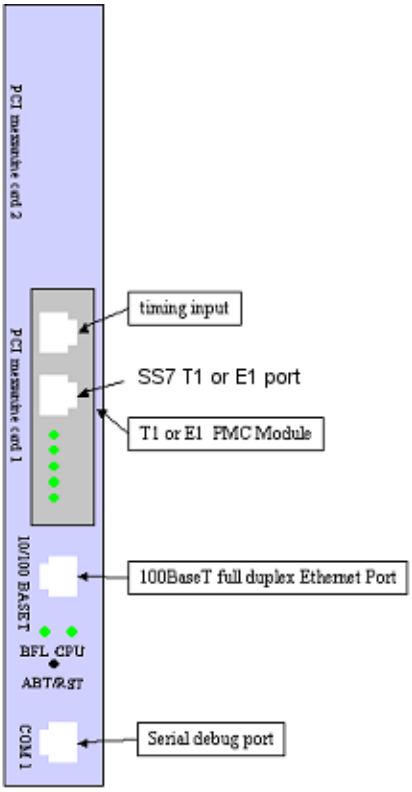
#### 2.1.7.1 Signaling Link Support

USP Compact supports a maximum of 16 links and linksets on 2 USP Compact blades and supports both channelized T1/E1 SS7 links and IPS7 connections.

For the SS7 Channelized T1/E1 Link, the (I)SN06 baseline hardware supports 8 channels per card, while the older hardware supports 4 channels per card.

USP Compact will not support m2pa IP High speed SS7 links, ATM based High speed SS7 links, DS0a SS7 links, or V-35 SS7 links.

**Figure 15 USP Compact Blade**




## 2.1.8 Universal Audio Servers

The Universal Audio Server (UAS) is built on the SAM16 platform. The UAS is engineered in an N+1 domain configuration, where “N” is the engineered number of UAS domains plus one (1) spare domain. The spare domain is an active spare, meaning it is processing calls but is not considered in engineering the office.

**Figure 16 CS-LAN Redundant SAM16 Universal Audio Servers**

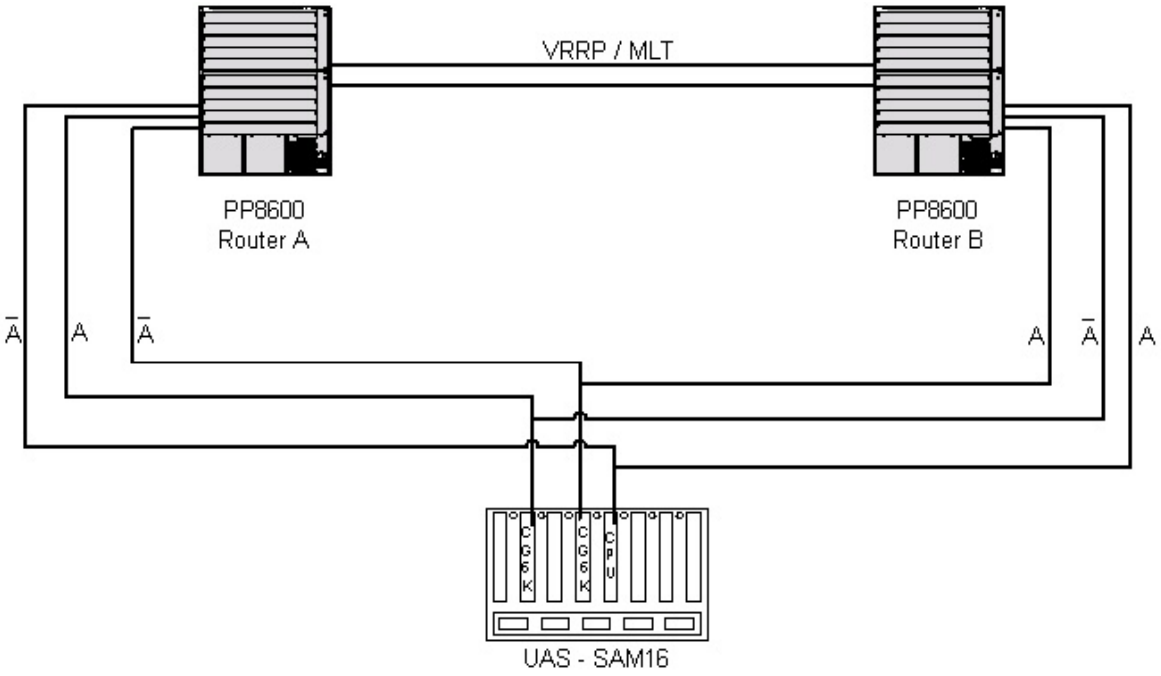
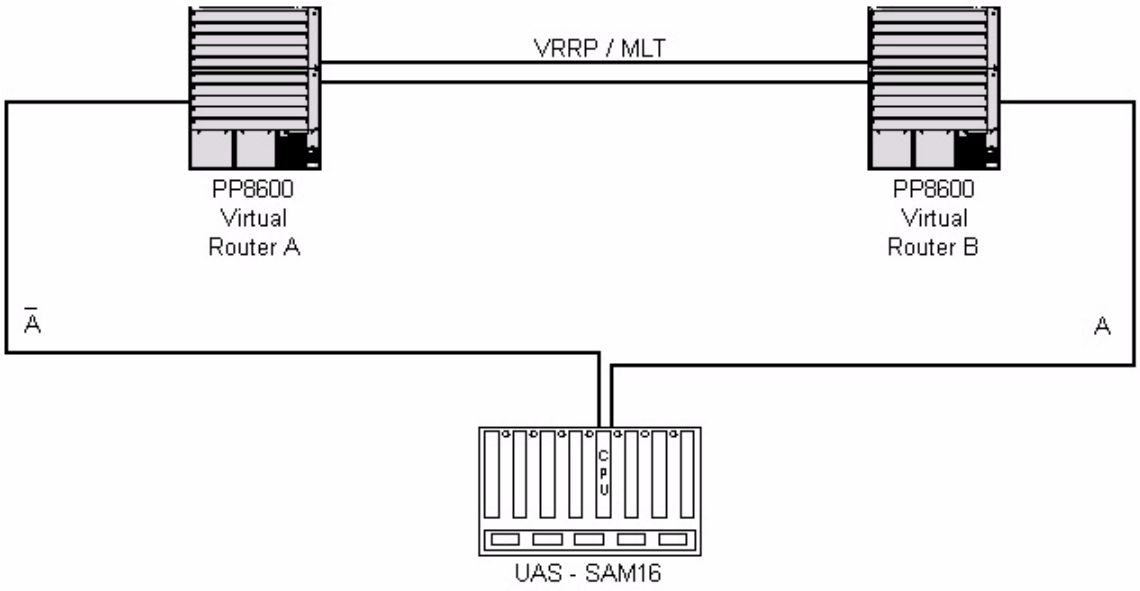



**Figure 17 CS-LAN Redundant SAM16 Universal Audio Servers**




The host interface is provided through dual 100 BaseT full duplex network interfaces on the system controller (or CPU) card and is configured in an active/standby mode with one (1) IP address on the CallP subnet.

Each CG6K card provides dual 100 BaseT full duplex network interfaces, which are both configured in Ethernet redundancy mode for receiving and transmitting audio. Each of the Ethernet interfaces on the CG6K should be connected to the Bearer subnet side of each Passport 8600. Figure 16 shows the connectivity between a UAS (containing CG6K and CPU cards) and the redundant Passport 8600s.

One SAM16 shelf requires two network connections per CG6K card and two for the CPU card. The UAS can have up to 6 CG6K cards per domain (a total of 12 per chassis) to provide 600 ports of functionality. Therefore, each SAM16 can have up to twelve (12) CG6K cards and up to two (2) CPU cards. In the UA-AAL1 solution, each SAM16 can have up to two (2) CPU cards.

Number of IP addresses used on one SAM16:

- 1 per CG6K card - (Bearer subnet)
- one (1) per CPU card - (CallP subnet)

A fully configured SAM16 configuration with twelve (12) CG6Ks and two (2) CPUs will need fourteen (14) IP addresses (1 x 12 + 1 x 2) and will utilize fourteen (14) ports per redundant Passport 8600. All the links are 100 BaseT full duplex.

***Note:*** In order for the UAS cards to communicate reliably, auto-negotiation MUST be enabled on ports of the remote end device (Passport 8600) to which they are connected. This will cause both ends to automatically negotiate to 100 BaseT full duplex.

***Note:*** Disable Spanning Tree Protocol on each of the Passport 8600 ports to which the UAS cards are connected. (Since these are end devices, no loops will be created.) For more details on configuring STP on the Passport 8600 refer to section “18.0 Appendix: Configuring the Passport 8600” on page 337.

## 2.2 CS-LAN OAM and Out-of-Band Subnets

### 2.2.1 IP Addressing and Subnetting Recommendations

In Figure 19, the OAM&P network management platforms are shown. It is recommended to place these devices on the same subnet in the CS-LAN, with each server interfacing to a separate port on the Passport 8600. In case a private addressing scheme is used for the CS-LAN devices, it is recommended to use public addresses for the management platforms if accessibility from a public network is a requirement (i.e., remote management from an operator's desk).

**Figure 18 CS-LAN OAM&P Network Management Platforms**

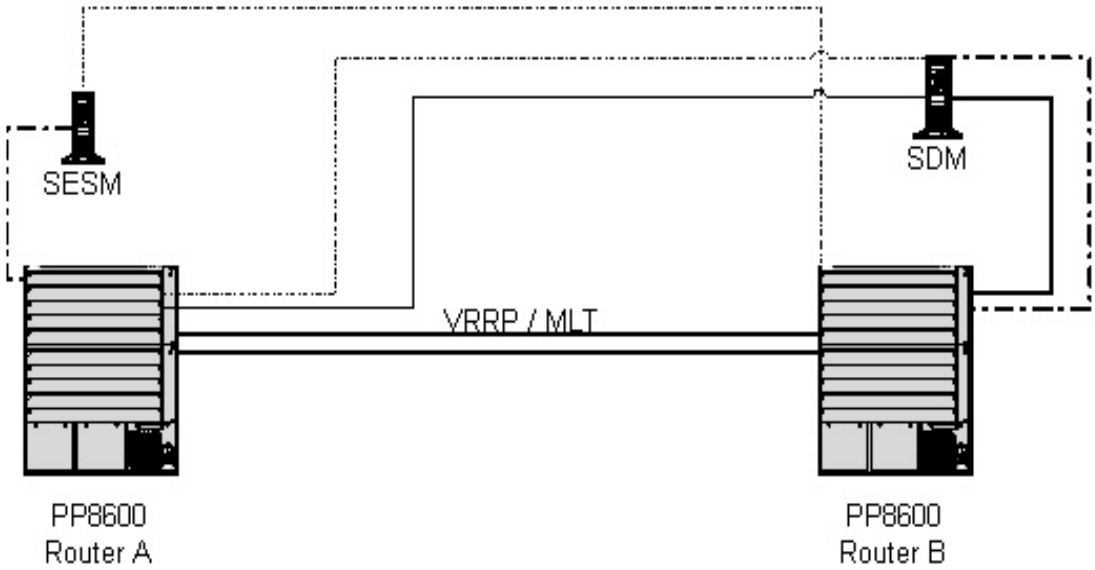
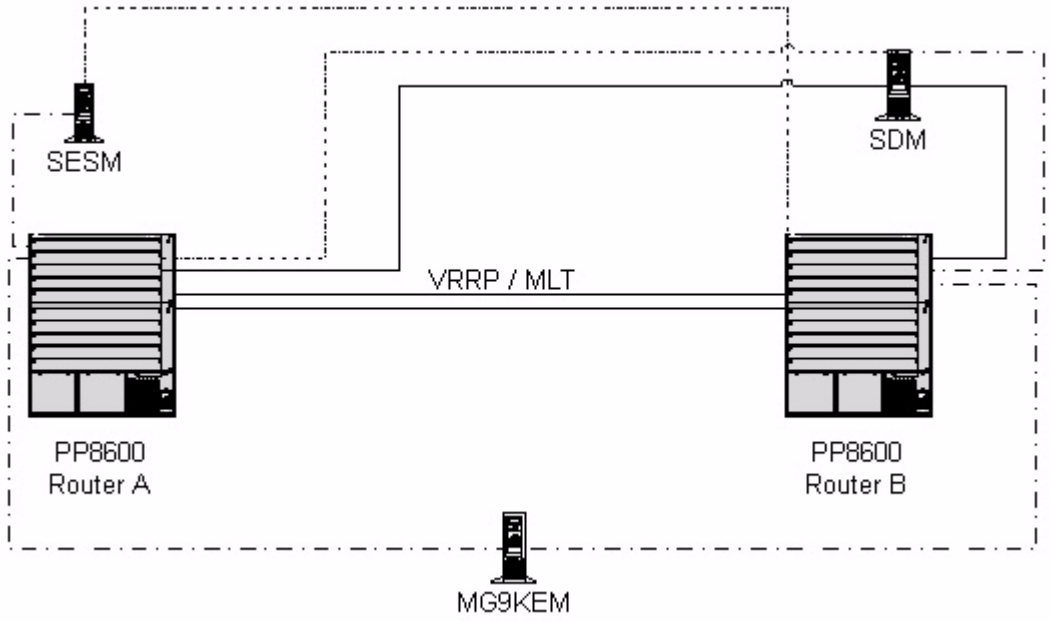



**Figure 19 CS-LAN OAM&P Network Management Platforms**




### 2.2.2 Remotely Located Servers

There is a distance limitation of 100m for any servers connected directly to the Passport 8600 over 100 BaseT. This distance may be extended, in the same building/geographical location by clustering the servers on a Layer 2 switch, such as the Baystack 450, and connecting that back to the Passport 8600 over GE.

The OAM servers may also be located remotely over the customer's internal OAM network.

### 2.2.3 OAM&P Clients and Servers

All of the OAM servers (i.e. CMT server) that require heartbeat should be provisioned with the VRRP IP address of the OAM subnet.

#### 2.2.3.1 Succession Element and Sub-Network Manager (CMT) Server

In an effort to reduce the number of OAM&P machines required for CS2000, several applications are being combined onto a single Sun Micro Systems T1400 server. This server will be called the "CS2000 Management Tools" (CMT)

The SESM is a management platform that provides a common Element Management Framework for the following Element Manager applications, which do not require any additional engineering or IP addressing:

- Packet Telephony Manager (PTM)
- Network Patch Manager (NPM) Client
- Trunk Maintenance Manager (TMM) Client
- Line Maintenance Manager (LMM) Client
- Line Test Manager (LTM) Client
- SAM21 Element Manager
- QoS Reporting — QoS Collector Application (QCA Server)

The Packet Telephony Manager (PTM)/Succession Element and Sub-element Manager (SESM) is a web-based application that manages Succession elements. The network elements managed by PTM/SESM are the Audio Provisioning Server (APS), Gateway Controller (GWC), and Universal Audio Server (UAS). The sub-network elements managed by PTM/SESM are the Line Maintenance Manager (LMM) and Trunk Maintenance Manager (TMM). The operating system for PTM/SESM is Solaris 8 running on a SUN Netra T1400 hardware platform with a common Oracle database for all PTM/SESM-based applications.

The SESM server is deployed on a single Netra T1400 and should be configured to use dual Ethernet links subtending the CS-LAN Passport 8600s. All three (3) IP addresses (see "OAM&P Server Hardware and Network Requirements" on page 55 for an explanation of the IP addresses) should be in the OAM subnet. One Ethernet link should be connected to each CS-LAN Passport 8600, for redundancy.

**SAM21 Element Manager**

The SAM21 Element Manager (SAM21EM) is the element manager for the SAM21 shelf that runs as an application on the SSPFS platform, but does not require any additional engineering or IP addressing. A separate client GUI is used for provisioning the shelf controller MAC addresses, IP addresses, Gateway IP, NTP servers and loads. The gateway controller IP addresses, PTM address, DNS server (See section "2.2.3.6 DNS Requirements" on page 55) and loads are provisioned here as well.

**QoS Collector Application Server**

The QCA Server is an application running on the SSPFS platform used for collecting and reporting end-of-call statistics to a customer provided OSS for the purposes of;

- Network engineering
- Trend analysis

- Trouble-shooting network problems
- Service Level Agreement (SLA) validation

For SN06, the QCA Server may have up to 2 instances, for added redundancy. Each instance can accommodate data feeds from up to 60 sources (GWC) for each CS2000 complex.

**Hardware Requirements**
A SESM Server is deployed in one of three configurations:

- Netra T1400 (simplex only),
- Simplex Netra N240, or
- Duplex Netra N240.

Refer to section “OAM&P Server Hardware and Network Requirements” on page 55 for details of each configuration.

All three configurations offer multiple Ethernet links, and should be configured to use multiple Ethernet links subtending the CS-LAN Passport 8600s. All IP addresses (see “OAM&P Server Hardware and Network Requirements” on page 55 for an explanation of the IP addresses) should be in the OAM subnet. One Ethernet link per server should be connected to each CS-LAN Passport 8600, for redundancy.

***Note:*** In order for the SESM NIC cards to communicate reliably, auto-negotiation MUST be enabled on ports of the remote end device (Passport 8600) to which they are connected. This will cause both ends to automatically negotiate to 100 BaseT full duplex.

***Note:*** Disable Spanning Tree Protocol on each of the Passport 8600 ports to which the SESM NIC cards are connected. (Since these are end devices, no loops will be created.) For more details on configuring STP on the Passport 8600 refer to section “18.0 Appendix: Configuring the Passport 8600” on page 337.

### 2.2.3.2 Integrated Element Management System (IEMS)

IEMS is developed for Carrier Succession Markets to provide a variety of OAM consolidation and functionality from the respective EMSs. In SN06.2, the IEMS will be deployed on a standalone platform. The supported hardware platforms are the N240 for in-service customers and the V100 for trial customers.

To ensure the proper operation of IEMS in SN06.2, following security setup and software and hardware configurations must be followed.

#### 2.2.3.2.1 IEMS Security setup (Firewall Considerations)

Refer to the section on Security for ports and protocols used for IEMS.

#### 2.2.3.2.2 IEMS SW Dependencies

- The PP8600 3.5 version or later version is required for IEMS integration
- IEMS requires SSPFS (I)SN06.2 software. The SSPFS SW load is required to be pre-loaded on N240 server in the COAM frame during the integration process at Solectron.
- DNS server is required for access and operation of the IEMS client.

IEMS and other EMS and NE secure GUI clients rely on DNS for resolving EMS server names. Therefore the customer must have a DNS service available on the network where clients are executed and the EMS servers must be listed in the service.

- DNS must be enabled on all SSPFS servers which are managed by IEMS (CS2M, MG9K EM), as well as the IEMS server itself
- IEMS Customer Client Dependencies:
    1. The IMS Element Management System client is only supported on a windows platform. To launch the IMS client from the IEMS client, the IMS System Management Console software (IMSC0001 package installation CD) must be installed co-resident on the IEMS PC client.
    2. When the IEMS is managing the PP8600 fault stream, the IEMS client must have the PP8600 JDM (Java Device Manager) software installed. Having the JDM installed allows the centralized launch of the JDM from the IEMS client. Note: There is a version of the JDM for both PC and UNIX platforms. Please refer to the "Upgrading the Succession Network Volume 1 or 5" NTP (NN10261-450P1) for details describing the JDM client installation procedures.
    3. In SN06.2, the USP client launch requires the installation of a Citrix ICA client on the IEMS client. Please refer to section "Installing the USP Manager" in the ATM/IPConfiguration Management NTP (NN10276-500) for a description of the USP client software requirements and installation procedures.
    4. When the IEMS is managing the Preside MDM, the IEMS client must either be a UNIX platform or a PC with Exceed installed to launch the MDM graphical interface.
    5. The IEMS client must have a supported version of the Sun’s JRE (JRE version 1.4.1_02 and JWS (1.2.0_02) software applications installed.
    6. The IEMS client is supported on the Windows NT4, Windows 98, Windows 98SE, Windows 2000, Windows XP, Solaris 2.7 and Solaris 2.8 Operating Systems.
    7. The IEMS client is supported using Netscape 6.1 or later and Internet Explorer 5.5 or later.

#### 2.2.3.2.3 IEMS SN06.2 Hardware

- Please see the COAM PRA # 20041119.01 for risks associated with deploying this hardware. You can access this plan at the following url: http://livelink.us.nortel.com/livelink/livelink.exe?func=ll&objId=4718241&objAction=browse&sort=name
- Purchase and deployment of the V100 hardware is a customer responsibility. Since IEMS is only supported on this platform for non-inservice trials during the (I)SN06.2 IEMS release, Nortel did not productize this platform for IEMS. This is a hand-managed configuration. There are no engineering rules and the customer must use the physical installation information provided by Sun.

### 2.2.3.3 SuperNode Data Manager (SDM)

The SuperNode Data Manager (SDM) subtends the DMS-BUS, interconnecting with the CS2000 through its DS-512 interface. As the data sever to the CS2000, the SDM continues its role providing access for CI users as well as OSS pass through and traditional billing, logging & operational measurement collection and delivery services. In addition to its traditional roles on the DMS these services are also extended to element managers in the Succession network offerings. These services are offered via Nortel provided applications running on the SDM interacting with the Nortel Succession network elements and the customers data access and collection systems. Due to the distance limitation imposed by DS-512, the SDM must be located with the CS2000 in the CS-LAN.

***Note:*** The Compact-CS2K solution does not support the DS-512 interface, therefore, this additional IP address is not required.

In addition, the SDM needs to reside within the same broadcast domain as the HIOPs and GWCs **(CallP subnet)** because it houses the BOOTP server, which provides the BOOTP tab file for configuring these devices.

Finally, in order to maintain network management access, the SDM also needs to be co-located in the **OAM subnet**. Due to these requirements as well as the fact that VRRP's virtual IP address can not act as an agent for the BOOTP/DHCP servers (which is a requirement in the BOOTP configuration), the SDM must be configured with three (3) IP addresses: one for the DS-512 interface and one for each of the two Ethernet interfaces described above.

***Note:*** The SDM requires three (3) IP addresses for handling billing traffic, for transferring BOOTP tab files, and for OAM&P access. As such, the SDM should be configured with redundant hardware including two fault tolerant Ethernet cards per domain. There is a single IP address associated with each pair of e-net cards (each of which has a physical interface that requires a network connection). Since the SDM requires two (2) ethernet IP addresses as described above, it will need to have a dual domain configuration supporting four (4) ethernet cards. For redundancy, each of the interfaces on a pair of e-net cards should be connected to one of the redundant Passport 8600.

***Note:*** In order for the SDM NIC cards to communicate reliably, auto-negotiation MUST be enabled on ports of the remote end device (Passport 8600) to which they are connected. This will cause both ends to automatically negotiate to 100 BaseT full duplex.

***Note:*** Disable Spanning Tree Protocol on each of the Passport 8600 ports to which the SDM cards are connected. (Since these are end devices, no loops will be created.) For more details on configuring STP on the Passport 8600 refer to section "18.0 Appendix: Configuring the Passport 8600" on page 337.

#### 2.2.3.3.1 SDM Edge Node Monitoring

The SDM employs fully redundant network interfaces on both the Call Processing and OAM&P subnets, for a total of four physical connections. Only one connection per subnet is active at any time. Connectivity failure on any active link results in activity switch to the inactive link for that subnet. This activity link switch can operate independently of SDM domain switchover.

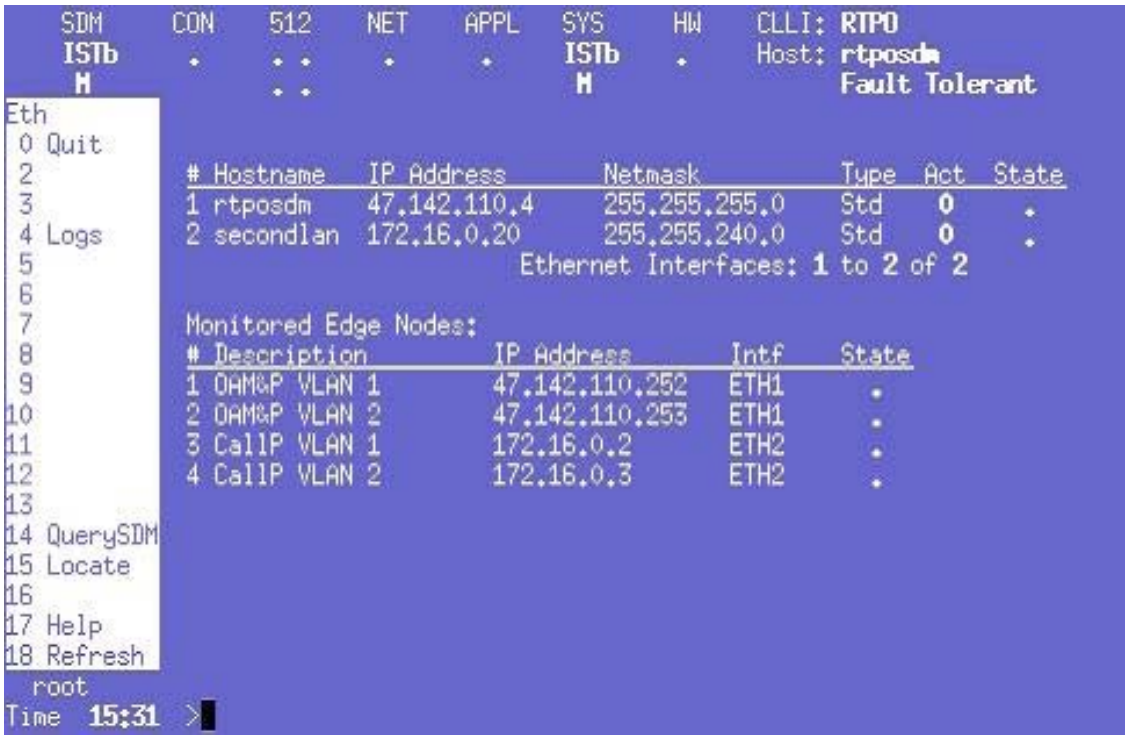
To increase reliability in failure situations of Layer 2 and Layer 3 messaging only, the SDM should be configured to use Edge Node Monitoring. Edge Node Monitoring provides the capability for the SDM to determine network connectivity by pinging network devices. When connectivity is lost, the SDM network interfaces will attempt to switch to the inactive links.

Edge Node Monitoring should be provisioned with two edge nodes per SDM interface. The edge nodes to be monitored should be the VLAN addresses on each Passport 8600 associated with the SDM interface. For instance, the SDM interface associated with the Callp VLAN should be configured to monitor the Callp VLAN addresses on both Passport 8600s in the CS-LAN.

In Figure 20, the SDMMTC ETH level is displayed with Edge Node Monitoring configured as described above. In this example the IP addresses 47.142.110.252 and 47.142.110.253 are the OAM&P VLAN addresses on each of the CS LAN Passport 8600s. Also, the IP addresses 172.16.0.2 and 172.16.0.3 are the Callp VLAN addresses on each of CS LAN Passport 8600s.

Refer to the manual NN10104511, CS2E Configuration, for additional information on Edge Node Monitoring configuration on the SDM.

**Figure 20 Edge Node Monitoring on SDMs**




### 2.2.3.4 Universal Signaling Point Element Manager (USP-EM) Server

The USP-EM Server is co-resident on the RTC System Node.

The USP-EM client can be deployed on a Win 95, Win 98SE, Win NT, or Windows 2000 PC platform which resides in the Corporate Network, like the rest of EM clients.

### 2.2.3.5 Preside Multiservice Data Manager (PMDM)

The standard deployment of the PMDM is on a single Netra T1400 and should be configured to use dual Ethernet links subtending the CS-LAN Passport 8600s. All three (3) IP addresses should be in the OAM subnet. One Ethernet link should be connected to each CS-LAN Passport 8600, for redundancy.

Optionally, the PMDM server is deployed on dual Netra T1400s and configured with a private intra-server link to synchronize the server databases. Additionally, each server should be connected via Ethernet to a different CS-LAN Passport 8600, for redundancy. The intra-server link requires two (2) IP addresses which are only visible internally to the PMDM servers. And two (2) more IP addresses on the OAM subnet are required to interconnect each server with its respective Passport 8600.

***Note:*** In order for the PMDM NIC cards to communicate reliably, auto-negotiation MUST be enabled on ports of the remote end device (Passport 8600) to which they are connected. This will cause both ends to automatically negotiate to 100 BaseT full duplex.

***Note:*** Disable Spanning Tree Protocol on each of the Passport 8600 ports to which the PMDM NIC cards are connected. (Since these are end devices, no loops will be created.) For more details on

configuring STP on the Passport 8600 refer to section “18.0 Appendix: Configuring the Passport 8600” on page 337.

### 2.2.3.6 DNS Requirements

A Domain Name Server (DNS) serves two independent functions in the CS LAN. Both functions are provided by a standard DNS server to be provided by the customer. Succession solution does not include a DNS server since the functions needed are standard DNS functions.

The first DNS function is required if security certificates are used for OAM&P system users. Security certificates can be installed at any time during or after the upgrade of the OAM&P system, but the OAM&P servers must be added to the customer's intranet DNS servers prior to installing the certificates. We would recommend that the certificates be installed at the end of the OAM&P installation process.

For this DNS function, a standard DNS service is used and hostnames are assigned to the CS2E/SDM, MG9KS and CS2M servers. The CS2E/SDM does not directly access DNS (i.e. internal DNS lookup). All of the EMS servers would need to be DNS listed so that SSL based protocols can use hostname based keys and to allow tools to reference the EMS servers by name. DNS is required to enable client workstations to lookup the CS2E/SDM, MG9KS and CS2M server addresses by name.

DNS services on the Telco Operations Network are required to allow the user clients to access the OAM&P servers. Many of the CS2M and MG9KS applications use a security certificate to secure the logon portion of the client to server communications, these security certificates require the use of server names when referencing the EMS servers. Refer to IM 24-9082 for additional information.

The DNS server used within the Telco Operations LAN and the CS-LAN do not need to be the same server. Separate servers with the same name for EMS servers can be used if desired.

The second DNS application is needed only in a small line gateway deployment, and is optional. This use of DNS allows for a more streamlined provisioning of small line gateways. In order for this DNS application to function properly, the following steps are required:

- DHCP should be configured for DDNS so that when it assigns a dynamic IP address to a known MAC-FQDN for the small line gateways, then, the IP address is updated in the DNS server.
- The SAM21 GWC card provisioning (performed through the SAM21 Manager) should be datafilled with the IP address of the DNS Server(s).
- The gateway’s IP address in GWC Manager is set to 0.0.0.0
- DNS is required in this case to re-establish control of small line gateways after a cold restart of the system.

The DNS Server(s) specified for each GWC in the SAM21 Manager may be distinct from the DNS servers used within the Telco Operations LAN, (or CS LAN) for EMS name lookups. This DNS Server must contain information on all the small line gateways served by this office. Multiple DNS Servers can be specified to provide reliability.

### 2.2.3.7 OAM&P Server Hardware and Network Requirements

This section applies to the following servers:

- SESM server,

An OAM&P Server is deployed in one of three configurations:

- Netra T1400 (simplex only),
- Simplex Netra N240, or
- Duplex Netra N240.

All three configurations offer multiple Ethernet links, and should be configured to use dual Ethernet links subtending the CS-LAN Passport 8600s. All three configurations require three (3) IP addresses (see the Network Requirements sections below for each configuration for an explanation of the IP addresses) and should be in the OAM subnet. One Ethernet link should be connected to each CS-LAN Passport 8600, for redundancy.

#### 2.2.3.7.1 Simplex Netra N240 Network Requirements

This configuration offers multiple Ethernet links, and should be configured to use dual Ethernet links subtending the CS-LAN Passport 8600s and using three (3) IP addresses from the OAM subnet.

To provision redundant Ethernet interfaces, the Netra N240 uses Quad Gigabit Ethernet (bge) card. “bge1” and “bge3” must be used to connect to the PP8600s. The machine should be functioning correctly on the network using “bge1” before you configure redundant interfaces. Both “bge1” and “bge3” must be connected to an Ethernet network (i.e. they must have link). One Ethernet link should be connected to each CS-LAN Passport 8600, for redundancy.

The software used to provide redundant Ethernet interfaces is Solaris Multipathing. It requires two “test” IP addresses. These must be UNUSED IP addresses on the same subnet as the Netra. “Test” IP addresses are for use only by multipathing and should not be used by clients to connect to the server. The existing IP address is now called the “data” IP address and clients connect to the server via the data IP Address. The “data” IP address will automatically move to a working network interface.

***Note:*** In order for the N240 NIC cards to communicate reliably, auto-negotiation MUST be enabled on ports of the remote end device (Passport 8600) to which they are connected. This will cause both ends to automatically negotiate to 100 BaseT full duplex.

***Note:*** Disable Spanning Tree Protocol on each of the Passport 8600 ports to which the N240 NIC cards are connected. (Since these are end devices, no loops will be created.) For more details on configuring STP on the Passport 8600 refer to section “18.0 Appendix: Configuring the Passport 8600” on page 337.

#### 2.2.3.7.2 Duplex Netra N240 Network Requirements

This configuration offers multiple Ethernet links, and should be configured to use dual Ethernet links subtending the CS-LAN Passport 8600s and using three (3) IP addresses from the OAM subnet.

This configuration uses two Netra N240s interconnected to serve as a single server. Each of the two N240s has a Quad Gigabit Ethernet (bge) card. On each N240, two interfaces are used for interconnecting the two servers together, and the other two interfaces are used to connect the two servers to the CS-LAN PP8600s.

The following connectivity scheme must be used for interconnecting the two servers:

- bge0 of server 0 to bge0 of server 1
- bge2 of server 0 to bge2 of server 1

Multipathing will not be used on the interconnect interfaces. In addition, these interfaces will be configured with IP addresses from a private subnet that only exists between the two servers. These interconnect IP addresses will be the same on every Duplex N240 server:

- 192.168.47.3 bge0 of server 0
- 192.168.47.4 bge0 of server 1
- 192.168.47.5 bge2 of server 0
- 192.168.47.6 bge2 of server 1

The following connectivity scheme must be used for connecting the two servers to the CS-LAN PP8600s:

- bge1 of server 0 to PP8600-0
- bge3 of server 0 to PP8600-1
- bge1 of server 1 to PP8600-1
- bge3 of server 1 to PP8600-0

***Note:*** Please take note of the asymmetry between server 0 and server 1 and which of bge1 and bge3 connects to each of the CS-LAN PP8600s.

It is important that this exact connectivity scheme be followed. Failure to properly connect the two servers to the CS-LAN PP860s will result in failure of the High-Availability feature of this redundant server.

In this configuration the three (3) IP addresses, from the OAM&P VLAN, are assigned as one (1) physical IP address on each of the two servers, assigned on bge1 interface, and one (1) logical IP address, that floats with the active server.

***Note:*** In order for the N240 NIC cards to communicate reliably, auto-negotiation MUST be enabled on ports of the remote end device (Passport 8600) to which they are connected. This will cause both ends to automatically negotiate to 100 BaseT full duplex.

***Note:*** Disable Spanning Tree Protocol on each of the Passport 8600 ports to which the N240 NIC cards are connected. (Since these are end devices, no loops will be created.) For more details on configuring STP on the Passport 8600 refer to section “18.0 Appendix: Configuring the Passport 8600” on page 337.

#### 2.2.3.7.3 Netra T1400 Network Requirements

This configuration offers multiple Ethernet links, and should be configured to use dual Ethernet links subtending the CS-LAN Passport 8600s and using three (3) IP addresses from the OAM subnet.

To provision redundant Ethernet interfaces, the Netra T1400/1405 uses Quad Fast Ethernet (qfe) card. The primary Ethernet interface must be “hme0” and the standby will be “qfe0”. The machine should be functioning correctly on the network using hme0 before you configure redundant interfaces. Both hme0 and qfe0 must be connected to an Ethernet network (i.e. they must have link). One Ethernet link should be connected to each CS-LAN Passport 8600, for redundancy.

The software used to provide redundant Ethernet interfaces is Solaris Multipathing. It requires two (2) “test” IP addresses. These must be UNUSED IP addresses on the same subnet as the Netra. “Test” IP addresses are for use only by multipathing and should not be used by clients to connect to the server. The existing IP address is now called the “data” IP address and clients connect to the

server via the data IP Address. The “data” IP address will automatically move to a working network interface.

***Note:*** In order for the T1400 NIC cards to communicate reliably, auto-negotiation MUST be enabled on ports of the remote end device (Passport 8600) to which they are connected. This will cause both ends to automatically negotiate to 100 BaseT full duplex.

***Note:*** Disable Spanning Tree Protocol on each of the Passport 8600 ports to which the T1400 NIC cards are connected. (Since these are end devices, no loops will be created.) For more details on configuring STP on the Passport 8600 refer to section “18.0 Appendix: Configuring the Passport 8600” on page 337.

**Netra T1400 Link Redundancy Configuration**
The Carrier Grade engineering requires that the server now use three (3) IP addresses (one (1) for the appearance of the server, one (1) for each physical interface for the heartbeat). Also, the recommended heartbeat sample time is 10 seconds. The sample time value is used as the range of time in which five (5) failed heartbeats will result in a switch of activity to the secondary link. If the primary link has failed but then recovers, activity will switch back to the primary link.

**Netra T1400 Multipathing Config Procedure**

- Login as root and run the “**cli**” tool. The cli command will display an option menu.
- Select Configuration
- Select IP Configuration
- Select ip_multi_on.
- Enter the two test IP addresses and the timeout value. It is recommended to set the timeout to 10 seconds. Your changes will take effect right away. You do not need to reboot the system.

**Netra T1400 Multipathing Unconfig Procedure**

- Login as root and run the “**cli**” tool. The cli command will display an option menu.
- Select Configuration
- Select IP Configuration
- Select ip_multi_off.

The changes will not take effect until you reboot the system.

## 2.3 Routing in the CS-LAN

### 2.3.1 OSPF Considerations and Recommendations

Open Shortest Path First (OSPF) is the recommended Interior Gateway Protocol (IGP) for the Passports 8600 to exchange route information with the rest of the customer’s network.

#### 2.3.1.1 OSPF Interfaces and Routes Redistribution

To optimize the overall routing design, OSPF should be configured only on the interfaces that are connected to the Core network and on the MLT interfaces.

Nortel Networks strongly suggests creating a separate OSPF area for all the CS-LAN interfaces running OSPF. This allows for a more flexible and scalable network design.

To improve the performance and the security of the system, it is recommended that OSPF should **not** be configured on the following interfaces/VLANs:

- Call Processing,
- OAM&P,
- Bearer,
- Portal-Int and
- Portal-Ext.

Instead, a redistribution policy should be implemented to advertise specific local subnets. This policy will announce the desired local and directly connected subnets; OSPF will import them in its database as AS External routes and then advertise them to its adjacent neighbors. Alternatively, the interfaces to the subnets that need to be advertised can be configured as passive OSPF interfaces. It is important to note that the Portal-Int subnet should not be advertised, since access to this subnet is only allowed from within the CS-LAN.
Please keep in mind that an announce/redistribution policy needs to be configured also for any static routing information that the customer wishes to be advertised to the rest of the network. Static routes are also imported by OSPF as AS External routes in its database.

It is important to remember that the Autonomous System Boundary Router (ASBR) function on the Passport 8600 needs to be enabled before redistribution of directly connected subnets and static routes can take place.

#### 2.3.1.2 OSPF Security Considerations

OSPF guarantees a secure communication between routers via authentication. For all customers who might have security concerns, Nortel Networks recommends the use of this method to minimize security threats.

Two types of authentication are possible:

- Authentication via simple key
- Authentication via MD5 key

Authentication via MD5 is considered more secure.

#### 2.3.1.3 OSPF Accept Policies

It is important to notice that an OSPF Accept policy needs to be configured to accept AS external routes into the routing table. This is typically the case if a default route advertised by OSPF needs to be added to routing table.

#### 2.3.1.4 OSPF on MLT Interfaces

To guarantee optimal routing and avoid inconsistencies, it is recommended to create a unique VLAN for the interfaces in the MLT connecting the two Passport 8600s. The MLT group also needs to be added to this VLAN. Finally, an IP interface needs to be created for this VLAN and OSPF has to be enabled on it.

This is recommended so that the two Passport 8600 are neighbors and adjacent. This will optimize the route exchange of all local routes.

#### 2.3.1.5 OSPF on the WAN Interfaces

It is recommended that OSPF be enabled on the interfaces that connect the pair of Passport 8600s to the WAN routers/switches. Each of these interfaces should be assigned to a unique port-based VLAN. This set-up guarantees flexibility and scalability in case other links are needed to support traffic growth.

## 2.4 CS-LAN Core Network Connectivity

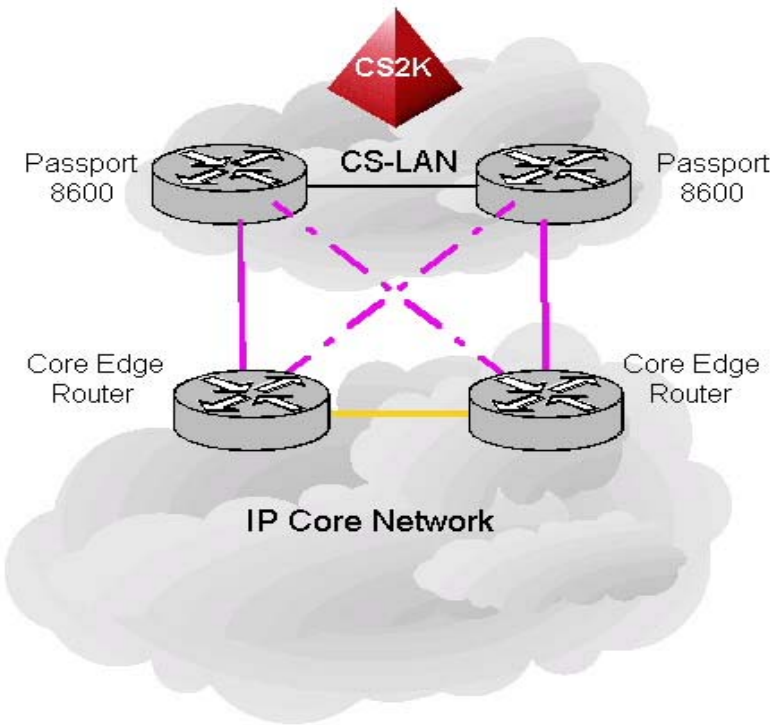
### 2.4.1 Interconnect to IP over Ethernet Networks

There are two (2) redundancy schemes for configuring the interconnection between the CS-LAN Passport 8600s and the IP over ethernet Core Network. The fully meshed scheme is the recommended configuration, however, the dual link scheme is a less robust, lower cost alternative.

**Fully Meshed Redundant Configuration**

To interconnect the CS-LAN Passport 8600s with an IP core network, connect 1 gigabit ethernet link between each Passport 8600 and each of two (2) different edge routers in the core network cloud.

**Figure 21 Fully Meshed Redundant Configuration into IP Core Network**

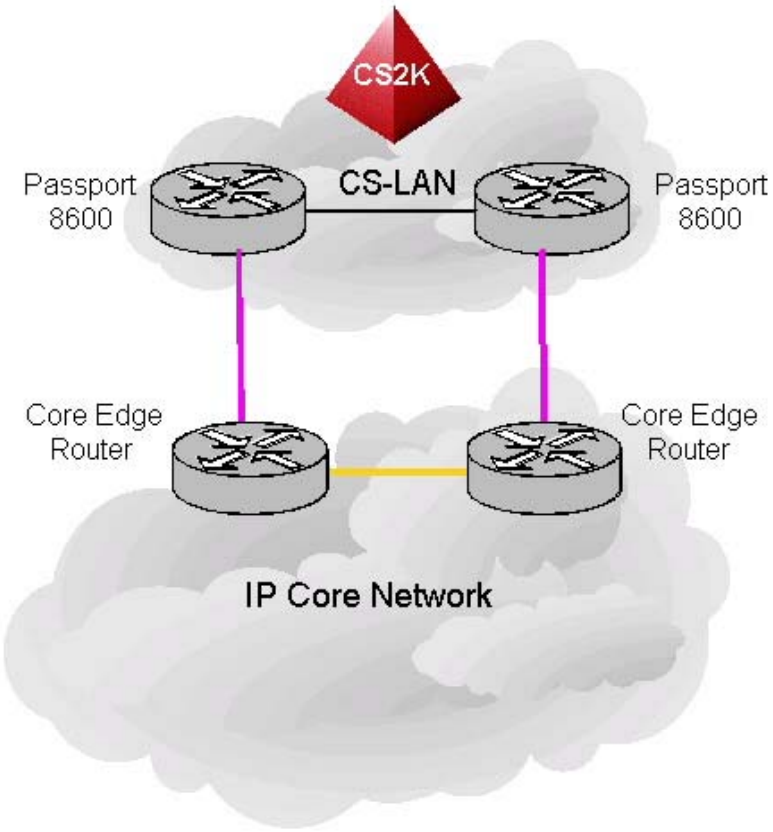



This fully meshed redundant configuration avoids a single point of failure between the CS-LAN and the Core network. Additionally, it is Carrier Grade because Call Processing is unaffected by WAN link failures. For added redundancy, the links between each of the CS-LAN Passport 8600 and the 2 edge routers should use ports from different modules on the Passport 8600.

**Dual Link Redundant Configuration**

Alternatively, to interconnect the CS-LAN Passport 8600s with an IP core network, connect 1 gigabit ethernet link between each Passport 8600 and two (2) different edge routers in the core network cloud

**Figure 22 Dual Link Redundant Configuration with Dual IP Core Edge Routers**




This dual link redundant configuration avoids a single point of failure between the CS-LAN and the Core network. However, although this solution is less expensive than the fully meshed one, it is less robust and offers reduced redundancy in comparison to the fully meshed configuration. Additionally, this configuration has a single point of WAN uplink failure per chassis which causes a VRRP failover between PP8600 chassis.

### 2.4.1.1 Engineering Considerations for IP over Ethernet Interconnect

This section discusses items related to the sizing of the WAN links from the CS-LAN to an IP over Ethernet core network.

When planning and building-out the interconnect to the core network, it is worthwhile considering all points where bearer traffic may originate and/or terminate. The sources include, but may not be limited to,

- UAS bearer traffic to/from the CS-LAN in the form of announcements and 3-way conferencing,
- IW-SPM bearer traffic to/from the CS-LAN interworking with legacy DMS peripherals such as LTCs, DTCs, and SPMs,

- PVG to PVG bearer traffic as inter or intra-CS2K calls.

Considering these key factors, multi-link trunks (MLTs) may be necessary in order to provide adequate bandwidth to/from the WAN.

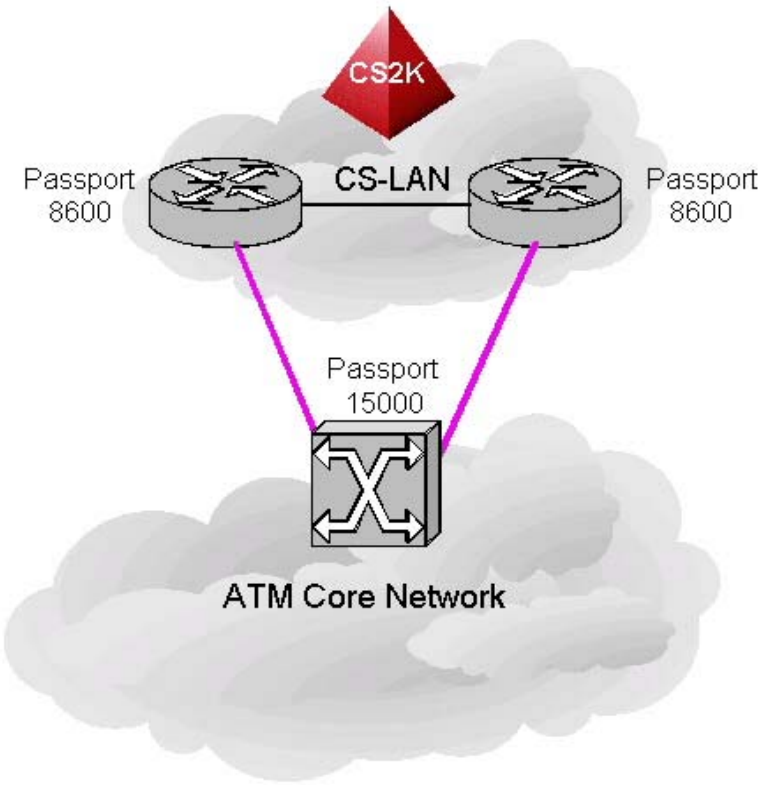
When providing MLT links to the WAN, it is not necessary to provide mated links since the WAN connections are already redundant, and routing to the redundant WAN connection during a failure is provided through the CS-LAN MLT.

### 2.4.2 Interconnect to Passport 15000 for IP over ATM Networks (AAL5)

There are two (2) options to interconnect the CS-LAN Passport 8600s with a Passport 15000 IP over ATM core network:

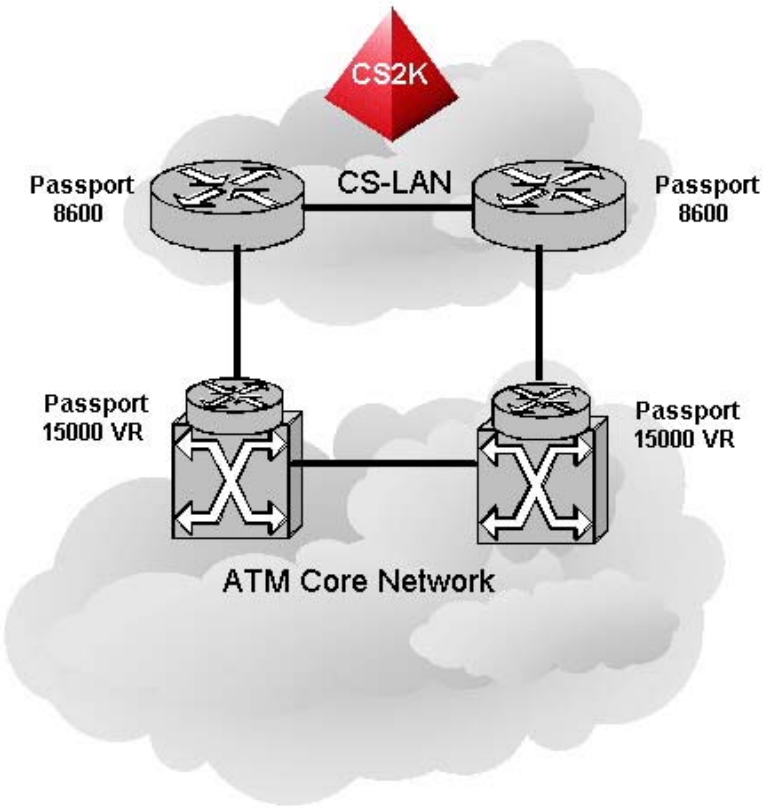
- connect an OC12 MDA from an 8672ATM-E module of each Passport 8600 to two (2) OC12 interfaces on one Passport 15000 (Figure 23 on page 62),
- or connect an OC12 MDA from an 8672ATM-E module of each Passport 8600 to an OC12 interface on two (2) separate Passport 15000s (Figure 24 on page 63).

**Figure 23 Dual Link Redundant Configuration with Single Passport 15000**




***Note:*** Hitless Software Migration (HSM) is not available on the Passport 15000 for unprotected ATM OC-n Function Processors (FP). As a consequence, an upgrade of the single Passport 15000 will result in an outage. Therefore, the configuration is not recommended for CS-LAN Core Network interconnect.

**Figure 24 Dual Link Redundant Configuration with Dual Passport 15000s**




This dual link redundant configuration avoids a single point of failure between the CS-LAN and the ATM Core network. This configuration also works with Passport 15000 VR feature enabled.

### 2.4.2.1 Passport 15000 Core Network Interconnect Scalability Considerations

The intent of this section is to address the CS-LAN to Passport 15000 core network interconnect, and the scalability considerations for aggregating traffic from a subtending PVG network.

When planning and building-out the interconnect to the core network, it is worthwhile considering all points where bearer traffic may originate and/or terminate. The sources include, but may not be limited to,

- UAS bearer traffic to/from the CS-LAN in the form of announcements and 3-way conferencing,
- IW-SPM bearer traffic to/from the CS-LAN interworking with legacy DMS peripherals such as LTCs, DTCs, and SPMs,
- PVG to PVG bearer traffic as inter or intra-CS2K calls.

The CS-LAN Passport 8600 ATME MDAs have limits to their throughput capacities. Therefore, if the aggregate amount of bearer and signaling traffic coming from either the UAS or IW-SPM exceeds those limits specified, additional ATME MDAs may need to be added. Furthermore, as more bearer traffic enters [and exits] the CS-LAN, additional OC-12 ports and/or OC-12 cards may also be required on the Passport 15000 Virtual Router (VR). If physical space in the chassis of the Passport 8600 or Passport 15000 is limited, then other alternatives must be considered.

Lastly, one should also consider the scalability limits of the Passport 15000 VR. The combination of traffic to/from the CS-LAN (discussed previously) in conjunction with the DPT associated bearer traffic traversing to/from other CS2K networks, the limits of scalability in the Passport 15000 VR may reach the OC-12/OC-48 forwarding throughput (PQC12) limit as shown in Table 3. When this point is reached, it may become necessary to add additional Passport 15000 VRs, and reconfigure the VCCs from the subtending PVG network as needed. However, the limits of scalability in the Passport 8600 ATME MDAs should not be ignored.

**Table 3 Throughput Limitation of Passport VR ATM Connections**

| Codec | # of WAN links per card | Max # of DS0s per card |
|---|---|---|
| G.711 (10ms) | 1 | 4646[a] |
| | 2,3,4 | 5400 |
| G.711 (20ms) | 1 | 5575[a] |
| | 2,3,4 | N/A |

a. Constrained by ATM bandwidth of OC12 port

Considering these key factors on scalability, it may be prudent to consider other alternatives if capacities beyond these levels are required and/or expected.

### 2.4.3 CS-LAN to WAN MLT Link Engineering

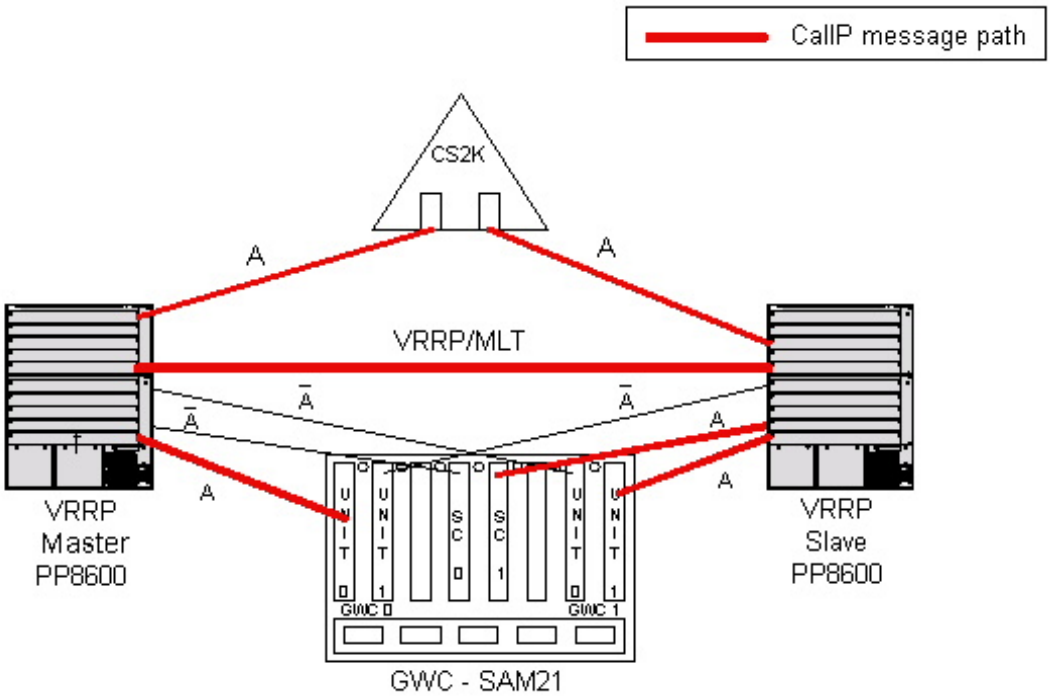
To be provided in a future release of this document.

## 2.5 CS-LAN Reliability Scheme

This section explains how the redundancy scheme for the CS-LAN Solution reliably maintains the system by utilizing the OSPF and VRRP protocols. The empirical failover test results used here are taken from the CS2K Robustness Test Plan.

At the foundation of the CS-LAN reliability scheme is the redundant Passport 8600co NEBS chassis. In addition, all the CS-LAN CallP (and most of the OAM) devices have redundant hardware and have redundant 100 BaseT links to each Passport 8600, to prevent a single point of failure in the CS-LAN system. During stable operation of the CS-LAN, the active units of the subtending CallP devices (i.e. GWC, UAS, HIOP) have Layer 2 connectivity with whichever Passport 8600 they are linked to, regardless of the Passport 8600's VRRP status. This configuration and an example of some possible message flows are depicted in the figure below.

**Figure 25 Example of Possible Message Flows in a Redundant CS-LAN**




## 2.5.1 Passport 8600 Reliability

### 2.5.1.1 Chassis Redundancy

In the redundant Passport 8600 configuration, each chassis is installed with a single 8691SF CPU switching fabric. Gigabit ethernet links are used for the intra-Passport 8600 MLT connection. VRRP is configured with default settings between the two Passport 8600s in the CS-LAN, which assigns the primary Passport 8600 to be the master and the secondary Passport 8600 to be the slave. This is a L2/L3 load-sharing configuration (with VRRP backup-master enabled) and the default gateways for the CS-LAN devices are associated with the master Passport 8600. As a result, the master and slave Passport 8600s share all the switching and routing decisions between the VLANs within the CS-LAN and out to the Core Network, making it a more robust system.

***Note:*** Dual 8691SF/CPU modules per 8010co chassis are not supported in SN06.2.

***Note:*** The VRRP critical IP address must be disabled. This will ensure that communication between CS2K network elements is not affected by failures such as complete WAN uplink failures.

### 2.5.1.2 Multi-Link Trunking (MLT)

For optimal reliability, **it is imperative that Multi-Link Trunking (MLT) be configured between the dual Passport 8600s using ports from multiple modules to prevent a single point of failure from disrupting the VRRP messaging, thereby, causing a potentially massive CallP outage.** Additionally, the 802.1Q tagging function MUST be enabled for the MLT in order to guarantee that the relevant CS-LAN subnets (and their correspondent broadcast domains) can span across the two switches. Please note that VRRP functions are based on this assumption. Finally, the MLT

group needs to be added to the CallP, OAM, Bearer, Portal-Int and Portal-Ext CallP and OAM VLANs on both Passport 8600s, in order to ensure that each of these subnets, which span the two Passport 8600 chassis, is a single broadcast domain across the two chassis.

***Note:*** In order to optimize routing within the CS-LAN, it is required that the MLT links must be configured with a 255.255.255.252 mask and OSPF enabled, thereby creating a routed link between the redundant Passport 8600s.

The MLT group should be comprised of at least two (2) gigabit ethernet interfaces per Passport 8600 chassis (i.e. one gigabit ethernet interface from each 8632TXE module), and must NOT be mixed with 10/100 BaseT or any other media type. Use of the fiber media instead of CAT5 media in this configuration serves the following purposes:

- limits the interference between the cables in the MLT group
- facilitates troubleshooting the CS-LAN
- simplifies the Passport 8600 configuration
- meets the CS-LAN traffic engineering and capacity requirements

It is recommended that cp-limit be disabled on the MLT ports and enabled on all edge links to safeguard against possible network storms created by undesirable network loops

***Note:*** Disable Spanning Tree Protocol on each of the Passport 8600 ports that are in MLT group. This is done to avoid confusion and provide consistency (by default, the MLT functionality overrides the STP setting to be disabled). For more details on configuring STP on the Passport 8600 refer to section “18.0 Appendix: Configuring the Passport 8600” on page 337.

#### 2.5.1.2.1 Inter-Switch Trunking (IST)

Whenever SMLT (Split MLT) needs to be configured on the PP8600s, IST needs to be enabled on the MLT interconnecting the two (2) PP8600s.

It is recommended that cp-limit be disabled on IST ports and enabled on all edge links to safeguard against possible network storms created by undesirable network loops

### 2.5.1.3 Link Redundancy

Gigabit ethernet uplinks should be used to interconnect the CS-LAN Passport 8600s and the Core network. For maximum redundancy, due to faster failover times, it is highly recommended to configure the CS-LAN Passport 8600s so that they are fully-meshed with two (2) Core network edge routers. Optionally, each Passport 8600 can be configured with a single WAN uplink, however, the failover time will be slower than the recommended fully-meshed scheme.

Refer to section 2.4 for details on CS-LAN to core network interconnect.

### 2.5.1.4 Software Load Redundancy

Additionally, it is required for the reliability of the system that the primary, secondary, and tertiary runtime and configuration file choice parameters on the Passport 8600 be set appropriately to eliminate a single point of failure during the boot-up sequence. Refer to section “18.0 Appendix: Configuring the Passport 8600” on page 337 for configuration details.

#### 2.5.1.5 Failover Scenario

When the master Passport 8600 has a fault due to a switching fabric failure or a chassis power failure, within 1 second, VRRP shifts the default gateways of the respective VLANs over to the slave Passport 8600 and assigns it the status of VRRP master. Simultaneously, within 10 seconds the standby units of the CS-LAN devices subtending the working Passport 8600 detect a loss of the heartbeat messages with their respective active units on the failed Passport 8600 and SWACT, thereby, establishing communication with the new master Passport 8600. (Note: The devices whose active units were already subtending the new master Passport 8600 do not SWACT.)

### 2.5.2 CS-LAN Device Reliability

All CallP (and most OAM) devices are installed with active/standby units and I/O interfaces. For maximum redundancy, these elements must have one link connected to each one of the dual VRRP Passport 8600s. Additionally, the VRRP logical IP address (instead of their respective physical IP addresses) of the VLANs on the redundant Passport 8600s MUST be assigned as the default gateway of the CS-LAN subtending devices.

***Note:*** Disable Spanning Tree Protocol on each of the Passport 8600 ports to which the CS-LAN device cards are connected. (Since these are end devices, no loops will be created.) For more details on configuring STP on the Passport 8600 refer to section “18.0 Appendix: Configuring the Passport 8600” on page 337.

#### 2.5.2.1 Failover Scenario

When the active unit for one of the CS-LAN devices fails or its LAN link to the Passport 8600 fails, within 10 seconds, the standby unit detects a loss of heartbeat messages from the active unit and SWACTs. Consequently, this unit becomes the active unit and proceeds to establish communication with the other Passport 8600, regardless of its VRRP status.

## 2.6 CS-LAN Geographic Survivability Configuration - SL100 cCS2K only

The Succession Geographic Survivability feature provides a CS-LAN configuration that is split into two geographic locations, up to 10 fiber-kilometers apart. In the case of a disaster in one of the two locations, this configuration enables the call server to maintain call processing capability by performing a warm switch of activity between the two geographically dispersed call agents and maintaining full operation in a non-redundant mode.

This section will only document the configurations that differ from the single location Succession CS-LAN. For features not specifically documented in this section, consult the remainder of this chapter.

### 2.6.1 Passport 8600

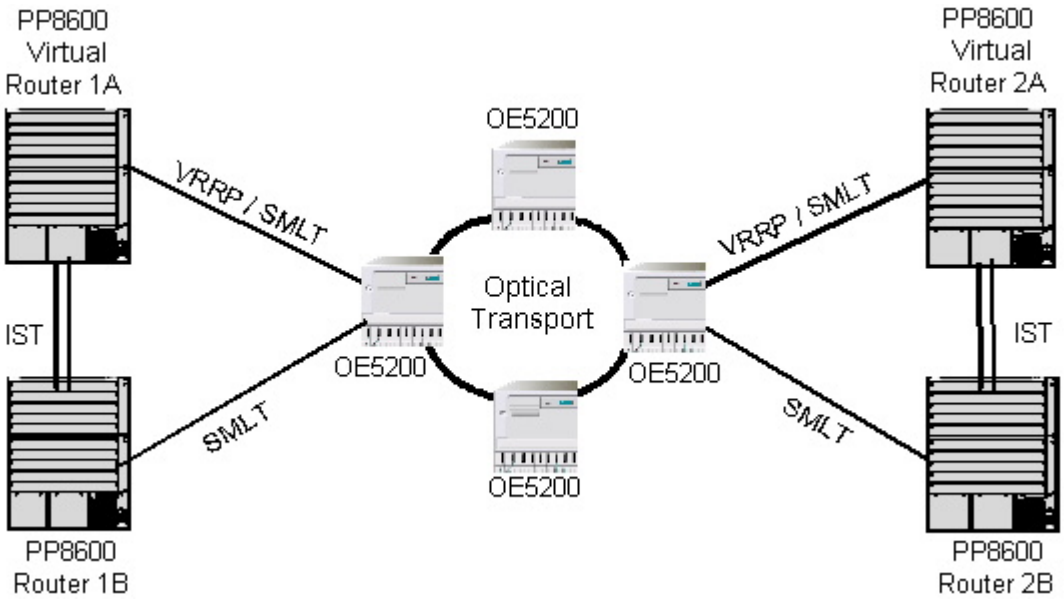
The central components of the geographically survivable CS-LAN are two (2) Passport 8600 in each geographical location. The two Passport 8600 at each location are interconnected with a minimum of two gigabit links. The two locations are interconnected through an optical network.

For load sharing, one of the Passport 8600s in each geographical location should be provisioned with VRRP in dual-active mode (i.e. enable backup-master) versus active-standby mode. This will facilitate sharing the network traffic load across the two geographical locations minimizing the use of the optical network between the two locations.

In Figure 26, the Passport 8600 configuration is shown. Currently, as a hardware baseline, each 8010co chassis must be configured with ONLY one (1) 8691SF/CPU module, along with a minimum of two (2) 8632TXE modules. See the Traffic Engineering Section for more details.

***Note:*** Dual 8691SF/CPU modules per 8010co chassis are not supported in SN06.

**Figure 26 CS-LAN Geographic Survivability Passport 8600 Configuration**




### 2.6.1.1 Geographically Survivable CS-LAN IP Addresses

Number of IP addresses used on the four (4) Passport 8600s:

- 1 per chassis for Management Interface [out-of-band (OOB) OAM Subnet]
- 1 per chassis (physical) for each of (5) configured VLANs (minimum) [CS-LAN CallP, CS-LAN OAM, Bearer (RTP), intra-Passport 8600 (IST), intra-Locations (SMLT)]
- 1 for each VRRP logical IP address per VLAN [CS-LAN CallP, CS-LAN OAM, Bearer (RTP)]

Therefore, at least 27 IP addresses (OOB - 4, CALLP - 5, OAM - 5, Bearer - 5, IST - 4, SMLT - 4) are required for the suggested configuration.

***Note:*** Since the Passport 8600 management interface is routable, it should be configured with an OOB IP address from a subnet that is not in the Passport 8600's routing table.

### 2.6.1.2 Passport 8600 Redundancy

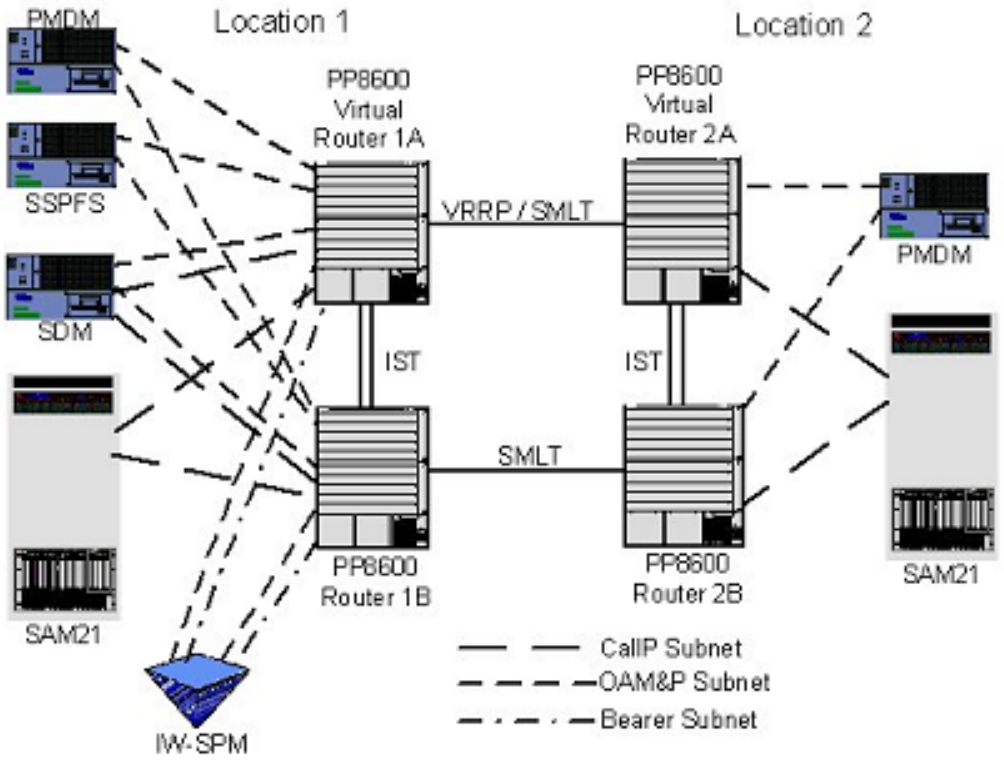
In the geographically survivable Passport 8600 configuration, each chassis is installed with a single 8691SF CPU switching fabric. Gigabit ethernet links are used for the inter-switch trunk (IST) connection between the two Passport 8600's in each location. VRRP is configured with default settings between two Passport 8600s, one in each geographic location, which assigns one Passport 8600 in one geographic location to be the master and one Passport 8600 from the other geographic location to be the slave. This is a L2/L3 load-sharing configuration across the two geographic location (with

VRRP backup-master enabled) and the default gateways for the CS-LAN devices are associated with the master Passport 8600.

As a result, all four Passport 8600s provide L2 functionality, but only one passport 8600 per location provides a L3 functionality (this is the Passport 8600 with VRRP configured). At each location, the Passport 8600 providing L2 only functionality depends on the other Passport 8600 in the same location for L3 functionality, or on the L3 Passport 8600 in the other location in the case where the local L3 Passport 8600 is unavailable. The master and slave L3 Passport 8600s share all the switching and routing decisions between the VLANs within the CS-LAN and out to the rest of the network, making it a more robust system.

***Note:*** Dual 8691SF/CPU modules per 8010co chassis are not supported in SN06.

**Figure 27 CS Geographic Survivability PP8600 Logical Configuration**




### 2.6.1.3 Inter-Switch Trunking (IST)

For optimal reliability, **it is imperative that Inter-Switch Trunking (IST) be configured between each pair of Passport 8600s in the same geographic location using Gigabit Ethernet ports from multiple modules to prevent a single point of failure from disrupting the VRRP messaging, thereby, causing a potentially massive CallP outage.** Additionally, the 802.1Q tagging function MUST be enabled for the IST in order to guarantee that the relevant CS-LAN subnets (and their correspondent broadcast domains) can span across the two switches. Please note that VRRP functions are based on this assumption. Finally, the IST group needs to be added to the CallP, OAM, Bearer and SMLT VLANs on both Passport 8600s, in order to ensure that each of these subnets,

which span the four (4) Passport 8600 chassis, is a single broadcast domain across the 2 chassis of a single location (See section “2.6.1.4 Split Multi-Link Trunking (SMLT)” for extending the subnets across the two geographic locations).

***Note:*** In order to optimize routing within the CS-LAN, it is required that the IST links must be configured with a 255.255.255.252 mask and OSPF enabled, thereby creating a routed link between the redundant Passport 8600s.

The IST group should be comprised of at least two (2) gigabit ethernet interfaces per Passport 8600 chassis (i.e. one gigabit ethernet interface from each 8632TXE module), and must NOT be mixed with 10/100 BaseT or any other media type. For more details on this requirements refer to section “2.5.1.2 Multi-Link Trunking (MLT)”.

It is recommended that cp-limit be disabled on IST ports and enabled on all edge links to safeguard against possible network storms created by undesirable network loops

***Note:*** Disable Spanning Tree Protocol on each of the Passport 8600 ports that are in IST group. This is done to avoid confusion and provide consistency (by default, the IST functionality overrides the STP setting to be disabled). For more details on configuring STP on the Passport 8600 refer to section “18.0 Appendix: Configuring the Passport 8600” on page 337.

### 2.6.1.4 Split Multi-Link Trunking (SMLT)

For optimal reliability, **it is imperative that Split Multi-Link Trunking (SMLT) be configured between the Passport 8600s and the optical routers in both geographic locations using Gigabit Ethernet ports from multiple modules to prevent a single point of failure from disrupting the VRRP messaging, thereby, causing a potentially massive CallP outage.** The same SMLT ID must be used on all four (4) Passport 8600s. Additionally, the 802.1Q tagging function MUST be enabled for the SMLT in order to guarantee that the relevant CS-LAN subnets (and their correspondent broadcast domains) can span across the four switches. Please note that VRRP functions are based on this assumption. Finally, the SMLT group needs to be added to the CallP, OAM and Bearer VLANs on all four (4) Passport 8600s, in order to ensure that each of these subnets, which span the four (4) Passport 8600 chassis, is a single broadcast domain across the four chassis of both locations. This configuration is shown in Figure 26 - CS-LAN Geographic Survivability Passport 8600 Configuration.

***Note:*** In order to optimize routing within the CS-LAN, it is required that the SMLT links must be configured with a 255.255.255.248 mask and OSPF enabled, thereby creating a routed link between the redundant Passport 8600s.

The SMLT group should be comprised of at least four (4) gigabit ethernet interfaces, one interface per Passport 8600 chassis, and must NOT be mixed with 10/100 BaseT or any other media type. For more details on this requirements refer to section “2.5.1.2 Multi-Link Trunking (MLT)”.

***Note:*** Disable Spanning Tree Protocol on each of the Passport 8600 ports that are in SMLT group. This is done to avoid confusion and provide consistency (by default, the IST functionality overrides the STP setting to be disabled). For more details on configuring STP on the Passport 8600 refer to section “18.0 Appendix: Configuring the Passport 8600” on page 337.

#### 2.6.1.5 OSPF on the IST Interfaces

To guarantee optimal routing and avoid inconsistencies, it is recommended to create a VLAN for the interfaces in the IST connecting the two Passport 8600s in the same location. The IST instance also needs to be added to this VLAN. Finally, OSPF needs to be enabled on the IST.

This is recommended so that the two Passport 8600 in the same location are neighbors and adjacent. This will optimize the route exchange of all local routes.

#### 2.6.1.6 OSPF on the SMLT Interfaces

To guarantee optimal routing and avoid inconsistencies, it is recommended to create a VLAN for the interfaces in the SMLT connecting the four Passport 8600s in both locations. The SMLT instance also needs to be added to this VLAN. Finally, OSPF needs to be enabled on the SMLT.

This is recommended so that the four Passport 8600 in both locations are neighbors and adjacent. This will optimize the route exchange of all local routes.

### 2.6.2 CallP Subnet

#### 2.6.2.1 Compact CS2K

The Compact CS2K consists of two shelves. One shelve will be located in each geographical location. Each shelve is comprised a cCS2K processor blade, a storm blade and a compact-USP blade.

The CMIC cards, or MC cards, normally deployed one per shelf, must reside in the SAM21 shelf that is in the same location as the MS equipment. That means one location will have a SAM21 shelf with a 3PC card and 2 MC cards, and the 2nd location will have a SAM21 shelf with a 3PC card and MC cards. All TDM equipment will be located at the first site, where the SAM21 shelf with the 2 MC cards is located.

#### 2.6.2.2 GWC Configuration

The GWC pairs must be configured in the split shelf configuration, with one shelf deployed in each of the 2 locations. This configurations allows all GWC pairs to be split between the two geographic locations.

For more details on GWC split shelf configuration, refer to section “2.1.4.3 Gateway Controllers Split-shelf Configuration”

#### 2.6.2.3 Inter-working SPM

The IW-SPM will be used for IP/TDM interworking. It must be deployed at the same site as the SAM21 shelf with the 2 MC cards.

### 2.6.3 OAM&P Subnet

In the SN06 release, the OAM&P devices will not be survivable. While all OAM&P device configurations are not affected by the geographic survivability feature, some devices must be co-located.

The following OAM&P servers will be deployed art the same site as the SAM21 shelf with the 2 MC cards:

- SSPFS server
- SDM server

There will be a PMDM server at each location.

# 3.0 Core Network: Backbone and Access

In this context, the core network is defined as the packet network for transporting voice, signaling and OAM traffic between gateways, or between gateways and the CS2K/ CS2Kc, or between two CS2Ks. The core network may include a combination of backbone and access networks.

## 3.1 Carrier Grade Voice-over Packet

Voice over Packet places an additional set of requirements on the network planner, in terms of performance and availability.

Voice quality in networks will be a function of;

- baseline quality, dictated by the choice of codec, packetization interval and whether silence suppression is enabled
- traffic engineering and use of QoS technologies to prevent, or route around congestion
- use of QoS technologies to give priority to speech
- ECAN and loss plan engineering

Availability for voice over packet will be a function of;

- quality of the specific network elements
- redundancy design, particularly for physical interconnection to combat link failure
- traffic engineering to reroute around failed network elements in the core network

CS2000 based Succession networks may be deployed with either Nortel, or 3rd party, core and access networks. Nortel has developed a set of performance and availability requirements which the core and access network must meet. These are available at the successionengineering web site.

### 3.1.1 Performance Requirement

The performance requirements for the core network can be summarized as follows;

- maximum latency of 150 msecs for the one-way, end-to-end bearer path connection: i.e. phone-to-phone including the contribution from other networks or TDM network elements in the end-to-end path
- maximum one-way latency for the signaling path between gateway and CS2K is governed by the signaling delay performance required. Note that signaling delays, such as dial tone delay and cross office delay, will increase by a factor of 4* transmission delay[1] from CS2K to gateway. Cross office delay for two gateways, each with 20 msecs latency to the CS2K, will be around 240 msecs. The max delay for robustness should be kept to below 50 msecs.
- maximum packet loss of 0.001%
- maximum jitter of 10 msecs

Some of the above objectives have been tightened up from the previous release of this document. The objectives aim for a performance level that is similar to that familiar to users of the current

1. Based on ASPEN connection control messaging.

PSTN. Note that the packet loss requirement is driven by modem and fax requirements. Voice and call control signaling are significantly more tolerant of packet loss.

### 3.1.2 Availability Requirements

The key availability requirements for Carrier Grade performance can be summarized as;

-a maximum of 1 second break in speech path on any link failure

-a cumulative maximum of <30 seconds per year isolation of a trunk gateway

These requirements drive the need for redundant, resilient interconnection between the Gateways and access and/or core network, and between CS LAN and the core network. The interconnection of Gateway to switch/router configurations supported by Succession for optimum carrier grade performance are detailed in other sections in these guidelines.

Optimum interconnection of Nortel Gateways to 3rd party routers which are not part of the standard Succession product offering, is not covered in these guidelines. A separate integration effort must be allowed for if planning to interconnect with 3rd party routers.

## 3.2 Core Network Engineering

### 3.2.1 Network Topology

The typical network will be a hierarchical network, comprising a set of backbone routers and a set of regional and/or access routers.

The access router will aggregate traffic onto the core backbone network. Typically, all gateways controlled by a CS2K will subtend the same regional, or access, router. An optional configuration is where the CS2K is across the backbone network from the gateways.

The choice of core router technology will be heavily influenced by the customers embedded network. Succession may be added to a Passport core network, an Optical Ethernet network, or a 3rd party router network.

The traffic from gateways with Ethernet connectivity may be aggregated onto separate access routers, or may also be aggregated onto the Passport 8600 CS LAN.

### 3.2.2 OSPF to IS-IS Interworking Considerations

To be provided in a future release of this document.

### 3.2.3 Traffic Estimation when Planning Networks

When upgrading an existing network, the traffic across the backbone network between two CS2Ks may be estimated from the current operational measurements on the trunk groups between the two offices. In a live network, this would gather the information from the OMs associated with the DPT trunk groups.

### 3.2.4 Passport 15000 Core

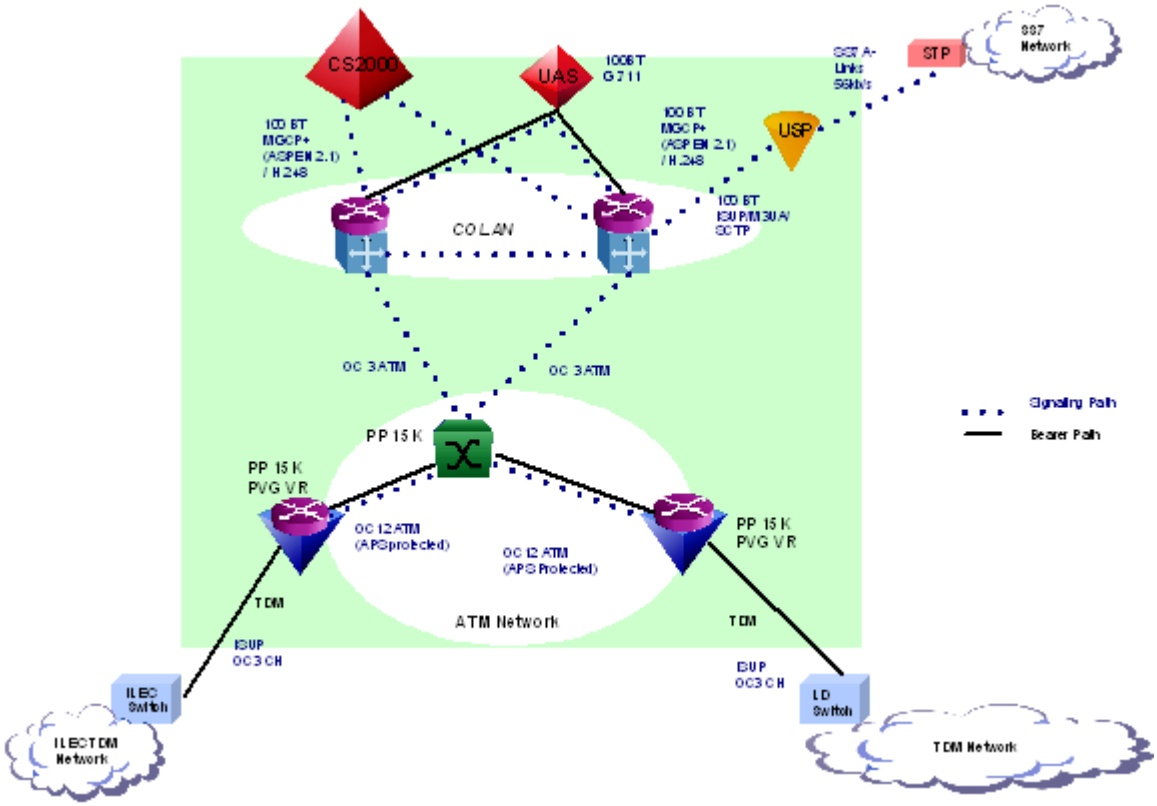
The Passport 15000 will support transport and routing of IP over ATM, using AAL5 for bearer traffic, signaling and OAM.

It is required that PVGs within a single CS2000 node implement the Virtual Router on the PVG shelf. This is required to optimize capacity as well as to aggregate the signaling and OAM traffic back to the CS LAN.

**Single Node CS2000 Office**

The PVGs served from a single CS2000 will be fully meshed with PVCs interconnecting each PVG. Static routes are used to route the bearer traffic between PVGs. OSPF is used to route the signaling control messages, OAM and any bearer traffic between the PVGs and the Passport 8600 CS LAN.

**Figure 28 Succession VoIP Network for Intra-CS2K Office Traffic**



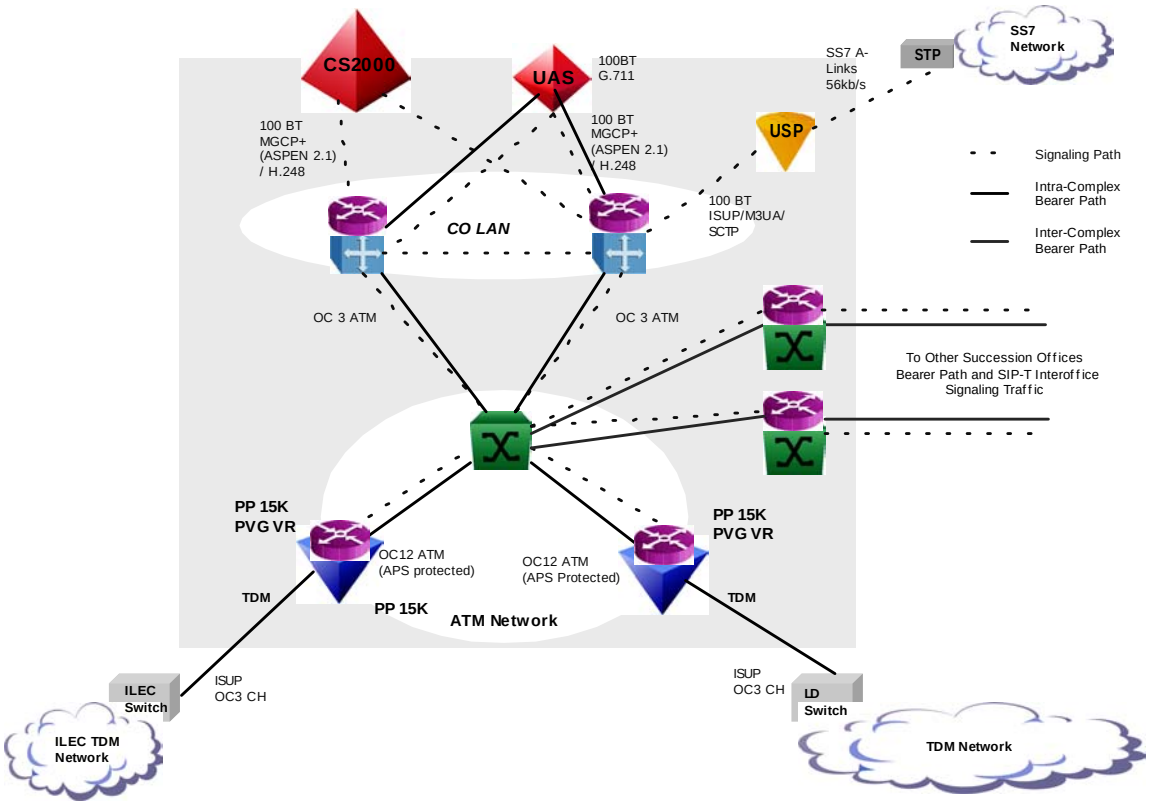

For this scenario, bearer traffic is exchanged between PVG VRs. Passport 8600 is located in the OSPF backbone and provides the route to MGC for all VSP cards. Static routes are added on PVG VR to route the bearer between them.

**Multiple CS2000 Offices**

When there are multiple CS2000 nodes in the network, bearer path interconnection between gateways supported by two different CS2000, can be routed over the Passport 15000 backbone. This is termed Dynamic Packet Trunking. In this instance, an aggregation VR, or router, should be deployed to groom the interoffice traffic, as it becomes impractical to fully mesh all the PVGs between nodes.

The aggregation VR will be fully meshed with every PVG supported by its associated CS2000. On the WAN side, the aggregation VR will be fully meshed with all other CS2000 in the network.

Succession VoIP Network for Inter-CS2K Office Traffic




A later chapter details the interconnection of the PVG to the Passport 15000. This also details the capacity of the Passport Virtual Router. Interconnect with the CS-LAN is detailed in the section titled See “CS-LAN Core Network Connectivity” on page 60..

***Note:*** In SN06, Succession solutions which utilize gateways, such as the IW-SPM, which only support gigabit ethernet connectivity should be based on native IP access or core routers. The Passport 15000 is expected to support a 4 port gigabit ethernet blade in a future release. See “Passport 15000 Core” on page 74. for details regarding this configuration.

### 3.2.5 OM8000 Core

To be added in a subsequent release of this document.

### 3.2.6 Juniper Core

A later section details the interconnection of the PVG to the Juniper M-series routers. The section on See “CS-LAN Core Network Connectivity” on page 60. details the connectivity of the Passport 8600 to the Juniper M-series. Specific network engineering guidelines for configuring a Juniper core network for Succession are not available in this document.

### 3.2.7 Cisco Core

Specific engineering and configuration details for interconnecting Cisco core routers with Succession are expected to be available under a Nortel integration service.

# 4.0 Access / Metropolitan Access Network Engineering

## 4.1 Access Network Topology

To be provided in a subsequent release of this document.

## 4.2 Passport 8600 as an Access Router

Within the Core Network, the Passport 8600 can be used in the following configurations:

- to aggregate PVG traffic with gigabit ethernet connectivity between Passport 8600 and PVG; the WAN interfaces should also be gigabit ethernet
- as a Cable Hub router in the IAC solution, with gigabit ethernet WAN interfaces
- an access router for small line gateways

### 4.2.1 WAN Ports

Gigabit ethernet is supported by Succession on the WAN interfaces of the Passport 8600. Redundant links should be set up from each of the pair of 8600s. OSPF should be used, as described in the CS LAN section on WAN connectivity.

OC3 or OC12 ports may be used, but should be used with great caution as the Passport 8600 ATM MDA capacity is limited. The maximum throughput to support good speech quality on the ATM MDA on the Passport 8600 is constrained as shown in the table below. Only 1 OC3 port on the 4port OC3 MDA can be used. OC12 is not supported as the throughput is no better than the OC3.

**Table 4 Passport 8600 ATM-E MDA Voice Connection Throughput**

| Encoding | G.711 10 msecs | G.711 10 msecs | G.711 20 msecs | G.711 20 msec |
|---|---|---|---|---|
| | OC3 | OC12 | OC3 | OC12 |
| # voice connections | 930 | 1032 | 1104 | 2016 |
| Management threshold # voice connections[a] | 820 | 1000 | 1050 | |
| Ports supported at 3.6ccs | 7585 | 9303 | 9788 | 1908 |

a. This is the threshold value at which traffic may begin to degrade due to packet loss. It is based on lines generating 3.6ccs high day traffic. Different ccs rates will change the number of ports supported.

Unlike when connecting a PVG to the Passport 8600, there is no admission control when using the Passport 8600 as a (concentrating) access router for small line gateways. The traffic from the remote gateways should be engineered such that High Day Busy Hour traffic, as measured on a 30 minute sample, should not exceed the threshold on the number of speech channels identified

above. This will allow for normal short term peakedness of the traffic to stay below the threshold where speech quality will be degraded due to packet loss.

Referring to the last two rows of Table 4, 820 channels can carry traffic from 7585 lines, generating 3.6 ccs High Day traffic.

The customer will be required to monitor the OC3 link usage to ensure the traffic stays below this level. In the event that the traffic approaches this level, then a 2nd OC3 WAN interface may be potentially be added, utilizing ECMP to spread the traffic over the two links. This is NOT currently verified within a Succession solution. There will be an increased need to monitor the link utilization to ensure traffic stays below the limits above.

### 4.2.2 Access Ports

Redundant gigabit ethernet links are supported to carry both voice and data traffic from Layer 2 aggregation devices in the access network. SMLT should be configured on these links.

Redundant OC3 links may also be used, with the same caution on throughput and thresholds on the number of simultaneous voice channels as stated above.

### 4.2.3 Other Configuration Items

DHCP Relay

Since the line media gateways in the CPEAH get their configuration from the service provider's network, the DHCP server providing the auto-configuration capability will be in the service provider's network, particularly in an OAMP subnet. Since the DHCP server is not in the same subnet as the line media gateways in the CPEAH, the Passport 8600 will need to relay the DHCP server to the Succession DHCP servers.The DHCP offer message sent back by the DHCP server provides the IP address, netmask, FQDN, DNS server address, TFTP server, configuration file path, RMGC address as well as other parameters.In case PPPoE is not used for the data service, data subscribers will be getting their IP address with DHCP; in this case the Passport 8600 will need to relay DHCP request based on VLAN memberships. The Passport 8600 has the ability to relay DHCP messages toward several DHCP servers based on the VLAN membership of the DHCP clients. This feature of the Passport 8600 will need to be used.

## 4.3 Data Services Engineering

To be added in a subsequent release of this document.

### 4.3.1 Shasta

To be added in a subsequent release of this document.

# 5.0 Network Surveillance

With the convergence of voice and data and the increasingly and carrier grade rservice expected, network management tools should be used to ensure continued performance.

## 5.1 Tools under evaluation

Several performance analysis and surveillance tools are available to proactively monitor and troubleshoot networks. These tools will be evaluated and further documented as we move forward.

### 5.1.1 Optivity

Optivity Network Management System is a comprehensive network management solution. Its key features include fault management, performance analysis, reporting, and access level security. Optivity Network Management System is based on a client/server architecture that supports today's popular operating systems. It provides powerful visualization and drill-down capabilities that allow network managers to troubleshoot and isolate network problems, and it offers core service capabilities that provide a strong foundation for fault, topology, and statistics gathering for the Nortel Networks family of products. Optivity Network Management System applications are engineered to be network-driven to support new hardware, helping network managers to quickly incorporate new equipment under a single management system.

### 5.1.2 MRTG

The Multi Router Traffic Grapher (MRTG) is a tool to monitor the traffic load on network-links. MRTG generates HTML pages containing graphical images which provide a LIVE visual representation of this traffic. It shows the bandwidth utlization over time.

Refer to www.mrtg.org for additional information.

### 5.1.3 Argus

Argus is a powerful tool for monitoring IP networks. It provides tools for sophisticated analysis of network activity that can be used to verify the enforcement of network security policies, network performance analysis and more.

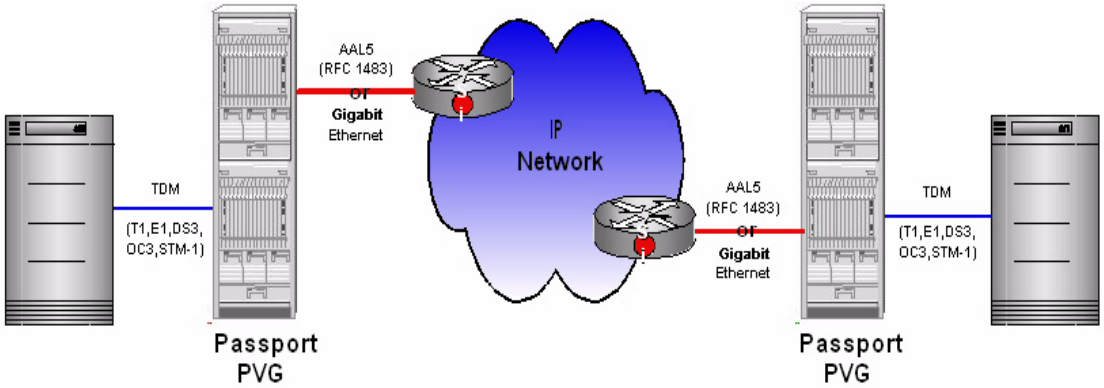
# 6.0 Trunk Gateway Site

This section discusses Engineering of different Trunk GWs, the Packet Voice Gateway (PVG) and AudioCodes Mediant 2000 (M2K).

## 6.1 Packet Voice Gateway

PVG acts as a gateway between the IP network and the time division multiplexing (TDM) switches in service provider networks. A typical PVG configuration is displayed in Figure 29.

**Figure 29 Typical PVG Media Gateway configuration - VoIP over ATM**




As depicted in the above figure, the TDM trunk connection to the PVG can be through channelized DS3s, E1s or OC3/STM-1s and the IP connection can be through ATM AAL5 (RFC 1483, obsoleted by 2684) or Gigabit Ethernet.

The PVG TDM Function Processors (FPs) provide the interface to the TDM network. They provide physical termination of the 2 port DS3 or 32 port E1 and OC3/STM-1 together with multiplexing/de-multiplexing of the DS0s from the DS1, E1, DS3, OC3/STM-1.

The PVG VSP FPs implement all voice services like tone generation, announcement playout, echo cancellation (ITU-T G.168). They also handle packetization of voice samples into RTP, together with the UDP and IP layers. Furthermore, they implement Media Gateway Control Protocol, or ASPEN 2.1, and MEGACO (H.248) message handling and IP datagram encapsulation using AAL5 and RFC 1483 (obsoleted by 2684) for ATM, and Ethernet for the VSP3.

The PVG supports either OC3 or OC12 for an ATM connection to the router. The router must support InATMARP (RFC 1577). ATM FPs implement all ATM layer and corresponding physical layer requirements, including ATM OAM functionality and ATM emission priorities. With the availability of the Gigabit Ethernet interfaces on the VSP3 faceplate, it is now possible to directly interconnect the PVGs to the IP network via Ethernet.

The PVG 7000 is housed in a Passport 7400 shelf. The Passport 7400 has 16 available slots.

- Slots 0 and 15 are dedicated for the Primary and spare control processor (CP) cards
- Fourteen slots are dedicated for function processors (FPs).
- On PVG 7000, the VSP2 FPs are Dual-slot processors.

The PVG 15000 is housed in a Passport 15000 shelf (NEBS 2000 frame). The Passport 15000 is installed in a frame that can hold two independent switches. Each Passport 15000 switch has 18 slots.

- Slots 0 and 1 are dedicated for the primary and spare control processor (CP) cards
- Fourteen slots are dedicated for function processor (FP) cards that are connected to fabric cards
- Two slots are reserved for future use

The PVG 20000 is similar to the PVG 15000 since they are both housed in the same Passport frame (NEBS 2000 frame). The Passport 20000 shares much of the Passport 15000 hardware, however the shelf assembly of the Passport 20000 has been re-designed with a scalable back-plane, ship-in-place hardware, and different plug-ins.

The Passport 20000 operates by the same Passport Carrier Release (PCR) software as the Passport 7000 series and the Passport 15000. Also, Processor cards from a Passport 15000 or 20000 can be shared.

***Note:*** Since the Control and Function Processor cards are common between the Passport 15000 and 20000, the PVG application of the PVG 20000 is identical to PVG 15000. Therefore, throughout this document, any PVG 15000 reference is applicable to PVG 20000 unless otherwise noted.

The two fabric cards interconnect the processor cards. Each processor card has redundant serial links to the two fabric cards.

The system requirements for a PVG include installing a Passport switch that contains the following hardware pieces:

- Control processor in a 1:1 sparing
- Voice services processor (VSP) function processor (FP) in a 1:1 or N:1 sparing. (N<= 4 on PVG 7000, N = Unlimited, constrained by available slots on PVG 15000)
- TDM FPs which may be 32 port E1, 2 port DS3 or 4 port OC3/STM-1 Ch
- ATM FP SONET/SDH for interconnect to the IP network via ATM
- If using VSP3s, option of the Gigabit Ethernet ports off the faceplate for interconnect to the IP network

Lastly, for VoIP, the PVG's interconnection to the IP network, e.g. ATM or Gigabit Ethernet, has to provide means of communications between the Media Gateway (PVG) and the Media Gateway Controller (MGC) in the CS-LAN.

## 6.2 Anchor Packet Gateway

The concept of an Anchor Packet Gateway (APG) comes from the need to access and manipulate the bearer channel associated with a call from a call context that normally would not have access to the bearer channel. In a typical two-party call between two PVGs, the services which are executing on behalf of either the originating party or the terminating party have access to the bearer path and the physical end-point via the PVG it serves. The core directs the PVG (via the GWC) to collect digits, apply local tones, or manipulate the connection between the two gateways. This is not the case, though, if one or both of the parties in the call is a dynamic packet trunk, or DPT. In these scenarios,

only call control signaling is received and processed by the CS2K from the dynamic packet trunk portion of the call. A dynamic packet trunk cannot use a media control protocol to access the bearer path because no physical gateway is currently associated with it.

An APG provides a physical device so that the DPT context can terminate and access the bearer path associated with a call. The DPT can instruct the anchor packet gateway to perform actions on the bearer path such as collecting digits, applying a tone, or redirecting the destination of the connection. The anchor packet gateway provides a DPT context to manage the bearer stream. Once the bearer path in anchored, it cannot be moved, i.e., it remains inserted for the duration of the call. Figure 30 illustrates the APG usage

**Figure 30 SIP-T Call Flow with APG**

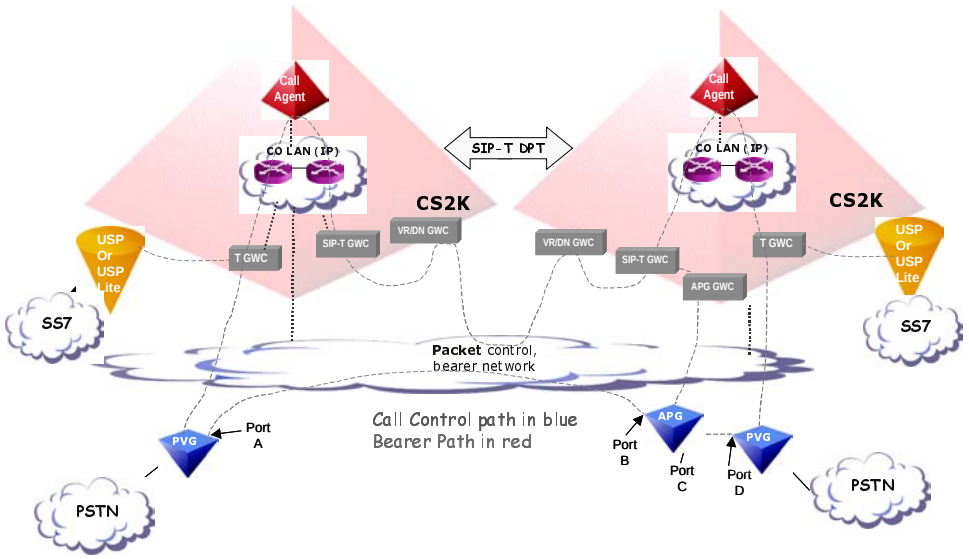
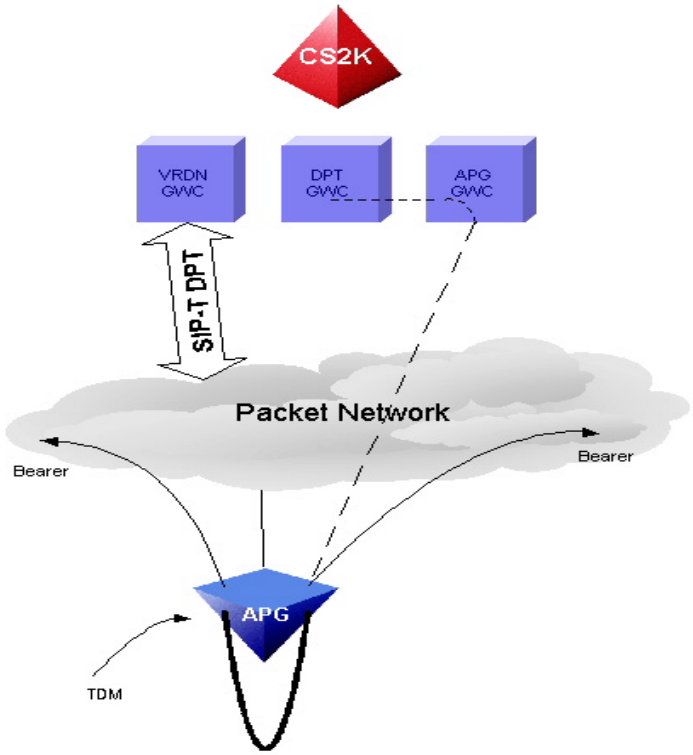



Figure 31 illustrates the APG use in the packet network. A DPT call using the APG would require two connection appearances on the APG. These two end-point connections are joined on the TDM–-side of the connection by a physical loop of the DS3/OC3 carrier. Utilizing the previous figure in conjunction with Figure 31, one can see that the bearer path from PVG Port A would terminate on the APG port B, then loopback through the TDM DS3/OC3, egress out Port C of the APG, then terminate on the ingress port D of the PVG subtending the second CS2K.

**Figure 31 APG Call flow**




***Note:*** An APG requires a dedicated VSP card. The VSP configured as an APG cannot also be used as a TDM trunk gateway.

The APG has identical addressing requirements to that of the PVG Trunk Gateway. For details on PVG IP addressing requirements, see section “6.5 IP addressing requirements” on page 86.

## 6.3 VSP capacity

### 6.3.1 Channel capacity

Each VSP FP type has different DS0 capacity levels with different CODECs. However, the actual DS0 capacity may not lead to an integral number of DS1s or E1s, and since the Succession CS2000 Management Tools prevent datafilling partial carriers, the usable number of DS0s for Suc-

cession MAY be lower that the VSP's true DS0 capacity. Table 5 summarizes these capacity levels for PVG 7000 and PVG 15000 for Succession.

**Table 5 PVG 7000/15000 VSP capacity**

| PVG | VSP | CODEC Type | VSP supported DS0s | Succession supported DS0s based on | | | | SPM total Monitored/Unmonitored Channels |
|---|---|---|---|---|---|---|---|---|
| | | | | using DS1s | | using E1s | | |
| | | | | DS1 | DS0 | E1 | DS0 | |
| PVG 7000 | VSP2[1] | G711 | 1008 | 42 | 1008 | 32 | 992 | 40 V5.2 C/D Channels or 40 PRI D-Channels |
| | | G729a/b | 720 | 30 | 720 | 23 | 713 | |
| PVG 15000 | VSP2[2] | G711 | 1120[3] | 46 | 1104 | 36 | 1116 | 40 V5.2 C/D Channel or 40 PRI D-Channels |
| | | G729a/b | 800 | 33 | 792 | 25 | 775 | |
| | VSP3[2] | G711 | 2016 | 84 | 2016 | 65 | 2015 | 64 V5.2 C/D Channels or 84 PRI D-Channels |
| | | G729a/b | 1512 | 63 | 1512 | 48 | 1488 | |

***Note:*** [1] Capacities stated are with or without the 32ms ECAN.

***Note:*** [2] Capacities stated are with or without the 32/128ms ECAN. PVG ECAN will not affect the VSP density.

***Note:*** [3] This is an example for a VSP2 supporting 1120DS0s, however since 1120 DS0s does not lead to an integral number of DS1s or E1s (1120/24=46.6666), the available number of DS0s is either 1104DS0s (46*24) or 1116DS0s (36*31).

### 6.3.2 BHHCA capacity

Busy Hour Half Call Attempts (BHHCA) is the number of half call attempts made during the busiest hour of the day. It is used as the measure for capacity of a VSP in one hour. As the VSP provides the connection services for one half of the call, another VSP is required to complete the connection. A VSP handles half of the messages for a particular call model. BHHCA is twice the Busy Hour Call Attempts (BHCA).

In contrast to ISUP/PRI calls, V5.2 calls require additional messages per call which results in reduced maximum BHHCA that warrants close consideration during network design.

Table 6 summarizes the POR committed BHHCA numbers:

**Table 6 BHHCA numbers for VSP2 and VSP3**

| Service | VSP2 | VSP3 | Signalling |
|---|---|---|---|
| ISUP/PRI | 24K | 43.5K | Aspen with HSM/HEP, H248 no HSM/HEP |
| V5.2 | 14K | 22K | Aspen, H.248 no HSM/HEP |

## 6.4 TDM Access

Each VSP can support either DS1 or E1 carriers, where the GWC can support both DS1 and E1 carriers since different VSPs(GWs) may be controlled via a single GWC.

The VSP3 (PVG15000/20000 only) supports both legacy TDM (2PDS3, 32pE1) cards as well as the 4 port OC3/STM-1 Ch TDM cards.

## 6.5 IP addressing requirements

Each Passport CP FP requires an IP address for the OAM management port. There is also an optional IP address used for debug purposes. The majority of PVG's required IP addresses are consumed by the individual VSP address requirements.

### 6.5.1 VSP2 and VSP3 - IP over ATM

Each VSP card can have up to three IP addresses associated with it:

- A media IP address,
- A control IP address for the Media Gateway (Aspen control, H.248),
- An optional control IP address for the Signalling Gateway (PRI, V5.2 backhaul).

For PVG using IP, SPVCs(Internally) and PVCs(Externally) must be used for the AAL5 VCCs carrying the Media traffic. For VCCs which carry control information (Aspen, H.248, or SCTP control Messages) you may use both PVCs as well as SPVCs.

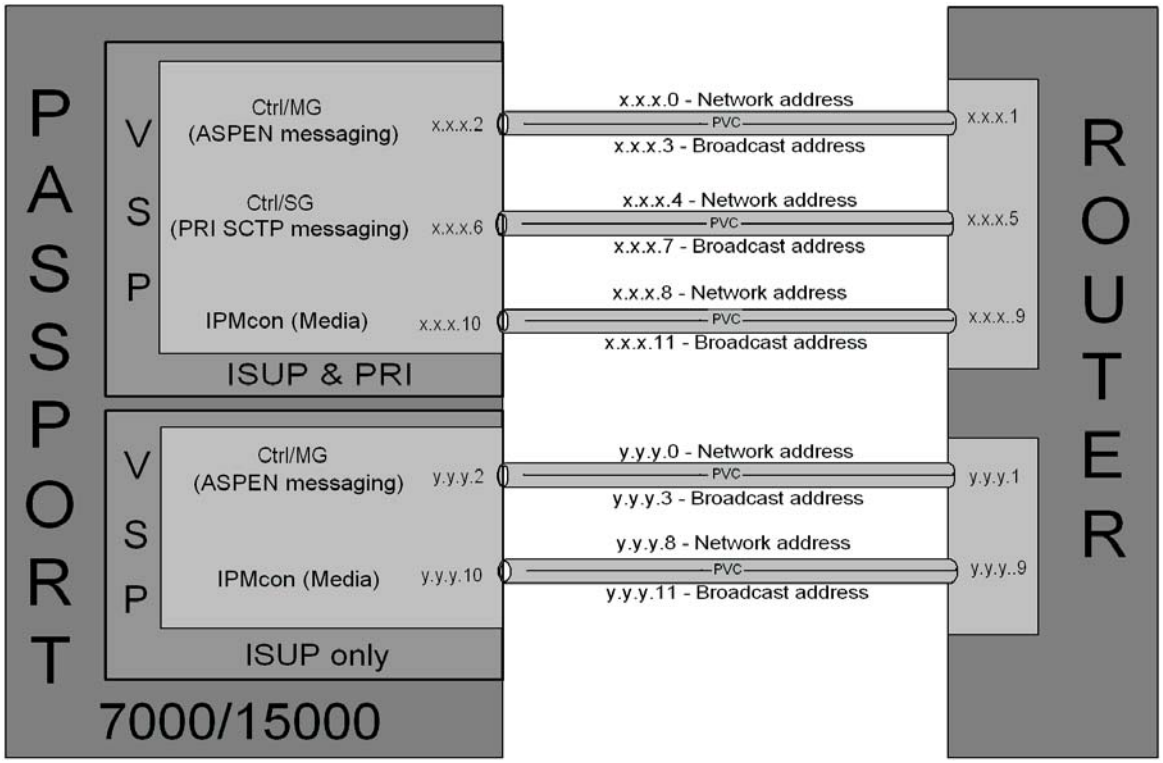
***Note:*** If utilizing PVG HSM/HEP, SPVCs must be used.

As illustrated in Figure 32, for PVG ATM interconnection to the Router, each Media Gateway (VSP), may require 2 or 3 PVCs depending on the type of traffic supported.

Each PVC will require 4 IP addresses. To conserve the number of IP addresses, it is suggested to use /30 subnet masks per PVC. For each /30 subnet 4 IP addresses are used as described below:

- 1 address is used as the Network address,
- 2 addresses are used for the VSP and the remote end (Router),
- 1 address is the Broadcast address.

**Figure 32 VSP IP addressing for ATM PVCs**




***Note:*** If PRI backhaul is to be supported, the IP address of the Control Signaling Gateway must be configured as IP address of the Control Media Gateway + 4.

***Note:*** Also note that the subnet mask is assigned on the interconnecting router and not on the PVG.

Table 7 details the IP address assignments of a single VSP2 or VSP3 card supporting ISUP and PRI and interconnecting to the Packet network via IP over ATM:

**Table 7 Total IP address assignment for a single VSP (IP over ATM)**

| | PVG | Router (PP8600, Juniper M Series) | Number of required IP addresses |
|---|---|---|---|
| Media Gateway (Ctrl/MG) | 1 | 1 | 4 (including Network & Broadcast addresses) |
| Signaling Gateway (Ctrl/SG) | 1 | 1 | 4 (including Network & Broadcast addresses) |
| Media (IPMconn) | 1 | 1 | 4 (including Network & Broadcast addresses) |

**Table 7 Total IP address assignment for a single VSP (IP over ATM)**

| | PVG | Router (PP8600, Juniper M Series) | Number of required IP addresses |
|---|---|---|---|
| Total of IP addresses for 1 VSP FP with ISUP and PRI service | | | 12 |

***Note:*** Spared VSPs DO NOT require additional IP addresses. The same IP addresses of the failed VSP will be used by the spare VSP once it takes over the role of the failed VSP.

Table 8 shows an example **PVG 15000** shelf with 6 VSP FPs (5:1 sparing), with provisioned ISUP & PRI services, requires a total of **61** IP addresses.

**Table 8 PVG 15000 with 6 VSP FP configuration IP address requirement**

| Element | Number of required IP addresses |
|---|---|
| PVG CP | 1 |
| VSP (5:1 Sparing)<br>5 X 12 | 60 |
| Total | 61 |

### 6.5.2 VSP3 -IP over Ethernet

***Note:*** This feature is only available on PVG 15000.

With the availability of the Gigabit Ethernet port on the VSP3 FPs, it is now possible to interconnect the PVG 15000 to the IP network via IP over Ethernet. Use of this feature requires a L2/L3 capable device such as the Passport 8600.

In addition to the three IP addresses (Ctrl/MG, Ctrl/SG, IPMconn) described in previous section, when using Gigabit Ethernet, an additional IP address needs to be provisioned. This address is the default gateway of the VSP3 and is the next hop address. The corresponding subnet mask also needs to be provisioned.

All the addresses, the Media (IPMconn), the control Media Gateway (Ctrl/MG), the optional control Signalling Gateway (Ctrl/SG), and the default gateway, must be configured in the same subnet. The maximum supported subnet size is /22 or 255.255.252.0 which limits the number of available hosts for that subnet to 1022.

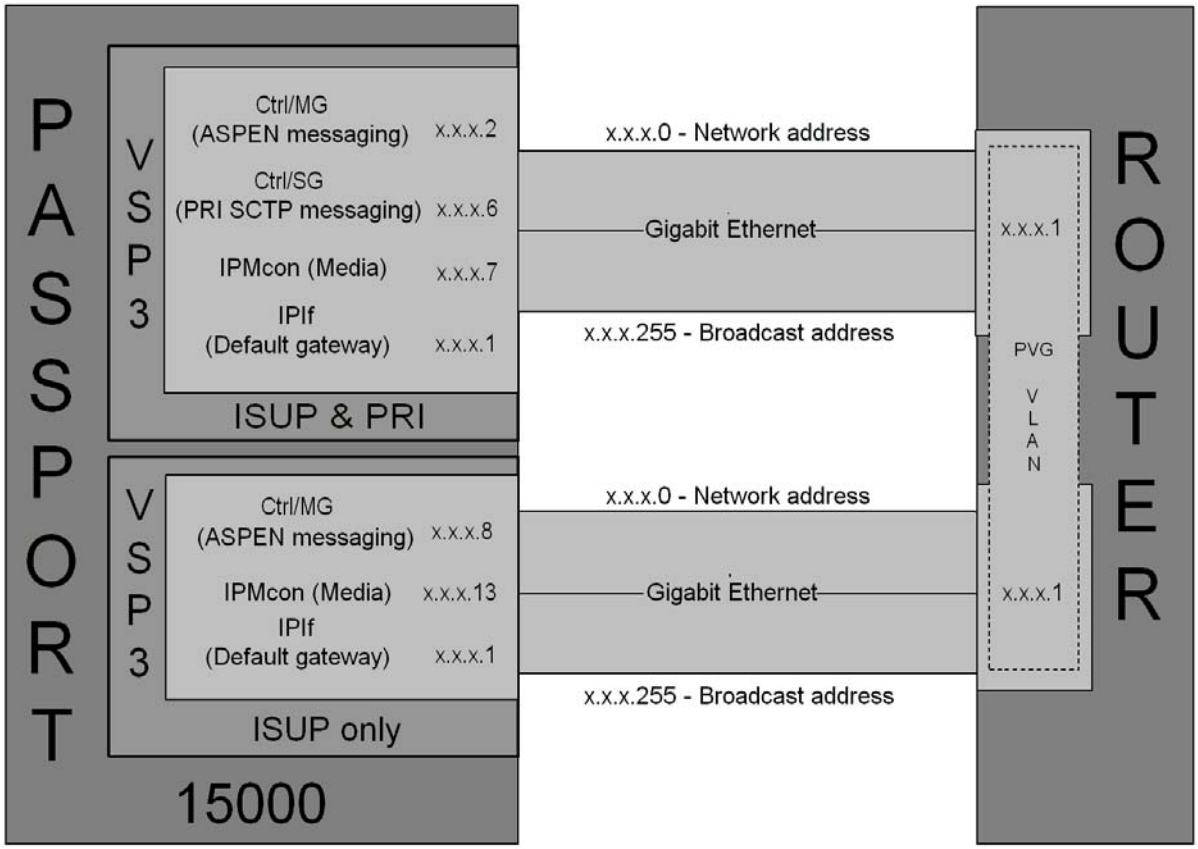
> ***Note:*** The Control Signaling Gateway IP address must be Control Media Gateway IP address + 4.

The default gateway IP address and the subnet mask is the IP address of the interconnecting router, and is provisionable under the IpInterface subcomponent of the VGS as "defaultRouterAddress" and "subnetMask".

As illustrated in Figure 33, the number of IP addresses required by each VSP3 differs based on the provisioned services. In this example, first VSP3 is provisioned for both ISUP and PRI backhaul, and it requires 3 addresses, where the second VSP3 only requires 2 addresses.

***Note:*** The IpIf address is common between the VSP3s and is the address of the interconnecting router (VLAN).

**Figure 33 VSP3 IP addressing for Gigabit Ethernet**




***Note:*** If PRI backhaul is to be supported, the IP address of the Control Signaling Gateway must be configured as IP address of the Control Media Gateway + 4.

Make note that the above example simply illustrates the use of a 255.255.255.0 (or /24) subnet mask and not enforcing any rules. The simple rule is that, the subnet mask used needs to support at least the total number of VSP3s that will be present in the PVG shelf.

Table 9 details the address assignments of a **PVG 15000** with a single VSP3 card supporting ISUP and PRI services and interconnecting to the IP network via Gigabit Ethernet:

**Table 9 Total IP address assignment for a single VSP3 (Gigabit Ethernet)**

| | PVG | Router (Passport 8600) | Number of required IP addresses |
|---|---|---|---|
| Media Gateway (Ctrl/MG) | 1 | | 1 |
| Signaling Gateway (Ctrl/SG) | 1 | | 1 |
| Media (IPMconn) | 1 | | 1 |
| IpIf (Default Gateway) | 1 common between VSP3 and router | | |
| Total IP addresses for 1 VSP3 FP with ISUP and PRI services | | | 4 |

Table 10 shows an example **PVG 15000** shelf with 6 VSP3 cards (5:1 sparing), all in the same sub-net, with provisioned ISUP & PRI services, requires a total of **17** IP addresses:

**Table 10 PVG 15000 with 6 VSP3 FPs configuration IP address requirement**

| Element | Number of required IP addresses |
|---|---|
| PVG CP | 1 |
| VSP3 (5:1 Sparing) 5 X 3 | 15 |
| IpIf (default gateway or the PVG VLAN address on the router) | 1 |
| Total | 17 |

***Note:*** This is the total number of IP addresses that are used by the PVG and does not account for the remaining addresses as part of that subnet. For example, if we chose to use a 255.255.255.224 (or /27) subnet mask, there are 30 usable IP addresses in that subnet, however for the VSP3s we would only need 15 addresses plus 1 for the default gateway address. The remaining IP address in this case will not be used by the PVG configuration and is available for other devices on the same subnet. The CP address is not necessarily in the same subnet.

## 6.6 PVG Engineering

The PVG offers SS7 and ISDN PRI backhaul services. The PVGs are aggregated to an edge router prior to connecting to the managed IP core network.

Also as stated before, there is a certain minimum hardware requirement that makes a PVG, however this minimum hardware set may not satisfy the Trunk Gateway Site's capacity requirements.

To engineer the capacity of a Trunk Gateway Site we need to analyze the bandwidth and throughput requirements of the site, which is usually in the form of a certain number of trunks within a given BHCA level. Once we know the requirement for the site, then each PVG needs to be engineered for the optimum capacity and bandwidth. The next step would then be to determine the required hardware needed to support the necessary bandwidth for each PVG.

The calculated bandwidth has a direct impact on the PVG interconnection to the IP network. The selected interfaces and hardware on either the PVGs or the interconnecting router must provide sufficient bandwidth engineered to support the amount of traffic generated toward the IP network as well as intra gateway site.

Another important factor is eliminating single points of failure. The PVGs need to be interconnected to the IP network in a redundant fashion, providing the best Carrier Gradeness and resilient interconnection to the uplink routers. Again this puts additional requirements on the selected hardware.

### 6.6.1 Calculating bandwidth based on desired number of Trunks

To calculate the required bandwidth based on the number of trunks, it is best to define the bandwidth on a single call or a single DS0. The following sections provides an outline for DS0 bandwidth calculations based on different CODECs and sampling rates with respect to IP over ATM and IP over Ethernet (VSP3).

#### 6.6.1.1 VoIP over ATM

The VSP FPs support both G711 and G729a CODECs with 10 and 20 ms sampling rates. Example of a G711@10 ms call is provided as a guide to determine a per call IP bandwidth requirement, and can be used for all the possible CODEC and sampling rate combinations.

G711, 10 ms sampling example

A voice packet in an IP/AAL5 application using G711 @ 10 ms sampling rate has a voice payload of 80 bytes. There are additional header bytes for IP/UDP/RTP, 20 bytes for IP header, 8 bytes for UDP header, and another 12 bytes for RTP header. This makes a total of 120bytes packet size without the ATM encapsulations. For IP/AAL5 there is an additional 39 bytes for the ATM headers and padding since each packet is broken up over 3 ATM cells at 53 bytes per cell, for a total of 159 bytes.

Finally with G711 @ 10ms there are 100 packets generated per second, so each DS0 or a TDM port requires 159bytes*8bits*100 = 127,200 bits/second/DS0 or 0.1272 Mbps of egress bandwidth. This unit can be multiplied by the Number of Trunks to calculate the preliminary bandwidth calculation on the ATM connections to the IP network. The actual ATM connectivity is dependent on the selected PVG interconnectivity/resiliency scheme.

Also, Table 11 provides a summary of DS0 IP bandwidth requirement based on different CODECs and packetization for VoIP over ATM.

**Table 11 Different CODECs and packetization summary for IP over ATM**

| Item | G711 10ms | G711 20ms | G729a 10ms | G729a 20ms |
|---|---|---|---|---|
| Bandwidth/DS0 in Mb/s | 0.127 | 0.106 | 0.084 | 0.042 |

### 6.6.1.2 VoIP over Ethernet

The VSP FPs support both G711 and G729a CODECs with 10 and 20 ms sampling rates. Example of a G711@10 ms call is provided as a guide to determine a per call IP bandwidth requirement, and can be used for all the possible CODEC and sampling rate combinations.

G711, 10 ms sampling

The IP portion of the packet size for G711 @ 10ms is 120 bytes as calculated in the IP/ATM section above. The additional Ethernet overhead of 38 bytes brings the total packet size to 158 bytes. With 10ms sampling rate, we generate 100 packets per second, so each DS0 or a TDM voice port requires 158bytes*8bits*100 = 126,400 bits/second/DS0 or 0.126 Mbps of egress bandwidth. This unit can be multiplied by the Number of Trunks to calculate the preliminary bandwidth calculation on the Gigabit Ethernet connections to the IP network.

Also Table 12 provides a summary of DS0 bandwidth requirement based on different CODECs and packetization for VoIP over Ethernet.

**Table 12 Different CODECs and packetization summary for IP over Ethernet**

| Item | G711 10ms | G711 20ms | G729a 10ms | G729a 20ms |
|---|---|---|---|---|
| Bandwidth/DS0 in Mb/s | 0.126 | 0.095 | 0.070 | 0.039 |

## 6.6.2 OM Monitoring

The Preside Multiservice Data Manager (MDM) is a workstation-based network management system that is used to maintain and monitor a number of Passports and in turn the PVGs which are housed in them. MDM provides a centralized reporting vehicle for monitoring and reporting multiple PVGs, and their individual VSPs.

For detail information on MDM please refer to appropriate NTPs.

## 6.6.3 ECAN and VAD

See section "11.0 ECHO & Network Loss Plan" for related information.

## 6.6.4 lossIntegrationPeriod setting

The setting of the Loss Integration Period is dependent on whether you are running with silence suppression (VAD) enabled or not.

For IAD:

- If silence suppression is enabled, then the setting should be 0 (disabled) if using IAD.
- If silence suppression is OFF, then you should use the default 5 seconds.

For PVG to PVG:

- the loss integration period is at the default 5 seconds.

This provides a mechanism where the PVG is looking for RTP stream. If it loses RTP stream due to an IP network issue, it will tear the call down. Note - the 1st timeout is ignored when establishing a call - so if calls are being torn down after 10 secs - then it's likely that connectivity through the IP network is impaired.

***Note:*** For offices configured with Lawfull Intercept, the Loss Integration Timer needs to be set to 0.

### 6.6.5 Packet Delay Variation Tolerance and buffer size settings

#### 6.6.5.1 VSP2

For VSP2 which has a fixed de-jitter buffer and is based on the setting of the Packet Delay Variation Tolerance (PDVT) setting. This setting is effective on each Brag subcomponent (equivalent of a DS1/E1). For VSP2 the following formula should be used:

- PDVT should be set to twice the packetization period, i.e., if 20 ms packetization period is expected to be used, then PDVT = 40 ms
- Buffer size is then two times the PDVT + the Packetization, i.e. for 20 ms packetization the buffersize is 2 * pdvt + 20 = 100 ms.

#### 6.6.5.2 VSP3

The VSP3 has an adaptive de-jitter buffer and the setting for the PDVT is recommended to be either a measured delay across the network or set to the lowest possible setting which is currently 5ms. However it is recommended to set the PDVT to 0 when possible.

The VSP3 buffer size will adapt upwards very quickly based on the first 2 to 3 packets received and will not adapt to below the PDVT. The bufferSize attribute only set the maximum PDVT to which the adaptive de-jitter function will adapt to, but will still buffer packets to a maximum of 100 ms. Thus setting this value has no effect on the end-to-end delay and it is recommend to set this value to 100 ms.

### 6.6.6 Hardware engineering considerations

Each PVG 15000 has 16 usable slots per shelf. Slots 0 and 1 can only house the Control Processors; the remaining 14 slots can be used for other Function Processors such as VSP, DS3, etc. When trying to engineer the PVG 15000s and determining the required hardware we need to be aware of the total available slots. If the PVG is fully populated and Trunk Gateway site's capacity is still not reached, additional PVG shelves with the required hardware have to be installed and provisioned. When using the VR and the external Hairpin option on the PVG as a mechanism for the Inter connectivity to the Packet Network, additional hardware is required.

## 6.7 PVG Reliability Scheme

The PVG is built on the Carrier Grade Passport platform with well known Carrier Grade and reliability standards. However, before the availability of Hitless Software Migration (HSM) and Hot Equipment Protection (HEP) features, the full data path of the PVG services on the Passport 15000 were not protected. With the advent of HSM and HEP the PVG 15000 provides a high carrier grade service level during a software upgrade or a hardware failure/switchover.

### 6.7.1 Hitless Software Migration

Hitless Software Migration or HSM provides the capability to upgrade the shelf software without impacting the active services on the shelf. The PVG service providing FPs, i.e. VSP(2,3), STM-1/OC-3 Ch or the ATM FPs, must be provisioned in a 1:1 (1+1 for optical FPs) FP sparing configuration in order to use HSM functionality. Note that Legacy TDM FPs are not HSM protected.

During a software migration switchover, for a short period (no longer than 15 seconds - Telcordia GR-929) the PVG will not process any control messages received from the GWC, however the path heartbeats are processed within 2 seconds making HSM switchover transparent to the GWC.

### 6.7.2 Hot Equipment Protection

Hot Equipment Protection or HEP provides the hot standby level of protection for PVG services. Note that for this functionality all the PVG service providing FPs, i.e. VSP(2,3), STM-1/OC-3 Ch or the ATM FPs, must provide the HEP capability and provisioned as 1:1 VSP(2,3), 1+1 ATM FP, and 1+1 for STM-1/OC-3 Ch FP for sparing cofiguration. HEP is not supported for 1:N sparing configuration.

HEP has the same switchover behavior as HSM.

The resiliency, and failover performance, when interconnecting to the Core or the Access router is dependent on the choice of router. This is discussed in the following sections.

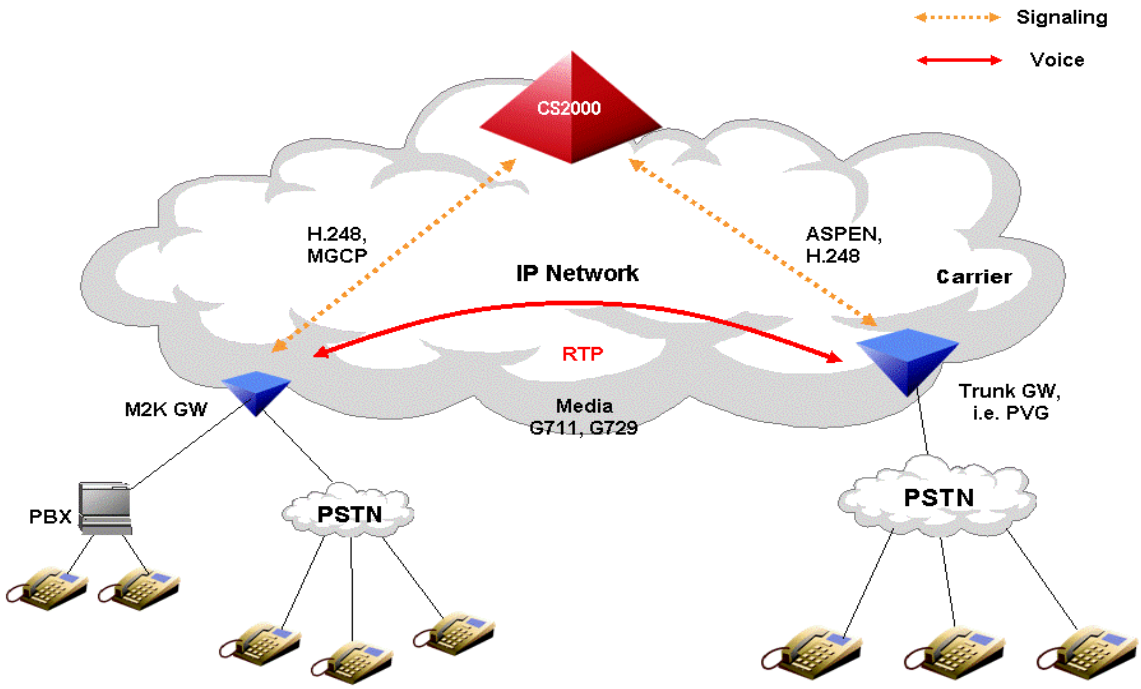
## 6.8 AudioCodes Mediant 2000 Trunk Gateway

> ***Note:*** Throughout this document the AudioCodes Mediant 2000 Trunk Gateway will be referred to as **M2K**.

The M2K is a Voice over IP Trunk access Gateway similar to a PVG with much smaller channel capacity (1 to 16 E1/T1 spans). On the IP (WAN) side, the M2K interconnects to the Packet Network via redundant 10/100 BaseT connections with a possibility of Gigabit Ethernet, fiber based port in the future. On the TDM side the M2K provides from 1 to 16 spans of E1 or T1 interfaces for connecting to, either PSTN telephony trunks directly or to an enterprise PBX.

A typical M2K configuration in a Succession deployment is displayed in Figure 29.

**Figure 34 Typical M2K Media Gateway configuration for Succession**




The M2K is equipped with a single compactPCI board front card (TP-1610), and Rear Transition Modules (RTM), either 1-span, 2-span, 4-span, 8-span, or 16-span where both the PSTN and the Ethernet interfaces are located.

> ***Note:*** The 16 span GW package is in reality two 8 span GWs with two separate IP addresses sharing the same physical link to the Packet network.

The TP-1610 cPCI VoIP communication board support all necessary functions for voice and fax packetization into RTP streams, as well as Voice CODEC selection, Echo Cancellation, Silence suppression, etc.,...

The following list highlights some of the features of the M2K:

- MEGACO (ITU-T H.248) and MGCP (RFC 2705) protocols for call control signaling
- G711 and G729A voice CODECs - can be selected per channel independently
- 32, 64 ms tail Echo cancellation compliant with G.168-2000 - 128 ms is also supported at lower channel density
- Adaptive jitter buffer
- T.38 fax relay over IP
- Silence suppression supporting VAD
- ISUP, ISDN PRI, CAS
- Embedded Web Server for management
- IP/RTP DSCP marking

## 6.9 M2K capacity

### 6.9.1 Channel capacity

As described above, the M2K can/may be equipped with 1, 2, 4, 8 and 16 E1/T1 Rear Transition Modules or RTMs. The channel capacity of the M2K then ranges from the minimum 24 DS0s in a 1 T1 span configuration to a maximum 496 DS0s in a 16 span E1 configuration.

### 6.9.2 BHHCA capacity

Busy Hour Half Call Attempts (BHHCA) is the number of half call attempts made during the busiest hour of the day. It is used as the measure for capacity of the M2K in one hour. BHHCA is twice the Busy Hour Call Attempts (BHCA). Table 6 summarizes the BHHCA capacity of M2K as provided by AudioCodes:

**Table 13 BHHCA numbers for M2K**

| M2K | H248 (PRI) | |
|---|---|---|
| | G711, 20ms | G729, 20 ms |
| **4 Span** | 36K | 10K |
| **8 Span** | 40K | 20K |
| **16 Span** | 80K | 40K |

## 6.10 TDM Access

As mentioned above, the M2K provides both T1 and E1 interfaces for TDM connectivity, however M2K **can only** be configured with either ALL T1 or E1 at a given time and not both. Each T1 or E1 can be configured for PRI or ISUP in the M2K.

A single GWC can/may manage several M2Ks with T1 and/or E1 carriers since GWC supports both T1 and E1. The total number of supported M2Ks per GWC may vary based on the proposed configuration, i.e., 4-span vs. 8-span M2Ks as long as the following rules are satisfied:

- Maximum of 4094 trunks per GWC
- Maximum of 24 large GWs associated with a single GWC
- Maximum BHHCA for PRI on a single GWC

So it is possible to associate 24 4-span (T1) M2Ks on a single GWC, and still be below the channel capacity of the GWC, i.e. 96 ch/GW * 24 GWs = 2304 vs. 4094. But when matching the BHHCA requirement, the 76K PRI limits the number of M2Ks that can be associated with a single GWC.

Refer to "Trunk-based Gateway Controller" of the "Network Element Traffic Engineering" section for detailed information on Engineering the GWCs.

## 6.11 Software requirements

M2K must be loaded with multiple software components before bringing it to service;

- An executable (.cmp) image firmware file, the operating software
- A configuration (.ini) ascii file, the M2K provisioning data
- An optional tones (.dat) file, Call Progress Tones generation

M2K is pre-loaded with the latest GA (.cmp) firmware load prior to shipment from AudioCodes, but may need to be upgraded prior to installation. Refer to upgrade procedures section for software upgrade instructions.

The provisioning data is captured in the .ini file which should be downloaded and stored in M2K's Non-volatile memory after the .cmp image file is downloaded to the M2K.

> ***Note:*** A default configuration (.ini) file will be provided by AudioCodes to ensure appropriate initial set up. It is recommended to use the provided .ini file as it defines values for a set of default parameters required for proper interworking between Nortel Networks equipment and M2K.

Once the default configuration file is loaded in the M2K any subsequent provisioning modifications should be performed via the M2K's Embedded WEB server. For some low level parameters which are not accessible via the WEB interface, modifying and reloading the ini file is the only option.

```
For example when using ISDN PRI, if/when there is a need to modify
the user/network termination side, the .ini file must be modified
and reloaded back to the M2K.
```

Upgrades to the M2K can be made via either an external BOOTP/TFTP server or HTTP using the embedded WEB server in the M2K. It is recommended to use the embedded WEB server as the primary method for software upgrades and configuration needs. For further instructions on either method refer to the accompanied AudioCodes documentation.

## 6.12 IP addressing requirements

The M2K requires a single IP address for OAM, CallP, and Bearer. This IP address is utilized for accessing the M2K's Embedded WEB server for management as well as all the Media and Non-Media traffic.

The M2K is shipped with a default IP address as listed in Table 14:

**Table 14 M2K default IP address and Subnet mask**

| Number of trunks | IP address | Subnet Mask | Default GW |
|---|---|---|---|
| **1 to 8** | 10.1.10.10 | 255.255.0.0 | 10.1.10.1 |
| **9 to 16** | 10.1.10.11 | 255.255.0.0 | 10.1.10.1 |

This IP address and its subnet mask must be modified according to the customer IP address domain. Also this address domain has to be reachable and visible by the CS-LAN for CallP and optional OAM.

***Note:*** It is recommended that this address space is contained in a subnet which is different from the existing subnets in the CS-LAN in order to segregate the M2K's traffic (Media and Non-Media) from CS-LAN's existing subnets.

For initial M2K configuration including IP address reassignment, refer to the accompanied documentation provided by AudioCodes.

## 6.13 M2K Engineering

As mentioned in the Software requirements section, the default .ini file provided by AudioCodes defines a minimum set of parameters and values required for basic operations of M2K in a Nortel Networks Succession environment.

Other parameter settings which are not included in the .ini file and are required for proper PRI interworking are listed in Table 15.

**Table 15 M2K parameter and value setting via the .ini file**

| Parameter | Value | Notes |
|---|---|---|
| IUAINTERFACEID_x, where x is the M2K's internal Span # starting from **0.** | See notes | D-Channel number that is datafilled in the SESM/Core. Must be set for each Span. |
| TERMINATIONSIDE_x, where x is the M2K's internal Span # starting from **0.** | 0 or 1 | User/Network termination side. Must be set for each Span. 0 = User, 1 = Network |

Further required provisioning such as IP address set up, Protocol configuration, MEGACO Call Agent (GWC) IP address set up, TDM settings and other miscellaneous site specific configurations should be done via M2K's embedded WEB configuration interface. M2K supports any standard web-browsing application such as Microsoft IE 5 and higher or Netscape Navigator 7 or higher for accessing it's WEB server. See AudioCodes accompanied documentation for detail instructions on how to access the WEB GUI.

**Trunk type considerations**

For PRI the M2K should be set up with "T1_IUA" Protocol type and for ISUP should be set up with "T1_Transparent". Note that with HKPRI trunk type, only T1s are supported and also Back Up D-Channels are also not supported.

M2K only supports the relay of ISDN signaling messages from the PSTN side to the GWC on the IP side via IUA/SCTP/IP. Once the trunks are brought in service, M2K is unable to provide a means of state changes or any ISDN parameter modifications via the WEB configuration interface. For example, after the trunk is in service, if/when there is a need to modify its user/network termination side of the D-Channel, the configuration file (.ini) file must be retrieved, modified, and reloaded back to the M2K for the changes to take effect.

> ***Note:*** Since this operation requires a Reset on the M2K, it is a service impacting operation and must be done during a maintenance window.

The M2K's Gateway, Trunk, and Endpoint names must match the datafilled Carrier name in the Succession CS2K Management Tools for proper endpoint representation as shown in Table 16:

**Table 16 M2K Gateway, Trunk, and Endpoint names match up**

| | Gateway name | Trunk name | End point Name |
|---|---|---|---|
| **M2K** | DS1 (T1_IUA) | /0 | / |
| **CS2K** | DS1/0x, where x = 1-4 or 8 | | /1-24 (Auto filled) |

### UDP port ranges

The Base UDP port number used by the M2K for all RTP messages has a valid range of 0-55000. The default lower boundary base UDP port is 4000. The upper boundary is equal to the lower boundary+10*(# of channels), and must be a multiple of 10. For example the valid range of the UDP ports for RTP messages for a 8 span M2K using the default base UDP port number of 4000 is 5920 as shown below:

Default UDP port = 4000

Lower boundary UDP port = 4000

Upper boundary UDP port = 4000 + 10 * (8*24) = 4000 + 1920 = 5920

It is recommended to leave the UDP port setting as default.

### Quality of Service considerations

Nortel Networks recommends the use of DiffServ Code Points (DSCP) for optimum service achievements. The recommended DSCP settings are:

**Table 17 DSCP settings**

| | DSCP setting | Value |
|---|---|---|
| **Voice Media** | EF | 46 (101110) |
| **Voice Signaling and T.38 Fax** | CS5 | 40 (101000) |
| **OAM&P** | CS6 | 48 (110000) |

Currently (SN06.2) M2K ONLY provides means of DiffServ settings on Media traffic. Nortel Networks recommends DS PHB setting of Expedited Forwarding (EF) for RTP packets.

When M2K provides Non-Media DS PHB setting capabilities, the DiffServ Code point should be set according to Table 17. While this capability is not available in the M2K, the DS Edge node must be set up to re-mark the M2K's Non-Media packets.

Refer to "Quality of Service" section for a full description of the Nortel Networks recommended QoS Engineering Rules.

**Signaling delay tolerance**

One of the metrics that determines the allotted geographical distance between the GW (M2K) and it's associated GWC, is the amount of tolerable delay on the signaling between the GW and the GWC while 100% call completion rate is achieved. 100% CCR was verified for up to 350ms bi-directing delay using an impairment device (PacketStorm).

**Intra M2K calls**

The M2K utilizes an internal Ethernet switch on the IP side. As a basic switch functionality all the traffic destined on the same subnet will be switched internally and will not leave the M2K toward the IP network.

### 6.13.1 OM Monitoring

M2K provides an embedded WEB server which is used for operational and management functionalists, utilizing any standard web-browsing application. It also provides run-time monitoring capabilities for Trunk and Channel status.

The M2K also provides a message log (syslog) capabilities that may be used for protocol logs as well as troubleshooting. A syslog server's IP address is configurable in the M2K WEB GUI.

### 6.13.2 ECAN and VAD

M2K sports G.168-2000 compliant Echo Cancellation with a 32, 64, or 128 (may reduced channel capacity) ms echo tail. ECAN is ON by default. Silence Suppression supporting VAD and Comfort Noise Generation (CNG) is also supported. Silence Suppression is disabled by default.

## 6.14 M2K Reliability scheme

On the IP side the M2K provides redundant 10/100 Base-T connection to the Packet network. This built in resiliency is on Layer 2 with failure detection on Ethernet layer.

The M2K has been tested with Dual 10/100 connections to two L2/L3 (Passport 8600s) utilizing VRRP functionality across the M2K VLANs for Layer 3 coverage. 100% Call Completion Rate (CCR) was maintained when an active link on the M2K was failed. The reported result by the traffic generator was verified using a Ping method as NO IP Packets were dropped.

M2K does not provide any Layer 3 resiliency, therefore layer 3 coverage must be provided by the Network Edge where the M2K is interconnected. See Figure 35.

Any software upgrade to the M2K will be service disruptive since there are no Hitless Software upgrades available at this time.

M2K supports both AC and DC power supplies. An optional Dual AC Power Cable Connectors is available.

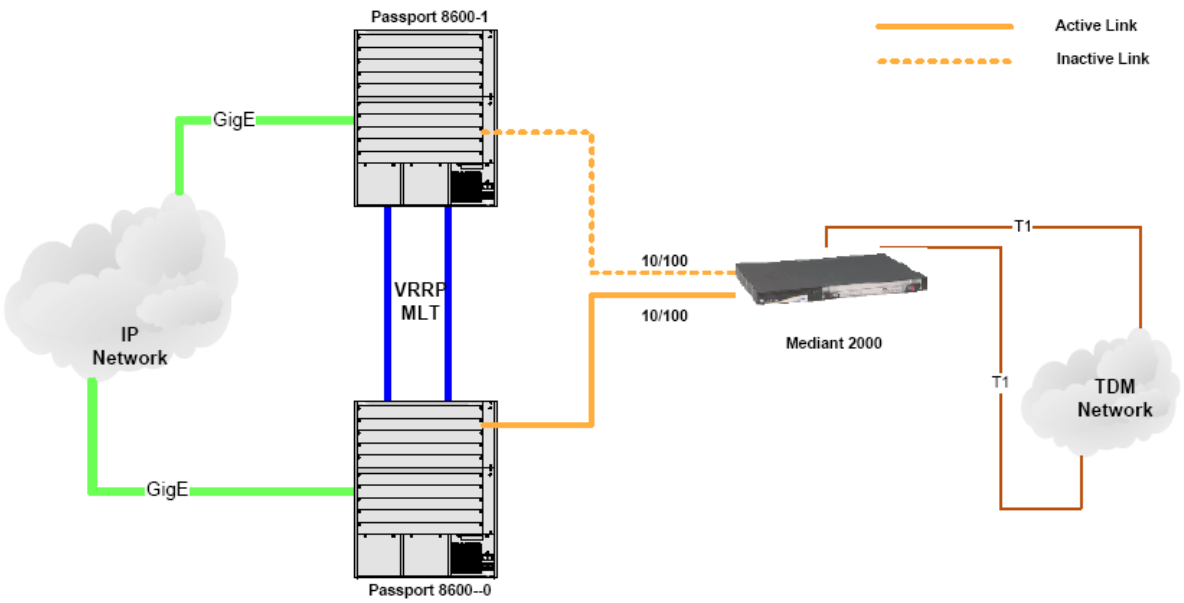
### 6.14.1 M2K inter connectivity to the Packet Network

The interconnecting device where the M2K will be connected must support:

- 10/100 BaseT Ethernet, (Gigabit Ethernet for future release)
- Auto Negotiation
- 802.1Q VLAN Tagging
- MLT and VRRP

For optimum carrier grade performance, the M2K must be interconnected to Dual L2/L3 devices (Interconnection to Passport 8600s has been verified as shown in Figure 35).

**Figure 35 M2K to Packet Network connectivity**



# 7.0 PVG to Packet network Interconnection Matrix

Table 18 lists the supported PVG inter connectivity to the IP network with different topologies.

**Table 18 Supported PVG interconnectivity matrix**

| Item | PP8600 | PP 15000 | PP 15000 VR | Juniper M Series |
|---|---|---|---|---|
| PVG VR (Hairpin) | | ÷ | ÷ (for Interoffice CS2K communications) | |
| PVG 15000 VSP3 (2port Gigabit Ethernet) | ÷ | | | |
| PVG 15000 VSP3 (OC12/STM-4) | ÷ | ÷ | ÷ | ÷ |
| PVG VSP2 (OC3/STM-1) | ÷ | ÷ | ÷ | |

In the following sections, each option is fully described with their full capacity.

## 7.1 Interconnecting to Passport 15000 — VoIP over ATM/AAL5

This section provides the general guidelines for interconnecting the Passport Voice Gateway (PVG) with a Passport 15000 based ATM network. Additionally, capacity and throughput limitations are provided in order to aid in the engineering of the VCCs and the ATM links on which they are carried.

This section intends to deliver the assessment of PVG VR together with configuration options to ensure PVG VR can provide seamless path to the IP network through Passport 8600/Passport VR. Interconnection.

### 7.1.1 Connection Summary

The PVGs served from a CS2000 must be fully meshed with PVCs interconnecting each PVG. Static routes are used to route the bearer traffic between PVGs. Additionally, PVCs from each PVG must terminate on the PP8600 for the purpose of carrying both OAM, connection control and signalling traffic (PRI). OSPF is used to route these messages between the PVGs and the PP8600 CS-LAN.

Use of static routes and OSPF on the PVG requires that the Virtual Router (VR) function be implemented on the PVG to support these capabilities. This is discussed in detail in the following section.

#### 7.1.1.1 PVG VR Options

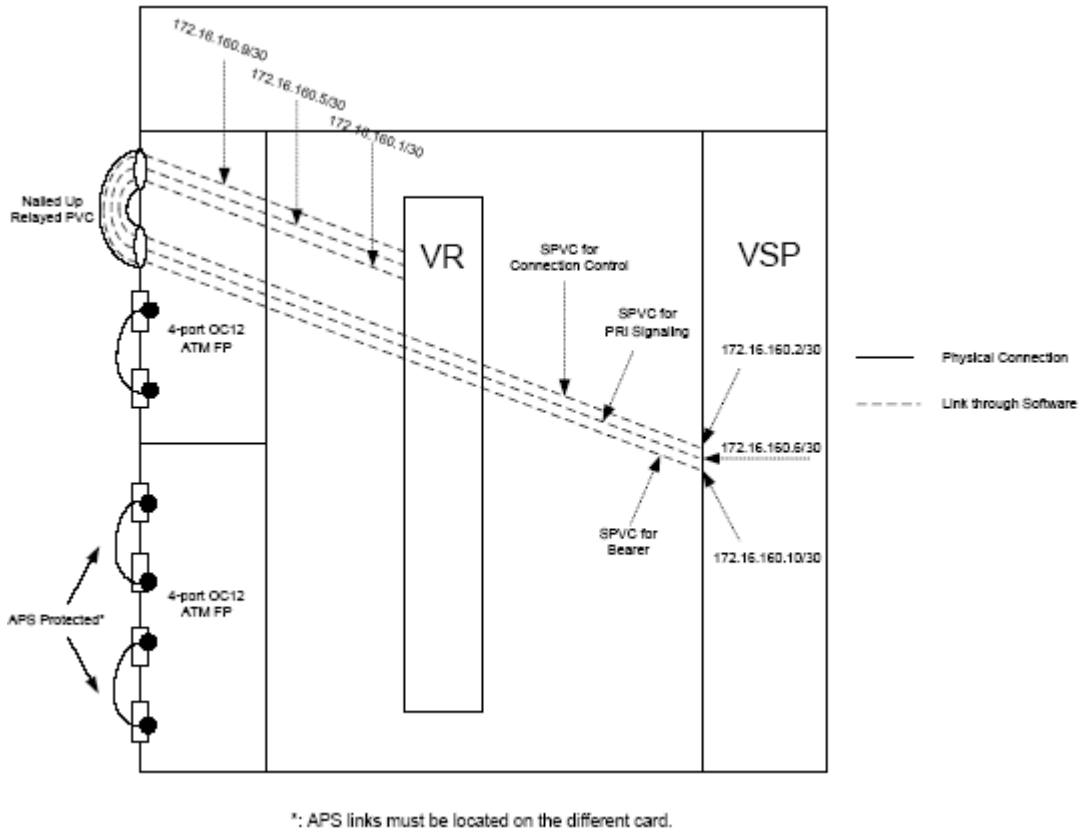
For SN06, implementation of the VR on the PVG has two options:

**Option 1: Local Hairpin**

As discussed earlier, the VR is required locally on PVG to support fully meshing the PVGs, as well as, to improve the nodal capacity and throughput performance. The PVG VR can also eliminate a potential VCC issue coming from Passport 8600s MDA modules.

Prior to SN06, setting up the VR on PVG requires hairpinning of ATM ports. The hairpin loop around provides the means for SPVCs to terminate on a Protocol Port on a local PVG VR. These VCCs are originated from each single VSP card to carry connection control messages, PRI signaling and bearer traffic. The following diagram illustrates the setup of the hairpin.

**Figure 36 Hairpin Connection**




As depicted in Figure 36, this configuration utilizes two ATM FPs to cover a single VSP card. One ATM card hosts the hairpin "working" connection and another one provides APS "protected" connections.

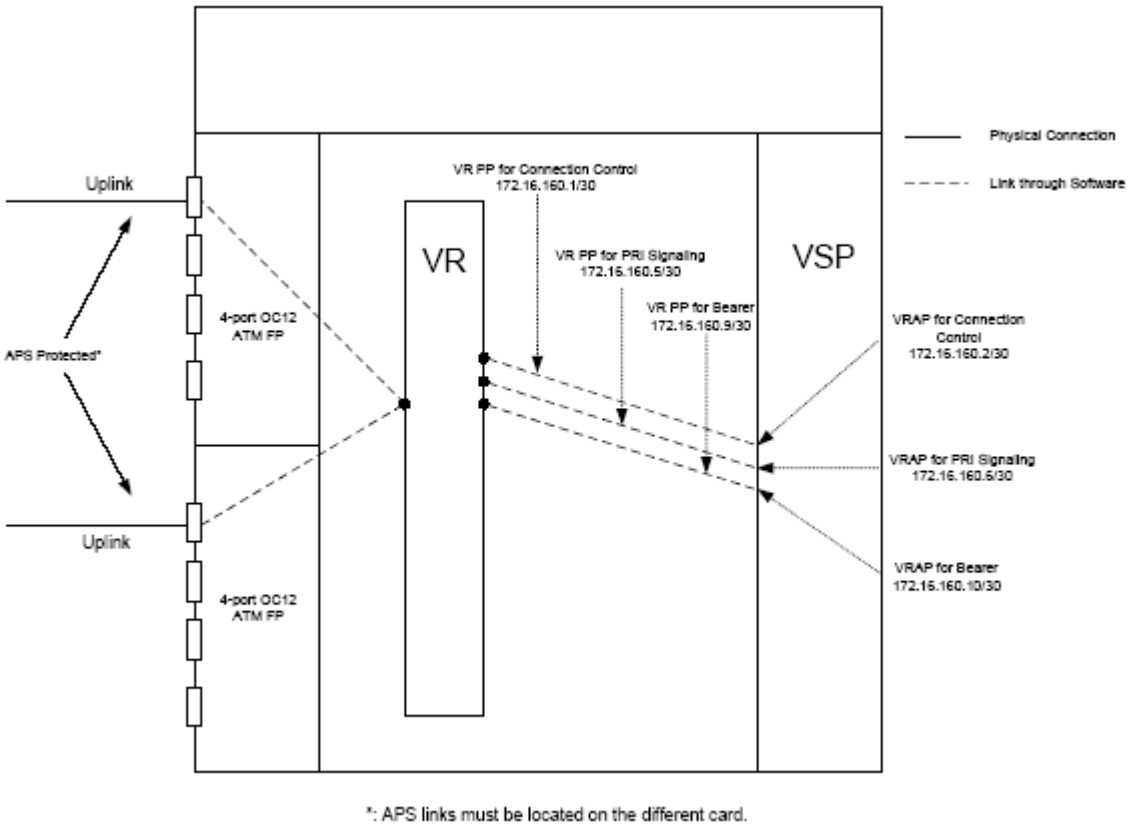
Each VSP card has one SPVC for control messages and one SPVC for bearer. Both terminate to a protocol port on the VR through the ATM loop around. If PRI trunks are also provisioned on the VSP, another SPVC needs to be added from the VSP cards to a different protocol port on the same VR via a similar hairpin path.

Option 2: VRAP (VR Access Point)

In SN06, Virtual Router Access Point (VRAp)[1] is introduced to offset partial routing responsibility from CP cards to VSP cards. Each individual VSP card has its own VRAp, which ships all locally-generated signaling and bearer traffic to VR. Because communication between VRAp and VR on CP cards is done through software, the need for the physical hairpin is removed [as was described in Option 1 above]. This feature gives customers the benefit of more efficient port utilization.

1. In SN06, VRAp is not Carrier Grade.

**Figure 37 VRAP Connection**




For the above two options described for PVG VR Options, the external connection methods are identical. Please refer Section 7.1.1.2 for details.

### 7.1.1.2 Inter-connections Options

Depending on the investment plan of customers, Nortel Networks supports two different approaches to implement Succession network.

Option A:

Phase I - Starting from Single CS-2K Site

If customers don’t plan to add inter-complex call service in the short term, Nortel Networks recommends starting with this option by connecting PVGs with Passport 8600s. The following diagram illustrates the high-level view of inter-connections.

**Figure 38 Network Diagram for Option A - Phase I**

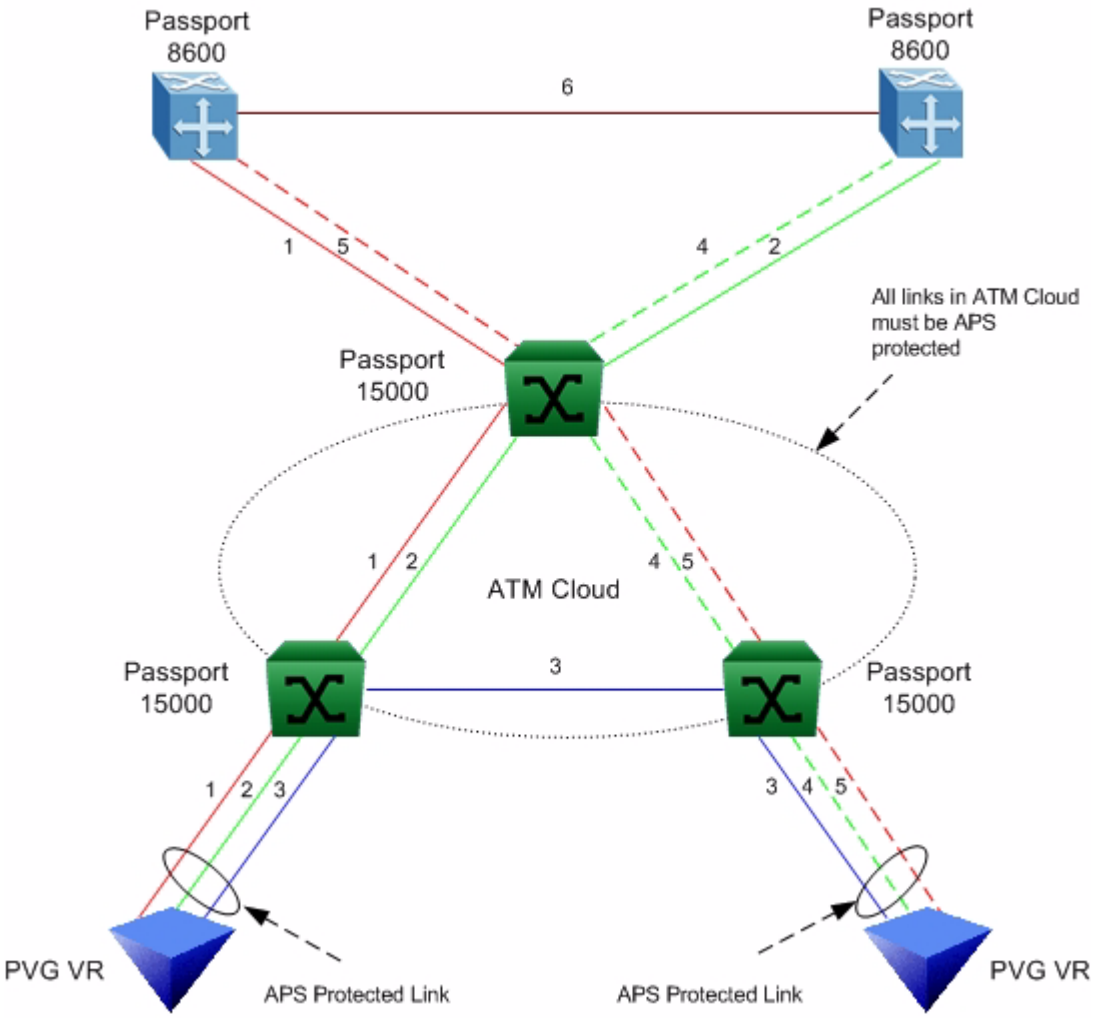


**Table 19 Legend of Figure 38**

**Table 0-1**

| Index | Type | Media | Traffic Type | Routing Method |
|---|---|---|---|---|
| 1, 2, 4, 5 | VCC | ATM | Connection Control, PRI Signaling, PVG OAM, Bearer from/to UAS, OSPF | OSPF + Static Route |
| 3 | VCC | ATM | Bearer between PVGs only | Static Route only |
| 6 | Broadcast | Fast Ethernet, Gigabit Ethernet | OSPF | OSPF + Static Route |

This diagram represents the case that there is no demand for inter-CS2K calls. As mentioned earlier, all PVGs in the network are fully meshed by PVCs. Bearer traffic between PVG VRs is directed by static routes through directly connected PVCs. It is mandatary to have all connections between PVGs and the Passport 15000s, or between Passport 15000s be protected by APS.

The Passport 8600 is located in the OSPF backbone and provides the entrance to CS-LAN for connection control and signaling messages from all VSP cards. OSPF needs to be enabled on PVG VRs in order to dynamically route the connection control and PRI signaling message to MGCs. Since control and signaling packets from each VSP card only generate a small volume of IP traffic, Passport 8600 MDA module has the sufficient resource to process them

***Note:*** The link failure between Passport 8600 and Passport 15000 is protected on Layer 2(ATM OAM F5) and Layer 3(OSPF).

Phase II - Multi-CS2K Network Considerations

When operating a multi-CS2K network, there must be an edge router to other VoIP networks if DPT calls to other CS2K complexes are expected. Depending on the call flow pattern, potentially a significant amount of bearer traffic will go through this router for inter-CS2K calls in addition to the SIP-T signalling traffic. Two dedicated Passport shelves with the VR are required to provide redundant exit points to other CS2Ks in the network. The following diagram shows the evolvement from initial phase to support Inter-complex calls.

**Figure 39 Network Topology for Option A -Phase II**

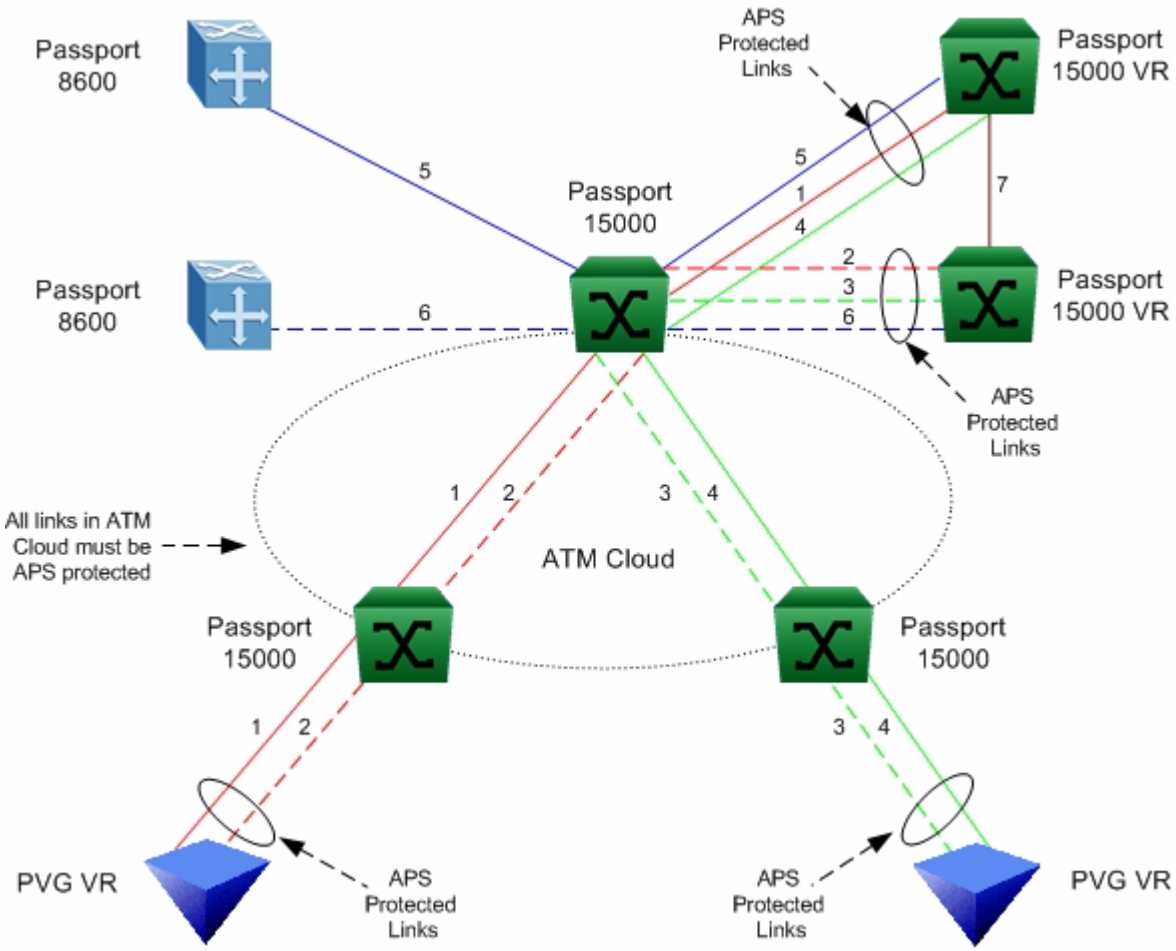



**Table 20 Legend of Figure 39**

**Table 0-2**

| Index | Type | Media | Traffic Type | Routing Method |
|---|---|---|---|---|
| 1, 2, 3, 4 | VCC | ATM | Bearer from/to other CS2K complex | Static Route only |
| 5,6 | VCC | ATM | SIP-T, OSPF | OSPF + Static Route |
| 7 | VCC | ATM | OSPF | OSPF + Static Route |

The major difference is the positioning of two Passport 15000 VRs on the edge. Keeping existing VCCs untouched, another set of VCCs are required between Passport 8600s and Passport VRs, as well as, between PVG VRs and Passport VRs. On a PVG, default routes point to the Passport VRs

for calls to other line/trunk gateways in the different CS2K complex. OSPF between Passport 8600s and Passport VRs ensures the DPT SIP-T messages can be delivered to the appropriate CS2K through one of Passport VRs.

This approach offers customers with the granularity of the investment. If the project begins with small number of PVGs, 100% intra-complex calls and no connection between multiple CS2K sites is expected in the short period of time, this option is the most recommended one. However, if customers try to expand the services later, the migration is comparatively sophisticated due to the fact that new equipment are introduced and new VCCs need to be added on every PVG.

## Option B:

Phase I - Starting from Single CS2K Network

If customers would like to start with complete intra-complex calls but also want to prepare for the growth at the beginning, a different approach should be considered to minimize network topology changes in the future.

**Figure 40 Network Diagram for Option B - Phase I**

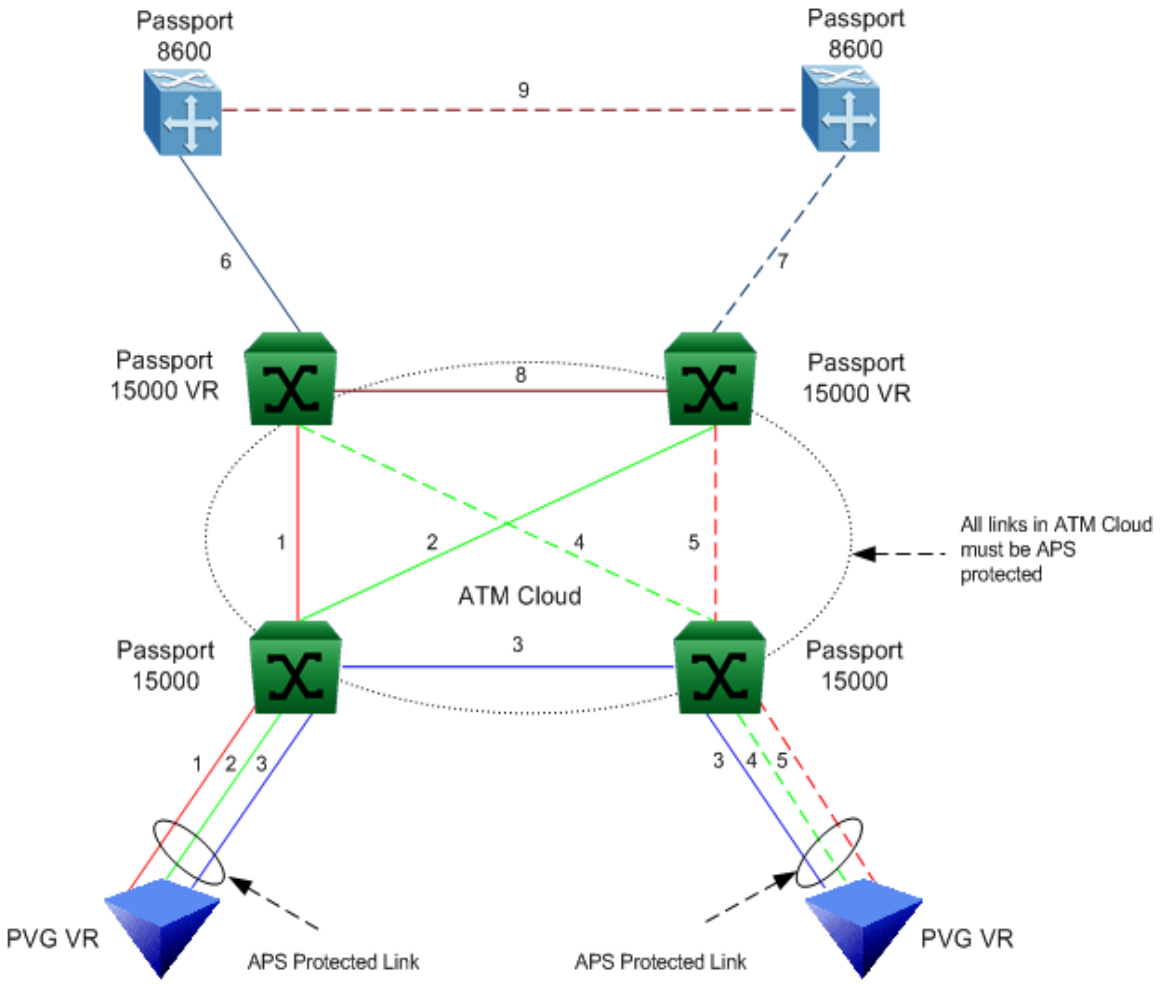

Passport
8600
Passport
8600
9
6
7
Passport
15000 VR
8
Passport
15000 VR
1
2
4
5
All links in ATM Cloud
must be APS
protected
ATM Cloud
Passport
15000
3
Passport
15000
1 2 3
3 4 5
PVG VR
APS Protected Link
APS Protected Link
PVG VR

**Table 21 Legend of Figure 40**

**Table 0-3**

| Index | Type | Media | Traffic Type | Routing Method |
|---|---|---|---|---|
| 1, 2, 4, 5 | VCC | ATM | Connection Control, PRI Signaling, PVG OAM, Bearer from/to UAS, OSPF | Static Route Only |
| 3 | VCC | ATM | Bearer between PVGs only | Static Route only |
| 6, 7 | VCC | ATM | Connection Control, PRI Signaling, PVG OAM, Bearer from/to UAS, OSPF | OSPF + Static Route |
| 8 | VCC | ATM | OSPF | OSPF + Static Route |
| 9 | Broadcast | Fast Ethernet, Gigabit Ethernet | OSPF | OSPF + Static Route |

Instead of building up VCCs between Passport 8600s and PVGs, Passport VRs appear here sitting in the middle of PVGs and Passport 8600s as the interface between CS-LAN and core network. Each PVG has VCC that are dual-homed on Passport VRs. Traffic from all PVGs to CS-LAN devices is terminated on Passport VRs and aggregated into a single VCC to each of the Passport 8600s. Passport VRs consult with Passport 8600s through OSPF for the routes within the CS-LAN. PVG to PVG bearer traffic does not go through Passport VRs because static routes use direct links as the preferred routes.

OSPF is only enabled inside the rectangle formed between two Passport 8600s and Passport VRs, i.e., connections 6,7,8 and 9 in Figure 40. PVGs are not part of OSPF domain and only support static routes.

It is required to have all connections between PVGs and the Passport 15000s, or between Passport 15000s, to be protected by APS.

Phase II - Multi-CS2K Network Considerations

When evolving from a single CS2K site to multiple CS2K sites, no additional Passports 15000 VRs are needed for the original site. Passport VRs are already implemented in Phase I. In addition to the traffic explained in the above section, Passport VRs must also route inter-CS2K complex packets, like bearer from PVG [via DPT trunks] and SIP-T signaling between CS2Ks.

**Figure 41 Network Diagram for Option B - Phase II**

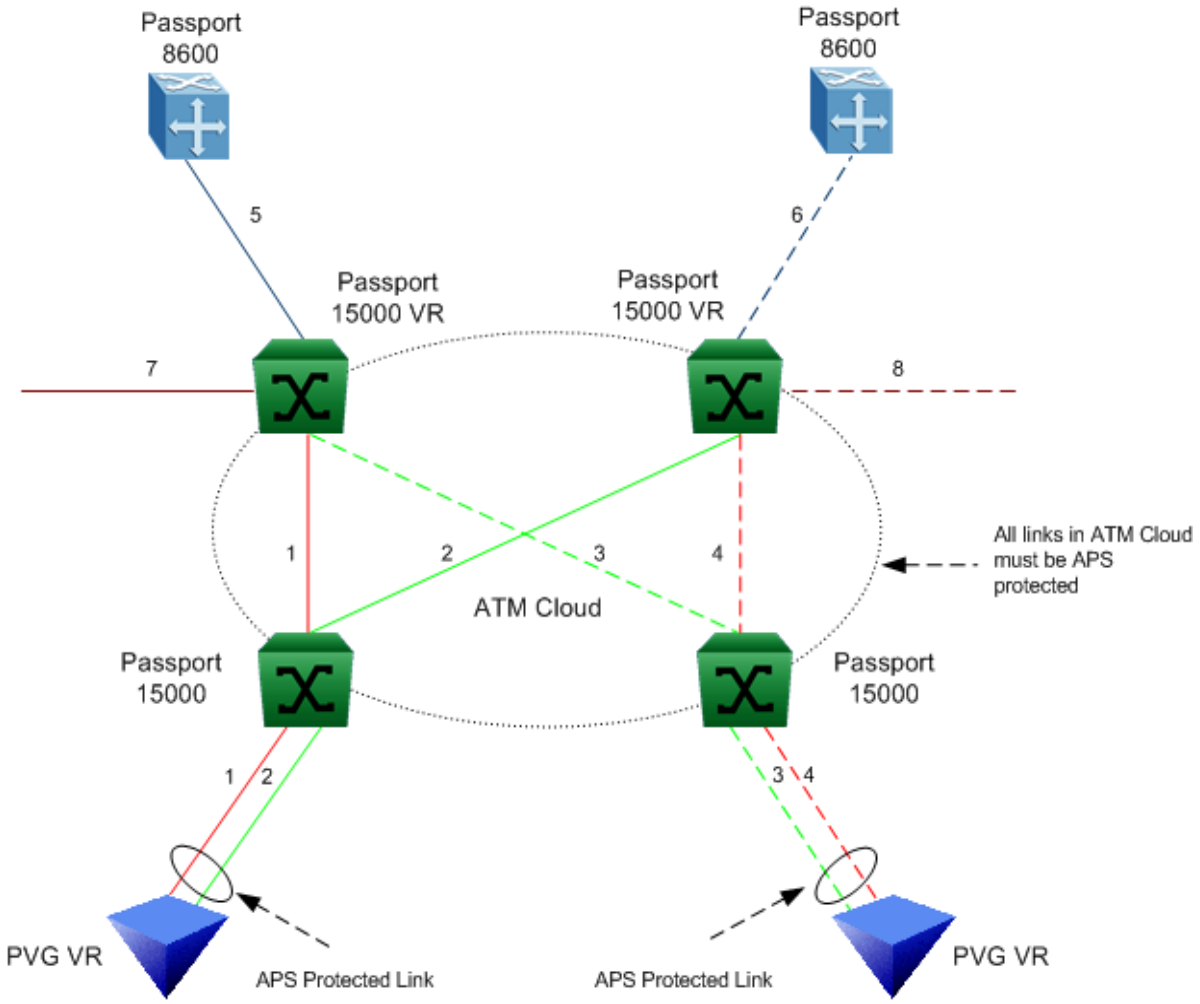


**Table 22 Legend of Figure 41**

**Table 0-4**

| Index | Type | Media | Traffic Type | Routing Method |
|---|---|---|---|---|
| 1, 2, 3, 4 | VCC | ATM | Bearer from/to other CS2K complex | Static Route Only |
| 5, 6 | VCC | ATM | Connection Control, PRI Signaling, PVG OAM, Bearer from/to UAS, OSPF, SIP-T | OSPF + Static Route |
| 7, 8 | VCC | ATM | Bearer from/to other CS2K complex, SIP-T | Static Route Only |

Although no new VCC are required, the former VCCs between Passport 8600s and Passport VRs, and between PVG VRs and Passport VRs need to be resized in order to accommodate the added traffic as the result of inter-CS2K complex calls. The routing architecture remains the same. Since the bearer for PVGs use static routes, the PVGs aren't involved in any OSPF processes. As mentioned in the prior section, OSPF continues to be enabled between Passport 8600s and Passport VRs.

## 7.1.2 ATM Throughput

### 7.1.2.1 4-port OC12 FP Throughput

Normally, switching of ATM cells is performed at the line speeds, however the ATM FP does has performance limits for frame-based traffic. Extreme care should be used when locating VCCs on an 4-port OC12 ATM FP in Succession solution. If the cumulative amount of traffic from all ports on an ATM FP exceeds the IP forwarding rate of the card, IP packets may be dropped leading to poor voice quality.

Please note that, for different PVG VR connection option, different value should be used. The maximum number of DS0s per card is listed below for both PVG VR Hairpin and VRAp configurations.

**Table 23 Throughput Limitation of PVG Hairpin**

**Table 0-5**

| Codec | # of Hairpins per card | Max # of DS0s per card |
|---|---|---|
| G.711 (10ms) | 1 | 4646[a] |
| | 2 | 5400 |
| G.711 (20ms) | 1 | 5575[a] |
| | 2 | 8064 |

a. Constrained by ATM bandwidth of OC12 port

**Table 24 Throughput Limitation of PVG Uplink**

| Codec | # of Uplinks per card | Max # of DS0s per card | |
|---|---|---|---|
| | | VR Hairpin | VRAP |
| G.711 (10ms) | 1 | 4646[a] | 4646 |
| | 2,3,4 | 6600 | 6516 |
| G.711 (20ms) | 1 | 5575[a] | 5575[a] |
| | 2,3,4 | 8064 | 8064 |

a. Constrained by ATM bandwidth of OC12 port

**Table 25 Throughput Limitation of Passport VR ATM Connection**

**Table 0-6**

| Codec | # of WAN links per card | Max # of DS0s per card |
|---|---|---|
| G.711 (10ms) | 1 | 4646[a] |
| | 2,3,4 | 5400 |
| G.711 (20ms) | 1 | 5575[a] |
| | 2,3,4 | 8064 |

a. Constrained by ATM bandwidth of OC12 port

### 7.1.2.2 PVG Shelf Capacity

The call capacity per PVG shelf primarily depends on the voice codec. Factors like IP throughput of ATM FP and resiliency requirements restrict the maximum number of DS0s that can be installed on a PVG shelf.

**Table 26 PVG Shelf Capacity for Different Codec with VSP3**

| Codec | Maximum DS0s | |
|---|---|---|
| | VR Hairpin | VRAP |
| G.711 (10ms) | 6048 | 8064 |
| G.711 (20ms) | 8064 | 8064 |

PVG shelf layouts are slightly different when different codecs are used or different connection methods are applied. Some common rules must be followed to ensure the carrier gradeness and the best performance.

- 1+1 is strongly recommended for CPs and FPs in order to provide seamless migration to SN06.
- All ATM connections must be protected by APS to minimize the down time. The protection line must be on the different ATM FP from the working line.
- If using hairpin, two ends of loop around must be terminated on the same ATM FP. Configure dual hairpins on a 4-port OC12 card if more than one hairpin connection is required.

Option 1: PVG VR with Hairpin

**Table 27 PVG VR Hairpin - Hardware List for G.711(10ms) Codec**

| Processor | Main | Spare |
|---|---|---|
| CP3 | 1 | 1 |
| 4-port OC3c TDM | 1 | 1 |
| VSP3 | 3 | 3 |
| 4-port OC12 ATM | 3 | 3 |

**Figure 42 PVG VR Hairpin - Sample PVG Shelf Layout for G.711 (10ms)**

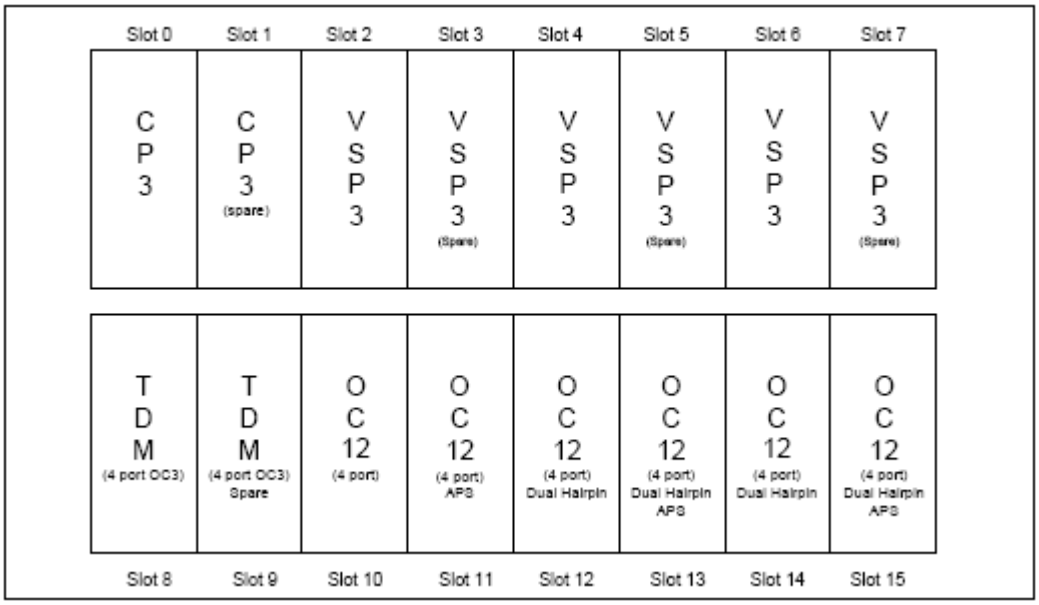


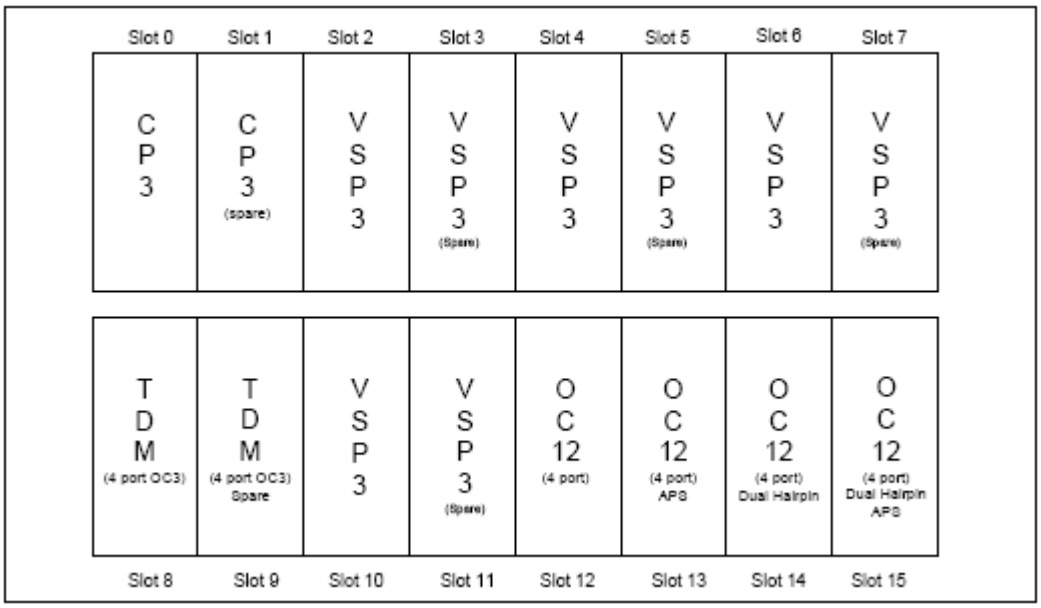

**Table 28 PVG VR Hairpin - Hardware List for G.711(20ms) Codec**

| Processor | Main | Spare |
|---|---|---|
| CP3 | 1 | 1 |
| 4-port OC3c TDM | 1 | 1 |
| VSP3 | 4 | 4 |

**Table 28 PVG VR Hairpin - Hardware List for G.711(20ms) Codec**

| | | |
|---|---|---|
| 4-port OC12 ATM | 2 | 2 |

**Figure 43 PVG VR Hairpin - Sample PVG Shelf Layout for G.711 (20ms)**




Option 2: PVG VRAP

**Table 29 PVG VRAP - Hardware List for G.711(10ms) Codec**

| Processor | Main | Spare |
|---|---|---|
| CP3 | 1 | 1 |
| 4-port OC3c TDM | 1 | 1 |
| VSP3 | 4 | 4 |
| 4-port OC12 ATM | 2 | 2 |

**Figure 44 PVG VRAP - Sample PVG Shelf Layout for G.711 (10ms)**

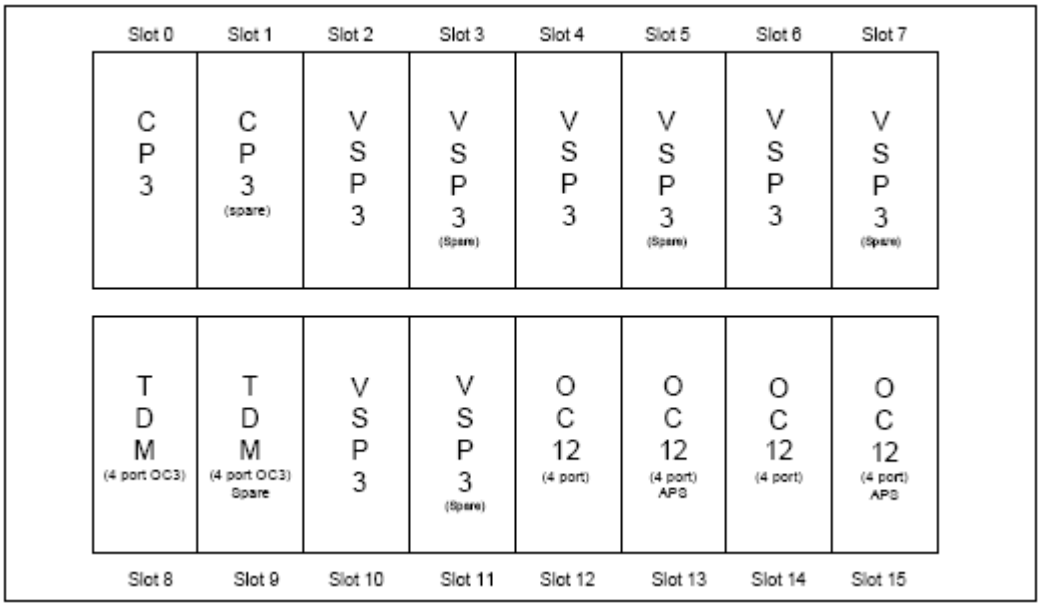
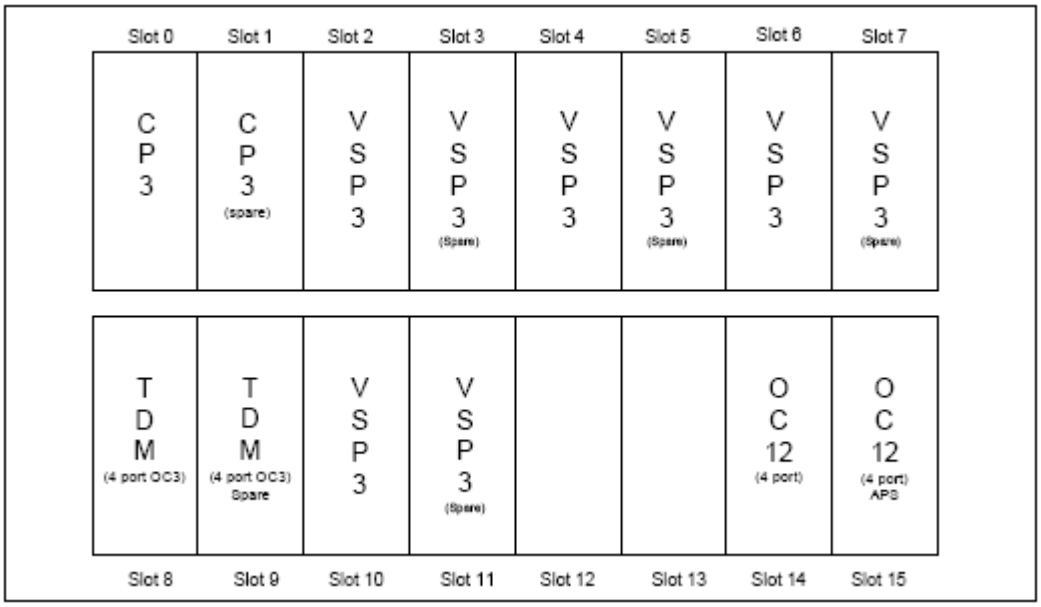



**Table 30 PVG VRAP - Hardware List for G.711(20ms) Codec**

**Table 0-7**

| Processor | Main | Spare |
|---|---|---|
| CP3 | 1 | 1 |
| 4-port OC3c TDM | 1 | 1 |
| VSP3 | 4 | 4 |
| 4-port OC12 ATM | 2 | 2 |

**Figure 45 PVG VRAP - Sample PVG Shelf Layout for G.711 (20ms)**


Slot 0
Slot 1
Slot 2
Slot 3
Slot 4
Slot 5
Slot 6
Slot 7
CP3
CP3 (spare)
VSP3
VSP3 (Spare)
VSP3
VSP3 (Spare)
VSP3
VSP3 (Spare)
TDM (4 port OC3)
TDM (4 port OC3) Spare
VSP3
VSP3 (Spare)
OC12 (4 port)
OC12 (4 port) APS
Slot 8
Slot 9
Slot 10
Slot 11
Slot 12
Slot 13
Slot 14
Slot 15

### 7.1.3 VCC Engineering Notes

#### 7.1.3.1 Determining the Number of VCCs

Option A:

Phase I - Starting from Single CS-2K Site

- PVG - PVG:
  In order to create shortest path between two MGs, it is mandatory to have all PVGs in the entire network fully meshed by PVCs. As the result, bearer traffic traverses between the source and the destination without bypassing the third device.
- PVG - Passport 8600:
  A PVC is required between a Passport 8600 and each PVG VR. This VCC is used to carry connection control, signaling (if PRI trunks are planed) traffic, PVG OAM (if out-of-band management is planed), bearer traffic to/from UAS and OSPF.

Phase II - Multi-CS2K Network Considerations

- PVG - PVG:
  In order to create shortest path between two MGs, it is mandatory to have all PVGs in the entire network fully meshed by PVCs. As the result, bearer traffic traverses between the source and the destination without bypassing the third device.
- PVG - Passport 8600:
  A PVC is required between a Passport 8600 and each PVG VR. This VCC is used to carry connection control, PRI signaling (if PRI trunks are planed), PVG OAM (if out-of-band management is planed), bearer traffic between PVGs and UAS and OSPF. Bearer traffic between PVGs doesn't travel through this kind of VCCs.
- PVG - Passport VR:
  A PVC is required between a Passport VR and each PVG VR. This VCC is used to carry inter-CS2K complex bearer under the normal situation.
- Passport VR - Passport VR:
  Between Passport VRs, one PVC must be set up in OSPF Area 0.0.0.0 to synchronize OSPF database. There should not be high volume of bearer traffic.
- Passport VR - Passport 8600:
  A PVC is required between a Passport VR and one of Passport 8600s. Four equipment physically form a rectangle. This VCC carries the SIP-T traffic to other CS-2K complex.

Option B:

Phase I - Starting from Single CS-2K Site

- PVG - PVG:
  In order to create shortest path between two MGs, it is mandatory to have all PVGs in the entire network fully meshed by PVCs. As the result, bearer traffic traverses between the source and the destination without bypassing the third device.
- PVG - Passport VR:
  A PVC is required between a Passport VR and each PVG VR. This VCC is used to carry connection control, signaling (if PRI trunks are planed) traffic, PVG OAM (if out-of-band management is planed), bearer to/from UAS.
- Passport VR - Passport 8600:
  A PVC is required between a Passport VR and one of Passport 8600s. This VCC aggregates all connection control, signaling (if PRI trunks are implemented) traffic, PVG OAM (if out-of-band management is planed), bearer to/from UAS from all PVGs in the network. It also carried OSPF messages between two nodes.

- Passport VR - Passport VR:
  Between Passport VRs, one PVC must be set up in OSPF Area 0.0.0.0 to synchronize OSPF database. There should not be high volume of bearer traffic.

Phase II - Multi-CS2K Network Considerations

- PVG - PVG:
  In order to create shortest path between two MGs, it is mandatory to have all PVGs in the entire network fully meshed by PVCs. As the result, bearer traffic traverses between the source and the destination without bypassing the third device.
- PVG - Passport VR:
  A PVC is required between a Passport VR and each PVG VR. This VCC is used to carry connection control, signaling (if PRI trunks are planed) traffic, PVG OAM (if out-of-band management is planned), bearer to/from UAS, bearer to/from other CS2K complex.
- Passport VR - Passport 8600:
  A PVC is required between a Passport VR and one of Passport 8600s. This VCC aggregates all connection control, signaling (if PRI trunks are implemented) traffic, PVG OAM (if out-of-band management is planned), bearer to/from UAS from all PVGs in the network. It also carried OSPF messages between two nodes and SIP-T traffic to/from other CS2K complex.
- Passport VR - Passport VR:
  Between Passport VRs, one PVC must be set up in OSPF Area 0.0.0.0 to synchronize OSPF database. There should not be high volume of bearer traffic.

### 7.1.3.2 Bandwidth Planning and VCC Sizing

There are two key areas to consider for VCC sizing and bandwidth planning. One is determining initial sizing, and the second is resizing when ongoing surveillance indicates the VCC is no longer appropriately sized due to traffic pattern shifts, or additional DS0s/trunks are added at the PVG gateway.

In general, VCC sizing is influenced by two variables:

1. Trunk group to trunk group calling/traffic patterns[2] and,
2. Trunk member selection within a trunk group, i.e., its appearance on the particular gateway.

For the purposes of network planning, Nortel Networks recommends starting with the following rules:

**a.** ATM links on PVG and Passport 8600 must be restricted to voice-related traffic only.

**b.** Overbooking is NOT allowed on PVG hairpin connections. VCCs on hairpin must be given full bandwidth according to the DS0s provisioned on the corresponding VSPs. In addition, the throughput limitation of hairpins need to be considered. See Table 23 on page 115.

**c.** On PVG uplinks, PVCs between PVGs are engineered according to the **lesser** of the DS0s provisioned at either the near-end or far-end PVG, i.e. assuming at the worst case, all traffic goes to the PVG.

**d.** Overbooking is allowed on PVG uplinks, i.e. the sum of all PVCs provisioned at a PVG may exceed the link speed.

2. On-switch Operational Measurements (OM group TRK) can show how much traffic comes from, or goes to, a particular trunk group. However, these groups can not show which trunk group members are making calls to another trunk group member.

**e.** The number of DS0s, i.e., the PCR, carried by a single PVC must not exceed the bandwidth of the uplink.

**f.** The total number of planned DS0s on PVG uplinks should not exceed the IP throughput limitation in the form of the maximum number of DS0 per card. If necessary, add more cards. See Table 24 on page 115.

**g.** On PVG uplinks, the PVC between a local PVG and one of two Passport VRs must be engineered to the **lesser** of either the number of DS0s provisioned on the local PVG or the expected amount of traffic from all VSPs at the local PVG that is anticipated to make DPT calls. The same method should be used for the PVC going to the other Passport VR.

**h.** PVCs between two different CS2K complexes are engineered based on the expected amount of traffic from all VSPs within a CS2K complex to other CS2K sites, i.e., the DPT SIP-T traffic. Each Passport VR should be capable of carrying all inter-CS2K complex calls independently.

**i.** Overbooking is allowed on Passport VR ATM links.

**j.** At any time, the number of active calls on Passport VR ATM links should not exceed the IP throughput limitation in the form of the maximum number of DS0 per card. If necessary, add more cards. See Table 25 on page 116.

After exiting the provisioning phase, real-time surveillance should be performed in order to understand the actual traffic flow pattern. Nortel Networks strongly recommend customers using the following procedure to ensure no subscriber will experience QoS problem:

**a.** Monitor ATM link utilization for all connected ports on a ATM card during the peak time. The result can be saved into clean text file.

**b.** Calculate the bandwidth usage for the whole card. Translate the ATM bandwidth to the number of active DS0s.

**c.** If current traffic load has already reached 75% of throughput limitation in the form of maximum DS0 per card, customers should begin to move PVCs to additional ATM cards.

### Bandwidth Parameters

For VCCs carrying non-media traffic, the guidelines for the traffic parameters is given in the following table. The recommendations are different for Passport 7000 and Passport 15000 platforms. The service category of the VCC are to be one lower than the media VCCs, that is nrt-VBR. Policing should be turned off.

**Table 31 Non-Media Bandwidth Requirement for a VSP Card**

**Table 0-8**

| Type | VSP | PCR(Cells/sec) | SCR(Cells/sec) | MBS(Cells) |
|---|---|---|---|---|
| Control | 7000 VSP2 | 700 | 350 | 100 |
| | 15000 VSP2 | 700 | 700 | 90 |
| | 15000 VSP3 | 1200 | 600 | 160 |
| PRI | 7000 VSP2 | 400 | 200 | 55 |

**Table 0-8**

| | | | | |
|---|---|---|---|---|
| | 15000 VSP2 | 450 | 210 | 60 |
| | 15000 VSP3 | 850 | 420 | 120 |
| V5.2 | 7000 VSP2 | 400 | 200 | 55 |
| | 15000 VSP2 | 450 | 210 | 60 |
| | 15000 VSP3 | 850 | 210 | 120 |

**Table 32 Non-Media Bandwidth Requirement for a PVG shelf**

**Table 0-9**

| Interface Type | Platform | PCR(Cells/sec) | SCR(Cells/sec) | MBS(Cells) |
|---|---|---|---|---|
| MDM | 7000 | 400 | 200 | 55 |
| | 15000 | 2100 | 1050 | 100 |
| OSPF | 7000 | 1000 | 500 | 220 |
| | 15000 | 1000 | 500 | 220 |

The bandwidth requirements for each CODEC type and rate for the VoATM solution is given in the following table. The overall bandwidth per DS0 values includes the RTP/UDP/IP, RFC1483 and ATM cell headers.

**Table 33 Media Traffic Bandwidth Requirement for A Call**

**Table 0-10**

| CODEC Type | Encoding Rate | Bandwidth per DS0 | PCR/SCR (Cells/sec) | MBS (Cells) |
|---|---|---|---|---|
| G.711 10ms | 64 kbits/s | 127.2 kbits/s | 300 | 1 |
| G.711 20ms | 64 kbits/s | 106 kbits/s | 250 | 1 |
| G.729a 10ms | 8 kbits/s | 84.8 kbits/s | 200 | 1 |
| G.729a 20ms | 8 kbits/s | 42.4 kbits/s | 100 | 1 |

In order to translate the above value to the traffic parameters, use the following formula to size the VCC between different equipment:

- PVG - PVG (Common for both Option A and Option B)

Only bearer traffic will travel on the VCC between PVG peers.

**Table 0-11**

| | |
|---|---|
| Service Category | rtvbr |
| PCR | N[a] * (PCR of Bearer)[b] |
| SCR | Same as PCR |
| MBS | 1 |

a. N is the number of planned DS0s between PVGs
b. Look up Table 9 at Column 4 for the value of different codecs

Option A:

Phase I - Starting from Single CS-2K Site

- PVG - Passport 8600

The traffic on VCCs between PVGs and Passport 8600s is the combination of connection control, PRI signaling, bearer traffic to/from UAS, OAM flow for PVG management and OSPF messages. Contribution from all components to the traffic volume should be considered.

**Table 0-12**

| | |
|---|---|
| Service Category | rtvbr |
| PCR | A[a] * (PCR of Control) + A * (PCR of Signaling) + B[b] * (PCR of Bearer) + (PCR of OAM) + (PCR of OSPF) |
| SCR | Same as PCR |
| MBS | 1 |

a. The number of VSP cards configured on the PVG
b. The number of estimated simultaneous conference call sessions between local PVG and UAS

Phase II - Multi-CS2K Network Considerations

- PVG - Passport VR

Only bearer traffic heading to other CS2K complex will be located on VCCs between PVGs and Passport VRs.

**Table 0-13**

| | |
|---|---|
| Service Category | rtvbr |

**Table 0-13**

| | |
|---|---|
| PCR | N[a] * (PCR of Bearer) |
| SCR | Same as PCR |
| MBS | 1 |

a. The number of planned DS0s for inter-complex calls

- Passport 8600 - Passport VR

The mixture of SIP-T and OSPF messages will appear on VCCs between Passport 8600s and Passport VRs.

**Table 0-14**

| | |
|---|---|
| Service Category | rtvbr |
| PCR | (PCR of OSPF) + (PCR of SIP-T) |
| SCR | Same as PCR |
| MBS | 1 |

- Passport VR - Passport VR

This kind of VCCs is added primarily for exchanging the OSPF topology database between Passport VRs. No other traffic is expected under the normal circumstance.

**Table 0-15**

| | |
|---|---|
| Service Category | rtvbr |
| PCR | PCR of OSPF |
| SCR | SCR of OSPF |
| MBS | MBS of OSPF |

- Passport VR - external network

Bearer traffic to other complex will leave Passport VRs to the external network. SIP-T exchanging between CS2Ks is also carried by this VCC.

**Table 0-16**

| | |
|---|---|
| Service Category | rtvbr |
| PCR | A[a] * (PCR of Bearer) + (PCR of SIP-T) |
| SCR | Same as PCR |
| MBS | 1 |

a. The number of estimated calls to different CS2K complex

Option B:

Phase I - Starting from Single CS-2K Site

- PVG - Passport VR

Traffic from PVGs to CS-LAN devices (GWC, USP, etc) will terminate on Passport VRs. No routing protocol is used in this case.

**Table 0-17**

| Service Category | rtvbr |
|---|---|
| PCR | $A^a$ * (PCR of Control) + A * (PCR of Signaling) + $B^b$ * (PCR of Bearer) + (PCR of OAM) |
| SCR | Same as PCR |
| MBS | 1 |

a. The number of VSP cards configured on the PVG
b. The number of estimated simultaneous conference call sessions between local PVG and UAS

- Passport 8600 - Passport VR

Traffic from all PVGs to CS-LAN is routed to Passport 8600s by Passport VR. In addition, OSPF traffic needs to be counted.

**Table 0-18**

| Service Category | rtvbr |
|---|---|
| PCR | $A^a$ * (PCR of Control) + A * (PCR of Signaling) + $B^b$ * (PCR of Bearer) + $C^c$*(PCR of OAM) + (PCR of OSPF) |
| SCR | Same as PCR |
| MBS | 1 |

a. The number of VSP cards within the CS2K complex
b. The number of estimated simultaneous conference call sessions between all PVGs and UAS
c. The number of PVGs within the CS2K complex

- Passport VR - Passport VR

This kind of VCCs is added primarily for exchanging the OSPF topology database between Passport VRs. No other traffic is expected under the normal circumstance.

**Table 0-19**

| Service Category | rtvbr |
|---|---|
| PCR | PCR of OSPF |
| SCR | SCR of OSPF |
| MBS | MBS of OSPF |

Phase II - Multi-CS2K Network Considerations

- PVG - Passport VR

Besides traffic from PVGs to CS-LAN devices (GWC, USP, etc), bearer heading to other complex should be considered too.

**Table 0-20**

| Service Category | rtvbr |
|---|---|
| PCR | $A^a$ * (PCR of Control) + A * (PCR of Signaling) + $B^b$ * (PCR of Bearer) + $C^c$ * (PCR of Bearer) + (PCR of OAM) |
| SCR | Same as PCR |
| MBS | 1 |

a. The number of VSP cards configured on the PVG
b. The number of estimated simultaneous conference call sessions between local PVG and UAS
c. The number of estimated calls to other complex from local VSP cards.

- Passport 8600 - Passport VR

The mixture of SIP-T will appear on VCCs between Passport 8600s and Passport VRs in addition to other types of traffic in Phase I.

**Table 0-21**

| Service Category | rtvbr |
|---|---|
| PCR | $A^a$ * (PCR of Control) + A * (PCR of Signaling) + $B^b$ * (PCR of Bearer) + $C^c$ * (PCR of OAM) + (PCR of OSPF) + (PCR of SIP-T) |
| SCR | Same as PCR |
| MBS | 1 |

a. The number of VSP cards within the same CS2K complex
b. The number of estimated simultaneous conference call sessions between all PVGs and UAS
c. The number of PVGs within the same CS2K complex

- Passport VR - Passport VR

This kind of VCCs is added primarily for exchanging the OSPF topology database between Passport VRs. No other traffic is expected under the normal circumstance.

**Table 0-22**

| | |
|---|---|
| Service Category | rtvbr |
| PCR | PCR of OSPF |
| SCR | SCR of OSPF |
| MBS | MBS of OSPF |

- Passport VR - external network

Bearer traffic to other complex will leave Passport VR to the external network. SIP-T exchanging between CS2Ks is also carried by this VCC.

**Table 0-23**

| | |
|---|---|
| Service Category | rtvbr |
| PCR | A[a] * (PCR of Bearer) + (PCR of SIP-T) |
| SCR | Same as PCR |
| MBS | 1 |

a. The number of estimated calls to different CS2K complex

Passport 8600 supports two service categories for ATM VCCs: VBR and UBR. However, UBR has better throughput performance then VBR and is the only service categories Nortel Networks support on Passport 8600 for Succession VoIP. Thus, for those VCCs which are terminated on Passport 8600s, UBR is defined as service category and no PCR/SCR/MBS is specified on Passport 8600 end.

### 7.1.3.3 IP Addressing

One /30 subnet is bound with a PVC in order to give each PVC a unique identification in Layer 3. No point-to-multipoint connection is supported in SN06 release. For additional details on PVC IP addressing, refer to section 6.5.

### 7.1.3.4 Static Routes

Bearer traffic between PVGs traverses the network by static routes. Static routes also provide added resiliency for routing capabilities when OPSF process fails. For example, at the time of a CP

failover, OSPF is restarted, thereby creating a 20-21 second service gap. During this period, the PVG VR routes the packets based on static routes because static routes are reinserted into the routing table much sooner than OSPF. The following rules must be followed when planning static routes:

### Option A:

Phase I - Starting from Single CS-2K Site

- On PVG VR, static routes should be added for IPMCONN subnets of all other VSP cards on the different PVGs.
- On PVG VR, default routes should be added pointing to dual Passport 8600s with equal costs.
- On Passport 8600, static routes should be added for all subnets of all VSP cards within the same CS2K complex.

Phase II - Multi-CS2K Network Considerations

- On PVG VR, static routes should be added for IPMCONN subnets of all other VSP cards on the different PVGs.
- On PVG VR, static routes should be added for CS-LAN subnets using Passport 8600s' IP address as the next hop with equal cost.
- On PVG VR, default routes should be added pointing to dual Passport VRs with equal costs.
- On Passport VR, static routes should be added for IPMCONN subnets of all VSP cards within the same CS2K complex.
- On Passport VR, static routes should be added for CS-LAN network using directly connected Passport 8600's IP address as the next hop.
- On Passport VR, static routes should be added to provide the path to other link/trunk gateways in the different CS2K complex.
- On Passport 8600, static routes should be added for all subnets of all VSP cards within the same CS2K complex.
- On Passport 8600, static routes should be added to provide the path to other gateways in the different CS2K complex using directly connected Passport VR's IP address as the next hop.

### Option B:

Phase I - Starting from Single CS-2K Site

- On PVG VR, static routes should be added for IPMCONN subnets of all other VSP cards on the different PVGs.
- On PVG VR, default routes should be added pointing to dual Passport VRs with equal costs.
- On Passport 8600, static routes should be added for all subnets of all VSP cards within the same CS2K complex using directly connected Passport VR's IP address as next hop.
- On Passport VR, static routes should be added for all subnets of all VSP cards within the same CS2K complex.
- On Passport VR, static routes should be added for CS-LAN network using directly connected Passport 8600's IP address as the next hop.

Phase II - Multi-CS2K Network Considerations

- On PVG VR, static routes should be added for IPMCONN subnets of all other VSP cards on the different PVGs.

- On PVG VR, default routes should be added pointing to dual Passport VRs with equal costs.
- On Passport 8600, static routes should be added for all subnets of all VSP cards within the same CS2K complex using directly connected Passport VR's IP address as next hop.
- On Passport 8600, static routes should be added to provide the path to other gateways in the different CS2K complex using directly connected Passport VR's IP address as the next hop.
- On Passport VR, static routes should be added for all subnets of all VSP cards within the same CS2K complex.
- On Passport VR, static routes should be added for CS-LAN network using directly connected Passport 8600's IP address as the next hop.
- On Passport VR, static routes should be added to provide the path to other link/trunk gateways in the different CS2K complex.

### 7.1.4 OSPF Engineering Notes

#### 7.1.4.1 OSPF Areas and Area Size

It is not advisable to place all equipment in the flat OSPF network. Extensive **Hello** packets and database maintenance can place an unacceptable burden on memory and processor resources. Furthermore, malfunctioning interfaces or connections can also trigger the continuous SPF calculation on all PVGs. Thus, Nortel Networks strongly recommend using a hierarchical design with multiple OSPF areas to reduce these adverse effects.

***Note:*** Due to the concern of frame-based forwarding capacity of ATM FP and VR routing capacity, Nortel Networks does NOT recommend using the PVG VR as an OSPF backbone router in the current release. Nortel Networks strongly recommend configuring Area 0.0.0.0 on Passport 8600s or Passport VRs.

The Passport 8600 can be placed in OSPF backbone if there is NO expected bearer traffic load on this router. In other words, the Passport 8600s can remain in CS-LAN connected to OSPF Area 0.0.0.0 in order to route the signaling and control packets between GWs and GWCs. If the role of the backbone router requires it to route bearer traffics, Passport 8600 is NOT recommended.

Besides the general rules discussed above, Passport 8600 also have its own OSPF restriction:

- No more than five OSPF areas (including Area 0.0.0.0) can be configured on Passport 8600s.
- Passport 8600s cannot support more than 75 OSPF neighbors on the device level.

#### 7.1.4.2 Totally Stubby Area

If the IP addressing scheme is not planned carefully, a PVG VR may maintain a very large database containing the routes flooded from OSPF backbone. This will cause a larger load on PVGs in order to maintain a large topology database. Thus Nortel Networks strongly recommend configuring the PVG VR areas as Totally Stubby OSPF areas. Routing to outside world is based on the default route advertised by the ABR (i.e. Passport 8600s). As a consequence, the number of routing entries for a PVG VR is dramatically reduced.

Totally Stubby Areas can also prevent PVG VR from continuously recalculating the SPF algorithm due to the unstable devices in other areas. Therefore, the PVG VR CPU time can be saved for voice packets processing.

***Note:*** Extreme caution should be used when provisioning PVG VR as a part of totally stubby area. If there are area type mismatches, the PVG VR cannot form adjacency with other OSPF devices.

Keep in mind that Totally Stubby Area may not be appropriate for all cases. For example, if CS-LAN network and PVG VR network are isolated by a IS-IS based IP backbone, some routing entries from IS-IS needs to be redistributed into OSPF area. However, Totally Stubby Area doesn't allow external routes to be imported from other routing protocols including static routes. Thus, in this case, Totally Stubby Area cannot be used.

***Note:*** Totally Stubby Area for PVGs only applies to Option A. PVGs in Option B are not located in any OSPF area.

The details of OSPF area design are summarized below for two network models, and illustrated in

Figure 46 to Figure 47 :

Option A:

Phase I - Starting from Single CS-2K Site

- OSPF must be enabled between Passport 8600s and PVG VRs. If possible, position Passport 8600s in the Backbone area (Area 0.0.0.0).
- PVG VRs must be in the area other than Area 0.0.0.0. If possible, try to use Totally Stubby Area type for those areas which PVGs are located.
- PVG VRs should be grouped into OSPF areas by the size of fifteen. However, no more than sixty PVGs exist within a CS2K complex.

Phase II - Multi-CS2K Network Considerations

- OSPF must be enabled between Passport 8600s and Passport VRs. If possible, put Passport 8600s and Passport VRs into Area 0.0.0.0.
- OSPF must be enabled between Passport 8600s and PVG VRs. If possible, position Passport 8600s in the Backbone area (Area 0.0.0.0).
- PVG VRs must be in the area other than Area 0.0.0.0. If possible, try to use Totally Stubby Area type for those areas which PVGs are located.
- PVG VRs should be grouped into OSPF areas by the size of fifteen. However, no more than sixty PVGs exist within a CS2K complex.
- OSPF should not be enabled on the link between PVG VRs and Passport VRs.
- OSPF should not be enabled on the Passport's link to other CS2K complex.

Option B:

Phase I - Starting from Single CS-2K Site

- OSPF must be enabled between Passport 8600s and Passport VRs. If possible, position Passport 8600s and Passport VRs in the Backbone area (Area 0.0.0.0).
- OSPF should not be activated on any PVG VR.

Phase II - Multi-CS2K Network Considerations

- OSPF must be enabled between Passport 8600s and Passport VRs. If possible, position Passport 8600s and Passport VRs in the Backbone area (Area 0.0.0.0).
- OSPF should not be enabled on those links which connect Passport VRs to other CS2K complex.
- OSPF should not be activated on any link from PVG VRs.

**Figure 46 OSPF Area Design for Option A, Phase I**

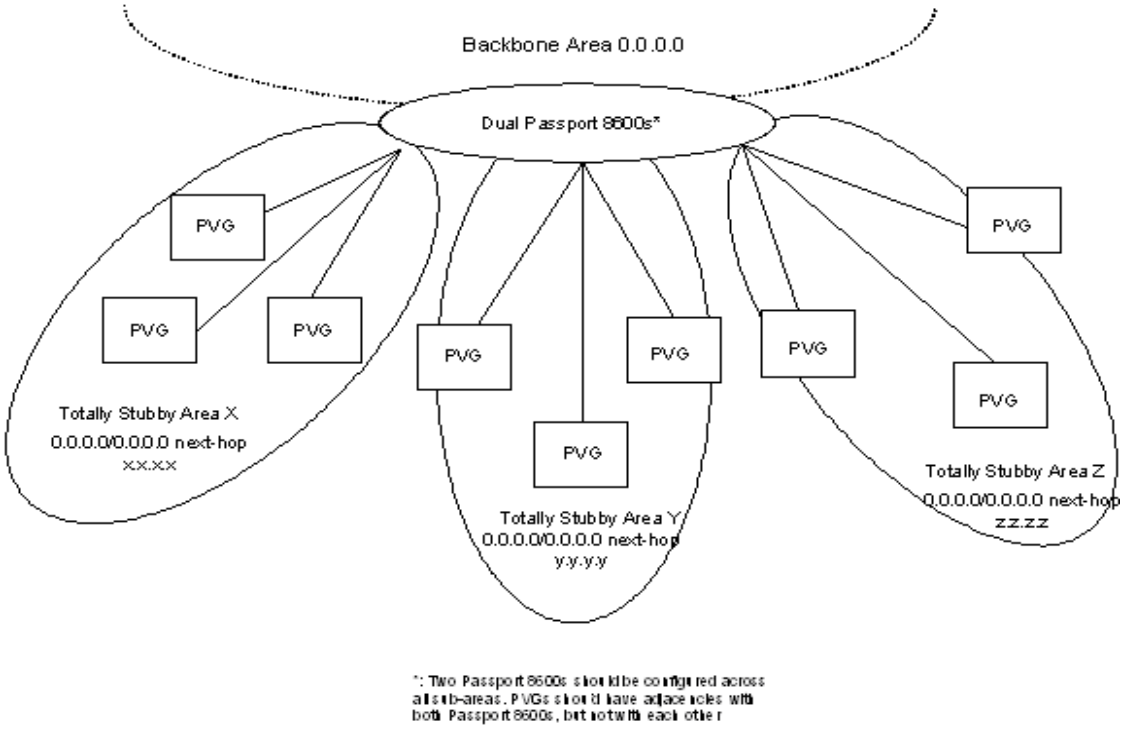



**Figure 47 OSPF Area Design for Option A, Phase II**

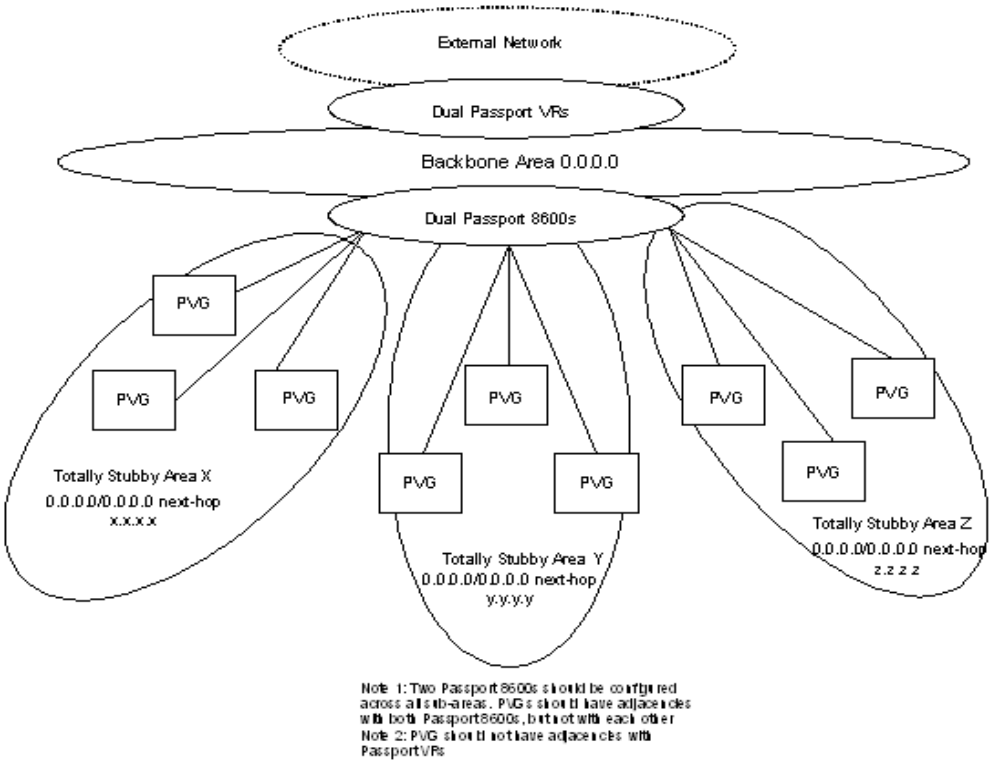
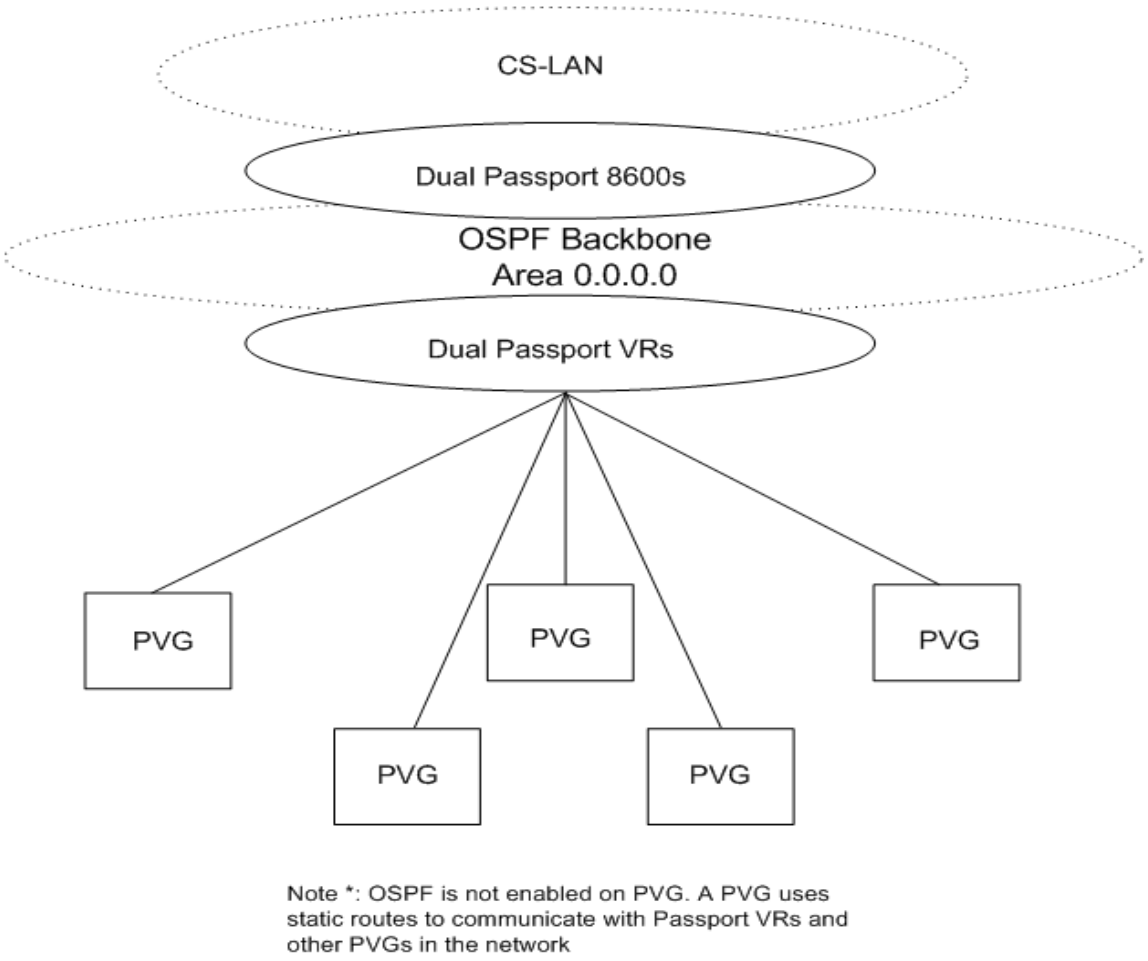


**Figure 48 OSPF Area Design for Option B:**




### 7.1.4.3 OSPF Interface Design

**Hello and Dead interval**

By default, for non-broadcast media, OSPF sends Hello packet to every neighbor every 30 seconds. If no Hello respond receives with 120 seconds, OSPF declares the neighbor down. **Nortel Networks recommends adjusting from the defaults for the Hello timer to 1 second and Dead interval to 4 seconds.**

***Note:*** Extreme caution should be used when manipulating OSPF timer on the PVG VR. If there are Hello timer mismatches, the PVG VR cannot form adjacency with other OSPF devices.

Loss of Hellos, which can lead to adjacencies breaking down and inconsistent DR elections, and loss of Hello acknowledgements or LSA acknowledgement, which will lead to retransmissions, MUST be avoided. The problem is aggravated when the number of routers in an area is large, which can then lead to an overload in the flooding of topology database information. To prevent this happen, a mechanism is needed to give OSPF prioritized treatment in Layer 2 and Layer 3.

Considering how OSPF packets travel through an ATM backbone, some network providers may oversubscribe the backbone connection in order to accommodate more user traffic, thereby impacting OSPF packets through the network. If the ATM service category of OSPF VCCs is NRT-VBR or UBR, during network congestion OSPF messages are at risk of being overridden by bursty traffic applications like FTP or Internet browsing. Thus, Nortel Networks strongly recommends assigning RT-VBR for VCCs between Succession OSPF nodes. By utilizing this service category, the chances of adjacencies breaking or LSA storms are significantly reduced.

**OSPF Network Type**

There are several OSPF network types defined in the RFCs. However, not all of them can be used in a Succession AAL5 network because Passport 8600 only supports Broadcast mode and Passive mode. The following describes those types for each of the network models:

## Option A:

Phase I - Starting from Single CS-2K Site

- On Passport 8600, OSPF network type of those VLANs for VCCs to PVG VRs must be set to "Broadcast".
- There must be one OSPF connection between Passport 8600s locating in Area 0.0.0.0. OSPF network type for the corresponding VLAN must be set to "Broadcast".
- On PVG, interface type for those IP connections to Passport 8600s must be set to "Broadcast".
- On PVG, interface type for those IP ports which terminate CTRL/MG and CTRL/SG of VSP cards must be set to "PASSIVE".
- On PVG, OSPF cannot be enabled on those IP ports which terminate IPMCONN of VSP cards. Furthermore, the subnets of IPMCONN cannot be exported into OSPF in the form of redistribution.

Phase II - Multi-CS2K Network Considerations

- On PVG VR, OSPF interface type for those IP connections to Passport 8600s must be set to "Broadcast".
- On PVG VR, interface type for those IP ports which terminate CTRL/MG and CTRL/SG of VSP cards must be set to "PASSIVE".
- On PVG VR, OSPF can NOT be enabled on those IP ports which terminate IPMCONN of VSP cards. Furthermore, the subnets of IPMCONN cannot be exported into OSPF in the form of redistribution.
- On PVG VR, OSPF can NOT be enabled on those IP connections to Passport VRs.
- On Passport 8600, OSPF network type of those VLANs for VCCs to PVG VRs must be set to "Broadcast".
- On Passport 8600, OSPF network type of those VLANs for VCCs to Passport VRs must be set to "Broadcast".
- There must be one OSPF connection between Passport 8600s locating in Area 0.0.0.0. OSPF network type for the corresponding VLAN must be set to "Broadcast".
- On Passport VRs, OSPF interface type for those IP connections to Passport 8600s must be set to "Broadcast"
- There must be one OSPF connection between Passport VRs locating in Area 0.0.0.0. Interface type for the corresponding IP port must be set to "Broadcast".
- On Passport VRs, OSPF can NOT be enabled on those IP connections to PVG VRs.
- On Passport VRs, OSPF can NOT be enabled on those IP connections to other complex.

## Option B:

- On Passport 8600, OSPF network type of those VLANs for VCCs to Passport VRs must be set to "Broadcast".
- There must be one OSPF connection between Passport 8600s locating in Area 0.0.0.0. OSPF network type for the corresponding VLAN must be set to "Broadcast".
- On Passport VRs, OSPF interface type for those IP connections to Passport 8600s must be set to "Broadcast"
- There must be one OSPF connection between Passport VRs locating in Area 0.0.0.0. Interface type for the corresponding IP port must be set to "Broadcast".
- On Passport VRs, OSPF can NOT be enabled on those IP connections to other complex.
- On PVG, OSPF can NOT be enabled on any link.

**IP Addressing and OSPF Summarization**

Since OSPF Broadcast mode is used, each single VCCs must be represented by a unique IP subnet. Nortel Networks recommend using /30 subnet mask (four addresses per subnet) to save the IP space.

Recalling from section 7.1.3.1, the number of subnets can grow very fast with the number of PVG nodes. By default, every subnet will appear in the routing table as a single entry and get advertised in the whole OSPF domain. OSPF summarization provides the added benefits of only injecting the summary-link LSA to the backbone area. This is very important because it prevents every router from having to rerun the SPF algorithm due to the topology change in the other areas. To create an environment capable of supporting route summarization, an effective hierarchical addressing scheme must be implement. The addressing structure can have a profound impact on the performance and scalability of the Succession OSPF networks. The ultimate goal is to put as few routes as possible into the routing tables and reduce the number of updates. In order to achieve this goal, Nortel Networks recommend the following rules:

- The IP scheme of VSP cards should be configured in the way that the subnet of all VSPs on a PVG shelf can appear as one static route entry on other devices.
- The range of subnets[3] assigned within an area should be contiguous so that multiple routes can be consolidated into one single advertisement to the backbone
- OSPF Summarization must be enabled on ABR and ASBR[4] (i.e. Passport 8600s or Passport VRs).

3. "Subnets" includes the IP space reserved for VSP cards and connections between PVG VR and Passport 8600/Passport VR.

4. When inter-CS2K complex calls are required, IP interfaces on Passport VRs which connect to PVG VRs do not have OSPF enabled. Passport 8600s are not be able to learn the VSPs' subnet through OSPF session unless Passport VRs redistribute the static routes into OSPF domain (Keep in mind that on Passport VR, static routes are added pointing to PVG VRs for VSPs' subnet). When exporting static routes, Passport VRs automatically become ASBRs which in turn makes address summarization possible.

### 7.1.5 Fault Tolerance

Network failure can present itself in various means. It is impractical to enumerate all possible conditions on the field. Since most of the instability is caused by the hardware problems, only link failure and card failure scenario are discussed in this section.

- Link Failure
  - With APS, if the ATM link goes down, the IP connection can be recovered within 50ms
  - Without APS, if the ATM link goes down, the IP packet can be rerouted by OSPF within 0-2 seconds
- CP Failure
  - By using OSPF plus static routes, CP failure on Passport VR can cause 0-2 second(s) outage. During this period of time, new calls cannot be made. However, established calls are not dropped.
  - By using OSPF plus static routes, CP failure on PVG VR can cause 0-2 second(s) outage. During this period of time, new calls cannot be made. However, established calls are not dropped.

#### 7.1.5.1 ATM OAM F5

ATM OAM F5 is required between the Passport 8600 and the PVG VR to ensure link resiliency. ATM OAM F5 allows the router to detect a failure on Layer 2 and cause the PVC(s) to become disabled if there is a disruption anywhere along the path. The main purpose of implementing OAM F5 is to accelerate the Layer 3 reaction on ATM service interruption along the path between PVGs and Passport 8600s. By default, no OAM F5 Loopback cells are sent. Table 34 shows the OAM F5 timers used on the Passport 8600. On Passport 8600, these timers should be adjusted from their defaults to make the link state change much quicker.

The Passport 15000 doesn't support the modification of these timers. All physical connections starting and ending at Passport/PVG must be configured with APS.

**Table 34 OAM F5 Loopback parameters for Passport 8600**

**Table 0-24**

| Parameters | Passport 8600 Default | Recommended Value |
|---|---|---|
| Transmission rate of OAM F5 Loop-back requests | 5 seconds | 1 second |
| Retry-transmission rate of OAM F5 Loopback requests | 1 seconds | 1 second |
| Number of consecutive OAM F5 Loopback replies that must be received to change the Loopback State to “up” | 3 responses | 1 response |
| Number of consecutive OAM F5 Loopback replies that must fail to change the Loopback State to “down” | 5 responses | 1 response |
| Enables/disables the transmission of an SNMP Trap when the OAM F5 Loopback changes from the<br><br>DOWN VERIFY to DOWN state or from the UP VERIFY to UP state. | disabled | enabled |

***Note:*** Static ATMInARP entries for the IP address of Passport 8600s must be manually provisioned on PVG VR/Passport VR end. In addition, dynamic ATMInARP should be turned on in the Passport 8600 with send-interval equal to 1 second. Dynamic ATMInARP is on by default in PVG VR/Passport VR. Fail to do this will cause the ip connectivity failure between Passport 8600 and PVG VR/Passport VR peers.

### 7.1.5.2 HSM/HEP and VRAP

Beginning from SN06, Nortel supports HSM (Hitless Software Migration) and HEP (Hitless Equipment Protection) for Succession VoIP solution. HSM/HEP is designed to equip customers with a carrier-grade solution as described below:

HSM gives Passport/PVG the capacitiy to upgrade software without incurring an outage to the services. HSM on PVG requires that CPs and FPs must be 1 + 1 spared so that the spare CP/FP can load the software image and provisioning data when the active CP/FP continues to provide services.

HEP is the feature to enable hot standby level of protection for the calls on PVG in the even of card failure. To achieve this goal, all FPs involving in the processing of a call must be configured as 1 + 1 spared.

Please note that, in SN06, VRAP is not carrier-grade yet. The way of VRAP operates imposes certain influence on HSM/HEP. When using HSM/HEP in parallel with VRAP active calls cannot survive CP card failure, VSP card failure, and software migration. Please check the following table before

any design or maintenance activity:

**Table 35 PVG Hardware Redundancy for VRAP**

**Table 0-25**

| FP Type | Sparing | Failure Scenario | Outage |
|---|---|---|---|
| CP3 | 1 + 1 | Active CP card reset<br>Inactive CP card reset<br>CP manual switchover | 5 - 9 sec<br>< 100 ms<br>5 - 9 sec |
| VSP3 | 1 + 1 | Active VSP card reset<br>Inactive VSP card reset<br>Active VSP card lock<br>VSP card unlock<br>VSP manual switchover | > 11 sec<br>100 - 200 ms<br>11 sec<br>< 100 ms<br>11 - 13 sec |
| ATM | Line APS | Active card reset<br>Inactive card reset<br>Active card lock/unlock<br>Inactive card lock/unlock<br>Active line lock/unlock<br>Inactive line lock/unlock<br>APS manual switchover | < 100 ms<br>< 100 ms<br>< 100 ms<br>< 100 ms<br>< 100 ms<br>< 100 ms<br>< 100 ms |

Nortel recommends customer enabling HSM/HEP with VRAP in order to gain more credit for card failure, although this combination is not carrier-grade.

## 7.2 VoIP over Gigabit Ethernet

This section provides rules for interconnecting the Passport Voice Gateway (PVG) to Gigabit Ethernet based access network by 4-port Gigabit Ethernet (GigE) FP. Additionally, capacity and throughput limitations are provided in order to aid in the engineering of traffic engineering.

***Note:*** Gigabit Ethernet connection through VSP3 front panel is not covered by this section. Also, Gigabit Ethernet implementation on other platform such as Passport VR will not be discussed here either.

### 7.2.1 Connection Summary

In SN06.2, using 4p GigE FP requires the installation of Virtual Router (VR) on PVG shelf. In addition, all VSP cards must be linked to VR by Virtual Router Access Point (VrAP). Signaling and Bearer traffic leaving VSP are sent to VrAP first and then routed by a VR to various destinations.

In order to eliminate single point of failure, dual 4p GigE FPs must be used to provide redundant entry points into core network. Each port on 4p GigE FP can route IP packets at line speed (1 Gbps). However, the maximum throughput per FP is limited to 2.5 Gbps. In consideration of this constrain, additional VR may be required as illustrated in the following diagram.

**Figure 49 Connection for PVG with Three Pairs or Less VSP3 Cards**

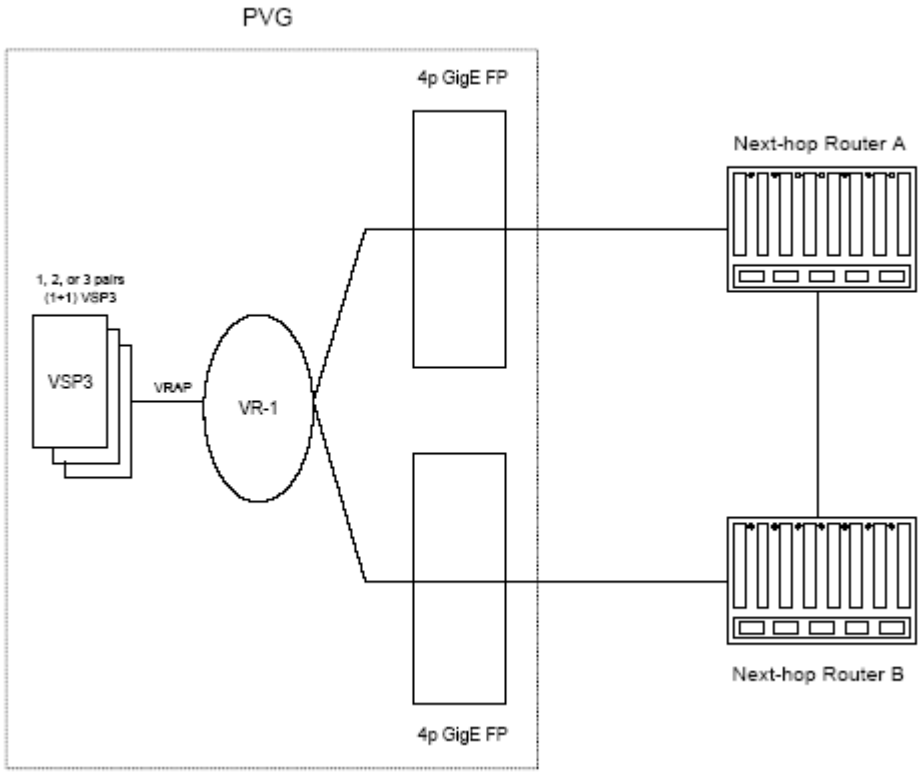


**Figure 50 Connection for PVG with Four Pairs VSP3 Cards**

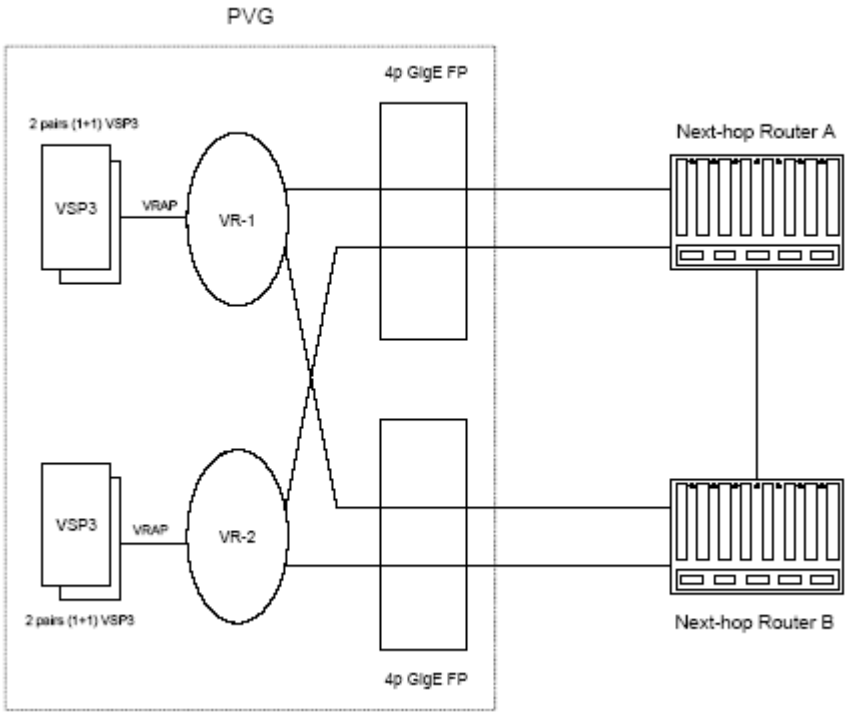
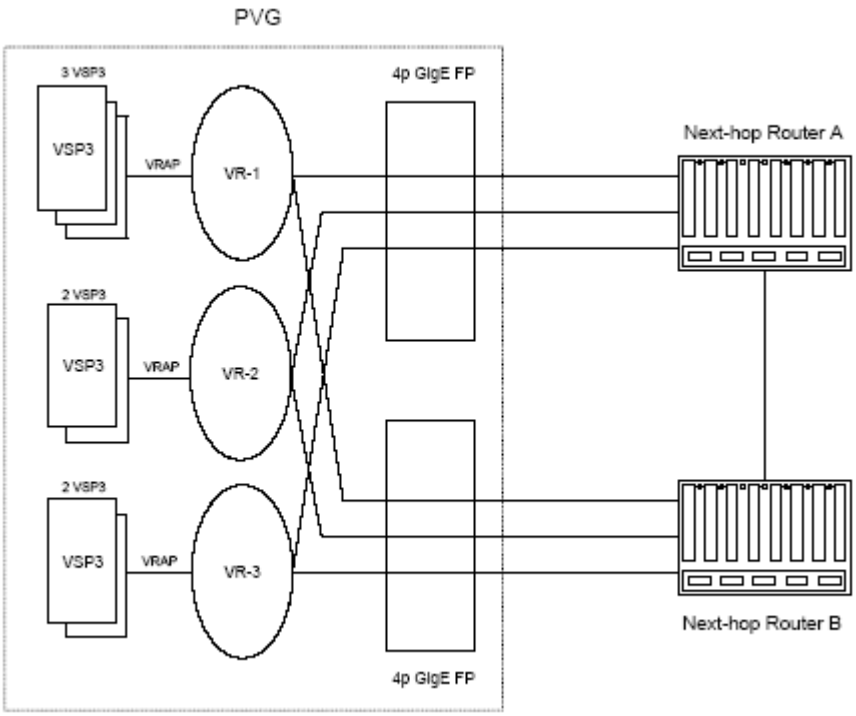



**Figure 51 Connection for PVG in N:1 Sparing**



If three or less VSP3 FPs are planned, only one VR is required as shown in Figure 49 . However, if four VSP3 FPs are installed, two VRs are required as shown in Figure 50 . Nortel also support PVG configuration with N:1 sparing, which means, one VSP card protects more than multiple other VSPs. Figure 51 shows seven (7) active VSPs subtended to three (3) VRs.

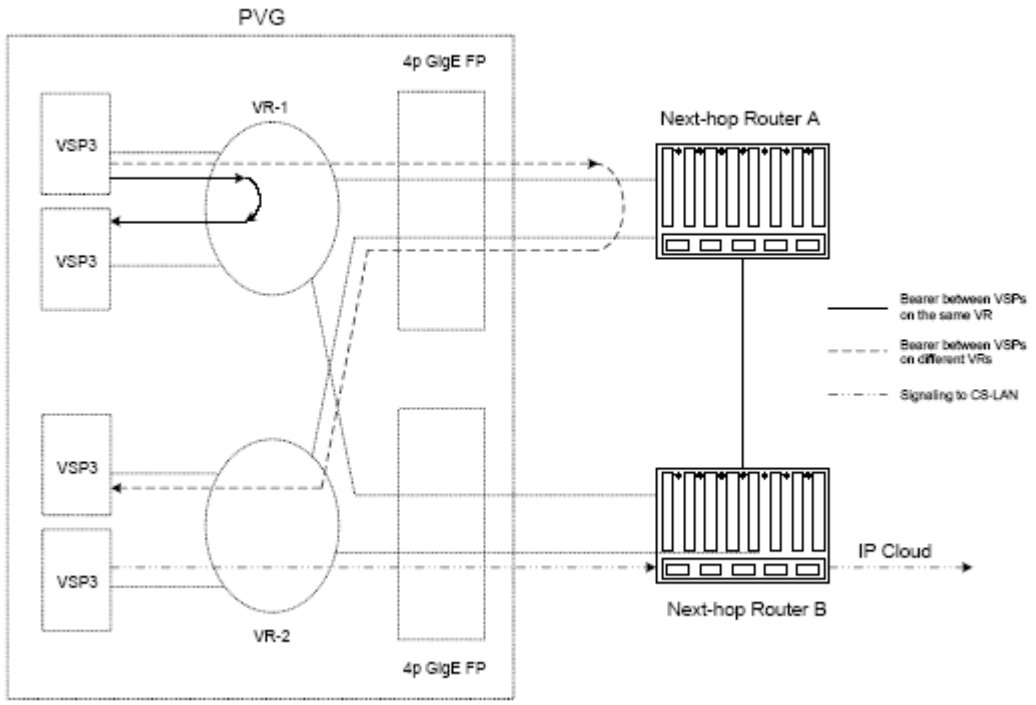
In all cases, each VR together with its associated VSP cards, is dual-homed to nexthop routers by two different links residing on different 4p GigE FPs. If link or card failure occurs, traffic can be rerouted to another available path by routing protocols.

***Note:*** When using N:1 sparing option, PVG loses carrier grade support. Nortel strongly recommend customer using 1:1 sparing to maximize redundancy and reliability. The discussion in the rest of the document is based on the assumption that 1:1 sparing is applied. Information related to N:1 sparing will be limited.

Virtual Media between VRs is not supported in SN06.2. In other words, no logical connection exists between VRs to carry routed traffic. In consideration of this constrain, the flow pattern for various streams is discussed below:

- Signaling traffic for connection control and PRI messages will leave PVG shelf to CS-LAN. It is not exchanged between VRs.
- Media traffic between VSPs which are hooked up to the same VR will be routed inside the shelf.
- Media traffic between VSPs which belong to the different VRs will be routed outside of the shelf to nexthop routers and then comes back from the different link

**Figure 52 Flow Pattern**



### 7.2.2 Redundancy Requirement on PVG

In SN06.2, Nortel recommend customer installing CP, VSP2/VSP3 FP, and 4p OC3 TDM FP in 1:1 sparing mode. The working module and protection module must be in adjacent slots.

Although card level redundancy for 4p GigE FP is not supported in current load, Nortel recommend locating 4p GigEP in adjacent slots too for future migration to HEP capable release.

**Table 36 Card Sparing Requirement**

Table 0-26

| Card Type | Support Cards | Sparing | Remarks |
|---|---|---|---|
| CP | CP3 | 1:1 | |
| VSP FP | VSP2, VSP3 | 1:1<br>N:1 | N can be up to seven (7) in current release. However, this is not Carrier Grade |
| TDM FP | 4pOC3ChSmIr | 1:1 | LAPS used to provide TDM HEP support |
| GigE FP | 4pGE | N/A | Failover is triggered by routing protocol |

### 7.2.3 Bandwidth Requirement

The bandwidth requirement for VoIP over Gigabit Ethernet is given below. The value is different for media traffic and non-media traffic.

**Table 37 Media Bandwidth Requirement for VSP Card**

Table 0-27

| Codec | Voice Sample Rate (ms) | Bandwidth per DS0 (kbps) | |
|---|---|---|---|
| | | VSP2 | VSP3[a] |
| G.711 | 10 | 126.4 | 127.25 |
| | 20 | 95.2 | 96.05 |
| G.729 | 10 | 70.4 | 71.25 |
| | 20 | 39.2 | 40.05 |

a. The voice stream will also include RTCP packets, 80 bytes per second. RTCP is not supported on VSP2

Given the fact that each VSP3 supports up to 2016 DS0s, the total amount of bandwidth required by a fully-provisioned VSP3 is 2016 * 127.25 = 257 Mbps. Leaving 5% of total bandwidth to signaling messages and routing protocols, each GigE port can only host traffic from maximum three (3) VSP3

cards. As the consequence, there can not be more than three (3) fully-provisioned active VSP3 cards per VR because each VR occupies one GigE port on each 4p GigE FP. By splitting local VSP cards into multiple groups and dedicating one VR for each group, we can guarantee that, even in the event of failure, there is no more than 1 Gbps traffic located on a GigE port. Also, at any time, no more than 2.5 Gbps traffic is demanded on a 4p GigE FP.

The number of VRs per PVG shelf is summarized in the following table:

**Table 38 Maximum Bandwidth**

Table 0-28

| Number of Active VSP3 | Number of VRs | Max Bandwidth per FP[a] |
|---|---|---|
| 1 | 1 | 257 Mbps |
| 2 | 1 | 514 Mbps |
| 3 | 1 | 771 Mbps |
| 4 | 2 | 1028 Mbps |
| 5 | 2 | 1285 Mbps |
| 6 | 2 | 1542 Mbps |
| 7 | 3 | 1799 Mbps |

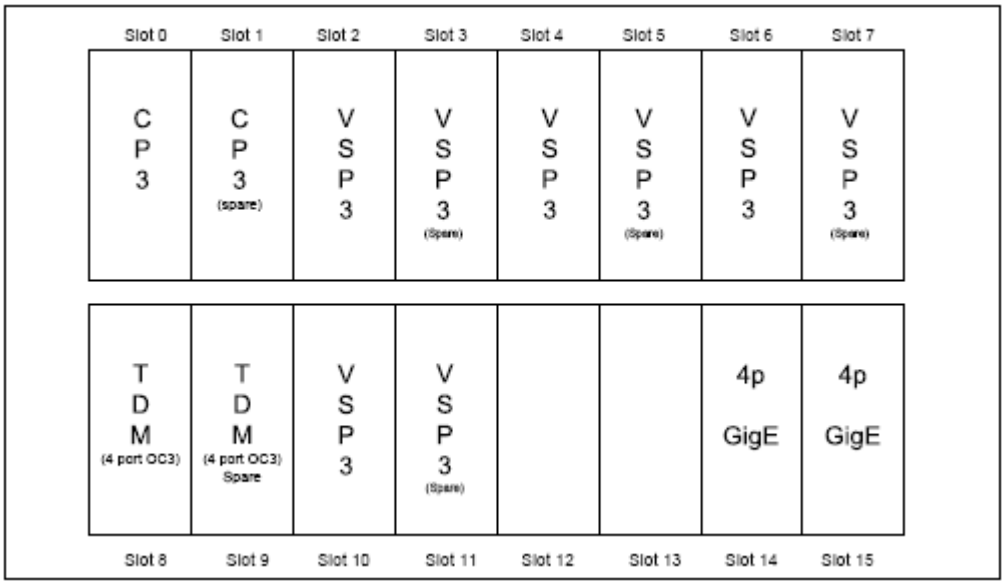
a. This represents the worst-case scenario, which is, one 4p GigE FP fails. As the result, all traffics are switched to another 4p GigE FP.

Please note that, Nortel do not recommend using the rest of open GigE ports on 4p GigE FP for any other purpose.

### 7.2.4 Shelf Layout

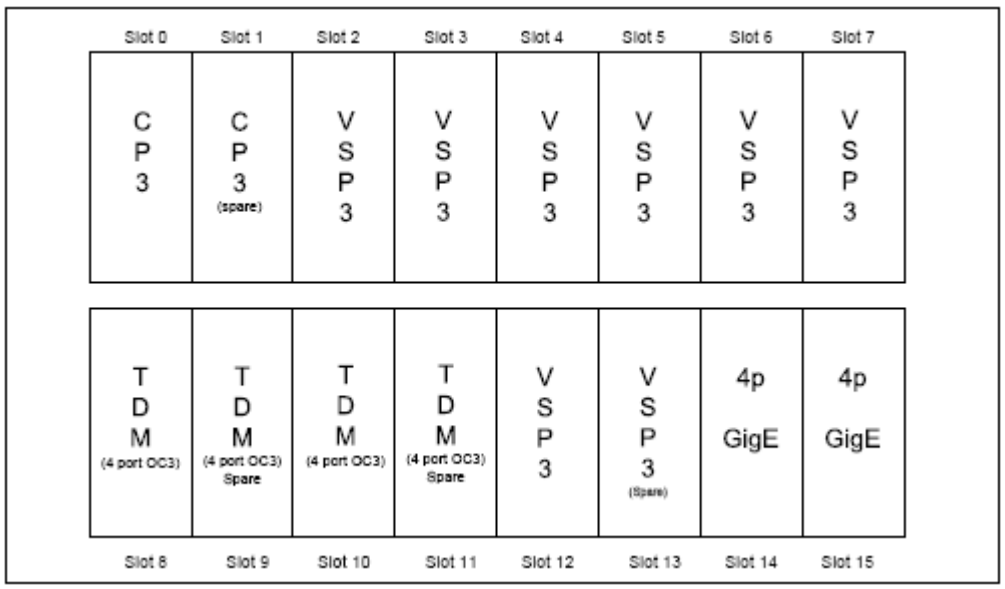
The following diagram shows shelf layout for a fully loaded PVG using 1:1 sparing option. The maximum PVG capacity in SN06.2 is 8064 DS0s. This limitation is imposed by 4-port OC3 TDM card.

**Figure 53 PVG Shelf Layout for 1:1 Sparing**




The following diagram shows shelf layout for a fully loaded PVG using N:1 (N = 7) sparing option. The maximum PVG capacity in SN06.2 is 14,112 DS0s. This limitation is imposed by maximum number of VSP cards.

**Figure 54 PVG Shelf Layout for 7:1 Sparing**



### 7.2.5 IP Addressing

Connection control (CTRL/MG) and bearer (IPMCONN) components on each VSP card must be identified by unique IP addresses. If PRI trunks are provisioned, one additional unique IP address should be added for PRI signaling (CTRL/SG), which must be equal to the IP address of Connection Control (CTRL/MG) plus four (4). All these addresses can be in the same subnet, or in the different /30 subnet. This gives our customers more room to introduce VSPs into their IP networks.

IP scheme for PVG is quite flexible too. Across the shelf, IP address space for all VSPs can be reserved in one subnet, or planed in /30 format.

**Single Subnet Option**

In this case, all VSP IP addresses on a PVG belong to the same subnet. The subnet mask depends on two factors:

- The number of VSP cards per VR
- Whether PRI trunk is expected

For instance, here is a PVG with 4 pairs of VSP cards serving PRI trunk. Two (2) pairs of VSP3 cards on a VR require a total amount of 6 IP addresses. To cover them by one subnet, we need /28 (255.255.255.240) subnet mask to book fourteen (14) usable IP addresses. six (6) of them are used by VSP cards and one (1) of them is used as default gateway on VrAP side. The whole shelf needs two /28 subnets.

Nortel recommend this approach for new-installed PVG shelf.

**Figure 55 IP Address Scheme for PVG with Dual VRs**

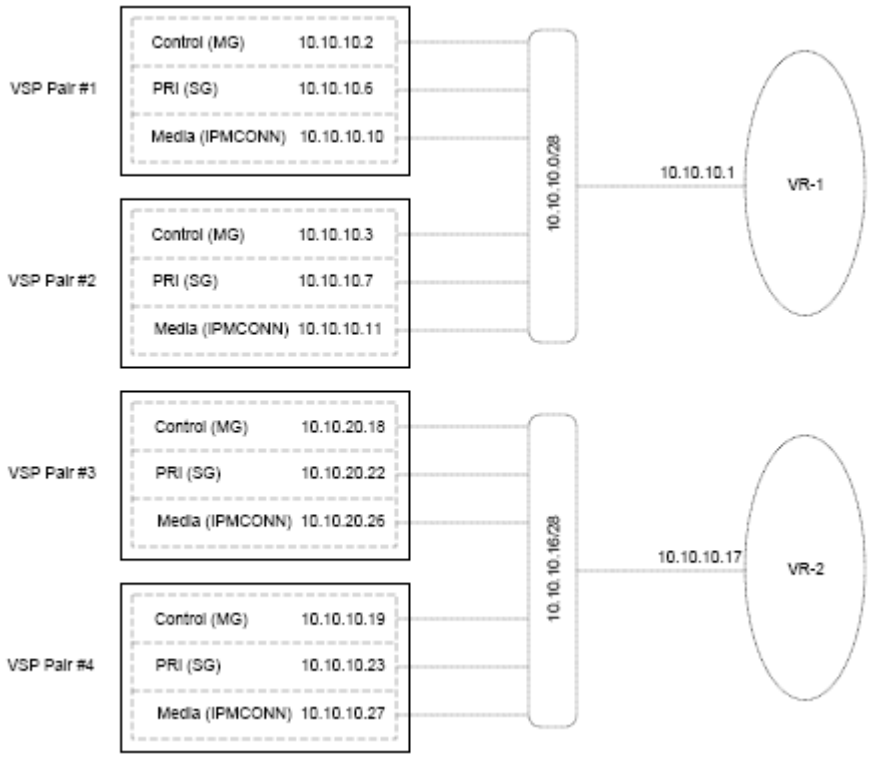
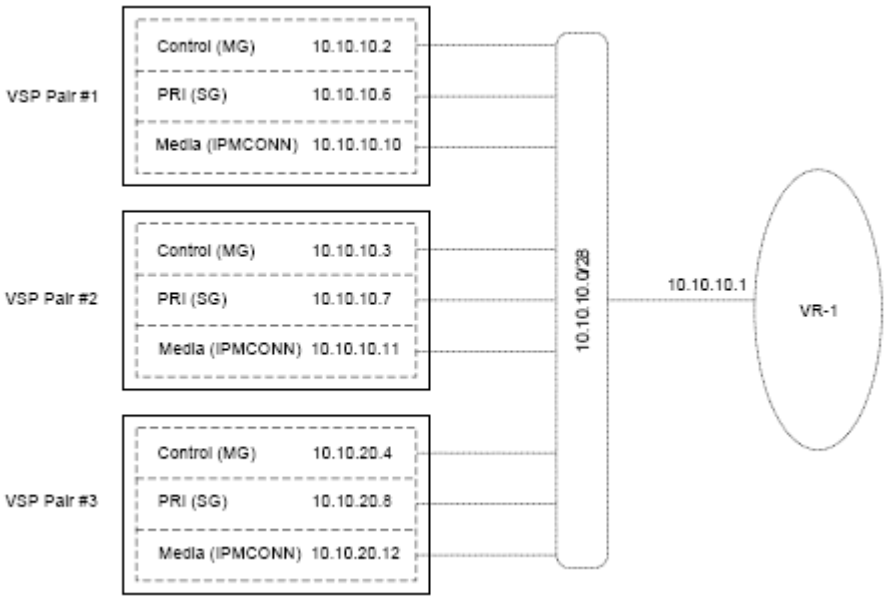



**Figure 56 IP Address Scheme for PVG with Single VR**



The following table lists all possible scenarios:

**Table 39 IP Address Space for ISUP-Only PVG in Single-Subnet Configuration**

Table 0-29

| Number of Active VSP3 per VR | Number of Required IP per VR[a] | Subnet Mask |
|---|---|---|
| 1 | 3 | /29 (8) |
| 2 | 5 | /29 (8) |
| 3 | 7 | /28 (16) |

a. Includes VrAP IP address as default gateway

**Table 40 IP Address Space for PVG with PRI Trunks in Single-Subnet Configuration**

Table 0-30

| Number of Active VSP3 per VR | Number of Required IP per VR[a] | Subnet Mask |
|---|---|---|
| 1 | 4 | /29 (8) |
| 2 | 7 | /28 (16) |
| 3 | 10 | /28 (16) |

a. Includes VrAP IP address as default gateway

**/30 Subnet Option**

In this setup, each component on each VSP needs one /30 subnet, which gives us two (2) usable IP addresses. One of them is provisioned on VSP side, and another one is provisioned on VrAP side as default gateway. For a fully loaded PVG, four (4) pairs of VSP cards require twelves (12) /30 subnets, which in turn, increases the total number of IP addresses to forty-eight (48).

Please note that, all /30 subnets for VSPs on a PVG must be designed in continuous manner so they can be summarized by routing protocol.

Nortel recommend this approach for those customers who are migrating their existing PVGs from ATM FPs to GigE FPs.

### 7.2.6 Routing Rules

If next-hop router is not carrier grade, Nortel require customers to connect PVG to dual GigE capable routers.

***Note:*** It is possible that customer connect PVG to a single carrier grade router. However, the rest of discussion is based on the assumption that daul routers exist.

In overall picture, Nortel position PVG VR using 4p GigE FP as an access device at edge. In any condition, PVG VR can only be used as access point for VSPs located on local shelf. Keep this in mind, we will discuss the detailed network design rules in the following sections.

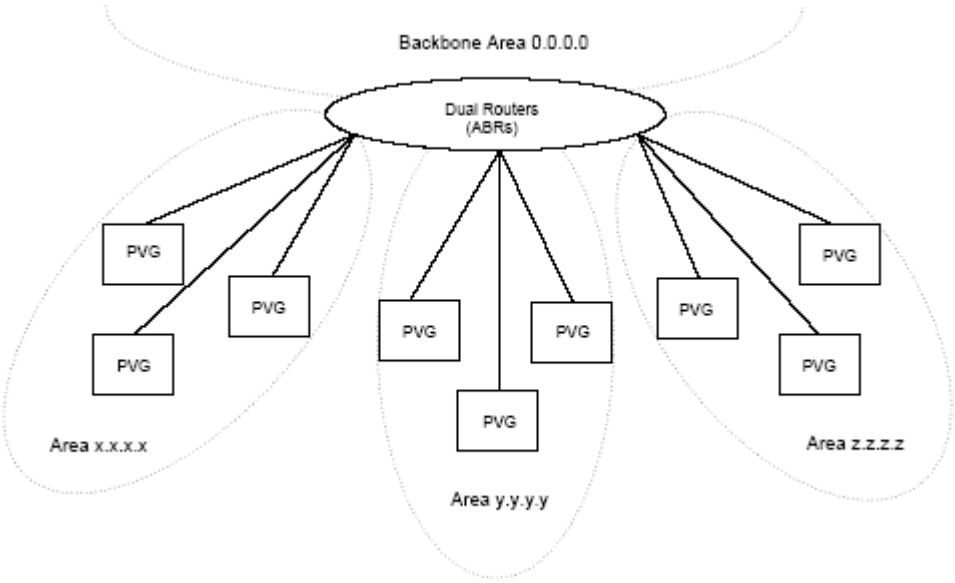
#### 7.2.6.1 OSPF

OSPF is the only routing protocol Nortel support in SN06.2. Routing table created by OSPF is checked for outbound traffic leaving PVG shelf to remote subnets. The destination can be CS-LAN devices, or other PVGs in the networks.

**OSPF Areas**

As a general rule, Succession recommends a hierarchical design with multiple OSPF areas to reduce the size of routing table and minimize the impact of flapping connections. For PVG, it must be positioned in non-backbone area. In other words, no interface should be put in Area 0.0.0.0.

**Figure 57 OSPF Areas Planning**




Please note that, the solid line between a PVG and dual routers in the above diagram only represents the logical connection. In reality, a PVG may, or may not be directly connected to ABRs.

### OSPF Interface Design

All GigE links must have OSPF enabled. Some parameters need to be adjusted from default values. The following table lists the rules for planning and provisioning OSPF on 4p GigE FPs:

**Table 41 OSPF GigE Interface Parameter**

Table 0-31

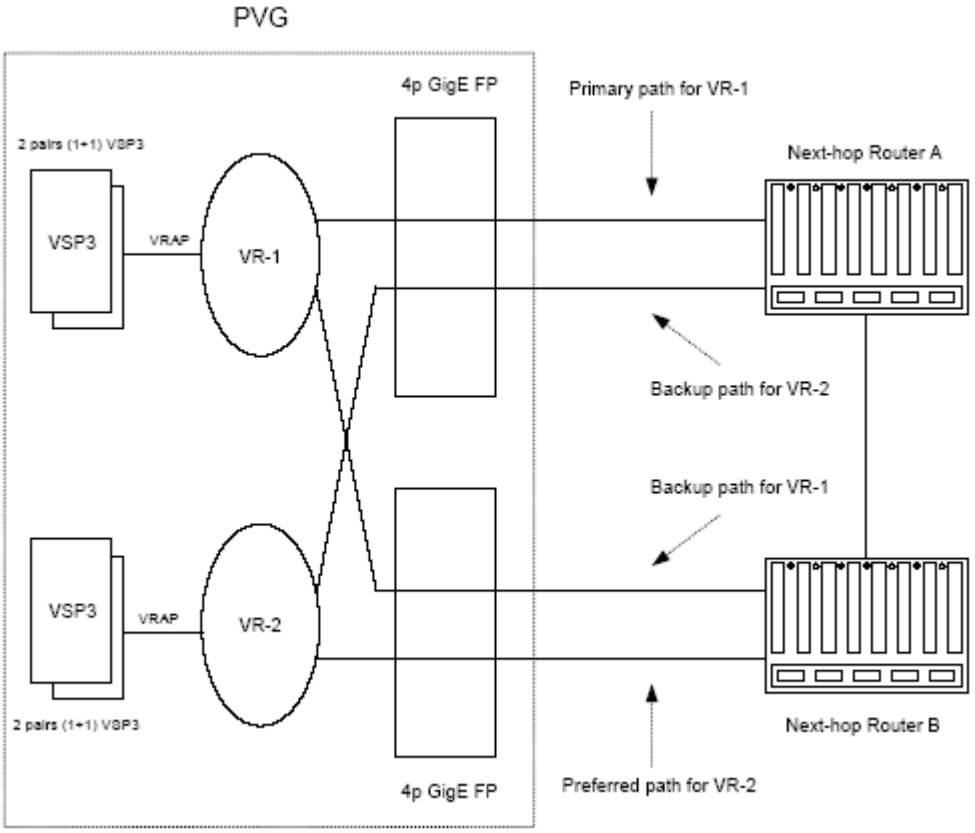
| Item | Default Value | Required Value |
|---|---|---|
| Area ID | 0.0.0.0 | x.x.x.x[a] |
| Interface Type (ifType) | broadcast | broadcast |
| Hello Timer (helloInterval) | 10 seconds | 1 second |
| Dead Timer (rtrDeadInterval) | 40 seconds | 4 seconds |

a. Cannot be all-zero

***Note:*** Extreme caution should be used when manipulating above parameters on PVG. The values should be adjusted and verified on nexthop routers too. Otherwise, PVG VR cannot form adjacency with other OSPF devices.

The cost of GigE interface should be designed in the way that, for each VR, one link is more preferred than another one by both incoming and outgoing traffic. As the result, for a given destination, only one GigE link to next-hop router is carrying traffic at a certain time. The standby link is only used when the primary link is impaired. Please note that, if multiple VRs exist, the preferred links cannot be on the same 4p GigE FP.

**Figure 58 Primary Path v.s. Backup Path**




Today, most routers have ability to manually define OSPF cost per interface. Another way to influence OSPF cost is to change the default reference bandwidth (100 Mbps) in the algorithm. Based on this fact, Nortel strongly recommend customers engineering the OSPF cost on next-hop router side carefully. Otherwise, non-optimal routing paths can represent themselves under certain circumstances. As the consequence, GigE ports on PVG can be used to route transmit traffic which is not terminated on local VSPs. This can potentially result in bandwidth starvation for Succession traffic.

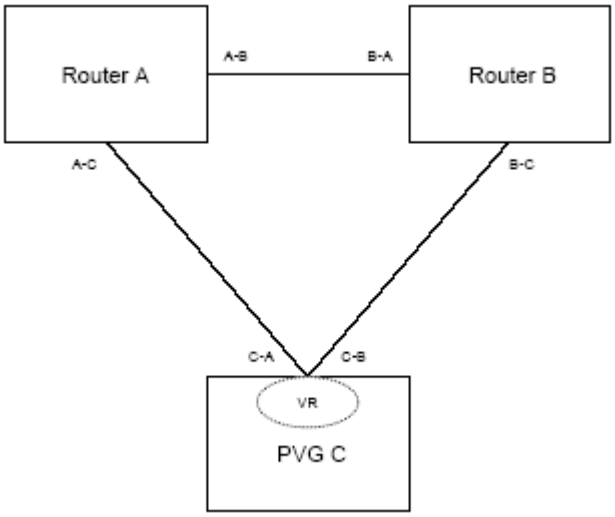
As a requirement, dual next-hop routers must have direct connection between them in the same OSPF area as PVG. This connection can be in the form of physical interface or subinterface. Nortel strongly recommends link and card level protection to minimize the possiblility of lossing this connection. If nexthop router is Passport 8600 from Nortel,  MLT in the form of multiple Gigabit Ethernet links across different cards is required.

The main reason to require protection on this connection is to avoid the scenario that GigE links to PVG VR become the best route, or even the only physical path from one next-hop router to a subnet on another next-hop router. In the case of link failure, it is possible that packets destined to non-PVG subnets traverse GigE links. This will lead to unexpected bandwidth consumption on both GigE ports and GigE FPs.

In normal situation, the above issue can be avoided by carefully engineering the OSPF cost per interface. On next-hop routers, the sum of OSPF cost on GigE interfaces to a VR must be greater

than the OSPF cost for their inter-connection. The following diagram uses single-VR configuration as an example to summarize the requirement. Please note that, the same rule applies to dual-VR configuration.

**Figure 59 OSPF Interface Cost**




Here, the syntax of OSPF cost value of X-Y means:

- OSPF cost is configured on device X
- The other end of the link is device Y
- The value of influence the route decision for traffic flowing from device X to device Y

Assuming PVG C chooses Router A as preferred path, here are the rules:

- A-B = B-A
- (C-A + B-C) > B-A
- (C-B + A-C) > A-B
- C-A < C-B
- A-C < B-C

The above rules can only guarantee the optimal OSPF route decision without network failure. However, at the time of link failure, PVG VR may still become a routing device for non-local traffic. Thus, if inter-router link between next-hop routers is not protected, or does not exist at all, Nortel strongly recommend customer applying IP filter on every GigE port, which drops the packets whose destinations are not VSP subnets advertised by the PVG VR associated with the port.

In addition to GigE links, all VSP subnets (including connection control, bearer, and PRI signaling if applicable) must be added to OSPF in the form of passive interfaces. In other words, on VrAP side, interface type for those IP ports which terminate CTRL/MG, IPMCONN (and CTRL/SG if applicable) of VSP cards must be set to "PASSIVE". The area ID must be identical to the one used by GigE interfaces.

**OSPF Summarization**

OSPF route summarization must be enabled on those routers which act as ABRs to PVGs in the direction of from and to the OSPF backbone. IP addressing scheme must be carefully designed so that the range of subnets assigned within each OSPF area is contiguous. By this way, the backbone receives all the aggregate addresses and in turn will publish them, already summarized, into other areas.

One of ultimate goals is to put as few routes as possible into PVGs' routing tables and reduce the number of updates. In addition, instability inside an area will not be propagated to the scope beyond the local area.

### 7.2.6.2 Static Routes

In SN06.2, Static Route is supported, but extreme caution should be performed. Due to the fact that Layer-1 failure may not trigger Layer-3 reaction, blackhole can be created in the network by using Static Route only.

### 7.2.7 Fault Tolerance

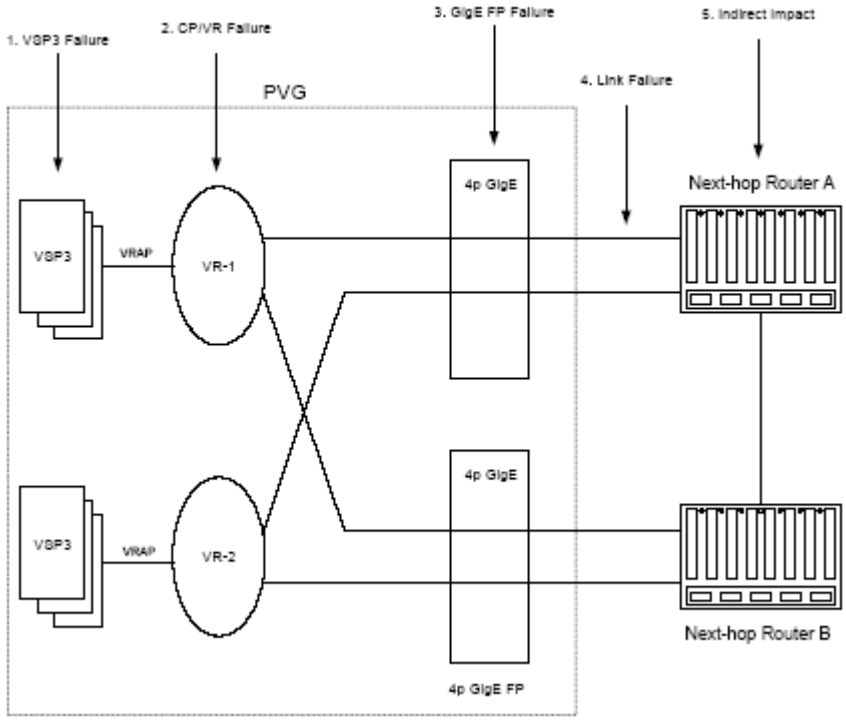
#### 7.2.7.1 HSM/HEP

To gain maximum benefit from HSM/HEP feature in the code, Nortel strongly recommend enabling HSM/HEP on PVG at shelf level.

#### 7.2.7.2 Network Failure

When using 4p GigE FP in Succession solution, network failure can present itself at various points as shown in the following diagram.

**Figure 60 Point of Failure**




As direct result of any type of failure, voice call can be interrupted. The following table provides the information for service outage in various failure conditions. Please note that, all values in this section is based on the assumption that PVG shelf is provisioned with maximum carrier grade support and all rules in the previous sections are strictly followed.

**Table 42 Outage for Various Failure Conditions**

Table 0-32

| Point of Failure | Failure Condition | Expected Outage |
|---|---|---|
| VSP3 | Manual Switchover<br>Card Reset<br>Card Lock/Unlock | < 100 ms |
| CP3 | Manual Switchover<br>Card Reset<br>Card Lock/Unlock | 70 - 90 seconds |
| 4p GigE | Card Reset<br>Card Lock/Unlock | 4 - 6 seconds |
| GigE Link | Link Pull | 4 - 6 seconds |
| Nexthop Router | Router Reboot<br>OSPF Restart<br>OSPF Hanging | Vendor specific |

### 7.2.8 QoS

DiffServ marking for Succession traffic is done automatically on VSP card at hardware level. So it will not bring down the throughput of GigE port/FP. Current release provides the flexibility to set Diff-Serv bits of packets for connection control, media traffic and PRI signaling seperately. According to general Nortel QoS requirement, the following values are recommended from defaults:

**Table 43 DiffServ Bits Marking**

Table 0-33

| Traffic Type | Component | Default | Recommended |
|---|---|---|---|
| Connection Control (CTRL/MG) | nsta vgs ctrl/mg UdpPort diffServ | 46 (EF) | 40 (CS5) |
| Media (IPMCONN) | nsta vgs defaultIpMediaDsf | 46 (EF) | 46 (EF) |
| PRI Signaling (CTRL/SG) | nsta vgs ctrl/sg SctpPort diffServ | 46 (EF) | 40 (CS5) |

The recommended value will not make any difference if routers in IP cloud only support 4 queues. However, if they support 8 queues, packets from connection control and PRI signaling sessions will have higher priority than those from bearer streams.

# 7.3 Frame Relay Multi Services on a PVG

## 7.3.1 Introduction

This section provides specific guidelines for a Multi-Service Passport Voice Gateway (PVG), where the PVG is connected to Juniper M-Series (IP over ATM) to provide voice services, and it is equipped with DS-3 Frame Relay interfaces to provide Frame Relay / BNX services.

This section describes the engineering required to ensure that the PVG will maintain optimal performance and reliability for voice and Connection Control traffic while also carrying Frame Relay over IP over ATM.

### 7.3.1.1 Scope

The recommendations presented in this section are based on release SN06 on a Passport 15000 platform, where the voice traffic was configured as G.711 and 10 milliseconds codec.

The analysis presented centers on the behavior of the 4-port OC-12 FP when 2 ports carry voice and Connection Control traffic (a.k.a the voice ports) and 1or 2 of the remaining OC-12 ports carry Frame Relay over IP over ATM.

In addition, this section is based on the impact to the PVG due to:

- addition of a Virtual Router. This VR is NOT used to carry PVG voice or Connection Control traffic, but *only* for Frame Relay services (FR over IP over ATM).
- The VR for the Frame Relay / BNX is not part of any core Frame Relay / BNX over IP network.
- Static Routes (no dynamic routing protocol) are used by the VR to route the Frame Relay (over IP over ATM) traffic to the CORE IP network.
- activation of 1792 Frame Relay UNIs and 3 DLCIs per FrUni, when there are 8 DS-3 Frame Relay interfaces (two 4-port DS3 FPs).
- activation of Frame Relay-related alarms
- activation of Frame Relay accounting to the Cp

This section does not include analysis of the impact caused by Frame Relay alarms on both the MDM and the SDM.

## 7.3.2 Multi Service considerations

### 7.3.2.1 Frame Relay traffic flow through a PVG

Figure 0-1 depicts a Frame Relay services-enabled PVG with 4 (1+1) protected VSP3s, 2 PQC-12 4-port OC-12 FPs and two 4-port DS3 Ch Frame Relay cards.

The voice and the Connection Control traffic is carried by two LAPS ports (a.k.a voice ports) of the 4-port OC-12 FP, whereas the FR/BNX traffic is carried on two of the available ports of the pair of 4-port OC-12 FPs (a.k.a the FR WAN ports). [1]

The Frame Relay / BNX traffic ingress the PVG through any of the ports of the 4-port Channelized DS3s. Since these ports are not protected, there are 8 ports injecting Frame Relay /BNX traffic to the PVG.

Since the Frame Relay traffic requires IP to reach its destination, a Virtual Router is required on the PVG. This VR is not used to carry neither the bearer nor the Connection Control traffic of the PVG.

The Frame Relay traffic can be routed by the VR to any of the FR DS3 ports, or it can be forwarded to an external router through any of the 2 FR WAN ports.

1. 2 LAPS ports are used to carry voice traffic on each pair of OC-12 FPs. In Figure 0-1 the remaining four ports, used to carry Frame Relay /BNX over IP over ATM, were configured as 2 LAPS ports.

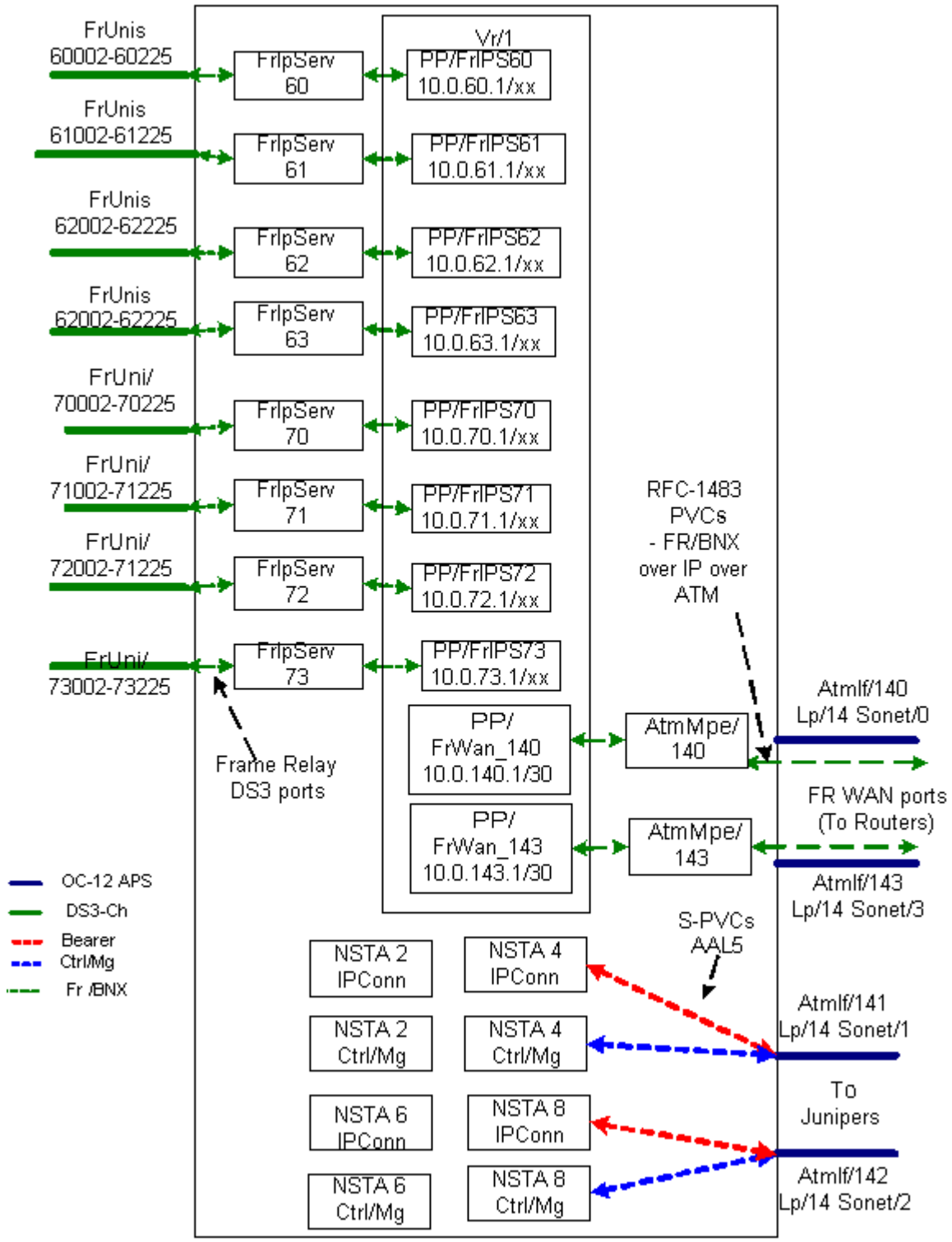



**Figure 0-1 High level view of a Frame Relay-enabled PVG (IP over ATM)**

### 7.3.2.2 Activation of Frame Relay Services

As depicted in Figure 0-1, Frame Relay traffic does not flow through the VSPs, but through the 4-port DS3 Ch, the VR and the 2 FR WAN ports of the pair of 4-port OC-12 FPs. In order to route this traffic, the PVG shelf (a.k.a the Passport 15000), has to be a member of a Frame Relay /BNX network. The following Passport attributes are required to configure the PVG as a Frame Relay node:

- Routing dpn routing ID XX
- Rtg dpn module ID
- set mod regionid XX
- Module vcs networkIdCode XXXX

Note: Configuration of these attributes will cause a shelf restart. All VSP traffic will be affected (i.e. all voice calls and Connection Control signalling will be reset).

### 7.3.2.3 Virtual Router

As depicted in Figure 0-1, the Virtual Router requires a a Protocol Port for each DS3 interface. The size of the subnet mask of the IP address of the Protocol Port depends on the number Frame Relay UNIs configured per port[2].

In order to forward the Frame Relay /BNX (over IP over ATM) traffic to the core Frame Relay / BNX over IP network, one or more Protocol port is required. These ports are referred to as FR WAN ports and require a /30 subnet mask each.

***For this release, the VR is NOT running any dynamic routing protocol***. In order to forward traffic to the core Frame Relay / BNX over IP network, the VR requires one static route for each of the FR WAN ports. They are the next hops to reach the core Frame Relay / BNX over IP network.

Additionally, the core Frame Relay / BNX over IP routers connecting to the PVG must be configured with one static route in order to reach any of the Frame Relay UNIs. The next hops for any of the static routes are the IP addresses of the FR WAN Protocol ports.

For this release, the VR can NOT be part of the core Frame Relay / BNX over IP network.

### 7.3.2.4 HSM / HEP

Carrying Frame Relay / BNX services on a PVG does not affect HSM with regards to the voice-related traffic. However, Frame Relay /BNX will not survive HSM. All Frame Relay / BNX traffic will be reset during the software migration.

### 7.3.2.5 Operational Considerations

When HSM takes place, after the Active Cp switches to the Stand-by Cp, each of the Frame Relay DS3 interfaces will generate an alarm. Generation of these alarms does not affect voice-related traffic, but it causes the CPU utilization of the active Cp to increase to 100%.

2. In Figure 0-1 each Protocol Port has a /24 subnet mask as there are 224 FRUnis on each DS-3 interface.

During the time when the Frame Relay alarms are generated, any other alarms (such as link utilization, if applicable) are not lost, but might not be noticed due to the high number of Frame Relay alarms.

**Note: any other additional feature such as IPCos and / or IPDiffServ may affect HSM and it should not be present on these FPs**[3].

### 7.3.3 Inter-connectivity Options

#### 7.3.3.1 Performance of the 4-port OC-12 FP for frame-based traffic

The bearer path and the Connection Control signalling are carried as AAL5 S-PVCS. These S-PVCs are switched at the line speed of the OC-12 port. There are no performance limitations for the 2 LAPS ports carrying voice-related traffic.

The Frame Relay / BNX over IP (over ATM) is carried as AAL5 PVCs. This traffic is frame-based and is not switched at line speed. The ATM FP 4-port OC-12 FP has performance limits for frame-based traffic. This limitation applies *only* to the Frame Relay WAN ports.

#### 7.3.3.2 Required number of Frame Relay-enabled OC-12 ports

**Table 0-34**

| # of 4-p FR DS3 FPs | # of VSP3s (1+1) | # of APS OC-12 ports (Voice) | # of APS OC-12 ports (FR/BNX) |
|---|---|---|---|
| 2 | 4 | 2 | 1 |
| 4 | 3 | 2 | 2 |
| 6 | 2 | 1 | 3 |
| 8 | 1 | 1 | 4 |

**Table 44 : Number of OC-12s required to carry voice and Frame Relay / BNX traffic**

Table 44 describes the number of OC-12 required to carry the Frame Relay / BNX traffic as a function of the number of 4-port DS3 Frame Relay interfaces.

#### 7.3.3.3 Minimum Frame Relay configuration

As depicted in Figure 0-2 and Table 44, a HSM / HEP-enabled PVG, equipped with 4 (1+1) VSP3s, can be equipped with two 4-port FR DS3s. This is referred to as the 'minimum' amount of Frame Relay DS3s that be carried by the PVG.

3. The Frame Relay / BNX over IP traffic is carried in two RFC-1483 PVCs (i.e. IP over ATM). In order to carry frame-based traffic such as the two AAL5 PVCs, the AtmMpe feature is required as part of the software for the pair of 4-port OC-12 FPs.

The bearer and the Connection Control signalling are carried by two OC-12 LAPS ports (a.k.a voice ports) connecting to the Junipers. The FR/BNX traffic can be carried on any of the available ports of the pair of OC-12 FPs (a.k.a the FR WAN ports).

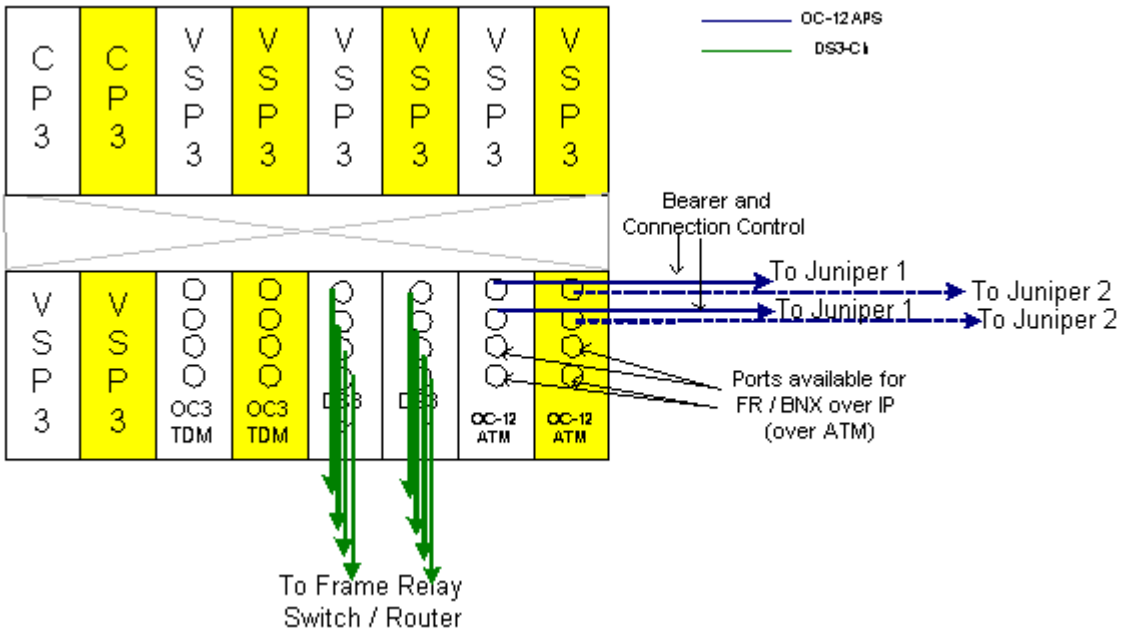



**Figure 0-2 Hardware view of a Frame Relay-enabled HSM PVG shelf (IP over ATM)**

In order to carry Frame Relay / BNX over IP (over ATM) traffic, the FR WAN port has to be linked to a Protocol Port of the Virtual Router. This port[4] can NOT be configured with any dynamic routing protocol (i.e. static routes are required to forward traffic to the Frame Relay / BNX core IP network). Traffic on these FR WAN ports must be traffic destined to the Frame Relay interfaces only.

Note: For SN06, Nortel Networks recommends:

- The VR must NOT part of the Frame Relay / BNX over IP core network
- The only IP traffic incoming / leaving the PVG through the FR WAN ports must be Frame Relay / BNX traffic destined to the Frame Relay DS3s of the PVG.

### 7.3.3.4 Maximum Frame Relay configuration

As depicted in Figure 0-3 and Table 44, a HSM / HEP-enabled PVG, equipped with 1 (1+1) VSP3s, can be equipped with eight 4-port FR DS3s. This is referred to as the 'maximum' amount of Frame Relay DS3s that be carried by the PVG.

4. Only one FR WAN port is required. However, the customer may decide to configure is as either LAPS or may decide to use to LAPS ports to forward the traffic to the Frame Relay / BNX IP core network.

The bearer and the Connection Control signalling are carried by one OC-12 LAPS port (a.k.a voice ports) connecting to the Junipers. The FR/BNX traffic will be carried by four of the available ports of the pair of OC-12 FPs (a.k.a the FR WAN ports).

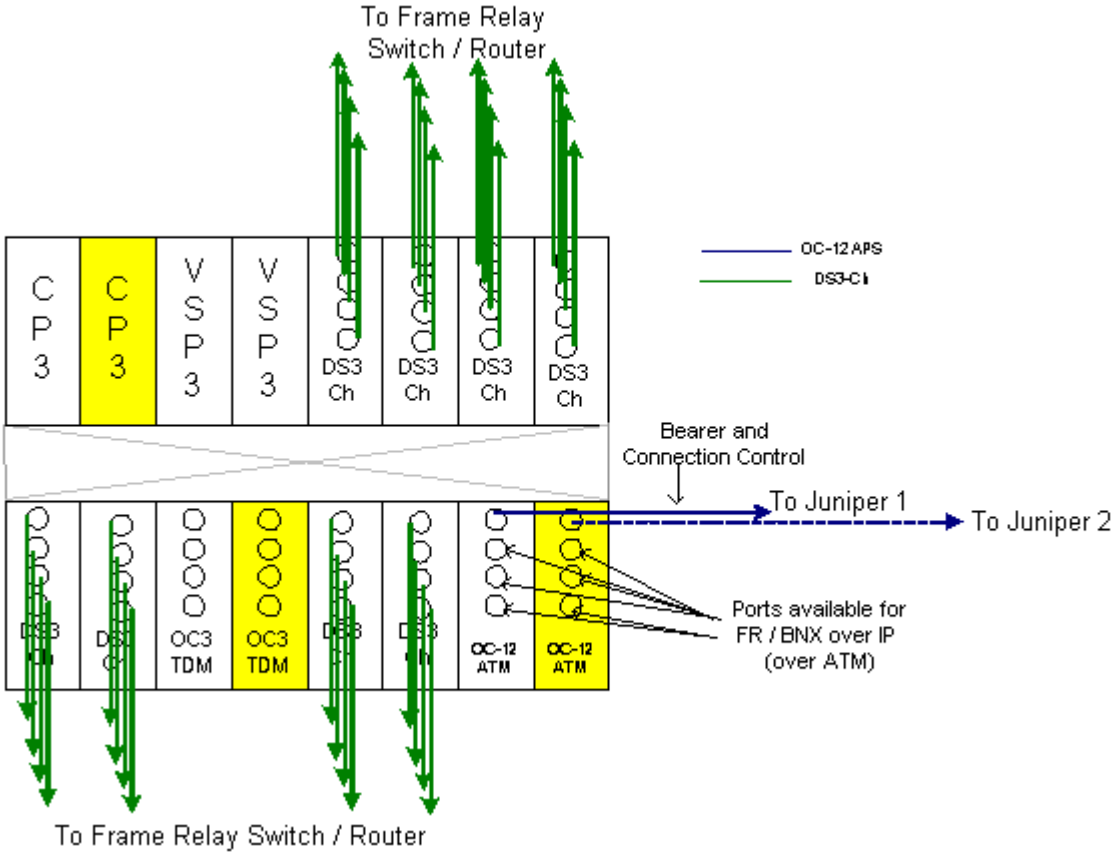



**Figure 0-3 Hardware view of a Frame Relay-enabled HSM PVG shelf (IP over ATM) - Maximum # of FR DS3s**

Due to the performance limitations of the 4-port OC-12 FPs, if the link utilization of the FR WAN ports exceeds 75% of an OC-12, Frame Relay traffic will be discarded. The voice and Connection Control signalling traffic is not affected by this limitation since it is forwarded at line speed.

Note: For SN06, Nortel Networks recommends:

- The VR must NOT part of the Frame Relay / BNX over IP core network
- The only IP traffic incoming / leaving the PVG through the FR WAN ports must be Frame Relay / BNX traffic destined to the Frame Relay DS3s of the PVG.
- On any of the OC-12 FPs, only 2 of the available ports can be used to carry Frame Relay WAN ports are configured on the same 4-port OC-12 FP.

## 7.4 PVG Gigabit Ethernet to Passport 8600s (IP over Ethernet)

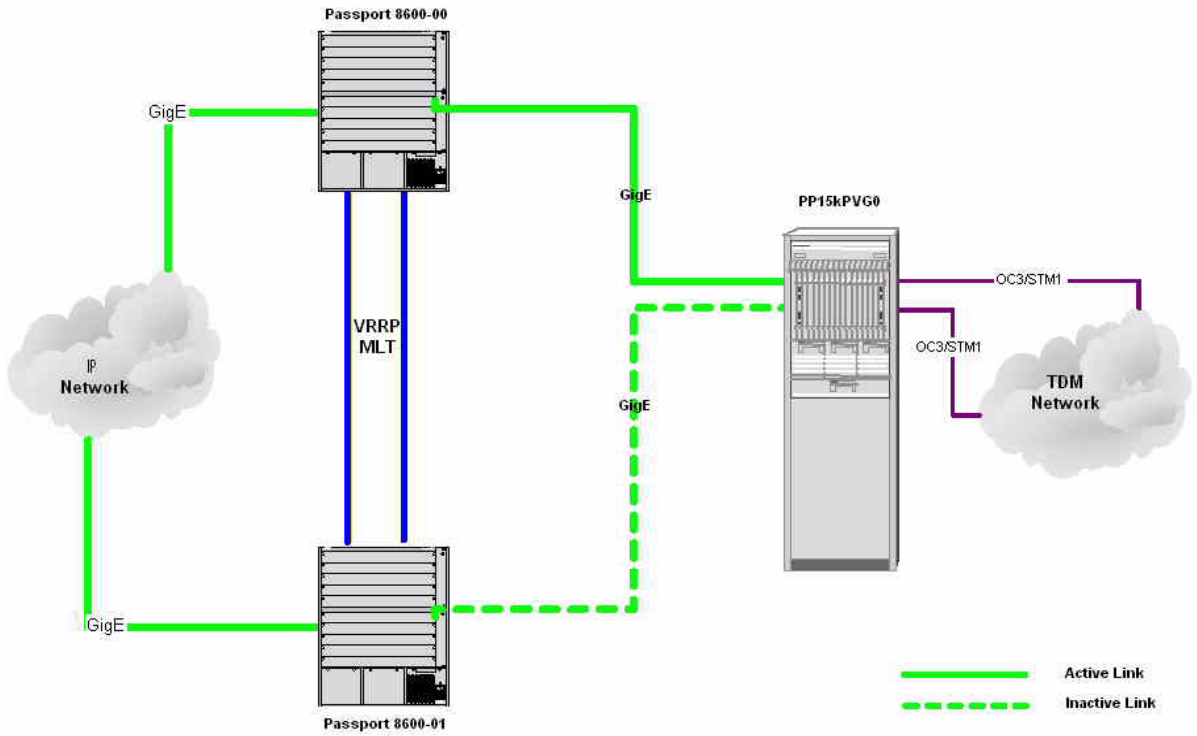
***Note:*** This option is only available on PVG 15000.

With the advent of Gigabit Ethernet on VSP3s, it is now possible to interconnect the PVG 15000s equipped with VSP3s into the Passport 8600s via Gigabit Ethernet and significantly expand the capacity of the Trunk Gateway Site while improving the Resiliency failover mechanism in comparison to the ATM interconnection to the Passport 8600.

The Passport 8600s equipped with 8608GBIC modules provide a cost effective solution for interconnecting PVG 15000s into the CS-LAN. Figure 46 depicts a PVG 15000 equipped with a single VSP3 interconnected (redundantly) to two Passport 8600s via Gigabit Ethernet directly off of the VSP3s faceplates.

***Note:*** The IP/Ethernet option is currently (in SN06) available only via the Gigabit Ethernet ports directly off the VSP3 faceplates, which implies only a single VSP3 is connected to a single Gigabit Ethernet port on the interconnecting router. When new Gigabit Ethernet options become available such as 4 port Gigabit Ethernet FPs, more than a single VSP can be aggregated onto a single Gigabit Ethernet port for IP traffic transport.

**Figure 61 PVG 15000 with a single VSP3 Gigabit Ethernet connected to two PP8600s**



In this redundant fashion each VSP3 is connected to a GBIC port on each Passport 8600 8608 carrier card. The two Gigabit Ethernet ports on the VSP3s, share the same MAC address provided by the PP15K MAC address module. Only one of the Gigabit Ethernet ports is active at a given time. The Port Protection on the VSP3 provides link failure detection (Layer 2) between it's ports and the link partner, only under the following 4 link failure conditions:

- Loss of Synchronization,
- Auto-negotiation failure,
- Remote off-line condition,
- Remote link failure condition.

In addition for Layer 3 failure protection/mechanism, the VRRP feature of the Passport 8600s should be utilized. The default router configuration on the VSP3 (IpInterface/0) should be assigned the VRRP address of the Passport 8600s, e.g. the PVG VLAN address. For detail information on the VSP3/Gigabit Ethernet IP addressing see "VSP3 -IP over Ethernet" on page 98.

### 7.4.1 Capacity

As mentioned above, the VSP3s bring increased capacity to the PVG 15000s. This capability is in conjunction with the use of the 4port OC3/STM-1 ch TDM FPs. Each single OC3/STM-1 TDM port supports a total of 2016 DS0s(with OC3) or 1953 DS0(with STM-1). So from a TDM capacity point of view, each 4port OC3/STM-1 Ch TDM FP can support up to 4 VSP3's end points requirement (total of 2016x4=8064 on OC3 and 1953x4=7812 on STM-1) and still consume only a single PVG 15000 shelf slot.

With higher port density and less slot consumption, additional hardware can be added in the same shelf, resulting in yet much higher Trunk capacity on the PVG shelf. As the PVG's TDM capacity increases, the IP bandwidth requirement is also impacted. The IP bandwidth requirements are driven by the type of CODEC and the sampling rates that are used.

See "VoIP over Ethernet" on page 104 in section "7.7 Trunk Gateways Engineering" for a detailed IP bandwidth calculations for IP over Ethernet based on different CODEC and packetization rates.

The following table summarizes the recommended hardware based on the number of DS0s on a PVG 15000 to Passport 8600s redundant interconnection. The PVG 15000's listed hardware is based on a 1:1 sparing configuration for best redundancy and carrier grade option. The calculated DS0s is based on different CODECs, sampling rates, and TDM configurations of the PVG 15000.

| PVG Hardware 1:1 sparing CP, VSP3 and OC3 TDM | PVG slots used | Number of DS0s G711 (10,20) | Number of DS0s G729a (10) | Passport 8600 hardware (Duplex) | 8600 ports used |
|---|---|---|---|---|---|
| CP | 2 | (2016x4) 8,064 (OC3) OR (1953x4) 7,812 (STM-1) | (1512x4) 6,048 (OC3) OR (STM-1) | two 8608 or 8616SXE Modules on two Passport 8600s | 8 ports |
| VSP3 | 8 | | | | |
| 4pOC3/STM-1Ch (TDM) | 2 | | | | |

***Note:*** As demonstrated in the above table, there remains 4 available slots in the PVG 15000 for future expansion. Specifically, this configuration provides a means for using the upcoming 4port Gigabit Ethernet FPs on the PVG 15000, to aggregate multiple VSP3s IP traffic into a single Gigabit link on the router, e.g., reducing the required number of GBIC ports on the Passport 8600s.

### 7.4.2 Engineering Notes

- Autonegotiation - Autoneg has to be enabled on the interconnecting GigE router ports.
- IP addressing - All the VPS3s may be in the same subnet, however for additional resiliency it is possible to configure groups of VSP3s in different subnets and provide different MLT coverage for different VLANs.
- VSP3s IpIf address - The IpIf address provisioned in the VSP3s should be defined as the VRRP address of their corresponding VLAN for Layer 3 redundancy.
- G711 vs. G729a - As described in section “7.7 Trunk Gateways Engineering” on page 103, the number of supported DS0s reduces from 2016 for G711 to 1512 when using G729a CODEC.

### 7.4.3 Failover metrics

- Impairing the fiber links used of the Gigabit Ethernet ports on the VSP3s to dual Passport 8600s, resulted in No impact on the active calls.
- Using the Ping command resulted in No packet loss.
- See the VSP3 CPR testing results as a reference.

Working config files are provided at the end of the guidelines.

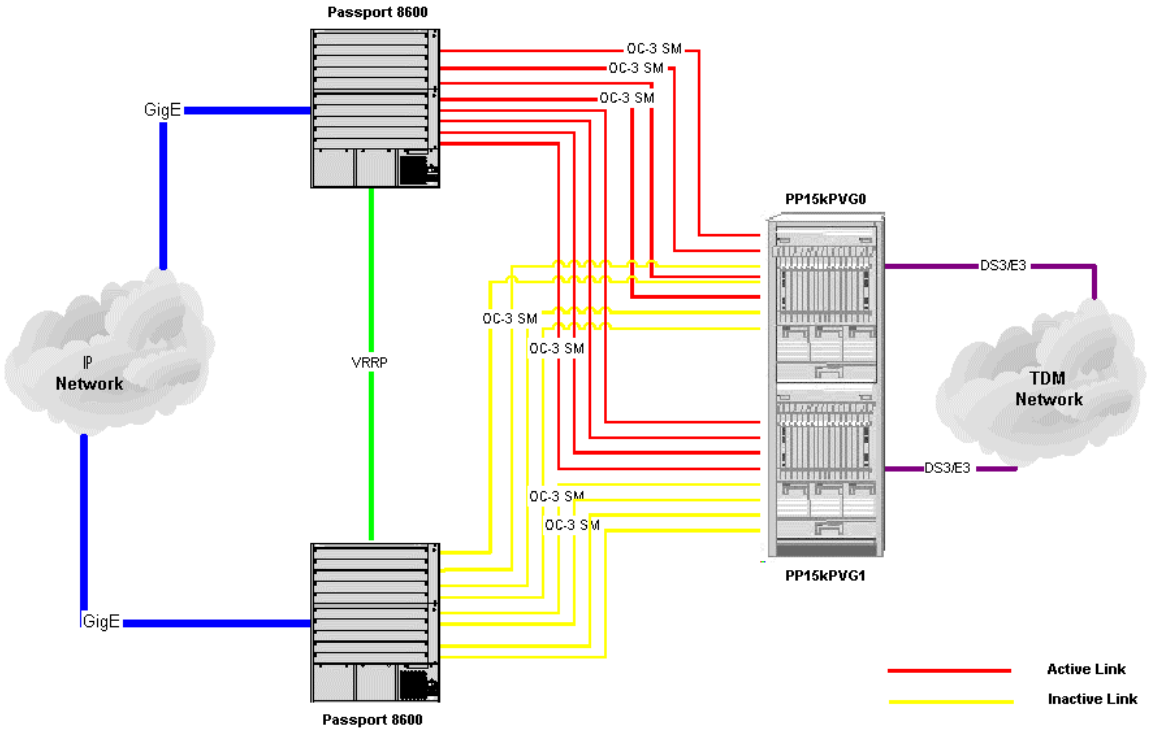
## 7.5 PVG OC3/OC12 to Passport 8600s (IP over ATM)

The Passport 8600 equipped with the Passport 8672ATME module, provides network transmission using ATM technology. This capability positions the Passport 8600 as a viable solution for interconnecting PVGs to the Packet network for IP/ATM solution. A Passport 8600 with an 8010 chassis has 10 available slots, two of which can only be occupied by 8691SF Modules. The other 8 can be populated with 10/100 MB and Gigabit Ethernet switch modules as well as 8672ATME modules.

To eliminate single point of failure in PVGs interconnectivity to the Packet network, redundant hardware in the PVGs as well as Dual Passport 8600s must be used.

Figure 47, illustrates a redundant interconnection topology between 2 PVGs and a pair of Passport 8600s.

**Figure 62 Connectivity Between 2 PVG 15000s and 2 Passport 8600s**



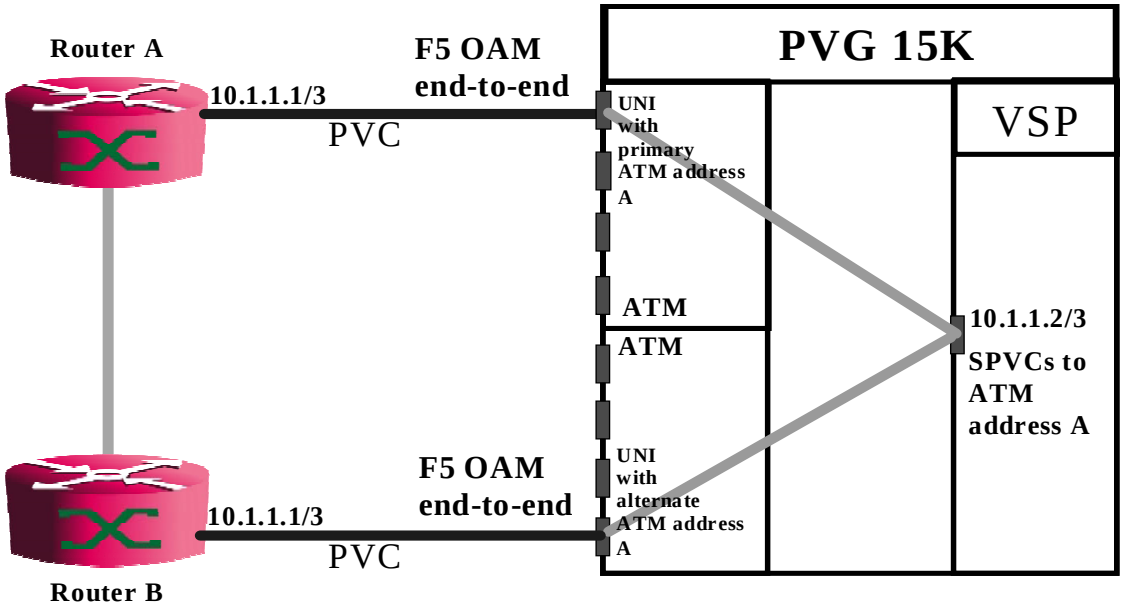

For proper redundancy operation, we have to implement some method of fault detection which is supported by both the PVG and the Passport 8600. The Passport 8600 does not support Automatic Protection Switching (APS), a Layer 1 failure detection mechanism, however it does support the OAM F5 cell exchange, which is considered as a Layer 2 fault detection mechanism. This feature is also supported on the PVG and it will be used as Fault tolerant mechanism for resiliency purposes.

In this configuration we use two ATM FPs on the PVGs to establish a redundant ATM connection to the two Routers A and B using PVCs. To select the active link to the Routers SPVCs are used internally to the PVG shelf.

The setup relies on OAM F5 cells originating from the Routers to the VSP as a fault detection mechanism per VCC. The OAM F5 message relate to VCC monitoring respectively. They exist at the ATM layer and the purpose of these messages is to monitor channel availability and enabling rerouting within Router A and B in case of a Layer1 or a Layer 2 (ATM PVC) failures.

Figure 48 illustrates a more detailed diagram of a single VSP in a PVG 15000 to Passport 8600 redundant interconnection.

**Figure 63 Detail PVG 15000 redundant interconnection to a pair of Routers (Passport 8600s)**




As depicted in Figure 48, this configuration utilizes two ATM FPs to provide traffic redundancy between a VSP card and the IP backbone.

Each VSP may have up to 3 IP subnets (2 for control signaling and 1 for media) therefore only 3 VCC connections are needed between each router and the PVG. SPVCs are used internally between the VSP card and the ATM interfaces on the PVG shelf.

The remote end of each VCC, being the IP address of each control or media VCC is duplicated on each router. However, only ONE of the PVCs is active at a given time, since the SPVCs within the VSP and the ATM port (internal to the PVG shelf), are only established on a single ATM port and not on both simultaneously. Since there can be only one connection active at a given time there is no problem with identical IP addresses on the two routers.

Within the PVG, per VSP card, up to 3 SPVCs may be needed. Each of these SPVCs gets the same ATM address to connect to and this address is configured on the terminating ATM ports on one as Primary address and as Alternate on the other. Upon initial SPVC establishment, the Primary ATM address is used as the preferred address and only on a failure the SPVC would re-establish on the Alternate ATM address.

Using OAM F5 messages on the ATM layer, provides a mechanism for the routers to properly detect which ATM port should be used to set up the path to the VSP. All the subtending remote addresses (VSP control and media addresses) are reachable via the active connection. If a fault occurs at the active connection side, e.g. broken fiber, lack of the end to end OAM F5 messages on the VCC layer will signal to the PVC that the VCCs are broken, therefore the active rotues to the remote end (VSP) will be removed from the active router.

At this point the VSP will re-establish (switch to) the SPVCs on the Alternate ATM port, and will cause the OAM F5 message to flow in this newly activated link. Once enough OAM F5 messages have been established between the two ends, the ATM port will be considered as Active and the subtending IP addresses (VSP control and media addresses) will now be reachable via the newly activated router.

Using a dynamic routing protocol like OSPF between the two routers guarantees that the VSP network (control and media addresses) is reachable via ONE and ONLY ONE router at a given time. During normal conditions while both physical connections between the Routers A and B and the PVG are up, the OAM F5 cells are the only way for the Routers to detect which connection is up and points towards the VSP and update their routing tables accordingly. It is advised to put all the SPVCs of one VSP on the same ATM port with their primary ATM connection.

### 7.5.1 Capacity

The capacity of the PVG to Passport 8600 is somewhat impacted by the existing limitations in the ATM MDA capabilities of the Passport 8600. Specifically, the throughput of the ATM MDAs are limited in smaller packet sizes such as Voice traffic. Therefore using different CODECs and packetization rates results in different capacity limits due to different packet generation rates and different packet sizes.

Following is a list of general engineering limits with the Passport 8600 ATM capabilities and should be considered when configuring PVGs off of Passport 8600s for IP/ATM solutions:

- The PP8600 ATM MDAs are rate limited at 512 byte packets. VoIP applications and the smaller packet sizes result in a ¼ throughput capacity of each MDA, i.e., an OC-12 MDA is limited to less than an OC-3 throughput.
- When creating PVCs on the PP8600 MDA, only use **UBR** service category. **VBR** service category is currently NOT supported.
- The capacities stated above, assume **Silence Suppression is DISABLED**.
- Make sure that all the created PVCs per MDA are OAM F5 managed.
- The fail over times in PVG to PP8600 interconnections is in the range of 2.5 to 4 Seconds.

The following lists additional limits categorized based on different ATM interfaces used with different CODECs and sampling rates. As shown below, different combinations result in different DS0 capacity per ATM MDA interface.

OC3 - G711@10ms specific limitations

- When connecting PVG Media VCCs to the PP8600s do not allocate more than a VSP2 per PP8600 MDA.
- Do not provision more than **936 DS0s (39 DS1s) for North America and 930 DS0s (30 E1s) for the International Market**. To achieve a full 1120 DS0 Silence Suppression must be enabled.

OC3 - G711@20ms specific limitations

- When provisioning PVGs off of the PP8600s do not allocate more than a VSP2 per PP8600 MDA.
- Do not provision more than **1104 DS0s (46 DS1s) for North America and 1116 DS0s (36 E1s) for the International Market**.

OC12 - G711@10ms specific limitations

- When provisioning PVGs off of the PP8600s do not allocate more than a VSP2/VSP3 per PP8600 MDA.
- Do not provision more than **1032 DS0s (43 DS1s) for North America and 1023 DS0s (33 E1s) for the International Market.** To achieve a full 1120 DS0 Silence Suppression must be enabled.

OC12 - G711@20ms specific limitations

- In this configuration, up to 2 VSP2s or a VSP3 may be allocated on a single PP8600 MDA for direct PVG-PP8600 interconnection.
- Up to **2016 DS0s (84 DS1s) for North America and 2015 DS0s (65 E1s) for the International Market**.

Table 31 summarizes the different DS0 capacities supported on each Passport 8600 MDA for IP/ATM when different ATM interfaces are used with different CODECs and sampling rates.

**Table 45 Passport 8600 MDA capacity based on different CODECs and ATM interfaces**

| MDA Interface | UBR | | | VBR (Currently not supported) | | |
|---|---|---|---|---|---|---|
| | G711 (10ms) | G711 (20ms) | G729a (10ms) | G711 (10ms) | G711 (20ms) | G729a (10ms) |
| 4 port OC3 | **936** DS0 for North America **930** DS0s for International | **1104** DS0s for North America **1116** DS0s for International | TBD | N/A | N/A | N/A |
| 1 port OC12 | **1032** DS0s for North America **1023** DS0s for International | **2016** DS0s for North America **2015** DS0s for International | TBD | N/A | N/A | N/A |

In the following section several tables are provided which list the required hardware for both the Passport 8600s and the PVG with respect to the above DS0 capacities. Separate tables are provided for using VSP2s and using VSP3s.

Table 32 provides a common list of required Passport 8600 hardware. The listed hardware provides:

- resilient interconnection of Two PVGs,
- the required hardware for maximum allowed DS0 capacity.

***Note:*** The redundant Passport 8600 also should be equipped with the same set of Modules.

**Table 46 Passport 8600 module list for redundant PVG interconnection**

| Module | Qty | Comment |
|---|---|---|
| 8691SF Module | 1 | Switching Fabric |
| 8632TXE Ethernet Modules | 2 | Required for CS-LAN equipment aggregation |
| 8672ATME Modules | 4 | Provides 2 MDA slots/Module |
| 4 port OC3/STM-1 MDA<br>or<br>1 port OC12/STM-4 MDA | 8 | Only a single port out of 4 must be used/VSP2<br><br>For VSP3 use |

Table 33, lists the required hardware for a single PVG based on using VSP2s and OC3/STM-1 ATM FPs. This configuration allows the maximum of trunk capacity per PVG shelf, when interconnected to dual Passport 8600s.

**Table 47 Single PVG hardware using VSP2 and OC3/STM-1 ATM to Dual PP8600s**

| CP/FP | Main | Spare |
|---|---|---|
| CP3 | 1 | 1 |
| 2 port DS3C TDM | 4 | 0 |
| VSP2 | 4 | 1 |
| 4port OC3/STM-1 | 2 | 0 |

Refer to Table 34 to see the total number of DS0s supported on 2 PVGs to Passport 8600s with different CODECs and packetization rates using VSP2 cards.

**Table 48 Total DS0 capacity for 2 PVGs using VSP2s on Dual Passport 8600s**

| **PVG / PP8600** | Qty | G711 (10ms) North America | G711 (10ms) International | G711 (20ms) North America | G711 (20ms) International |
|---|---|---|---|---|---|
| **4-port OC3 MDAs on Dual Passport 8600s**<br>(1:1 Sparing) | 16<br><br>**8** Active<br>8 Spare | **936** DS0s per MDA<br>X<br>**8** MDAs<br>=<br>7488 DS0s for 2 PVGs | **930** DS0s per MDA<br>X<br>**8** MDAs<br>=<br>7440 DS0s for 2 PVGs | **1104** DS0s per MDA<br>X<br>8 MDAs<br>=<br>8832 DS0s for 2 PVGs | **1116** DS0s per MDA<br>X<br>**8** MDAs<br>=<br>8928 DS0s for 2 PVGs |
| VSP2s on 2 PVGs<br>(4:1 sparing) | 10<br><br>**8** Active<br>2 Spare | | | | |

Table 35, lists the required hardware for a PVG based on using VSP3s and OC12/STM-4 ATM FPs. Also 4 port OC3/STM-1ch TDM FPs are utilized for additional DS0 capacity. Again this configuration allows the maximum of trunk capacity per PVG shelf, when interconnected to a pair of Passport 8600s.

**Table 49 Single PVG hardware using VSP3 and OC12/STM-4 ATM to Dual PP8600s**

| CP/FP | Main | Spare |
|---|---|---|
| CP3 | 1 | 1 |
| 4 port OC3 ch TDM | 1 | 1 |
| VSP3 | 4 | 4 |
| 4port OC12/STM-4 ATM | 2 | 0 |

Refer to Table 36 to see the total number of DS0s supported on 2 PVGs interconnected to Dual Passport 8600s with different CODECs and packetization rates using VSP3 cards.

**Table 50 Total DS0 capacity for 2 PVGs using VSP3s on Dual Passport 8600s**

| **PVG / PP8600** | Qty | G711 (10ms) North America | G711 (10ms) International | G711 (20ms) North America | G711 (20ms) International |
|---|---|---|---|---|---|
| **1-port OC12 MDAs on Dual Passport 8600s** (1:1 Sparing) | 16<br><br>**8** Active<br>8 Spare | **1,032** DS0s per MDA<br>X<br>**8** MDAs<br>=<br>8,256 DS0s for 2 PVGs | **1,023** DS0s per MDA<br>X<br>**8** MDAs<br>=<br>8,184 DS0s for 2 PVGs | **2,016** DS0s per MDA<br>X<br>8 MDAs<br>=<br>16,128 DS0s for 2 PVGs | **2,015** DS0s per MDA<br>X<br>**8** MDAs<br>=<br>16,120 DS0s for 2 PVGs |
| VSP3s on 2 PVGs (1:1 sparing) | 16<br><br>**8** Active<br>8 Spare | | | | |

## 7.5.2 Engineering Notes

- F5 timers - Since OAM F5 messages is used as the Layer 2 failure detection mechanism, use of the lowest possible timers is recommended:
  - Send = 1
  - Retry = 1
  - Up = 1
  - Down = 1

— See the working configuration file at the end of the guidelines.

- Disable Spanning Tree Protocol on the participating ATM ports

— e.g. config atm 7/1 stg 1 stp disable

- See the VSP2/1120 testing results for reference.
- On the Passport 8600 MDAs use only UBR ATM service category.
- On the PVG use RTVBR for Media and NRTVBR ATM service category. Table 37 and Table 38 can be used as a guide for setting the PCR, SCR, and MBS numbers for both Media and Non-Media VCCs.
- Note SPVCs must be used for both Control messaging as well as the bearer if utilizing PVG HSM/HEP.

**Table 51 ATM PCR/SCR/MBS for Media (IPMcon)**

| VSP | CODEC Type | Sampling rate | PCR | SCR (NO VAD) | MBS (NO VAD) | ATM Interface |
|---|---|---|---|---|---|---|
| VSP2 (7K) | G711 | 10 | 302,400 | 302,400 | 1 | OC3 |
| | | 20 | 252,000 | 252,000 | 1 | OC3 |
| | G729a/b | 10 | 144,000 | 144,000 | 1 | OC3 |
| | | 20 | 72,000 | 72,000 | 1 | DS3 |
| VSP2(15K) | G711 | 10 | 336,000 | 336,000 | 1 | OC3 |
| | | 20 | 280,000 | 280,000 | 1 | OC3 |
| | G729a/b | 10 | 160,000 | 160,000 | 1 | OC3 |
| | | 20 | 80,000 | 80,000 | 1 | DS3 |
| VSP3(15K only) | G711 | 10 | 608,832 | 608,832 | 1 | OC12 |
| | | 20 | 508,032 | 508,032 | 1 | OC12 |
| | G729a/b | 10 | 305,424 | 305,424 | 1 | OC3 |
| | | 20 | 1554,224 | 1554,224 | 1 | OC3 |

**Table 52 ATM PCR/SCR/MBS for Non-Media (ctrl/x)**

| VSP | Service | PCR | SCR | MBS |
|---|---|---|---|---|
| VSP2 (7K) Aspen | ISUP | 700 | 350 | 100 |
| | PRI | 400 | 200 | 55 |
| | V5.2 | 400 | 200 | 55 |
| | MDM | 400 | 200 | 55 |

**Table 52 ATM PCR/SCR/MBS for Non-Media (ctrl/x)**

| VSP | Service | PCR | SCR | MBS |
|---|---|---|---|---|
| VSP2(15K) Aspen | ISUP | 700 | 700 | 90 |
| | PRI | 450 | 210 | 60 |
| | V5.2 | 450 | 210 | 60 |
| | MDM | 2100 | 1050 | 100 |
| VSP2(15K) H.248 | ISUP | 1400 | 500 | 100 |
| | PRI | | | |
| | V5.2 | | | |
| | MDM | 2100 | 1050 | 100 |
| VSP3(15K only) Aspen | ISUP | 1200 | 600 | 160 |
| | PRI | 850 | 420 | 120 |
| | V5.2 | 850 | 210 | 120 |
| | MDM | 2100 | 1050 | 100 |
| VSP3(15K only) H.248 | ISUP | 2000 | 800 | 210 |
| | PRI | | | |
| | V5.2 | | | |
| | MDM | 2100 | 1050 | 100 |

### 7.5.3 Failover metrics

- Using the OAM F5 timers, the ATM link failures introduce an average of 2.5 to 4 seconds outage in the speech path.

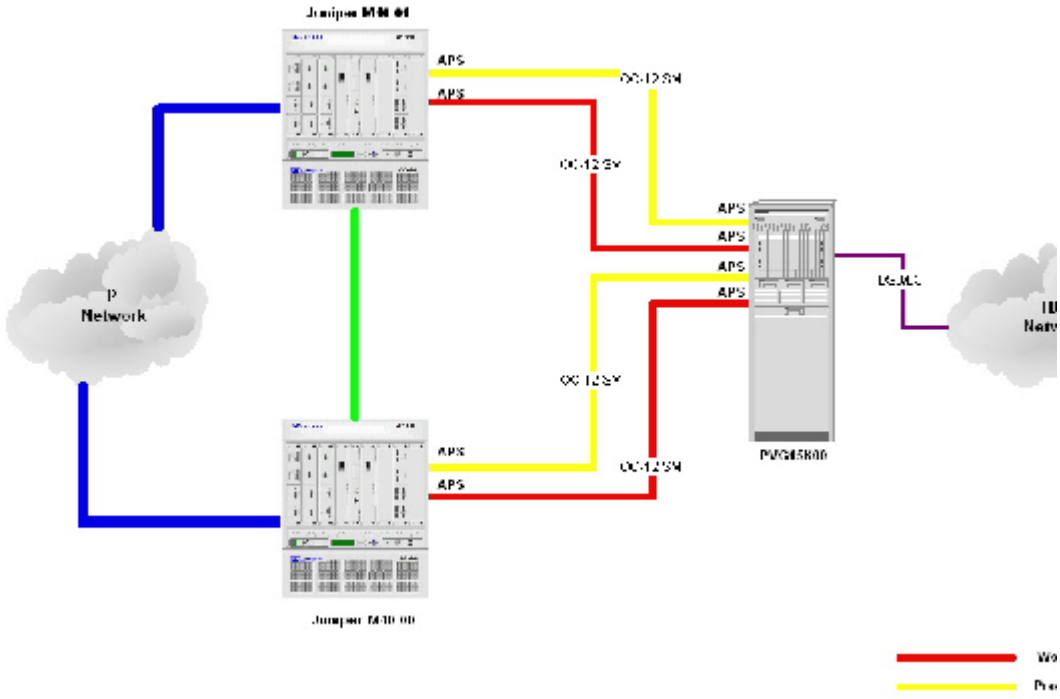
Working config files are provided at the end of the guidelines.

## 7.6 PVG to Juniper M-Series (IP over ATM)

To meet the Carrier grade requirements and eliminate single point of failure, the PVG shall be connected to Dual Juniper M Series with Distributed APS configuration.

Figure 49 depicts a single PVG 15000 connection to the IP network for illustration purposes only and is not indicative of any limitations. The total number of interconnecting PVGs is determined by the trunk Gateway site's capacity requirements as well as the available bandwidth capacity of the transport network.

**Figure 64 Redundant connectivity between a PVG 15000 and 2 Juniper M40s**




Automatic Protection Switching, as stated above, is one of the requirements on the interconnecting router. Distributed APS is used by SONET add/drop multiplexers (ADMs) to protect against circuit failures. The APS implementation on Juniper, allows for protection against circuit failures between a Line Terminating Equipment (LTE), e.g. the PVG's OC-12 interfaces, and one or more routers, and between multiple interfaces in the same router.

When a circuit or router fails, a backup immediately takes over. For the purpose of eliminating a single point of failure, dual Juniper M Series are recommended, and distributed APS is utilized for protection against both router and link failures.

Juniper supports APS 1+1 switching, bi-directional only, and either revertive or nonrevertive mode. In an APS resilient connection, you configure two circuits, a *working circuit* and a *protect circuit*. Normally, traffic is carried on the working circuit (that is, the working circuit is the active circuit), and the protect circuit is disabled. If the working circuit fails or degrades, or if the working router fails, the LTE, e.g. PVG, and the protect router, e.g. M Series router, switch the traffic to the protect circuit, and the protect circuit becomes the active circuit.

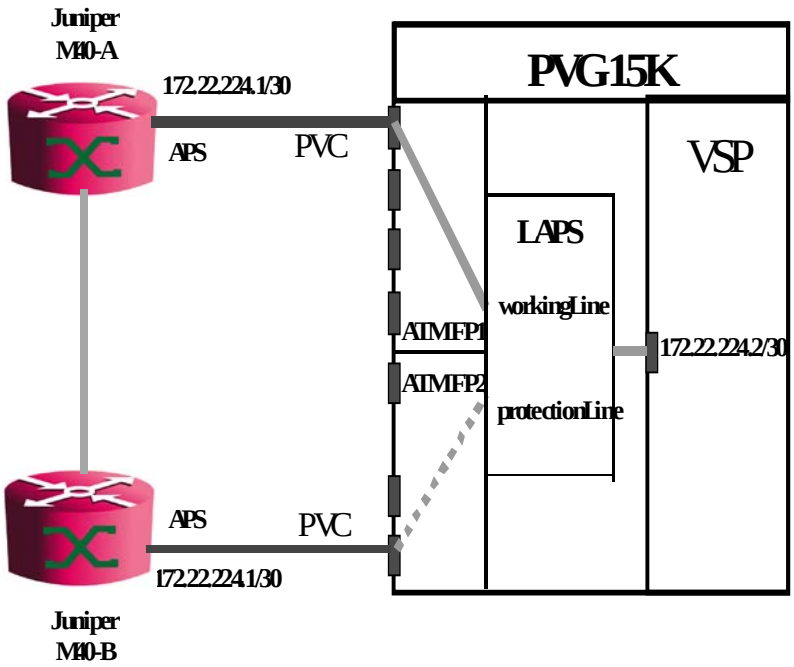
For proper APS operations, since the M Series routers only support bi-directional mode, the PVG side has to be modified from its default unidirectional setting to bi-directional since both ends have to match. In addition there is the possibility of Revertive and non-revertive switching. When line switching occurs, the protected line becomes active. Under revertive switching, when the error condition or operator command causing the switchover is cleared, the working line reverts to being the active line. Under non-revertive switching, the protected line remains active.

In order to minimize the impact of another switch back, both the PVG and the M Series router are set to non-revertive mode.

Since APS provides redundancy on the physical layer, for a redundant interconnection between the PVGs and the M Series router, redundancy must be working on the IP Layer as well. For this reason, the same IP address (Control and Media addresses of the VSPs) are provisioned on both Juniper M Series routers. Therefore only one router can have an active connection to the PVG.

OSPF on the other router, which has an inactive link to the PVG, has to be aware of the port down status and updates it's database accordingly. The Juniper M Series do this automatically by exchanging proprietary APS link state information via the Ethernet link between them. Each APS interface of the Juniper M Series router has the IP address of its APS neighbor provisioned. Figure 50 shows a detailed example of a PVG 15000 with APS enabled interconnected to dual Juniper M40s.

**Figure 65 Dual M40s with APS PVG 15000 interconnection**




## 7.6.1 Capacity

When trying to size the PVG to Juniper M Series routers for IP over ATM, we can look at each DS0s IP bandwidth requirements as described in Table 17, section "7.7.1 Calculating bandwidth based on desired number of Trunks" on page 103 and calculate the required IP egress bandwidth for a fully populated PVG shelf.

As summarized in Table 39, the IP egress bandwidth requirement of each DS0 varies based on the different CODEC and sampling rates.

**Table 53 IP Egress bandwidth requirement summary for IP over ATM**

| DS0 IP bandwidth requirement | G711 10ms | G711 20ms | G729a 10ms | G729a 20ms |
|---|---|---|---|---|
| Egress bandwidth per DS0 in Mb/s | 0.127 | 0.106 | 0.084 | 0.042 |

Each VSPs IP bandwidth requirement is then a result of the supported DS0s multiplied by the DS0 bandwidth. As an example, to support a single VSP2 using G711@10ms, we will require 143 Mb/s of IP egress bandwidth which is roughly the limits of an OC3 link. These calculations will help to determine the PVG required hardware for maximizing the DS0 capacity.

Details of maximum engineered capacity of PVG to Juniper M Series routers for both VSP2s and VSP3s with respect to different CODEC and sampling rates are provided in the following sections.

Using VSP2 and 2port DS3c TDM

Table 40, summarizes the required hardware based on using VSP2s, DS3c TDM, and OC12/STM-4 ATM FPs to maximize the PVG shelf capacity of 6720 DS0s. This configuration provides the maximum trunk capacity per PVG shelf, when interconnected to a pair of Juniper M Series routers.

**Table 54 Single PVG hardware using VSP2s and OC12 ATM to Dual Juniper M Series**

| CP/FP | Main | Spare |
|---|---|---|
| CP3 | 1 | 1 |
| 2 port DS3c TDM | 5 | 0 |
| VSP2 | 6 | 1 |
| 4 port OC12/STM-4 ATM | 2 | 0 |

As shown above, we use 5 2port DS3c TDM cards for a total 6720 DS0s. Also the 6 active VSP2s support a total of 6720 end points so there is no under utilization on any FPs. To carry the IP traffic generated by the 6720 DS0s to the packet network, 4 port OC12s are used. As detailed in Table 41, both G711 @ 10ms and G711@20ms require the same number of OC12 ports to carry the IP traffic to the packet network.

**Table 55 Single PVG shelf with 7 (6:1 sparing) VSP2s, OC12 port requirement**

| VSP2 | DS0s | G711 (10ms) | G711 (20ms) |
|---|---|---|---|

**Table 55 Single PVG shelf with 7 (6:1 sparing) VSP2s, OC12 port requirement**

| | | | |
|---|---|---|---|
| 7 VSP2s<br>on<br>1 PVG<br>(6:1 sparing)<br><br>**6** Active<br>1 Spare | 6 VSP2<br>X<br>1120 DS0<br>=<br>**6720** DS0s<br>per PVG | 6720 DS0s<br>X<br>0.127 Mb/s/DS0<br>=<br>853.44 Mb/s<br>equates to<br>2 OC12 ports<br>(engineered at 90%) | **6720** DS0s<br>X<br>**0.106** Mb/s/DS0<br>=<br>712.32 Mb/s<br>equates to<br>2 OC12 ports<br>(engineered at 90%) |

***Note:*** With the single PVG capacity of 6,720 DS0s, the PVG Frame (2 PVGs) can support up to 13,440 DS0s when interconnected to Dual Juniper M Series routers.

Using VSP3s and 4port OC3/STM-1 ch TDM

***Note:*** This option is only available on PVG 15000.

Table 42, lists the required hardware for a single PVG based on using VSP3s and OC12/STM-4 ATM FPs. Also 4 port OC3/STM-1ch TDM FPs are utilized for additional DS0 capacity of 8064 DS0s. Again this configuration allows the maximum of trunk capacity per PVG shelf, when interconnected to Dual Juniper M Series routers.

**Table 56 Single PVG hardware using VSP3s and OC12 ATM to Dual Juniper M Series routers**

| CP/FP | Main | Spare |
|---|---|---|
| CP3 | 1 | 1 |
| 4 port OC3 ch TDM | 1 | 1 |
| VSP3 | 4 | 4 |
| 4 port OC12/STM-4 ATM | 2 | 0 |

As shown above, we use 2 4port OC3/STM-1 ch TDM cards for a total 8064 DS0s. Also the 4 active VSP3s support a total of 8064 end points. To carry the IP traffic generated by the 8064 DS0s to the packet network, 4 port OC12s are used. As detailed in Table 43, both G711 @ 10ms and G711@20ms require the same number of OC12 ports to carry the IP traffic to the packet network.

**Table 57 Single PVG shelf with 4 (1:1 sparing) VSP3s OC12 port requirement**

| VSP3 | DS0s | G711<br>(10ms) | G711<br>(20ms) |
|---|---|---|---|
| 8 VSP3s<br>on<br>1 PVG<br>(1:1 sparing)<br><br>**4** Active<br>4 Spare | 4 VSP3<br>X<br>2016 DS0<br>per VSP3<br>=<br>**8064** DS0s<br>per PVG | 8064 DS0s<br>X<br>0.127 Mb/s/DS0<br>=<br>1024.13 Mb/s<br>equates to<br>2 OC12 ports<br>(engineered at 90%) | **8064** DS0s<br>X<br>**0.106** Mb/s/DS0<br>=<br>854.78 Mb/s<br>equates to<br>2 OC12 ports<br>(engineered at 90%) |

***Note:*** With the single PVG capacity of 8,064 DS0s, the PVG Frame (2 PVGs) can support up to 16,128 DS0s when interconnected to Dual Juniper M Series routers.

### 7.6.2 Engineering Notes

- See Table 37 and Table 38 for details on PCR, SCR, and MBS numbers.
- Note SPVCs must be used for both Control messaging as well as the bearer if utilizing PVG HSM/HEP.

### 7.6.3 Failover metrics

- Distributed APS on the Juniper Mseries and LAPS on the PVG is used for Layer 1 failure detection mechanism,
- Any link failure in the speech path between the PVG and the Junipers resulted in an average of 600-800ms Gap in the speech path.

Working configuration files are provided at the end of the guidelines.

# 8.0 IP Addressing

This section intends to provide an end-to-end view on IP addressing strategies for new customers as well as migrating customers. The following addressing strategy was written keeping in mind three main requirements to be satisfied:

- Scalability,
- Flexibility,
- Ease of management.

One of the most serious problems facing the evolution of the Internet is IP address depletion. The Internet community, in particular IETF, has developed the IPv6 standard in order to remedy this situation. Unfortunately, it will be a long time before a widespread use of IPv6; consequently, IPv6 becomes a long-term solution. Therefore, we recommend the use of private IP addresses in the Integrated Lines Access network. Depending on the customers' requirements or current network architecture, this can be done in two ways:

- Using only private IP addresses
- Using a mix of both public and private IP addresses.

It is important to know that throughout this Chapter the term “public address” means an IP address that belongs to a block that is considered public for the customer. This block can either be assigned directly by IANA or be defined in [RFC1918].

***Note:*** As described in the following paragraphs, some caution needs to be taken when using private IP addressing strategies, especially Network Address Translation (NAT) and Network Address and Port Translation (NAPT).

## 8.1 IP Addressing Considerations

Nortel Networks recommends using private IP addressing for the Succession elements in the Carrier space. There are typically two exceptions to this general strategy:

- the CS-LAN OAM&P subnet - since the Corporate networks of the majority of the Carriers are publicly addresses, the communication between the NOC/OSS and the CS-LAN OAM&P subnet is greatly facilitated. As it will be seen later on in the document, the use of public addresses is very limited and it is clearly indicated wherever it is recommended.

When private addressing are used in the Carrier space, the following guidelines must be observed:

- Routing protocols (and possibly static routes) need to be configured properly in order to prohibit private routes from being published to the Internet.
- Depending on a customer's network topology, a segmentation of the Media Gateway sites into VLANs (subnet-based &/or protocol-based) might be required to separate the data and voice broadcast domains.
- No overlap of IP addresses is possible without the use of NAT.

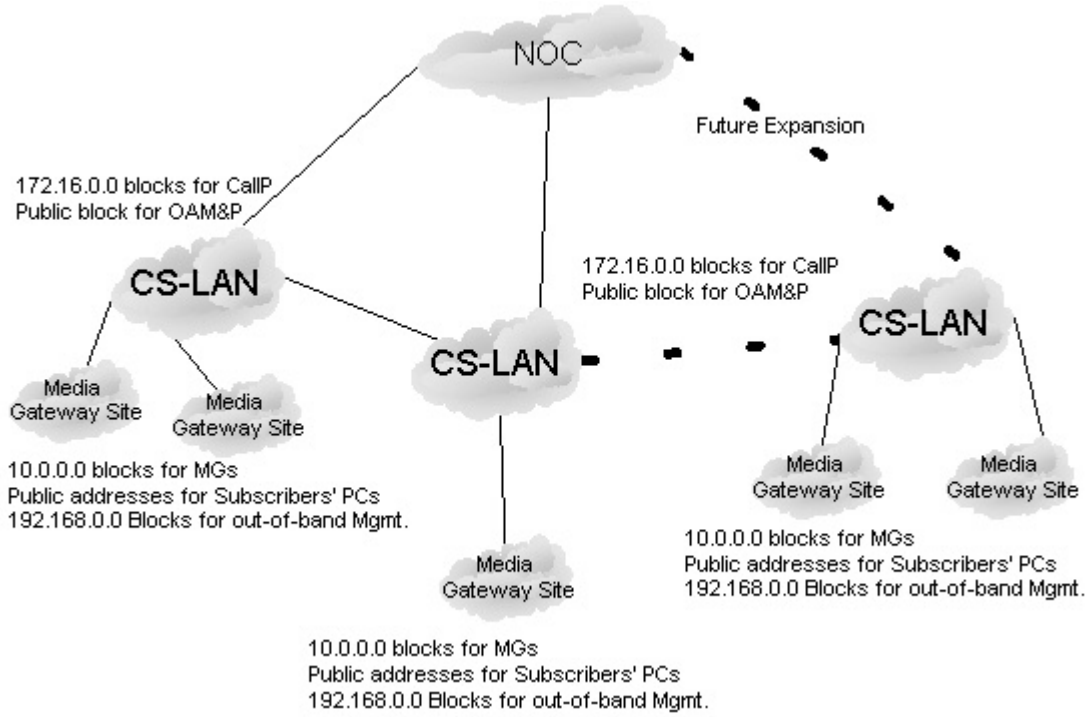
**Note**: It is important to note that the private subnets described in RFC1918 are used across this document as an example. Depending on the customer’s requirements on current addressing, on the system size and future growth, only one of the RFC1918 subnets or a public subnet might be selected for addressing the entire solution. The key point of this document is the size of the subnets

that are described throughout the document. The Network Sales Engineer should investigate during interaction sessions with customers if the described private subnets and the subnetting scheme agree with the customer requirements.

## 8.2 Network View and General Strategy for IP addressing

The following picture (Figure 66) shows a high level example of our strategy. The addressing schemes are designed with maximum scalability in mind. The design described in the following document is an example based on the current Media Gateways (MG) requirements (for both capacity and IP addressing).

**Figure 66 High Level View**




For more details, the following chapters will provide an example of the addressing scheme that is recommended. In addition, the diagram will show an example of the subnets used for all the logical components.

### 8.2.1 Private Address Space

The Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of the IP address space for private Internets (the reader can review RFC1918 [1] for additional details):

- From 10.0.0.0 to 10.255.255.255 (10.0.0.0/8 prefix)
- From 172.16.0.0 to 172.31.255.255 (172.16.0.0/12 prefix)
- From 192.168.0.0 to 192.168.255.255 (192.168.0.0/16 prefix)

Nortel Networks recommends the use of these classes to provide an extremely scalable design. At the same time, the different areas and entities of the solution will be logically separated for better

management and troubleshooting strategies when/if problems occur.

### 8.2.2 Strategy Summary

The addressing strategy is mainly designed around the following logical areas:

- The Call Processing elements
- The OAM&P elements
- The Media Gateways
- Out-of-band management
- The NOC

#### 8.2.2.1 Call Processing Subnet

The Call Processing elements are common across all Succession solutions and they are located in the CS-LAN Call Processing subnet. To address these elements, Nortel Networks recommends the following steps:

- Subnetting the 172.16.0.0/12 subnet with a 19-bit mask,
- Subnetting each block with a 23-bit mask to address the CS LAN Call Processing subnet for a single CS2000.

It is important to remember that this subnet might need to be allocated in a public address space for the Succession line solutions that have Enterprise based gateways (for instance, H.323). This recommendation is based on the Carrier topology and its overall addressing requirements.

#### 8.2.2.2 The OAM&P Subnet

The OAM&P elements are located in the CS-LAN OAM&P subnet. It is recommended to use a public address block for this subnet. To address these elements, Nortel Networks recommends the following steps:

- Reserving a /26 public subnet to address the CS-LAN OAM&P subnet.

#### 8.2.2.3 The NOC

The NOC is typically already existing in a customer's network. In case a NOC is not already present, Nortel Networks recommends the following steps:

- Reserving a /27 public subnet to address the NOC/OSS subnet

#### 8.2.2.4 Out-of-band management

Out-of-band management is a solution mainly used to add extra-reliability network management. If the customer uses this strategy, Nortel Networks recommends the following steps:

- Using the 192.168.0.0/16 for out-of-band management (if and where it is required).
- Resubnet this subnet according to the number of elements that need to be managed and their physical location.

#### 8.2.2.5 The Media Gateways

The Media Gateway are located in a Media Gateway site (either local to the CS-LAN or remote). Their addressing is dependant on the Succession solution. This document will describe the details

of the addressing strategy for each Solution in later Chapters. As a general initial step for all solutions, Nortel Networks recommends:

- Using the 10.0.0.0/8 subnet,
- Resubnetting it with a 9-bit subnet mask (255.128.0.0),
- Resubnetting the resulting subnets with a 15-bit mask.

The next subnetting steps are related to the specific Succession solution. Please see the following chapter for the summary of the steps.

#### 8.2.2.5.1 Media Gateways in Packet Trunking

For Packet Trunking Succession solutions, Nortel Networks recommends the following steps:

- Subnetting a 15-bit subnet with a 21-bit mask,
- Reserving one of the resulting subnets to address all PVGs, APGs and IW-SPMs.

### 8.2.2.6 IP Address Assignment

The supported design requires a dynamic IP address assignment (via BOOTP) for the UAS, GWCs, and the SCs. The out-of-band management interface of the MG4000 (for UA-AAL1 solutions only) will also obtain its IP address via BootP.

All the other devices (OAM&P platforms, CS2000, trunk Media Gateways, routers and switches) will be statically given an IP address.

### 8.2.2.7 Passport 8600 Addressing

The IP addresses that are required on the pair of Passports 8600 are the following:

- 1 per chassis for Management Interface (only needed for out-band-management)
- 1 per chassis for each of configured VLANs. Please note that VLANs and subnets are equivalent in the CS-LAN. The typical configured VLANs are:
    - 1 VLAN for Call Processing elements
    - 1 VLAN for OAM&P elements
    - 1 VLAN for Media Gateways (**not applicable for UA-AAL1**)
    - 1 VLAN for intra-Passport 8600 communication
    - 1 VLAN for NOC connectivity
- 1 for each VLAN/subnet that requires a VRRP instance. The subnets that require VRRP are:
    - Call Processing subnet
    - OAM&P subnet
    - Media Gateways subnet (**not applicable for UA-AAL1**)

Therefore, at least 15 IP addresses (1x2 + 5x2 + 3x1) are required for the suggested configuration for Succession IP solutions.

# 8.3 Addressing Schemes for CS LAN and NOCs

## 8.3.1 CS LAN Overview

A typical CS LAN will be composed mainly of five subnets: one subnet for the Call Processing elements, one subnet for the OAM&P platforms, one subnet for the CS-LAN based Media Gateways, one subnet for inter Passport 8600 communication, and one for inter connectivity with the Corporate network.

It is suggested to use the same addressing scheme that the customer currently uses to interconnect routers in its Corporate Network for the VLAN interconnecting the Passport 8600s. The typical subnet size for these links is 255.255.255.252.

The CS LAN elements requiring IP addresses are:

- A Contivity will require 1 address for the CS LAN interface + 1 for the NMI,
- A Passport 8600 will require 1 address per configured VLAN + 1 for NMI. In a dual configuration where VRRP is used for redundancy, it is required to assign another IP address (the Virtual IP address) for each configured VRRP instance.
- A fully configured USP will require 4 IP addresses.

## 8.3.2 Addressing for the Call Processing Subnet

Since the Call Processing elements will have to interact only with other Voice-over-Packet elements, Nortel Networks recommend using private addresses for this subnet.

The network elements requiring an IP addresses that will be typically in this subnet are:

- XA-Core will require 6 addresses for the HIOPs.,
- A fully configured SAM21 will need 36 IP addresses (4 per GWC pair, 4 per SC pair).
- The SDM requires 1 address in the Call Processing subnet. Please note that other two addresses are required: 1 address in the OAM&P subnet and 1 address in the out-of-band space (see the “Out-of-Band Management” section for more details).
- A SAM16 (UAS) will require 1 IP address per CPU card. Therefore a fully configured SAM16 with two domains will require 2 IP addresses. Please note that 12 additional addresses are required in the Media Gateway subnet.
- USP will require 1 address for each of the M3UA IP Link System cards. A total of 6 addresses in the Call Processing subnet are required for a fully configured USP. Please note that other two addresses are required: 1 address for each of the RTC cards in the OAM&P subnet

Because the second largest private subnet (from 172.16.0.0 to 172.31.255.255) has up to 1,048,574 usable addresses, it is the perfect choice to address the CS LAN devices.

Nortel Networks recommends using a 19-bit subnet mask (255.255.224.0). In this fashion, 128 subnets are obtained with 8190 usable addresses each (as shown in the example of Table 58). Each of the /19 subnets will support up to 16 CS2000 nodes and each will be able to grow beyond 64 Gateway Controllers.

| Subnet | Mask | Size | Host Range | Broadcast | Usage |
|---|---|---|---|---|---|
| 172.16.0.0 | 255.255.224.0 | 8190 | 172.16.0.1 to 172.16.31.254 | 172.16.31.255 | 1st block with 16 CS2k nodes |
| 172.16.32.0 | 255.255.224.0 | 8190 | 172.16.32.1 to 172.16.63.254 | 172.16.63.255 | 2nd block with 16 CS2k nodes |
| 172.16.64.0 | 255.255.224.0 | 8190 | 172.16.64.1 to 172.16.95.254 | 172.16.95.255 | 3rd block with 16 CS2k nodes |
| ……. | ……. | …. | ……. | ……. | ..... |
| 172.31.160.0 | 255.255.224.0 | 8190 | 172.31.160.1 to 172.31.191.254 | 172.31.191.255 | 127th block with CS2k 16 nodes |
| 172.31.192.0 | 255.255.224.0 | 8190 | 172.31.192.1 to 172.31.223.254 | 172.31.223.255 | 127th block with CS2k 16 nodes |
| 172.31.224.0 | 255.255.224.0 | 8190 | 172.31.224.1 to 172.31.255.254 | 172.31.255.255 | 128th block with CS2k 16 nodes |

**Table 58 Initial Subnetting**

Nortel Networks recommends using the first 8 subnets (172.16.0.0/19, 172.16.32.0/19, 172.16.64.0/19, 172.16.96.0/19, 172.16.128.0/19, 172.16.160.0/19, 172.16.192.0/19 and 172.16.224.0/19) to address up to 128 CS2000s. It is suggested to reserve the other 120 subnets (from 172.17.0.0/19 to 172.31.224.0/19) for other uses (i.e., the addressing of the OAM&P subnets or NOC/OSS) or future growth.

The next step is to subnet the 172.16.0.0/255.255.224.0 subnet with a 23-bit mask (255.255.254.0), yielding 16 subnets with 510 usable addresses each (see Table 59 for an example).

| Subnet | Mask | Size | Host Range | Broadcast | Usage |
|---|---|---|---|---|---|
| 172.16.0.0 | 255.255.254.0 | 510 | 172.16.0.1 to 172.16.1.254 | 172.16.1.255 | CS LAN-1 CS2k node 1 |
| 172.16.2.0 | 255.255.254.0 | 510 | 172.16.2.1 to 172.16.3.254 | 172.16.3.255 | CS LAN-2 CS2k node 2 |
| ……. | ……. | ..... | ……. | ……. | ……. |
| 172.16.28.0 | 255.255.254.0 | 510 | 172.16.28.1 to 172.16.29.254 | 172.16.29.255 | CS LAN-15 CS2k node 15 |
| 172.16.30.0 | 255.255.254.0 | 510 | 172.16.30.1 to 172.16.31.254 | 172.16.31.255 | Reserved |

**Table 59 Subnetting to obtain CS2000 blocks**

The first 15 of the above /23 subnets will be used to address all the Call Processing devices in the CS LAN (and the MG4000 out-of-band management interfaces if present in UA-AAL1 solutions).

The last subnet (172.16.30.0/23) is reserved for CS-LAN based Media Gateways. Please see the next section for more details.

### 8.3.3 Addressing for the Media Gateways in the CS-LAN

Depending on the customer's requirements and network topology, the Succession IP solutions can have Media Gateways co-located with the CS2000 in the CS-LAN. Nortel Networks recommends using the subnet reserved in the previous paragraph to address these elements.

The network elements requiring an IP addresses that will be typically in this subnet are:

- A SAM16 (UAS) will require 1 IP address per CG6000 card. Therefore, a fully configured redundant SAM16 configuration will require 12 CG6000 cards and 12 IP addresses. Please note that 2 additional addresses are required in the Call Processing subnet.
- IW-SPM will require 3 IP addresses for each GEM card.
- PVG (Gigabit Ethernet only) will require 3 addresses per VSP card. Please see the "Detailed Media Gateway Addressing for PVGs/APGs" on page 191 section for more details.

### 8.3.4 Addressing for the OAM&P Subnet

The OAM&P subnet will be connected (logically and/or physically) with the NOC/OSS, a network that would traditionally use public addresses. For this reason, it is recommended to use public IP addresses for the OAM&P subnet. However, if a NOC/OSS does not currently exist or the customer prefers using private IP addresses, this choice does not impair functionality.

The network elements requiring an IP addresses that will be typically in this subnet are:

- CS2000 Management Tools server will require 4 addresses if multipathing is enabled
- The SDM requires 1 address in the OAM&P subnet. Please note that other two addresses are required: 1 address in the Call Processing subnet and 1 address in the out-of-band space (see the "Out-of-Band Management" section for more details).
- USP will require 1 address for each of the RTCs. A total of 2 addresses in the OAM&P sub-net are required for a fully configured USP. Please note that other six addresses are required: 1 address for each of the M3UA IP Link System cards in the Call Processing sub-net
- The USP Manager will require 1 IP address.
- Preside MDM server:
    - For a clustered solution with two servers, it will each require 2 addresses - one external + one for internal communication only.
    - For a stand-alone configuration, it requires 4 addresses if multipathing is enabled.

In addition, the following network elements might have an interface on the OAM&P subnet:

- Contivity and/or Firewall (for Remote Access).

Please note that there might be some network elements provided by the customer that might be residing in the OAM&P subnet. Typically, these elements will all require 1 address. Examples are:

- DCE Server.

If customer prefers or requires private addresses, it is suggested to use one of the reserved /19 subnets (from 172.16.32.0/19 to 172.31.224.0/19).

Independently from the choice of a public or private subnet, Nortel Networks recommends applying the same subnetting scheme described in the "Addressing for the Call Processing Subnet" (where a

/23 subnet mask is used) and then using a /26 subnet mask (255.255.255.192) to reduce the subnet size. Nortel Networks suggests using a single /26 subnet to address the OAM&P subnet in each CS2000 node. Such a scheme will yield 62 usable IP addresses.

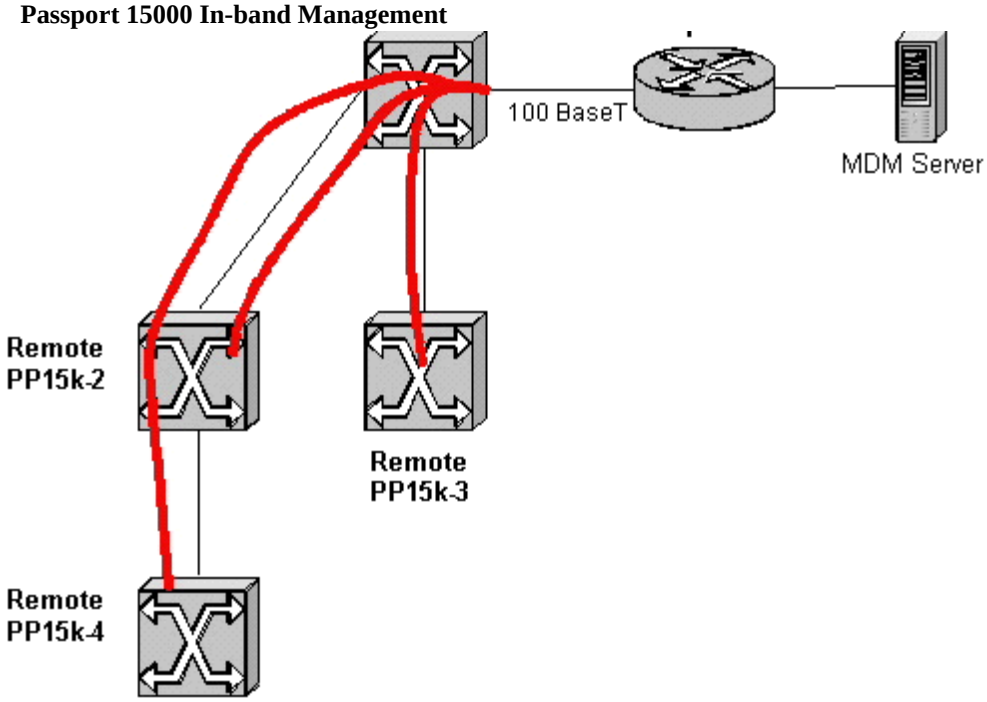
### 8.3.5 In-Band Management for the Passport 15000

In the Succession solutions where Passports 15000 are present, a topology with a centralized PMDM can be the preferred solution to manage all Passports 15000 in the network. If this is the case, Nortel Networks recommends using a public block (i.e., visible from the centralized Preside MDM) to address the Passport 15000 logical in-band management interface.

The CP of the Passport 15000 (PP15000-1 in Figure 67) collocated with the CS-LAN is connected to the Passport 8600 via a 100 BaseT link. All other remote Passports 15000 will have one IP over AAL5 PVC (used for management) to the CS-LAN Passport 15000. PP15000-1 will have the task of routing the traffic coming from the management PVC to the CS-LAN.

The IP addresses of the remote and CS2000 location CPs can be in the same subnet. Alternatively, multiple 30-bit mask subnets (i.e., one per remote Passport 15000) can be used.

**Figure 67 Passport 15000 In-band Management**




### 8.3.6 Connecting the CS LAN to the Corporate Network

It is recommended to configure a VLAN on the Passport 8600 for the sole purpose of interfacing logically with the access routers of the Corporate Network. For this reason, it is suggested to use the same addressing scheme that the customer currently uses to interconnect routers in its Corporate Network. The typical subnet size for these links is 255.255.255.252.

### 8.3.7 NOCs and Future Expansion

Depending on the customer's requirements, the NOC/OSS might be using public or private IP addresses. Given the number of addressable elements, it is suggested to reserve a /27 subnet. Therefore, Nortel Networks recommends again applying the same subnetting scheme described in the "Addressing for the Call Processing Subnet" (where a /24 subnet mask is used) and then using a /27 subnet mask (255.255.255.224) to reduce the subnet size to 30 usable addresses.

It is recommended to use private IP addresses for the Network Operation Center/OSS when such networks do not yet exist. For such a case, it is suggested that one of the reserved /19 subnets (from 172.16.32.0/19 to 172.31.224.0/19) be used.

The following are the typical clients that are needed for managing Succession solutions. Please note that the physical platform where the clients run is typically provided by the customer.

- Preside MDM Client
- SESM Client
- SAM21 Manager Client
- Passport 8600 Manager Client (Device Manager)
- DCE Server
- Clients for other OAM&P network servers (DNS, DHCP, NTP, etc.).

***Note:*** For security reasons, OAM&P Clients should NOT be provisioned on the OAM&P VLAN. For further details see section "16.3.1 Logical Separation between CS-LAN subnets" on page 329.

### 8.3.8 Out-of-Band Management, Router Interfaces and Loopback Interfaces

Nortel Networks recommends the use of the 192.168.0.0/16 subnet for providing fixed addressing to the out-of-band interfaces of the devices (Passport 8600, other routers/ATM switches, Passport 15000/PVGs) supporting this functionality.

In addition, it is recommended to reserve a subnet in this space for the private communication between the SDM and XA-Core.

This strategy, paired with a parallel management network, allows the network administrators access to the network elements even in case of catastrophic failures. We further scale the 192.168.0.0/16 subnet by using a 24-bit mask (255.255.255.0) because this yields 256 subnets with 254 usable addresses each. We then use the first two subnets (192.168.0.0/24 and 192.168.1.0/24) and reserve the others for future expansion.

In addition, a further subnetting of the above blocks would yield enough subnets for Router interfaces and Loopback addresses where these are required.

## 8.4 Detailed Media Gateway Addressing for PVGs/APGs

### 8.4.1 General approach

The addressing scheme is designed to accommodate 165000 trunks, which translates to 148 VSP2s. VSP2s are used as the reference network element because their IP addressing requirement is greater than Gigabit Ethernet VSP3s. Nevertheless, the overall addressing strategy will use 150 (instead of 148) VSP2s as a base number to allow for future growth.

The key points of our approach are:

- Subnetting the 10.0.0.0/8 subnet with a 21-bit mask,
- Reserving one 21-bit mask subnet for PVGs and APGs,
- Subnetting the reserved subnet with a 24-bit mask,
- Using the eight subnets to address the Media Gateway sites with the PVGs,

In addition, it is recommended to reserve one of the remaining subnets with the 21-bit mask for future expansion.

Last but not least, it is important to note that the subnets used across this document are shown as an example. The Network Sales Engineer should investigate during interaction sessions with customers if the described private subnets and the subnetting scheme agree with the customer requirements.

### 8.4.2 Addressing Requirements for Multiple Nodes

If multiple CS2000s need to be connected across an IP network, it is fundamental that non-overlapping addresses are used.

#### 8.4.2.1 Connectivity between different Service providers

The more specific case of CS2000 inter connectivity between Service Providers is currently supported only if non-overlapping public IP addresses are used in both the networks of both providers. All other cases are not currently supported.

### 8.4.3 Detailed PVG Addressing

The elements of a remote Media Gateway site that require addresses are:

- PVG 15000/APG will require:
    - 12 addresses per VSP2 and ATM VSP3s, 1 IP address for in-band management. If out-of-band management is used, another IP address is required.
    - 3 addresses per Gigabit Ethernet VSP3 and 1 IP address for in-band management. If out-of-band management is used, another IP address is required. Please keep in mind that three additional IP addresses (two physical and one virtual) are also needed on the switch/router where the PVGs are connected to.
- The router will require 1 address per configured interface + 1 for NMI (addresses to interconnect with PVG are included above),

As described above, the first step is to subnet the 10.0.0.0/8 block with a 21-bit mask: this scheme is applied below to the 10.16.0.0/16 subnet. For the rest of this chapter, Nortel Networks will use the

10.16.0.0/16 subnet as an example. Please keep in mind that the same process applies to all the other subnets if required.

**Table 0-35**

| Subnet | Mask | Size | Host Range | Broadcast | Usage |
|---|---|---|---|---|---|
| 10.16.0.0 | 255.255.248.0 | 2046 | 10.16.0.1 to 10.16.7.254 | 10.16.7.255 | Block for 1st CS2k Node |
| 10.16.8.0 | 255.255.248.0 | 2046 | 10.16.8.1 to 10.16.15.254 | 10.16.15.255 | Reserved |
| ……. | ……. | …. | ……. | ……. | Reserved |
| 10.16.240.0 | 255.255.248.0 | 2046 | 10.16.240.1 to 10.16.247.254 | 10.16.247.255 | Reserved |
| 10.16.248.0 | 255.255.248.0 | 2046 | 10.16.248.1 to 10.16.255.254 | 10.16.255.255 | Reserved |

**Table 60 Initial Subnetting**

Nortel Networks recommends using the first subnet (10.16.0.0/21) for the first CS2000 node. To optimize scalability, the remaining subnets should be reserved for other CS2000 nodes.

The 10.16.0.0/21 subnet will be subneted more to obtain a smaller subnet that is more suitable for the VSPs. To accommodate the current requirements, it is recommended re-Subnetting with a 24-bit mask to split the original 21-bit mask subnets into 8 subnets with 254 hosts each.

**Table 0-36**

| Subnet | Mask | Size | Host Range | Broadcast | Usage |
|---|---|---|---|---|---|
| 10.16.0.0 | 255.255.255.0 | 254 | 10.16.0.1 to 10.16.0.254 | 10.16.0.255 | 1st block for VSPs |
| 10.16.1.0 | 255.255.255.0 | 254 | 10.16.1.1 to 10.16.1.254 | 10.16.1.255 | 2ndt block for VSPs |
| ……. | ……. | …. | ……. | …….. | …… |
| 10.16.6.0 | 255.255.255.0 | 254 | 10.16.6.1 to 10.16.6.254 | 10.16.6.255 | 7th block for VSPs |
| 10.16.7.0 | 255.255.255.0 | 254 | 10.16.7.1 to 10.16.7.254 | 10.16.7.255 | 8th block for VSPs |

**Table 61 VSP Blocks**

### 8.4.3.1 Resubnetting for Gigabit Ethernet VSP3s

If Gigabit Ethernet VSP3s are used, it is recommended to use the 24-bit blocks above and resubnet them one more time.

In the configuration with maximum capacity, a PVG will have 8 VSP3 cards. Therefore, to optimize port density and bandwidth on the switch/router the PVGs are connected to, it is recommended using a maximum of 16 VSPs per Media Gateway site. This is equivalent to 48 IP addresses, a number that can be accommodated with a 26-bit mask subnet. As a result, it is recommended resubnetting the 24-bit blocks with a 26-bit mask to optimize the subnet size. In this fashion, each of the /24 blocks can address up to four remote Media Gateway sites.

An example of this scheme is shown below. The 10.16.0.0/24 subnet is used as an example.

**Table 0-37**

| Subnet | Mask | Size | Host Range | Broadcast | Usage |
|---|---|---|---|---|---|
| 10.16.0.0 | 255.255.255.192 | 62 | 10.16.0.1 to 10.16.0.62 | 10.16.0.63 | 1st block for 16 VSPs |
| 10.16.0.64 | 255.255.255.192 | 62 | 10.16.0.65 to 10.16.0.126 | 10.16.0.127 | 2ndt block for 16 VSPs |
| 10.16.0.128 | 255.255.255.192 | 62 | 10.16.0.129 to 10.16.0.190 | 10.16.0.191 | 3rd block for 16 VSPs |
| 10.16.0.192 | 255.255.255.192 | 62 | 10.16.0.193 to 10.16.0.254 | 10.16.0.255 | 4th block for 16 VSPs |

**Table 62 Resubnetting the VSP Blocks**

***Note:*** Please note that the maximum supported subnet size on a Gigabit Ethernet VSP3 is /22 or 255.255.252.0 which limits the number of available hosts on that subnet to 1022.

### 8.4.3.2 Resubnetting for ATM VSP3s and VSP2s

To accommodate the PVGs requirement of 3 subnets with a 30-bit mask (255.255.255.252) per VSP2 and ATM VSP3, Nortel Networks recommends using one of the /21 blocks in Table 10 and then applying a /24 mask as seen in the previous chapter.

Then, Nortel Networks suggests applying a 30-bit mask to the 24-bit mask subnets. This process is demonstrated in Table 63 using the 10.16.1.0/24 subnet as an example.

**Table 0-38**

| Subnet | Mask | Size | Host Range | Broadcast | Usage |
|---|---|---|---|---|---|
| 10.16.1.0 | 255.255.255.252 | 2 | 10.16.1.1 to 10.16.1.2 | 10.16.1.3 | VSP1 |
| 10.16.1.4 | 255.255.255.252 | 2 | 10.16.1.5 to 10.16.1.6 | 10.16.15.7 | VSP1 |
| 10.16.1.8 | 255.255.255.252 | 2 | 10.16.1.9 to 10.16.1.10 | 10.16.1.11 | VSP1 |
| ..... | ..... | ..... | ..... | ..... | ..... |
| 10.16.1.244 | 255.255.255.252 | 2 | 10.16.1.245 to 10.16.1.246 | 10.16.1.247 | VSP64 |
| 10.16.1.248 | 255.255.255.252 | 2 | 10.16.1.249 to 10.16.1.250 | 10.16.1.251 | VSP64 |
| 10.16.1.252 | 255.255.255.252 | 2 | 10.16.1.253 to 10.16.1.254 | 10.16.1.255 | VSP64 |

**Table 63 VSP2 and ATM VSP3s**

This re-subnetting will yield a total of 512 (64*8) 30-bit mask subnets, which covers the SN06 total number of VSPs per CS000 node.

In addition Nortel Networks strongly recommends reserving the remaining /21 subnets for future scalability and growth of the number of VSPs.

# 9.0 Network Element Traffic Engineering

This section details the capacity limits of the different network elements. Additionally, it addresses the engineering rules to configure, or size the number of elements, required to satisfy a specific customer traffic demand.

## 9.1 Port Capacity and Engineered BHCA

### 9.1.1 Port Capacity

The port capacity of the Succession PT-IP solution is as shown in Table 64 below.

**Table 64 Packet Trunking Port Capacity**

| | SN05 | SN06 |
|---|---|---|
| **Max Number ports** | 165,000 | 165,000 |
| **Max Number TDM GW Ports[a]** | 165,000 | 165,000 |
| **Max Number ANSI PRI ports** | 48,000 | 48,000 |
| **Max Number of ETSI PRI ports** | 62,000 | 62,000 |
| **Max Number Dynamic Packet Trunk ports** | 82,500 | 82,500 |

a. This limit is also the maximum number of ISUP trunks supported in the office.

### 9.1.2 Engineered BHCA Capacity

The baseline CM processor in SN06 is the 3+1 XA-Core (Rhino). Table 65 shows the number of full calls supported by release.

**Table 65 Packet Trunking IP Engineered BHCA Capacity by Release**

| | SN03 | SN04 | SN05[a] | SN06[a] |
|---|---|---|---|---|
| **XA-Core 3+1 (Rhino)** | 1.1M BHCA | 1.50M BHCA | 2.15M BHCA | 2.09M BHCA |
| **XA-Core 2+1 (Atlas)** | | | 2.65M BHCA | 2.60M BHCA |
| **XA-Core 3+1 (Atlas)** | | | 3.97M BHCA | 3.97M BHCA |

a. Engineered Capacity

### 9.1.3 POR BHCA Capacity

**Table 66 Packet Trunking IP PoR BHCA Capacity by Release**

| | SN03 | SN04 | SN05 | SN06.x |
|---|---|---|---|---|
| **XA-Core 3+1 (Rhino)** | 1.10 M BHCA | 1.50 M BHCA | 1.65 M BHCA | 1.65 M BHCA |
| **XA-Core 3+1 (Atlas)** | | | 1.65 M BHCA | 1.65 M BHCA |
| **XA-Core 2+1 (Atlas)** | | | 1.65 M BHCA | 1.65 M BHCA |
| **CS2K–Compact** | | | 1.30 M BHCA | 1.30 M BHCA |

While the supported capacity of the XA-Core 3+1 configurations is no higher than that of the XA-Core 2+1 configuration, the XA-Core 3+1 configurations are able to process more

CPU intensive calls as shown in section 9.1.2. When the Call Processing occupancy of the XA-Core 2+1 configuration reaches 80% or more, an additional Processor Element (PE) should be considered.

This example illustrates a call model that fully engineers an XA-Core:

Call interworkings: 100% enbloc trunk calls (ISUP => ISUP)

Number of call agents: A = 112,000
Call hold time: H = 90s
Erlang: E = 0.74
Capacity: C = A/2 * 3600/H * E = 1.65 M BHCA

A similar equation could be used for PRI => PRI calls because they have a similar call processing cost to ISUP => ISUP calls. But call models including any other type of call (e.g. calls involving Analogue lines, DPT, overlap signalling, IN) would push the call processing occupancy over 80%. For these call models, the number of call agents should be reduced, or the number of Processor Elements increased.

Due to the multi-processing and resource sharing nature of the XA-Core architecture, determining the call processing cost (and hence the BHCA capacity) can only be determined empirically.

## 9.2 CS2K / CS2K c Port Capacity

| PORT CAPACITY | | | | |
|---|---|---|---|---|
| | | SN05 | SN06 | SN07 PLANNED |
| Total Number of Ports in SESM | | 165000 | 165000 | 200000 |
| Number of Lines | | | | |
| | IBN | 100000 | 135000 | 150000 |
| | RES | 150000 | 150000 | 150000 |
| Number of Trunks | | | | |
| | ANSI ISUP | 165000 | 165000 | 200000 |
| | ETSI ISUP | 112000 | 165000 | 200000 |
| | ANSI PRI | 48000 | 48000 | 48000 |
| | ETSI PRI | 62000 | 62000 | 62000 |
| DPT | | 82500 | 82500 | 100000 |

### 9.2.1 GWC Port and BHCA Capacity

There are a number of types of gateway controllers: trunk-GWC, line-GWC, Audio Controllers, SIP-T GWC and VRDN. Although the hardware is identical, the software and data fill distinguish these devices. Table 67 illustrates the capacity limitations.

**Table 67 GWC Capacities**

**Table 0-39**

| GWC | Number of Ports | Half-Calls / Hour | Max Simultaneous Connections |
|---|---|---|---|
| North American (SN06) | | | |
| Trunk (ISUP) GWC | 4094[a] | 96,000 | 4094 |
| Trunk (PRI) GWC | 4094 D and B channels | 76,800 | 4094 |
| Audio Controller | - | 80,000 | 300/85[b] |
| SIP-T GWC | 4094 | 96,000 | 4094 |
| VRDN | - | 900,000[c] | |
| APG GWC | 6048 | 72,500 | 6048[d] |
| International (SN06) | | | |
| ETSI PRI | 4094 D and B channels | 60,000 | 3870 |
| TUP | 4094 | 96,000 | 4094 |
| ETSI ISUP variants | 4094 | 80,000 | 4094 |

a. The number of ports is 4094, but is constrained by the integral number of spans. Therefore, the actual number of usable endpoints may be slightly lower. See "Table 5 PVG 7000/15000 VSP capacity" on page 85 for more details.

b. Announcements/conference circuits

c. If the VRDN uses SCTP (pre-SN04) rather than UDP (SN04 and later), the BHCA is 200,000.

d. The APG GWC supports 3024 simultaneous calls

The total number of GWC pairs supported is 60. For each GWC, there is a maximum of 6400 small gateways or 27 large gateways per GWC. A small gateway, in general, is any gateway containing no more than 30 endpoints. Large Gateways, on the other hand, are gateways with greater than 30 endpoints.

## 9.3 Call Server Engineering

### 9.3.1 CS2K XA-Core

XA-Core is implemented as a symmetric, tightly coupled multiprocessor system. Implementation of XA-Core allows processing capacity to increase to many times that of a single processor. The XA-Core system consists of a shared memory which is redundantly implemented, a series of processors to provide computing capacity, and a number of I/O cards that provide mass storage and external interfaces. The processing capacity, memory, and the I/O capacity are all scalable by inserting more cards.

The following configuration are provided:

- NTLX02CA (RHINO) N+1 where N = 2 or 3 Processor Elements + 1 spare
- NTLX02DA (ATLAS) N+1 where N = 2, 3 or 5 Processor Elements + 1 spare

Memory configurations from 768 MB to 1728 MB is supported in 192 MB increments.

### 9.3.2 CS2K-Compact

The CS2K compact runs on 3rd party Motorola CPCI boards. A  configuration is available which offers 1.2 GB of memory. This configurations allows the operator to grow data store datafill to just over 1GB.

### 9.3.3 CS2K Surveillance

Various tools exist for monitoring the capacity of the CS2K. Proper engineering recommends that planning for future capacity upgrade starts when the switch utilization reaches 80%.

**>capci**

CATMP/HR UTIL ENGCATMP ENGLEVEL SYNC CCOVRLD IDLE

931920  84%  1107475    ABOVE  YES     OFF   NO

SCHED  FORE MAINT   DNC AUXCP    OM GTERM   BKG  NETM  SNIP

162%   59%   19%    0%    1%    4%    0%  144%    0%   49%

Measurements at the CS2K XA-Core or CS2K Compact (customers typically collect these measurements at the SDM) are accumulated just as they are on the DMS100. Accumulation classes are defined and specific OM groups are added to the accumulation class.

The OM Register BRSTAT can be used for the CS2Kc to monitor switch utilization on a hourly, daily or monthly approach depending on how the OM group is setup. The OM registergroup XASTAT can be used on CS2K XA-Core switches to monitor switch utilization on a hourly, daily or monthly approach depending on how the OM group is setup.
>OMSHOW BRSTAT ACTIVE

BRSTAT

CLASS: ACTIVE

START:2003/06/20 10:30:00 FRI; STOP: 2003/06/20 10:52:55 FRI;

SLOWSAMPLES: 14 ; FASTSAMPLES: 138 ;

BRSCAP BRSCMPLX BRSSCHED BRSFORE
BRSMAINT BRSDNC BRSOM BRSGTERM
BRSBKG BRSIDLE BRSAUXCP BRSNETM
BRSSNIP

0 84 0 165 59
18 0 3 0
171 0 1 0
22

Available at the office level from the CS2K, the existing OM group OFZ has registers that record call disposition, such as Line to Line, Line to Trunk, and Trunk to Line calls. OFZ can continue to be used as it is today on the DMS100. This OM group will include peg count from both the succession packet gateways as well as existing legacy peripherals. For example the NORIG register will include the number of line originations for both small and large line gateway originated calls and legacy LCM line originated calls.

Key registers are:

NORIGNumber of line originations

ORIGTRM: Number of Line to Line calls

ORIGOUT:Number of Line to Trunk calls

OUTNWAT: Number of outgoing call attempts including Line to Trunk and Trunk to Trunk calls

NIN:Number of Incoming call attempts to the office

INTRM: Incoming calls that terminate on a line

Each of the registers noted above has an associated extension register which is scored when the register reaches a count of 65535. The extension register is identified by the number 2 after the name. For e.g., the extension register for NORIG is NORIG2. Using OFZ to determine the Calls Per Hour:

CPH= (NIN + (NIN2 * 65535)) + (NORIG + (NORIG2 * 65535))

The OM group DTSRPM, available at the XA-Core provides a measurement of the Grade-of-Ser-

vice (Dial Tone Speed Recording) provided by line type. Each LGRP will have it's own key in DTSRPM just as an LCM does on the DMS100. Below is an example of the DTSRPM OM showing an LGRP

CC04 is the four digit site identifier, 00 is the frame number, 0 is the shelf number within the frame.

```
DTSRPM
CLASS: HOLDING
START:2003/xx/xx 12:15:00 TUE; STOP: 2003/xx/xx 12:20:00 TUE;
SLOWSAMPLES:        3 ; FASTSAMPLES:        30 ;

    INFO (DTSRPM_OMINFO)
      DPLTOT    DPLDLY    DGTTOT    DGTDLY
       KSTOT     KSDLY

 CCO4  00 0
         0        0        227        0
         0        0
```

Register DGTTOT provides a peg count of the total originations from DT lines at the LGRP. Register DGTDLY provides a peg count of the total originations that experienced a Dial Tone Delay > 3 seconds. These registers can be used to calculate a GOS as follows:

%DTD = 100% * DTD > 3 Seconds / Total Line originations

= 100% * DGTDLY / DGTTOT

OM group LMD, available at the XA-Core provides a peg count on a per shelf basis of the originations and terminations, as well as a traffic usage (CCS) register. From these registers, the total call volume and CCS per line can be calculated. Below is an example of the LMD OM group As with the DTSRPM OM, LMD provides a key for each LGRP.

```
LMD
CLASS: HOLDING
START:2003/xx/xx 15:00:00 TUE; STOP: 2003/xx/xx 16:00:00 TUE;
SLOWSAMPLES:        36 ; FASTSAMPLES:        360 ;

    INFO (LMD_OMINFO)
     NTERMATT   NORIGATT     LMTRU    TERMBLK
```

```
    ORIGFAIL    PERCLFL   STKCOINS     REVERT
    MADNTATT    ORIGBLK    ORIGABN

CC02  02 1
        600        800        26         0
         0         0          0          0
         0         0          0
```

Total CA (Call Attempt) volume on an MG9000 shelf is found using the following formula:

Total CA = NORIGATT + NTERMATT

Call attempts per second on an MG9000 shelf is calculated as follows:

CA/sec = Total CA / Number of seconds in OM accumulation period

LMD should be used to verify that the shelf is operating within the call attempt capacity.

Other tools such as SPMS can be used to monitor switch performance and DMSMON to monitor CPU utilization and memory usage.

### 9.3.4 Traffic Surveillance

The Call Server provides many Operational Measurements above those listed in section “CS2K Surveillance” on page 199. The following list of OM groups should be used to monitor the solution level traffic disposition (call mix), call server utilization, feature activations, trunk group usage, etc.

An OM accumulation class should be established with these OM groups collected during the office Busy Hour.

CP - Call Server call processing resources

CP2 - Additional Call Server call processing resources

EXT - Records seizures, overflows, high water mark of various software resources such as AMA recording units, feature extension blocks

OFZ - Office level call mix, i.e. Line-Line, Line-Trunk, Trunk-Line, Trunk-Trunk

BRSTAT - CS2Kc call server call processing utilization

XASTAT - CS2K XA-Core call processing utilization

TRK - Per trunk group traffic measurements, attempts, CCS or Erlang

LMD - Per LGRP traffic measurements, attempts, CCS

AMA - Automatic Message Accounting attempts

TCAPUSAG - TCAP messaging measurements

ISUPUSAG - ISUP messaging measurements

DPTNODE - Dynamic Packet Trunk node level usage

DPTOFC - Dynamic Packet Trunk office level usage

IBNGRP - Attempts per IBN customer group

ACDGRP - Automatic Call Distribution, per group measurements

CND - Class feature calling number delivery activations

AIN - Advanced Intelligent Network measurements

LNP - Local Number portability measurements

CNAMD - Class feature calling name delivery activations

ANN - Announcement attempts and usage

CF3P - 3 port conference circuit attempts and usage

CF6P - 6 port conference circuit attempts and usage

C7ROUTER - External Router utilization (LPP platform only)

C7RTESET - SS7 route set measurements

C7LKSET - SS7 link measurements

C7LINK1 - SS7 link measurements

C7LINK2 - SS7 link measurements

COT - Class feature Customer Originated Trace measurements

ACB - Class feature Automatic Call Back measurements

AR - Class feature Automatic Recall measurements

SCRJ - Selective Call Rejection measurements

SCF - Selective Call Forwarding measurements

SCA - Selective Call Acceptance measurements

UCDGRP - Universal Call Distribution group measurements

SCPOTS - Speed Calling on POTS measurements

TWCPOTS - Three Way Calling on POTS lines

TWCIBN - Three Way Calling on IBN lines

CWTPOTS - Call Waiting measurements on POTS lines

CALLFWD - Call Forwarding activations

CALLWAIT - Call Waiting activations

XPMOCC - Gateway Controller call processing occupancy and call attempts

IWBM - InterWorking SPM attempts

STORE - Call Server memory measurements

#### 9.3.4.1 OM Accumulation Class

The following steps can be used as an example to setup an OM accumulation class

TABLE OMACC

ADD <NEW ACC GRP> Y DPRECISION HOURLY C00  % C00 -> top of the hour

OMACCGRP <NEW ACC GRP> ADD GROUP <OM GROUPS>

OMDUMP CLASS <NEW ACC GRP> COMMANDS

TABLE OMPRT

pos <rep #> ..... CHA Y N ALLCLASS <NEW ACC GRP>  HOURLY C00 N SINK

### 9.3.5 Trunk Traffic Engineering

Time Division Multiplexed (TDM) Trunk traffic engineering on Succession is the same as TDM trunk traffic engineering on the legacy DMS100/DMS250 products, and is consistent with the use of the trunk operational measurements (OM group TRK). Members of the same trunk group can be supported across VSPs and across PVGs, and across switching fabrics. For example, a TDM trunk group may contain members subtending both an SPM and a PVG.

On the other hand, Dynamic Packet Trunks (DPT) between any two CS2000 nodes are engineered as separate trunk groups[1]. However, a DPT group may not contain both DPTs and TDM trunks. As well, a DPT trunk group is limited to 256K 64K members[2], however, it is constrained by the maximum number of trunks for the office which is currently 165K ports (although it is not likely that the number of DPT trunks in the office would grow beyond 50% of the total trunks in the office).

***Note:*** The number of other SIP-based application servers, e.g., other CS2000 nodes or MCS 5200 nodes, is limited to 100 which is the size of table MGCINV. This implies that any single CS2000 can communicate with no more than 100 other SIP-based applications servers.

### 9.3.6 LIU7 SS7 Traffic Engineering

SEB 99-01-001 details the traffic engineering of the LIU7 External Routers and LIU7s for the estimated volume of SS7 ISUP and TCAP messaging.SIP-T signaling between CS2000s is not counted as part of this as it is transported through the IP network via the SIP-T GWC and VRDN. When DPTs are supported in SN06.2, additional allowance has to be made for the increased SS7 message size with the BICC protocols.

***Note:*** To allow table C7TRKMEM to grow beyond 100,000 entries, the 32Meg LIU7s (NTEX22CA) must be provisioned in the LPP.

1. Trunk groups are limited to 2048 trunk members each.

2. For SIP-T. BICC signalling is limited to 64K members.

***Note:*** Any office containing SPM-based peripherals, including IW-SPM, must use external routers. A minimum of two (2) must be used. The engineering of external routers can be found in SEB 99-01-001.

#### 9.3.6.1 Monitoring SS7 Link Utilization

To monitor LIU7 link capacity for purposes of determining if more links are required, the user should utilize the following registers from the Operational Measurement group C7LINK2 for all links in the linkset:

- C7BYTTX – Number of bytes transmitted during the interval period.
- C7BYTTX2 – Extension register for C7BYTTX.
- C7BYTRX – Number of bytes transmitted during the interval period.
- C7BYTRX2 – Extension register for C7BYTRX.

Next using the contents of these registers, apply the following algorithm for each link being verified.

$$LinkUtil = (MAX(bytesTX,bytesRX)) \div (maxUtil \times OMSamplePeriodSeconds) \times 100$$

where,

$$bytesTX = C7BYTTX2 \times 65535 + C7BYTTX$$

and,

$$bytesRX = C7BYTRX2 \times 65535 + C7BYTTRX$$

and *maxUtil* is 7000 for 56kbps links or 8000 for 64kbps links at 100% utilization.

If the result is greater than 40%, then additional link capacity is needed.

The following is used as an example of a 56kbps link with a 5 minute (300 second) sample:

CLASS: HOLDING

206

START:2002/09/25 07:00:00 WED; STOP: 2002/09/25 07:05:00 WED;

SLOWSAMPLES: 3 ; FASTSAMPLES: 30 ;

KEY (C7_LINKSET_NUMBER)

INFO (C7LINK_OMINFO)

C7MSUTX C7MSUTX2 C7MSURX C7MSURX2

**C7BYTTX C7BYTTX2 C7BYTRX C7BYTRX2**

C7BYTRT C7BYTRT2 C7MSUDSC C7ONSET1

C7ONSET2 C7ONSET3 C7ONSETV C7ABATE1

C7ABATE2 C7ABATE3 C7ABATEV C7MSUDC1

C7MSUDC2 C7MSUDC3 C7STRET C7MSBRET

C7MSGLOS C7MSGMSQ C7MSUOR C7MSUOR2

C7MSUTE C7MSUTE2 C7MSUTS C7MSUTS2

0 SP1LK

0

36671 0 25226 0

63105 6 60923 11

0 0 0 0

0 0 0 0

0 0 0 0

0 0 1 1

0 0 36674 0

25228 0 0 0

$$bytesTX = 6 \times 65535 + 63105 = 456315$$

$$bytesRX = 11 \times 65535 + 60923 = 781808$$

$$LinkUtil = (MAX(456315,781808)) \div (7000 \times 300) \times 100 = 37.23$$

### 9.3.7 Universal Signaling Point Link Engineering

The Universal Signaling Point is introduced as an alternative to the LPP/LIU, thereby eliminating the need for the DMS-BUS (Message Switch). With the USP, two types of messaging are provided for ISUP messages internal to the CS2K. One type is direct messaging and the other is message bounce. Direct messaging sends messages to/from the GWC whereas message bounce directs the messages to/from the XA-Core for routing to/from the GWC.

Note that BICC DPT GWCs must always use direct messaging with the USP.

For SN06 and later, only direct messaging is supported. The following table illustrates pre-SN06 limits for direct messaging based on the number of point codes required in the office. These limits have

**Table 0-40**

| Number of Point Codes | Messaging type |
|---|---|
| 4 or less point codes | Direct Messaging or Message Bounce |
| 5 to 16 point codes | Message Bounce Only[a] |

a. The XACore SS7 capacity is limited to 1.5M BHCA when this option is used.

been removed since SN06.

#### 9.3.7.1 System Node Engineering

The following tables illustrate the engineering of the USP in USP8.0.

**Table 68 USP8.0 Engineering, multi-shelf (four-shelf systems)**

| System Node | Max Number of Links per CAM shelf | Max Number of Links with CAM Extension shelf | Total Links per USP8.0 (four-shelf system) |
|---|---|---|---|
| RTC | 2 | NA | 2 |
| CC | 2 | 2 | 8 |
| SS7 DS0A Link | 12 | 16 | 60 |
| SS7 V.35 Link | 12 | 16 | 60 |
| IP Link | 8[a,b] | 8[a] | 16 |
| ATM HSL Link | 8[a] | 8[a] | 32 |
| SS7 IP HSL Link | 8[a] | 8[a] | 32 |

a. The sum of the SS7 IP HSL Link nodes, IP-Gateway-Link nodes, and ATM HSL Link nodes must not exceed 8 per shelf.

b. The maximum number of IP Link nodes in the USP must not exceed 16.

### 9.3.7.2 SS7 Link Engineering and Capacity

USP-based SS7 links are traffic provisioned. Each link operates at either 56- or 64-kbits/sec in each direction, and should be engineered in mated pairs to meet the dual STP routing in the SS7 network. Each V.35 link (SS7 V.35 Link System Node) or DS0A link (SS7 DS0A System Node) will support a full 0.8 Erlang traffic load under a single-failure condition.

**Table 69 SS7 Link System Node Throughput**

| **Typical Message Length (bytes)[a]** | **56 kbits/sec (112 kbits/sec bi-directional)** | | **64 kbits/sec (128 kbits/sec bi-directional)** | |
|---|---|---|---|---|
| | **Msg/sec @ 0.4E** | **Msg/sec @ 0.8E** | **Msg/sec @ 0.4E** | **Msg/sec @ 0.8E** |
| 25 | 224 | 448 | 256 | 512 |
| 33 | 170 | 339 | 206 | 388 |
| 80[b] | 70 | 140 | 80 | 160 |

a. ISUP messaging.

b. Average message size for TCAP or LNP query/response pairs

**Table 70 Messages per Call Attempt**

| Description | ISUP/TUP Msg/CA | TCAP Msg/CA |
|---|---|---|
| Line to SS7 Trunk | 6 | |
| SS7 Trunk to Line | 6 | |
| DP/MF Trunk to SS7 Trunk | 6 | |
| SS7 Trunk to SS7 Trunk | 12 | |
| E800 Service (E800) | | 2 |
| Exchange Alternate Billing Service (EABS) | | 2 |
| Private Virtual Network (PVN) | | 2, 4 |
| Automatic Callback (ACB) | | 13 |
| Automatic Recall (AR) | | 2 |
| Ring Again (RAG) | | 4 |
| Local Number Portability (LNP) | | 2 |

Using the above tables, the link capacity in terms of call attempts per hour, can be determined using the following algorithm:

$$\frac{\text{Maximum link messaging rate} * 3600}{\text{Number of Messages/CA}}$$

For example, the following is the link capacity (56kbps) at 0.8E for message sizes of 33 bytes for a Tandem (SS7 Trunk to SS7 Trunk) application (12 msgs/CA).

$$\frac{339 \text{ msg/sec} * 3600 \text{ sec/hour}}{12 \text{ msg/CA}} = 101{,}700 \text{ CA/hour}$$

To calculate the number of links pairs, use the following algorithm.

$$NumberofLinkPairs = \frac{HDBHCA \times msgPerCA / 3600}{MaxLinkMessagingRate}$$

For example, assume the HDBHCA rate for ISUP is 760K BHCA for a Tandem application,

$$NumberofLinkPairs = \frac{760000 \times 12/3600}{339} = 8$$

From the above example, rounding to the next even integer, it can be seen that 8 link pairs (16 links to support dual routing to STP) are required to support 760K BHCA of ISUP traffic.

A similar approach should be used for expected office-wide HDBHCA rates for LNP and other TCAP-based services' (E800, ACB, RAG, AR, etc.) messaging. The following table shows the number of messages per second based on varying message sizes.

**Table 71 TCAP Message Throughput**

| Average Message Length (bytes)[a] | 56 kbits/sec (112 kbits/sec bi-directional) | | 64 kbits/sec (128 kbits/sec bi-directional) | |
|---|---|---|---|---|
| | Msg/sec @ 0.4E | Msg/sec @ 0.8E | Msg/sec @ 0.4E | Msg/sec @ 0.8E |
| 80 | 70 | 140 | 80 | 160 |
| 100 | 56 | 112 | 64 | 128 |

a. ISUP messaging.

Once all the link-pair requirements have been determined for all messaging, then the number of system nodes (V.35 or DS0A) can be determined.

Recall from section "2.1.6 Universal Signaling Point (USP)" on page 41 that the V.35 and DS0A System Nodes each contain four (4) links each. So when determining the number of these system nodes required, multiply the total link pairs required by two (2), and divide the results by four (4), rounding up to the next highest integer. So using the above example, four (4) system nodes would

$$TotalSystemNodes = \frac{8 \times 2}{4} = 4$$

be required.

### 9.3.7.3 Monitoring SS7 Link Utilization

To monitor USP link capacity for purposes of determining if more links are required, the user should utilize the following registers from the Operational Measurement Application Group "**Link Traffic**" on the USP Element Manager for all links in the linkset:

- Octets Received Count – Number of bytes received during the interval period.
- Octets Transmitted Count – Number of bytes transmitted during the interval period.

Next using the contents of these registers, apply the following algorithm for each link being verified.

$$LinkUtil = (MAX(bytesTX,bytesRX)) \div (maxUtil \times OMSamplePeriodSeconds) \times 100$$

where *bytesTX* is the value from the "**Octets Transmitted Count**" and *bytesRX* is the value contained in the "**Octets Received Count**" for the interval period. The value used for *maxUtil* is 7000 for 56kbps links or 8000 for 64kbps links at 100% utilization.

If the results is greater than 40%, then additional link capacity is needed.

***Note:*** The number of octets received in a 5 minute interval should never exceed 1,680,000 octets for a 56kbps link, or 1,920,000 octets for a 64kbps link. If this condition is true, then the links are operating above 0.8 erlang.

### 9.3.7.4 IPS7 Link Engineering

The IPS7 Links are traffic provisioned. The IPS7 Links can handle, at 0.8E, a continuous throughput of 1792 messages per second. Typically, the IPS7 Links must be engineered in mated pairs to a maximum rated capacity of 40% of their maximum capacity in order to meet the reliability requirements for transporting SS7 messages.

In failure mode, the IPS7 Link can support a sustained message throughput rate of 2240 messages per second for approximately 30 seconds.

**Table 72 IPS7 Link System Node Throughput**

**Table 0-41**

| Message Size | Capacity | | | |
|---|---|---|---|---|
| 19 bytes - 273 bytes | Normal | | Fault | Overload |
| | 20% | 40% | 80% | 100% |
| | 448 msg/sec | 896 msg/sec | 1792 msg/sec | 2240 msg/sec |

In order to correctly engineer the number of IPS7 links required by the USP, the following data is required:[3]

- **a.** Number of GWCs controlling ISUP trunks
- **b.** Number of DS0/V.35 SS7 links
- **c.** Number of ATM SS7 links
- **d.** Number of IP SS7 links
- **e.** Max engineered traffic rate on SS7 links (i.e. 40%)

3. This is applicable to SN06 through SN06.2 only.

The number of IPS7 links cards required is the greater of the following values (all values must be rounded up to the nearest even number, i.e. 4.1 = 6):

SS7 Traffic limited

$$IPS7Links = \left(\frac{b \times e}{3.2}\right) + c + d$$

or Application Server Path limited

$$IPS7Links = \frac{a}{7.5}$$

or a minimum of two (2) IPS7 Link cards.

For example,

- **a.** The number of ISUP Gateway Controllers required has been determined to be 25 (“9.4 Gateway Controller Engineering” on page 213).
- **b.** Sixteen (16) DS0A or V.35 signalling links (see “9.3.7 Universal Signaling Point Link Engineering” on page 207).
- **c.** Zero (0) ATM SS7 links
- **d.** Zero (0) IP SS7 links
- **e.** Max engineered traffic rate on SS7 links (i.e. 40%)

Using the above algorithms and taking the larger of the two, the number of IPS7 links can be determined as follows,

SS7 Traffic limited

$$IPS7Links = \left(\frac{16 \times 0.40}{3.2}\right) + 0 + 0 = 2$$

or Application Server Path limited

$$IPS7Links = \frac{25}{7.5} = 4$$

then taking the largest of the two results, with two (2) being the minimum required.

#### 9.3.7.4.1 Application Server Paths

***Note:*** Each IPS7 Link card has a limit of 16 paths to Application Servers such as the Gateway Controllers or the XACore. If the total number of ISUP-based Gateway Controllers exceeds 16, then two (2) additional IPS7 Link cards should be added since each Gateway Controller should have two paths each.

When configuring the ASP, paths to both the CS2000 (XACore or Compact) and Gateway Controllers are required. For the pathes to the CS2000, upto the first four (4) mated IPS7 cards (2 pairs) should each have a path between the USP and CS2000 for a total of four (4) pathes. The remaining 15 paths per card should be directed to the Gateway Controllers. If still more IPS7 cards are required to support the Gateway Controllers, then the paths should be placed on these cards, up to

16 paths each.

#### 9.3.7.5 Monitoring M3UA IP Link Capacity

To monitor M3UA IP Link capacity for purposes of determining if more links are required, the user should utilize the following registers on the USP OM Form, ASP Path Traffic:

- Transmit path:
  - Through-Switched MSU Count — Messages from the SS7 network to the IPS7 (CS-LAN side) network.
  - Originated MSU Count — Messages originating from the USP to the XACore
- Receive path:
  - Terminated MSU Count — Messages from the XACore, terminating on the USP
  - Received MSU Count — Messages from the XACore such as TCAP query/response pairs or LNP queries.

Applying the following algorithm with data from the above sampled registers, one can determine link utilization for purposes of engineering more links as needed.

- MSUTX = Sum of Through-Switched MSU Count + Originated MSU Count
- MSURX = Sum of Terminated MSU Count + Received MSU Count

LinkUtil = MAX(MSUTX,MSURX)/(2240 x OM_Sample_Interval_sec) x 100%

If the combined utilization of the mated links exceeds 80%, an additional set of mated links should be added.

### 9.3.8 USP-Compact

The USP Compact supports a maximum of 16 links and linksets on 2 USP Compact blades and supports both channelized T1/E1 SS7 links (4 or 8 channels per card), and IPS7 connections. Each of the 8 channelized DS0A SS7 channels on a single T1 carrier can be configured for all channels on that connection to utilize either the 64kbps or 56kbps data rate. These eight channels may be assigned to any of the available time slots on the T1.

SS7 messaging capacity is restricted by the bandwidth of the SS7 channels. Each channel is engineered at 0.4 Erlang, much the same as the USP described in the previous section. Please refer to section 9.3.7 for engineering each of the SS7 links.

***Note:*** USP Compact will not support m2pa IP High speed SS7 links, ATM based High speed SS7 links, DS0a SS7 links, or V-35 SS7 links.

## 9.4 Gateway Controller Engineering

### 9.4.1 Trunk-based Gateway Controllers

The gateway controllers have sufficient real time to accommodate up to 4094 trunks, not to exceed more than 23 call attempts/trunk/hour. The engineering approach is to divide the total number of ISUP (or PRI) trunks in the office by 4094 to determine the Number of trunk GWC required.

Attention should also be paid to optimize the engineering between gateway and GWC.

For this solution, the unit assigned to the GWC is the VSP, a sub unit of the PVG. A VSP2 can support a maximum of 1120 trunks and a VSP3 can support a maximum of 2016 (1512 when using G.729). It is recommended to assign only three VSP2s to a GWC, or 3312 trunks, or two VSP3. This will optimize the use of the Gateway ports.

Therefore, with PVGs, to determine the number of trunk-based GWC required, simply divide the total number of trunks in the office the supported trunks of VSP type being used, rounding up to the nearest integer.

If the average per-port call rate should exceed the rate specified in the previous paragraph, or the number of simultaneous calls exceed the value specified in Table 67, then each of the capacity limit must be considered

1. Determine the number of GWC pairs based on port limits.

$$NumberofGWC_{ports} = \frac{TotalNumberofPorts}{4094}$$

2. Determine the number of GWC pairs based on engineered BHHCA limits, where $GWC_{BHHCA}$ is the value for ISUP or PRI respectively in Table 67.

$$NumberofGWC_{BHHCA} = \frac{(TotalNumberofPorts \times BHHCAperPort)}{GWC_{BHHCA}}$$

3. Determine the number of GWC pairs based on the maximum of the previous steps, rounding up to the next whole integer.

$$NumberofGWC = MAX(NumberofGWC_{ports}, NumberofGWC_{BHHCA})$$

For an example of an office requiring 95,000 ISUP trunks at 16 BHHCA and 5,000 PRI at 20 BHHCA per port.

1.

$$NumberofGWC_{ports} = \frac{95000 + 5000}{4094} = 24.4$$

2.

$$NumberofGWC_{BHHCA} = \frac{(95000 \times 16)}{96000} = 15.8$$

$$NumberofGWC_{BHHCA} = \frac{(5000 \times 20)}{76800} = 1.3$$

3.

$$NumberofGWC = MAX(24.4, (15.8 + 1.3)) = MAX(24.4,17.1) = 25$$

In this example, 25 GWC pairs are required to satisfy the capacity needs.

### 9.4.2 Audio Controller-based Gateway Controllers

One AC GWC pair (active+spare) can be deployed with one UAS. The engineering of the UAS is detailed in section 9.8.

### 9.4.3 Anchor Packet Gateway-based Gateway Controller

> ***Note:*** A decision has been made to restrict further deployment of APG for SN06 & SN07. **Further deployment of APG is restricted requiring approval from PLM.**

As discussed earlier, Anchor Packet Gateway, or APG, is a gateway that has its basis in the PVG. As such, it must be controlled by a Gateway Controller. The GWC that supports the APG may be provisioned in one of two configurations. In.one configuration the APG function is combined with a DPT GWC, and the other where the APG is configured on a standalone GWC. The following table illustrates the APG GWC capacity.

**Table 0-42**

| APG GWC Type | Max. Number of VSP Gateways | | Number of Endpoints | | Number of Calls | | BHCA |
|---|---|---|---|---|---|---|---|
| | VSP2 | VSP3 | VSP2 | VSP3 | VSP2 | VSP3 | |
| DPT/APG | 1 | 1 | 1120 | 2016 | 560 | 1008 | 24,000 |
| APG Only | 3 | 3 | 3360 | 6048 | 1680 | 3024 | 72,000 |

To determine the number of APG–based GWCs required, first determine the number of office–wide APGs required. Refer to section 9.7.1. Once this number has been determined, the number of APG–based GWC can be calculated by the Max. Number of VSP Gateways allowed per APG GWC type as illustrated in the previous table.

***Note:*** The number of gateways supported per APG–based GWC remains constrained as shown above regardless of whether a VSP2– or VSP3–based APG is used. However, the number of endpoints are reduced when utilizing a VSP2–based APG.

### 9.4.4 SIP-T DPT Gateway Controllers

The rated capacity of the SIP-T GWC is 96,000 BHCA. The SIP-T GWC has sufficient real time to accommodate up to 4094 ports at 23 call attempts/trunk/hour. Each port corresponds to a Dynamic Packet Trunk (DPT). The engineering approach is to divide the total number Dynamic Packet Trunks in the office by 4094 to determine the number of SIP-T GWC required.

If the average per-port call rate should exceed the rate specified in the previous paragraph, or the number of simultaneous calls exceed the value specified in Table 67, “GWC Capacities,” on page 198, then apply the following algorithm to calculate the correct number of gateway controllers.

1. Determine the number of GWC pairs based on port limits.

$$NumberofGWC_{ports} = \frac{TotalNumberofPorts}{4094}$$

2. Determine the number of GWC pairs based on engineered BHHCA limits.

$$NumberofGWC_{BHHCA} = \frac{(TotalNumberofPorts \times BHHCAperPort)}{96000}$$

3. Determine the number of GWC pairs based on the maximum of the previous steps, rounding up to the next whole integer.

$$NumberofGWC = MAX(NumberofGWC_{ports}, NumberofGWC_{BHHCA})$$

For an example of an office requiring 50,000 DPT trunks at 20 BHHCA per port.

1.

$$NumberofGWC_{ports} = \frac{50000}{4094} = 12.2$$

2.

$$NumberofGWC_{BHHCA} = \frac{(50000 \times 20)}{96000} = 10.4$$

3.

$$NumberofGWC = MAX(24.4, (15.8 + 1.3)) = MAX(12.2,10.4) = 13$$

***Note:*** In this example, 25 GWC pairs are required to satisfy the capacity needs.

### 9.4.5 VRDN Gateway Controllers

The VRDN is used to route SIP-T signaling messages to other CS2000 nodes while supporting signaling to a number of other CS2000 nodes. In a CS2000 office, multiple VRDNs can exist, however, the signaling path between any two (2) specific CS2000 nodes is only supported on single VRDN. That is, individual DPT trunk groups to an adjacent CS2000 can not exist on more than a single VRDN.

Trunk traffic engineering is required to ensure that the sizing of the DPT trunk groups keeps the call volume through the VRDN to less than the rated capacity of 900K calls/hour.

***Note:*** If an SN06-based VRDN is communicating with a far-end VRDN at another CS2K, and that far-end VRDN is running a pre-SN05 load, the two VRDNs will negotiate to use SCTP rather than UDP. This lowers the capacity of the near-end VRDN.

### 9.4.6 GWC Surveillance

Table SERVRINV can be used to identify the number of GWCs. Table LGRPINV identifies the LGRPs (field srvrname) as discussed above with their associated GWC. Also, Table LTCINV (field OPT-ATTR, datafilled as EXTDS512) should be used to determine the ABI DS-512s associated with a particular GWC. All of these tables are datafilled in the XA-Core.

An important part of determining proper engineering of GWC is monitoring their performance. This is achieved by using the XPMOCC OM group. Available on fifteen minute intervals, these registers provide processor occupancy of the GWC. Most processor occupancy registers peg the number of 1 minute intervals the CPU was at a given level. The following registers are of key importance to the discussion of surveillance:

- AVGCPOCC – Average call processing occupancy (expressed as a percentage)
- PMORIGS – Total call originations attempts
- PMTERMS – Total call termination attempts

- NUMRPTS – Total number of fifteen minute reports added to the accumulation registers during the accumulation period to normalize AVGCPOCC.

The following algorithm should be used to calculate the number of half-call BHCA,

$$BHHCA = \frac{PMORIGS + PMTERMS}{S} \times 3600$$

where *S* is the number of seconds for the accumulation period. If this result is approaching the associated value in Table 67, “GWC Capacities,” on page 198, additional ports should not be provisioned on this GWC pair but rather on another GWC pair.

Additionally, the average call processing occupancy should also be monitored to ensure proper engineering or that the engineering point is not being exceeded. The following algorithm should be applied.

$$CallProcessingOcc = \frac{AVGCPOCC}{NUMRPTS}$$

If the result is approaching 80%, then it is recommended that no additional ports be provisioned on this GWC pair, but rather on another GWC pair.

***Note:*** Nortel Network recommends an accumulation period of at least one hour for more accurate results. Also this should be done, if possible, during the office’s HDBH.

### 9.4.7 Shelf Controller

Each master shelf on the MG9000 will establish 2 signaling SVCs to the Shelf Controller (SC). In addition, each DS512 interface pack will establish a separate (3rd) SVC back to the SC.

The SVCs from each MG9000 node must terminate on the SC of the SAM21 shelf which houses the GWCs serving the MG9000 shelves. There are no rules for having to assign LGRPs of an MG9000 node to the same GWC, however all of the LGRPs and ABIs of an individual MG9000 node must be assigned to GWCs on the same SAM21.

If there is a need for more than one SAM21 shelf, it is preferable to spread the load across the shelves, still maintaining the LGRP rule described above.

## 9.5 Passport 8600 Engineering

### 9.5.1 Capacity

The bearer traffic from voice gateways (i.e. IW-SPM and PVG) directly subtending these PP8600s accounts for the majority of the traffic in the CS-LAN. Each voice gateway will introduce about 0.5Mpps (or ~500Mbps) worth of traffic. Even by provisioning enough voice gateways to fully populate all the ports on the PP8600s (while taking engineering of the MLT and WAN ports into consideration), the traffic generated will still be well within the 96Mpps maximum forwarding rate of the CS-LAN PP8600s.

***Note:*** As more voice gateways are added to the CS-LAN and the expected bearer traffic leaving the CS-LAN surpasses 3-4Gbps, it is recommended for cost-effectiveness to upgrade the PP8600 WAN uplink interfaces from 1-GigE ports to 10-GigE ports.

### 9.5.2 Hardware Engineering

The 8010co chassis is a ten (10) slot chassis, which can be configured with various combinations of interface modules depending on the customer's requirements. With two (2) slots reserved solely for switching fabric modules, the total number of interface modules supported on the Passport 8600 is eight (8). The minimum number of interface modules required for a particular solution depends strictly on how many ports are needed for the VRRP/MLT connectivity, needed to uplink to the Core network, and needed to interconnect the subtending devices (i.e. GWC, HIOP, UAS, CMTS).

***Note:*** Due to the extensive recovery time of the PP8600 with dual CPUs installed, it is a requirement that ONLY one (1) CPU be installed per redundant PP8600.

Note that additional ports/modules may need to be included when taking scalability into consideration. If the network needs to be scaled, then:

- Read through all of this chapter to determine the additional GWCs, UASs, etc. required and resize the network accordingly
- Reapply the following engineering rules
- Order additional parts if necessary.

**PP8600 Series E-Modules**

The PP8600 Series E-modules are direct replacements for the original Passport 8600 I/O modules and are the baseline for newly commissioned sites. The release notes are available on the Nortel Networks Customer Service Documentation Web page (http://www.nortelnetworks.com/documentation). The Series E-Modules contain changes to all modules that will improve manufacturing yields and are completely compatible with non-E-modules in a mixed environment. Furthermore, minor changes have been made to ASICs for the RAPTillion Address Resolution Unit (RAPTARU4) and the Octal Port Interface Device (OCTAPID3B) to support egress port mirroring.

The following step-by-step rules were defined to engineer the redundant CS-LAN Passport 8600s.

Two (2) 8632TXE routing switch modules are required as a baseline, which includes 32 10/100 BaseT ports and 2 GBIC ports.

***Note:*** The MLT group should only be configured using 2 GigE interfaces per PP8600 chassis. For more details, refer to the MLT guidelines in the PP8600 section of the CS-LAN Common Components Chapter.

With the remaining six (6) interface slots, determine the number of 10/100 BaseT modules required to interconnect with the CallP and OAM&P devices not already linked to the 8632TXE modules.

The number of 48-port 8648TXE modules required per redundant chassis is defined by:

1. Determine the number of devices remaining in the CallP and OAM VLANs with 100 BaseT Ethernet interfaces.
   a. GWC
   b. XA-Core

**c.** PP15000

**d.** SAM21 SC

**e.** UAS

**f.** SDM: one for CallP and one for OAM&P VLANs

**g.** OAM&P: CS2K Management Tools Server, CMTS EM, NMS, etc.

2. From this total subtract the Number of 10/100 BaseT ports not used on the 8632TXE module.
3. Divide this difference by 48 and round up.
4. Order/install this many 8648TXE modules per chassis as a baseline.

With the remaining interface slots, determine the number of 8-port 8608GBE GigE modules required per redundant chassis for VRRP/MLT and WAN uplink once the GBICs on the 8632TXE modules have already been populated.

The number of 8608GBE GigE modules required per redundant chassis is defined by:

1. If the WAN uplink is GigE, then order/install an additional GBIC MDA per chassis as a baseline.
2. Calculate the total number of GBIC MDAs used.
3. Divide this total by eight (8) and round up.
4. Order/install this many 8-port 8608GBE GigE baseboard modules per chassis as a baseline.

***Note:*** To avoid a single point of failure the VRRP/MLT links need to be evenly separated across multiple modules.

## 9.6 Engineering an IW–SPM

Recall from section “2.1.5 Inter-working SPM (not applicable to Compact CS2K solutions)” on page 40 that an IW–SPM is a switch element which provides bearer path bridging between the ENET and IP fabric. Each IW–SPM is capable of supporting a call-rate of 12 bridges per seconds with a maximum of 2016 simultaneous bridges.

The IW–SPM is engineered as a “bridging” function rather than as a trunk peripheral. The number of IW–SPMs is determined by the volume of announcement traffic and interworking traffic, including Dynamic Packet Trunk (DPT) traffic, expected across the fabric. The total number of simultaneous bridges required is dependent on the split of trunk groups across the ENET and IP fabrics.

***Note:*** T.38 Fax, and RFC 2833 are supported in SN06 on PVG and IW-SPM. However, when both T.38 and RFC 2833 are configured on PVG, PVG will generate a large SDP that the IW SPM currently does not support SN06. Therefore, if the office has both PVG and IW-SPM, then the PVG should not be configured to support both RFC2833 and T.38 Fax. This should have no impact if G.711 the preferred codec.

Detailed engineering guidelines are in SEB 01-11-001: Interworking SPM Engineering Guide for VToA

### 9.6.1 IW SPM Capacity

The IW SPM is a switch element which provides bearer path bridging between the ENET and ATM fabrics. The IW SPM will carry announcement traffic and interworking traffic between MG9000 and MG4000 gateways and legacy line and trunk peripherals.

Each IW SPM supports 2016 bridges. A minimum of 1, and a maximum of up to 14 IW SPMs can be supported on a CS2000.

The IW SPM will interconnect over DS512 with the ENET, and over OC3c with the ATM fabric. ENET ports will be consumed. The number of IW-SPMs equipped in a Call Server can be identified in Table MNNODE. In Table MNNODE the “class” field datafilled with “IW” identifies IW-SPMs.

When an office is equipped with IW SPMs, Inter Message Switch Links (IMSL) must be provisioned. The IMSL is a link connecting both shelves of a Message Switch (MS or DMS-BUS) and is used for providing alternate route for messages destined to IW SPMs. For details refer to SEB 00-12-001: Inter MS link Capacity and Provisioning guide.

### 9.6.2 Determining the Number of IW–SPMs needed in a Office

To be provided in a future release.

### 9.6.3 Monitoring IW–SPMs

A new Operational Measurement group, **IWBM**, is available to monitor bridge usage at the office level. Two registers should be considered:

- **IWGBATT/IWGBATT2** — Contains a count of the number of bridge attempts for both DPT and Gateway trunk to/from legacy peripherals such as SPMs, and DTCs.
- **IWGBFAIL** — Contains a count of the number of bridge attempts failures for both DPT and Gateway trunk to/from legacy peripherals such as SPMs, and DTCs.

In addition to the above mentioned registers, a number of other registers are defined to provide a threshold view of the number of bridges in use:

- **IWONSET1** — Indicates that the number of IW bridges in use exceeds 70% of the office total.
- **IWONSET2** — Indicates that the number of IW bridges in use exceeds 90% of the office total.

#### 9.6.3.1 IW–SPM Average Bridge Attempt Rate

Using the register definitions discussed in the previous section, it is possible to determine the average number of bridge attempts per second for the IW–SPM. Recall that the IW–SPM is rated at 12 bridges per second. The following represents a calculation of a busy-hour data collection period.

$$\frac{(IWGBATT + 65535 \times IWGBATT2)}{(N \times 3600)} = AverageBridgeAttempt$$

where N is the number of in-service IW–SPMs.

#### 9.6.3.2 IW–SPM Bridge Attempt Failure Rate

A key IW–SPM performance measure is the failure rate in getting bridges. Available at the office level only, OM group IWBM contains two key registers used to calculate the interworking grade of service levels, expressed as a percentage, as follows:

$$\frac{IWGBFAIL}{(IWGBATT + 65535 \times IWGBATT2)} \times 100 = IWGoS$$

***Note:*** If the IW–SPM GoS criterion of 0.00001% is exceeded, then an additional IW–SPM should be provisioned.

### 9.6.4 Monitoring Voice Quality

Provided in a future release.

## 9.7 Anchor Packet Gateway Capacity

***Note:*** A decision has been made to restrict further deployment of APG for SN06 & SN07. **Further deployment of APG is restricted requiring approval from PLM.**

As discussed earlier, Anchor Packet Gateway, or APG, is a gateway that has its basis in the PVG.

The concept of an Anchor Packet Gateway comes from the need to access and manipulate the bearer channel associated with a call from a call context that normally would not have access to the bearer channel. In a typical two-party call between two PVGs, the services which are executing on behalf of either the originating party or the terminating party have access to the bearer path and the physical endpoint via the PVG it serves. The core directs the PVG (via the GWC) to collect digits, apply local tones, or manipulate the connection between the two gateways. This is not the case, though, if one or both of the parties in the call is a dynamic packet trunk. In these scenarios, only call control signaling is received and processed by the CS2K from the dynamic packet trunk portion of the call. A dynamic packet trunk cannot use a media control protocol to access the bearer path because no physical gateway is currently associated with it.

An anchor packet gateway provides a physical device so that the DPT context can terminate and access the bearer path associated with a call. The DPT can instruct the anchor packet gateway to perform actions on the bearer path such as collecting digits, applying a tone, or redirecting the destination of the connection. The anchor packet gateway provides a DPT context to manage the bearer stream. Once the bearer path in anchored, it cannot be moved, i.e., it remains inserted for the duration of the call.

### 9.7.1 Determining the Number of APGs Required in an Office

To determine the number of APGs required per office, one must know the following items:

- Office BHCA
- Percentage of Office BHCA that is DPT
- The feature usage (expressed as a percentage of DPT BHCA). These are the features that reside on the trunk group and require access to the bearer path. For example,

    - Expected DPT trunks with RECALLDT set to MANUAL on the EANT trunk group (IXC Service)
    - Expected DPT trunks with MCCS on the EANT trunk group (IXC Service)
    - E911 on IT DPT trunks
    - Other services or translations on DPT trunks that require Authorization codes, PIN codes or Account code entry, or other types of digit collection.
- AHT of an DPT call (since the APG is inserted for the duration of the call)
- Grade–of–Service (GoS) desired, e.g., 1% blocking.

1. Determine AHT for DPT trunks from the OM group TRKS, or use an expected AHT.
2. Next, determine the office–wide Erlang load (Note that the DPTEANT percentage may be other trunk types such as IT)

$$officewideErlangLoad = (officeBHCA \times AHT \times DPTEANT \times (FeatureX + FeatureY + \ldots)) \div 3600$$

3. Then, using Erlang B, determine the number of trunks required based on GoS requirement.
4. Finally, determine the number of APGs required, rounding up to the next integer.

$$NumberofAPG = (NumberofServers) \div (NumberofVSPendpoints)$$

Where *NumberofVSPendpoints* is

- 2016 for VSP3–based APG, or
- 1120 for VSP2–based APG

### 9.7.2 Monitoring APG Usage

A key measurement in monitoring the APG is the failure rate. This determines the GoS being offered to the DPT trunks requiring bearer path manipulation. An SNMP–based Performance Monitoring Poller is available to collect performance attributes from Succession–based network elements. Using this poller, it is possible to collect data from the APG GWC(s) on the usage of the APGs in an office. For the purposes of this discussion, it is assumed that the reader has configured the poller to collect the GWC profile data.

The following attributes are of relevance to the measurement:

- resourceRequestError — Number of failures to provide a resource.
- apgInsertions — Total number of APG invocations
- apgCallFailGWException — Number of APG call failures due to gateway exceptions
- apgCallFailGWLost — Number of APG call failures due to lost heartbeat with gateway.

The above mentioned attributes are a running total for that GWC. Since each GWC may contain up to three (3) APG, these values would include all the APG for that GWC. The value of these attributes should be collected for every APG–based GWC in the office. Recall that the poller collects device attributes at the specified interval. The interval is configurable, and should be set for at least a 15 minute interval or higher. After multiple intervals have passed (e.g. 1 hour’s worth, 1 day’s, etc.), determine the difference between the first and last interval, and apply the results to the following to determine the GoS.

$$GoS = \sum_{GWC=1}^{GWCn} (resourceRequestError + apgCallFailGWException) / (apgInsertion + resourceRequestError)$$

If the GoS drops below the desired GoS, say 1.0%, then more APGs should be added.

***Note:*** *resourceRequestError* is added to apgInsertion since *apgInsertion* is not pegged when *resourceRequestError* is pegged. Although *resourceRequestError* is recorded as an error, it is considered an APG attempt none-the-less.

### 9.7.3 Monitoring APG Average Attempt Rate

Recall that APGs are based on VSP2 or VSP3 Function Processors, and as such, are rated at approximately 7 and 13 calls per second, respectively. To determine the average insertion rate across the office, collect two polling intervals (e.g., 2– 1 hour intervals) utilizing the SNMP–based Performance Monitoring Poller to collect performance attributes from all APG–based GWCs. Use the following to calculate the average APG attempt rate.

$$APGAverageInsertionRate = \frac{\sum_{1}^{n} (I_2 - I_1)_1 + (I_2 - I_1)_2 + \ldots + (I_2 - I_1)_n}{(N \times 3600)}$$

where,

- *N* is the number of APGs in the office,
- *n* is the number of APG–based GWCs,
- $(I_2 - I_1)$ is the difference in the two collected polling intervals, with $I_2$ being the most recent interval collected and $I_1$ being the prior interval collected.

## 9.8 Universal Audio Server

The Universal Audio Server will ONLY be used for Lawful Intercept.

The Universal Audio Server (UAS) supports tones and announcements, including branding, as well as 3-port and higher port conference circuits, and Lawful Intercept. UAS engineering must accommodate the demands of short holding time (high real time) announcement traffic and long holding time (high port usage) conference traffic. This section uses models based on field data in engineering the UAS.

Operational Measurement (OM) data can be used to develop UAS models. In OM group ANN, register ANNATT counts total announcement attempts, and register ANNTRU provides traffic usage. Suppose these registers give the following busy hour values:

- ANNATT= 5700

- ANNTRU= 684 (based on 100 sec scans)

The average holding time (AHT) in seconds for announcements is then:

- ANN AHT = 684 * 100 / 5700, or 12 sec (realistic value).

In 3-port conferencing OM group CF3P, analogous attempt and usage registers with example data are:

- CNFSZRS= 570
- CNFTRU= 19380 (based on 10 sec scans)

The AHT for 3-port conferences is:

- 3-Port AHT = 19380 * 10 / 570, or 340 sec (high end of realistic).

In 6-port conferencing OM group CF6P, attempt and usage registers with example data are:

- CF6SZRS= 285
- CF6TRU= 19950 (based on 10 sec scans)

The AHT for 6-port conferences would be:

- 6-Port AHT = 19950 * 10 / 285, or 700 sec (not known if this is realistic because 6-port usage was zero in most sample offices).

When total call attempts in the switch are known (for example, by summing OFZ registers NIN with extension NIN2, and NORIG with extension NORIG2), the percentage of call attempts with announcements can be found. Suppose there are 82,000 call attempts and 5,700 announcement attempts, as above, then about 7% of call attempts require an announcement. For North American end offices, the following model was developed using OMs from several offices.

**Table 0-43**

| Call Type | % of Attempts | Average Holding Time (secs) |
|---|---|---|
| Announcements | 7% | 12 |
| 3-port Conference | 1% | 340 |

To illustrate UAS engineering, we apply the model percentages above to call volumes of 275,000 and 550,000 BHCAs, that is, 50% and 100% of the SN06 maximum of 550,000 BHCAs. It is expected that Lawful Intercept (LI) will generate some load on the UAS, but the amount of LI traffic is not known accurately. However, LI is not expected to require more than two CG6000 cards with redundancy.

The following table provides UAS provisioning results for the number of UAS, cards and ports, as well as a sensitivity results. The base case is as follows:

- 550K BHCA (SN06 capacity)
- 7% of CAs require announcements with 12 sec AHT
- 1% of CAs are 3-Port Conference Calls with 340 sec AHT
- G.711 codec with 10 ms packet size
- Lawful Intercept (LI) required
- N+1 Redundancy
- GWC Restrictions in effect

**Table 0-44**

| Case | Provisioning Results |
|---|---|
| Base | 8 UAS, CG6000: 34 AC & 2 LI, 4 GWC; Ports: 309 Ann, 2435 Conf, 176 LI |
| 20ms Packet Size | 7 UAS, CG6000: 29 AC & 2 LI, 4 GWC; Ports: 309 Ann, 2598 Conf, 176 LI |
| G.729 Codec | Same as Base Case |
| 275K | 6 UAS, CG6000: 16 AC & 2 LI, 1 GWC; Ports: 154 Ann, 1169 Conf, 176 LI |
| 3P AHT 200 seconds | 7 UAS, CG6000: 24 AC & 2 LI, 4 GWC; Ports: 309 Ann, 1528 Conf, 176 LI |
| No LI | 8 UAS, CG6000: 33 AC & 0 LI, 4 GWC; Ports: 269 Ann, 2435 Conf, 0 LI |

The first row in the above table is for the base case identified above. The base case requires 8 UASs containing a total of 34 CG6000 cards for Announcements and Conferencing (AC), and 2 for Lawful Intercept. In addition, 4 GWC pairs are needed. The ports required break down into 309 for announcements, 2435 for conferencing and 176 for Lawful Intercept. Using this information, the required number of ports can be datafilled.

The next row shows provisioning requirements for the case when IP Packet Size is increased from 10 ms in the Base Case to 20 ms. The table also shows that results are unchanged if the codec is G.729, rather than G.711. The impacts of a reduced call volume, lower holding time for 3-Port conference calls, and removing Lawful Intercept are also shown.

***Note:*** Prior to SN06, hybrid office configuration, that is, a mix of legacy DMS peripherals and CS2K peripherals with bearer interworking through the IW–SPM, legacy DMS peripherals could not utilize the conferencing capabilities of the UAS. As such, no conference circuits could be provisioned in the CS2K for hybrid configurations. This restriction has been removed in SN06.

## 9.9 AMS Audio Server

The Universal Audio Server (UAS) supports tones and announcements, including branding, as well as 3-port and higher port conference circuits, and Lawful Intercept. UAS engineering must accommodate the demands of short holding time (high real time) announcement traffic and long

holding time (high port usage) conference traffic. This section uses models based on field data in engineering the UAS.

Operational Measurement (OM) data can be used to develop UAS models. In OM group ANN, register ANNATT counts total announcement attempts, and register ANNTRU provides traffic usage. Suppose these registers give the following busy hour values:

ANNATT= 5700

ANNTRU= 684(based on 100 sec scans)

The average holding time (AHT) in seconds for announcements is then:

ANN AHT = 684 * 100 / 5700, or 12 sec (realistic value).

In 3-port conferencing OM group CF3P, analogous attempt and usage registers with example data are:

CNFSZRS= 570

CNFTRU= 19380 (based on 10 sec scans)

The AHT for 3-port conferences is:

3-Port AHT = 19380 * 10 / 570, or 340 sec (high end of realistic).

In 6-port conferencing OM group CF6P, attempt and usage registers with example data are:

CF6SZRS= 285

CF6TRU= 19950 (based on 10 sec scans)

The AHT for 6-port conferences would be:

6-Port AHT = 19950 * 10 / 285, or 700 sec (not known if this is realistic because 6-port usage was zero in most sample offices).

When total call attempts in the switch are known (for example, by summing OFZ registers NIN with extension NIN2, and NORIG with extension NORIG2), the percentage of call attempts with announcements can be found. Suppose there are 82,000 call attempts and 5,700 announcement attempts as above, then about 7% of call attempts require an announcement. For North American end offices, the following model was developed using OMs from several offices. An Asian site showed similar 3-Port Conference attempt rates and similar AHTs in the 300 sec range. However, Announcements at the Asian site were less than 3%, but the AHT was 10 sec.

| Call Type | % of Attempts | Av. Holding Time (sec) |
|---|---|---|
| Announcements | 7% | 12 |
| 3-Port Conferences | 1% | 340 |

**Table 1 – North American Announcement and 3-Port Conferencing Model**

To illustrate UAS engineering, we apply the model percentages in Table 1 to call volumes of 300,000 and 600,000 BHCAs. It is expected that Lawful Intercept (LI) will generate some load on the UAS, but the amount of LI traffic is not expected to require more than two CG6000 cards with redundancy.

Table 2 provides UAS provisioning results for the number of UAS, cards and ports, as well as sensitivity results. The base case is as follows:

- 600K BHCA
- 7% of CAs require announcements with 12 sec AHT
- 1% of CAs are 3-Port Conference Calls with 340 sec AHT
- G.711 codec with 10 ms packet size
- LI required
- N+1 Redundancy
- GWC Restrictions in effect

| Case | Provisioning Results (Including Spares) |
|---|---|
| Base | 8 UAS, CG6000: 34 AC & 2 LI, 4 GWC; Ports: 309 Ann, 2435 Conf, 176 LI |
| 20 ms Pkt Size | 7 UAS, CG6000: 29 AC & 2 LI, 4 GWC; Ports: 309 Ann, 2598 Conf, 176 LI |
| G.729 Codec | Same as Base Case |
| 275K | 6 UAS, CG6000: 16 AC & 2 LI, 1 GWC; Ports: 154 Ann, 1169 Conf, 176 LI |
| 3P AHT 200 sec | 7 UAS, CG6000: 24 AC & 2 LI, 4 GWC; Ports: 309 Ann, 1528 Conf, 176 LI |
| No LI | 8 UAS, CG6000: 33 AC & 0 LI, 4 GWC; Ports: 269 Ann, 2435 Conf, 0 LI |

**Table 2 – UAS Provisioning Results and Sensitivities**

The first row in the above table is for the base case identified above. The base case requires 8 UASs containing a total of 34 CG6000 cards for Announcements and Conferencing (AC), and 2 for Lawful Intercept. In addition, 4 GWC pairs are needed. The ports required break down into 309 for announcements, 2435 for conferencing and 176 for Lawful Intercept. Using this information, the required number of ports can be datafilled.

The next row shows provisioning requirements for the case when IP Packet Size is increased from 10 ms in the Base Case to 20 ms. The table also shows that results are unchanged if the codec is G.729, rather than G.711. The impacts of a reduced call volume, lower holding time for 3-Port conference calls, and removing Lawful Intercept are also shown.

The UAS also supports T1 trunk testing via a Sage trunk testing device. Additional UAS provisioning for T1 trunk testing is as follows:

- One (1) additional card CG6000 card (i.e., in addition to the Provisioning Results provided above)
- The additional card can be accommodated in any UAS which is not already filled with cards [i.e., six (6) CG6000 cards]
- If all UASs provisioned are completely filled and have no room for a trunk testing card, then one (1) additional UAS must be provisioned to house the CG6000 card needed for trunk testing.

Explanantory Notes:

- 1) The trunk testing card is a dedicated resource, unavailable for any other activities on the UAS. It does NOT require sparing.
- 2) Trunk testing is carried out in a period of low traffic, and does not affect the busy hour erlang load and call rates given above.
- 3) Given Note 2, there is no need for additional GWC pairs based on erlang and call rate loads.

**AMS Engineering**

AMS2010 (AudioCodes Media Server 2010) is introduced in SN06.2 as an alternative to the UAS, which is not undergoing further development. The AMS has similar functionality to the UAS, and its engineering is simplified by not being depending on IP packet size or CODEC type. The AMS is available as a 120 port version (with 1 TPM) or a 240 port version (with 2 TPMs). Both versions can be deployed together. For example, if 11 TPMs are needed, five (5) 240 port AMS's and one (1) 120 Port AMS would be provisioned. The resources needed for LI are lower compared with the UAS, which requires that one or more cards be dedicated to LI.

To illustrate AMS engineering, we proceed in a similar way to that for the UAS. The base case is as follows. It is similar to that for the UAS, but CODEC and packet size do not have to be specified. This allows a comparison between UAS and AMS provisioning.

- 550K BHCA
- 7% of CAs require announcements with 12 sec AHT
- 1% of CAs are 3-Port Conference Calls with 340 sec AHT
- LI required
- N+1 Redundancy
- GWC Restrictions in effect
- No T1 Trunk Testing (TT)

| Case | Provisioning Results (Including Spares) |
|---|---|
| Base | 20 TPM; 1 GWC; Ports: 179 Ann, 2165 Conf, 9 LI, 0 TT |
| 275K | 11 TPM; 1 GWC; Ports: 99 Ann, 1191 Conf, 10 LI, 0 TT |
| 3P AHT 200 sec | 13 TPM; 1 GWC; Ports: 191 Ann, 1355 Conf, 10 LI, 0 TT |
| No LI | 20 TPM; 1 GWC; Ports: 179 Ann, 2165 Conf, 0 LI, 0 TT |
| T1 Trunk Testing | 20 TPM; 1 GWC; Ports: 179 Ann, 2165 Conf, 9 LI, 16 TT |

**Table 3 – AMS Provisioning Results and Sensitivities**

Looking at results for the base case in Table 3, 20 TPM modules are needed. This translates into ten (10) 240 port AMSs. The 179 ports needed for announcements include spares. Conferencing and LI ports also include spares. Trunk testing (not in the above base case) does not require spares. All ports are spread as uniformly as possible across TPMs when a single GWC is needed.

For each case in the table, 1 GWC pair is sufficient. For the base case above, the BHCA volume would have to increase to a hypothetical value of almost 800,000 to trigger a need for a second GWC pair. If more than 1 GWC is needed, all conferencing is controlled by a single GWC, and all announcement traffic is controlled by additional GWC(s).

Looking down the table at ports provisioned in the various cases, we see some variations due to modularity and sparing effects, but largely linear relationships. For example, when the call volume is reduced by 50% from 550K to 275K, the number of announcement ports falls only about 45%, or a bit less than half.

Interpolation between the tabulated values can be used to estimate provisioning requirements for other cases.

## 9.10 OAM&P Server Engineering

### 9.10.1 CS2K Management Tools Server Engineering

#### 9.10.1.1 Traffic Engineering

The CS2K Management Tools Server is a management platform, on a single Sun NetraT1400, that provides a common Element Management Framework and supports 60 GWC with up to 165K end-points.

The Netra T1400 supports the following applications without requiring engineering:

- Gateway Controller Element Manager
- Universal Audio Controller Element Manager
- Line Maintenance Manager
- Trunk Maintenance Manager
- Alarm Manager
- Network Patching Manager / EPM
- Audio Provisioning Server – APS
- SAM21 Element Manager (up to eight SAM21 shelves)

#### 9.10.1.2 Number of Clients Supported

The large system capacity and performance verification of the CS2K Management Tools Server has used a model of no greater than;

- 10 client machines (GUIs) open for alarm browsing / maintenance
- 4 client machines (GUIs) open for LMM/TMM

#### 9.10.1.3 Bandwidth and Network Performance

It is recommended to interconnect the CS2K Management Tools Server with Ethernet 100 baseT, full duplex.

### 9.10.2 SuperNode Data Manager (SDM)

#### 9.10.2.1 Traffic Engineering

The SDM is an application server that resides between the CS2000 and the OAM&P Management Plane.

The SDM supports the following functions:

- SAM21 EM up to 8 SAM21 shelves
- Bootp Server up to 60 GWC
- TFTP Server up to 60 GWC (for reboots)
- DDMS

- ERM
- OMDD
- SBA up to 1.5M billing records/hour
- SFT
- ETA
- NTPd
- ATA
- EADAS over TCP/IP
- Log Delivery
- RPC

The SDM executes on the Nortel Networks F/X platform and is a high-performance, fault tolerant, UNIX-based processing platform that utilizes a Motorola PowerPC 750 dual processor system utilizing the IBM AIX operating system. System I/O is achieved using fault tolerant I/O buses, mirrored disk storage, and redundant communication links. The SDM/FT is housed is a C28 Model B streamlined cabinet.

#### 9.10.2.2 Number Clients Supported

The SDM will support up to 32 client machines (GUIs).

#### 9.10.2.3 Bandwidth

It is recommended that the SDM interconnect to the CS-LAN with Ethernet 100 BaseT, full duplex. Although this is not the hardware baseline requirement, it is recommended for recovery scenarios, particularly in offices with more than two (2) SAM21 shelves.

### 9.10.3 PVG Element Manager

The PVG Element Manager utilizes the Preside Multiservice Data Manager (MDM) platform to provide provisioning, SNMP alarm collection, and performance measurements display in support of the PVG7K or the PVG15K.

Up to 30 PVGs can be supported on a single PMDM. Multiple PMDM will need to be deployed to support greater than 30 PVGs.

## 9.11 Per-Path OAM Messaging, Bandwidth, Latency and Loss Requirements

This section provides a per-path view of OAM traffic functional and capacity requirements. The term “path” refers to bi-directional lines of communication between pairs of network elements that connect to the OAM network. The MG4000 and MG9000 requirements are discussed in Chapter 6.0.

### 9.11.1 Preside MDM to SDM

The traffic between the Preside MDM and the SDM consists of the following message types:

- Alarms
- Performance measurements (PMs)

The SDM-resident application software (either alarm or PM) will determine the SUN server from

which to obtain the data.

**Table 73**

| **Performance** |
|---|
| Bandwidth = 1.23 x $10^6$ bps |
| Maximum latency = less than one second |
| Maximum packet loss = not applicable |
| **Protocols** |
| IP, ICMP, TCP, ARP, FTP |
| **Physical Connection Characteristics** |
| SDM: 10Base-T Ethernet, two links, one IP address |
| Preside MDM: 10Base-T Ethernet, one link/t1400 server, one IP address |
| **Notes** |
| 1. Link connecting t1400s is on a separate (private) subnet. |
| **Security Needs** |
| A network isolated from all non-Succession traffic with a dedicated path from the SDM to the Preside MDM |

The following table illustrates examples of OAM capacity data for two Ethernet links associated with the SDM.

**Table 74**

| **Application** | **Bandwidth (bits/second)** | **Packets (per second)** | | |
|---|---|---|---|---|
| | | | **SDM Link 1 (secs)** | **SDM Link 2 (secs)** |
| ARP | 4.64 x $10^2$ | 1.00 | 1 | |
| Alarms (from Preside MDM to SDM | 6.69 x $10^2$ | 0.02 | 5 | |
| 5-minute performance measurements (from Preside MDM) | 1.26 x $10^5$ | 72.00 | 3 | |

**Table 74**

| | | | | |
|---|---|---|---|---|
| 5-minute performance measurements (from SDM) | $1.55 \times 10^5$ | 72.00 | 3 | |
| 30-minute performance measurements (from Preside MDM) | $1.26 \times 10^5$ | 72.00 | 3 | |
| SDM to Preside MDM connection audit alarms | $4.64 \times 10^2$ | 1.00 | 2 | |
| SDM to SDM link audit | $3.36 \times 10^2$ | 1.00 | 1 | |
| SDM to Preside MDM connection audit performance measurements | $2.58 \times 10^0$ | 0.01 | 2 | |
| | | **Total Bandwidth** | $1.23 \times 10^6$ | 0.00 |
| | | **Total Packets** | 652.12 | 0.00 |

## 9.11.2 Passport 15000 to Preside MDM

The traffic on the path from the Passport 15000 to the Preside MDM consists of the following message types:

- Alarms
- Performance measurements (PMs)
- State change notifications (SCNs)
- Security log files
- Time-of-day (TOD)
- Statewalk audits

The 10Base-T Ethernet links between the Passport 15000 and the IP edge equipment are load-spared (only one is active at any given time).

The following table specifies requirements that apply to this path:

**Table 75**

| **Performance** |
|---|
| Bandwidth = $3.39 \times 10^5$ bps |
| Maximum latency = one second |
| Maximum packet loss = not applicable |

**Table 75**

| |
|---|
| Tolerance for out of order packets = not applicable |
| **Protocols** |
| IP, ICMP, ARP, TCP, UDP, FMIP, Telnet, FTP, NTP |
| **Physical Connection Characteristics** |
| Passport 15000: 10Base-T Ethernet |
| Preside MDM: 10Base-T Ethernet |
| **Notes** |
| **1.** Both the Passport 15000 and the Preside MDM support 10/100Base-T Ethernet, but only the 10Base-T Ethernet has been tested in the Succession configuration. |
| **Security Needs** |
| Not applicable: but a user ID and password are required for all access |

The following table illustrates examples of capacity data for the 10Base-T Ethernet path from the Passport 15000 to the Preside MDM:

**Table 76**

| **Application** | **Bandwidth (bits/second)** | **Packets (per second)** | | |
|---|---|---|---|---|
| | | | **PP15K Link 1 (secs)** | **PP15K Link 2 (secs)** |
| ARP | $4.64 \times 10^2$ | 1.00 | 1 | |
| Alarms from Passport 15000 | $1.42 \times 10^3$ | 0.40 | 2 | |
| SCNs from Passport 15000 | $7.10 \times 10^2$ | 0.20 | 2 | |
| State walk to Passport 15000 | $3.92 \times 10^1$ | 0.02 | 2 | |
| 5-minute performance measurements from Passport 1500 | $3.85 \times 10^4$ | 24.00 | 2 | |
| Network time of day | $1.00 \times 10^4$ | 8.33 | 1 | |
| Download to Passport 15000 | $2.47 \times 10^5$ | 53.67 | 1 | |
| MDM connection query for Passport 15000 | $2.56 \times 10^1$ | 0.22 | 1 | |

**Table 76**

| | | | | |
|---|---|---|---|---|
| | | **Total Bandwidth** | $3.39 \times 10^5$ | 0.00 |
| | | **Total Packets** | 112.46 | 0.00 |

### 9.11.3 SDM to OSS Network

The traffic on the path from the SDM to the OSS Network consists of the following message types:

- Performance measurements (PM) generated at five or 30-minute intervals
- Operational measurements (OM) generated at five-minute intervals
- logs
- automatic message accounting (AMA) billing records
- MAPCI data forwarded to the OSS Network from the SDM during remote MAPCI sessions

The CS2000 sends AMA billing records to the SDM. This path is implemented via Nortel Networks proprietary DS512 protocol.

The following table specifies requirements that apply to this path

**Table 77**

| **Performance** |
|---|
| Bandwidth = $3.49 \times 10^6$ bps |
| Maximum latency = less than one second |
| Maximum packet loss = not applicable |
| **Protocols** |
| IP, ICMP, SNMP, ARP, TCP, FTP |
| **Physical Connection Characteristics** |
| SDM: 10Base-T Ethernet |
| OSS: 10Base-T Ethernet |
| **Notes** |
| |
| **Security Needs** |
| Firewall protection is recommended on the OSS side. |

The following table illustrates examples of capacity data for the two OAM&P Ethernet links between the SDM and the OSS Network:

**Table 78**

| Application | Bandwidth (bits/second) | Packets (per second) | | |
|---|---|---|---|---|
| | | | **OSS (Link 1) (secs)** | **OSS (Link 2) (secs)** |
| ARP | $4.64 \times 10^2$ | 1.00 | 1 | 0 |
| SDM to SDM link audit | $3.36 \times 10^2$ | 1.00 | 1 | 1 |
| Alarms from SDM to OSS | $1.00 \times 10^3$ | 0.30 | 5 | 0 |
| DMS-100 alarms from SDM to OSS | $3.34 \times 10^2$ | 0.10 | 51 | 0 |
| 5-minute performance measurements from SDM | $1.55 \times 10^5$ | 72.00 | 3 | 0 |
| 30-minute performance measurements from SDM | $1.55 \times 10^5$ | 72.00 | 3 | 0 |
| AMA billing from SDM to OSS | $8.62 \times 10^5$ | 411.11 | 1 | 0 |
| 5-minute operational measurements from SDM to OSS | $1.07 \times 10^5$ | 51.00 | 1 | 0 |
| MAPCI Telnet remote display | $1.42 \times 10^5$ | 31.00 | 10 | 0 |
| Client Preside MDM | $1.23 \times 10^4$ | 3.00 | 1 | 0 |
| Remote X display | $1.42 \times 10^5$ | 31.00 | 1 | 0 |
| | | | | |
| | | **Total Bandwidth** | $3.49 \times 10^6$ | $3.36 \times 10^2$ |
| | | **Total Packets** | 1246.71 | 1.00 |

## 9.11.4 Preside MDM to OSS Network

The traffic on the path from the Preside MDM to the OSS Network consists of the following message types:

- Remote display of the graphical user interface (GUI)

The following table specifies requirements that apply to this path:

**Table 79**

| **Performance** |
|---|
| Bandwidth = 1.64 x $10^5$ bps |
| Maximum latency = less than one second |
| Maximum packet loss = not applicable |
| **Protocols** |
| IP, TCP, ICMP, FTP, ARP |
| **Physical Connection Characteristics** |
| OSS: 10Base-T Ethernet |
| Preside MDM: 10Base-T Ethernet |
| **Notes** |
| |
| **Security Needs** |
| Firewall protection is recommended on the OSS side. |

The following table illustrates examples of capacity data for the two OAM&P Ethernet links between the SDM and the OSS Network:

**Table 80**

| **Application** | **Bandwidth (bits/second)** | **Packets (per second)** | | |
|---|---|---|---|---|
| | | | **Preside MDM Link 1 (secs)** | **Preside MDM Link 2 (secs)** |
| Network time of day | 1.00 x $10^4$ | 8.33 | 1 | 1 |
| Client Preside MDM | 1.23 x $10^4$ | 3.00 | 1 | |
| Remote X display | 1.42 x $10^5$ | 31.00 | 1 | |
| | | **Total Bandwidth** | 1.64 x $10^5$ | 1.00 x $10^4$ |

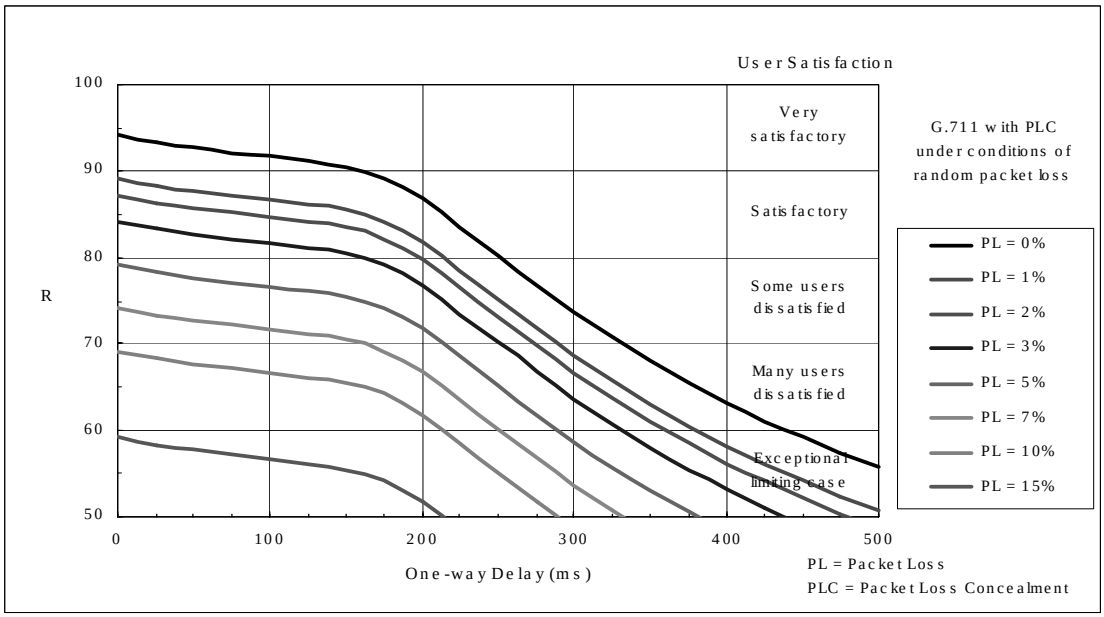
**Table 80**

| Application | Bandwidth (bits/second) | Packets (per second) | | |
|---|---|---|---|---|
| | | | **Preside MDM Link 1 (secs)** | **Preside MDM Link 2 (secs)** |
| | | **Total Packets** | 3.00 | 1.00 |

# 10.0 Voice Quality and Traffic Engineering

## 10.1 Choice of Codec

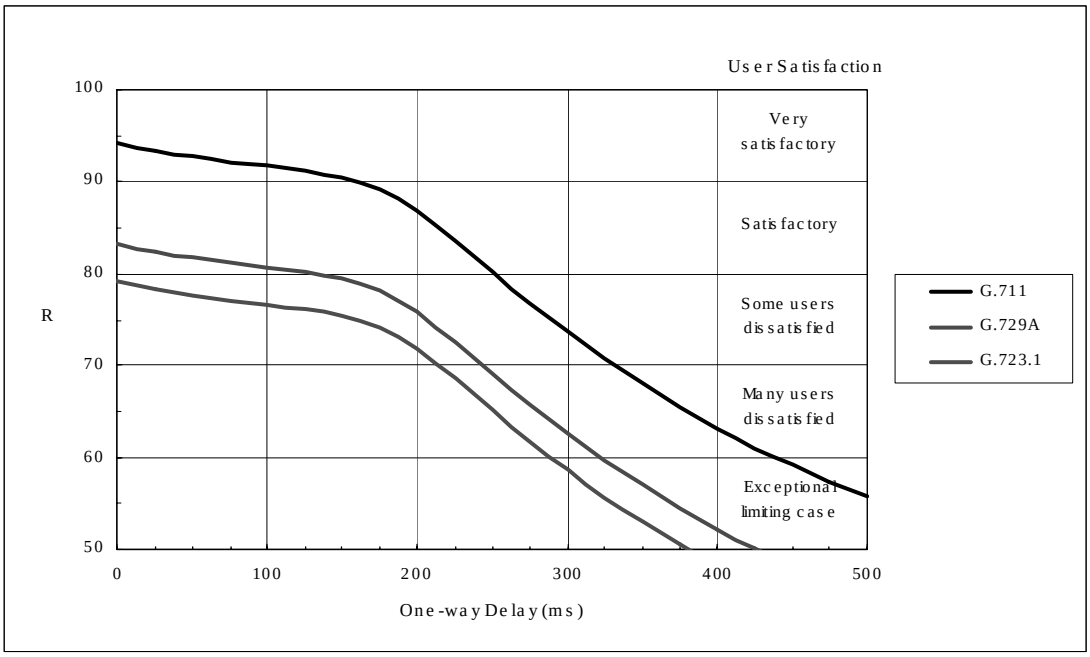
The best speech quality will be achieved with G.711 uncompressed speech, with 10 msecs encoding. The following figure shows the impact on voice quality with G.711 under different levels of network impairments.




The next figure shows a comparison of voice quality achieved with G.711 and G.729 codecs. G.729 may be considered where it is necessary to conserve bandwidth. G.729 compresses the speech to 8 kbit/s. However, once the packetization overhead had been added in, the effective bandwidth saving is around 50%.

The bandwidth saving comes at the price of lower voice quality. The figure below shows the drop in voice quality when using G.729 vs. G.711. Note, when reading this figure. G.729 encoding introduces an additional 25 msecs latency. The network planner should also be aware that the capacity and number of voice channels supported by some gateways may be lower when using G.729.

# E-Model: Speech Compression Impairment




## 10.2 Choice of 10/20 msecs Packetization

The 150 msecs latency objective for the bearer path applies on an end-to-end basis, or phone-to-phone basis. It should be noted that bearer path may traverse a number of carriers, wireline and wireless.

As voice-over-packet technology is deployed more widely, a bearer path may traverse multiple carriers, each with voice-over packet but with interworking based on TDM. A single call may be subject to more than one packetization/depacketization with subsequent increase in end-to-end latency. Wireless to wireline calls will also be subject to the additional latency due to the wireless compression algorithms.

It is good engineering practice to minimize the latency in each network segment. This can be done by selecting 10 msecs encoding over 20 msec encoding. 10 msecs is recommended for best quality.

Note, some small line gateways may only support 20 msecs encoding.

Also, some network elements have a greater throughput when handling 20 msecs encoded voice, due to the smaller number of packets/sec that need to be routed. These elements are noted in the appropriate sections in these guidelines.

## 10.3 Network Traffic Engineering for Voice Quality

Sharing of network resources is a basic part of IP network design. Congestion is one of the most significant problems that have to be addressed in an operational IP context. Congestion must be avoided in order to meet the QoS requirements demanded by VoIP services.

Traffic Engineering is intended to combat the congestion problem. Different techniques apply based on the time scale:

- Capacity / bandwidth planning, i.e. router and link provisioning. This works on a relatively long time frame of weeks or months. Provision of sufficient bandwidth should be planned to accommodate the traffic peaks and growth that is forecast over the study period.
- Control policies. These are reactive techniques that can operate within a short time interval. These techniques involve:
    - Use of redundancy of routers, employing VRRP or similar proprietary strategies. In the event that an Access Router or CS-LAN fails, the traffic will be immediately switched through the newly active unit
    - Use of integrated network layer routing such as OSPF or MPLS, to set up alternate label switched paths through the network to quickly reroute traffic around network failures or congestion.
- Packet level processing functions, built into the network equipment. Examples of these are passive and active buffer management and queue management. These techniques work in the pico-second intervals.

### 10.3.1 Routing Protocols

OSPF is the suggested Interior Gateway Protocol (IGP). A separate OSPF area should be created for the CS-LAN, the Core Network, and each Access router. One of the Core network routers will aggregate subscriber data traffic and provide an interface to the public Internet. This will also provide the demarcation point, such that the private IP addressing used by the gateways and other elements are not advertised outside the voice-over-packet routing domain. The router providing the interface to the public Internet is expected to support both OSPF and BGP.

The Core Network may comprise multiple routers and switches. The access router would interconnect directly to a core network router. In this scenario, the core routers will be required to support additional protocols in order to reserve bandwidth through the multi-service network and maintain Grade-of-Service by:

- The shortest path, lowest latency, between Access Router and CS-LAN. It is recommended that the core routers support a constrained shortest path first algorithm such that the shortest path allows for constraints such the required bandwidth can be supported on the shortest path selected.
- Fast rerouting around congestion or network failures. MPLS may be used to identify alternate label switched paths that can be used if the default path is congested.

### 10.3.2 Quality-of-Service Control Mechanisms

Succession is a multi-service network supporting packet voice, call signaling, OAM signaling and subscriber data traffic, each of which has different performance requirements. A number of capabilities exist to maintain the QoS requirements.

Bandwidth

Bandwidth on the various transport links can be engineered to accommodate the expected simultaneous peak traffic from the multiple services. This is most straightforward on links that only carry a mix of call signaling, voice and OAM traffic, such as the network router to CS-LAN. The nature of the call signaling and voice traffic is time consistent.

However, it is a different problem on links that carry a mix of voice and subscriber data traffic. The subscriber data traffic is expected to be self-similar in nature, with an extreme peak to average ratio. For these links it is advisable to deploy additional QoS mechanisms. These are as follows;

DiffServ

DiffServ is recommended on the Access router and CS-LAN to network router links. DiffServ will give preferential transport to the voice, call signaling, and OAM traffic over subscriber data traffic. The DiffServ basic elements are implemented within the network and include:

- Packet classification functions
- A small set of per-hop forwarding behaviors
- Traffic metering, marking, and policing.

Details on the DiffServ strategies and configuration are included in later sections.

802.1P

To guarantee End-to-End QoS, it is important to implement a strategy in purely switched networks, for example, the CS-LAN subnet. Since at Layer 2 there is no awareness of which traffic is carried, it is necessary use IEEE 802.1P to differentiate priority traffic at the MAC level.

IEEE 802.1P is an OSI Layer 2 standard for prioritizing network traffic at the data link/Mac sublayer. Traffic is classified and sent to the destination but no bandwidth reservations are established. Since 802.1P is a spin-off of the 802.1Q (VLANs) standard, the 802.1P field is contained in the VLAN tag (which carries VLAN information). The VLAN tag has two parts: The VLAN ID (12-bit) and the Prioritization (3-bit). Therefore, 802.1P establishes eight levels of priority which network adapters and switches use to route traffic. The use of a Layer 3 switches (such as the Passport 8600) allows you to map 802.1P prioritization schemes to DiffServ schemes before forwarding to routers.

### 10.3.3 Voice Quality Verification

In Voice over IP networks, Quality of Service (QoS) can be adversely affected by the components in the network. Unlike TDM networks where the voice quality is consistent for all calls, VoIP networks can experience different voice quality on all calls.

The common parameters that make up voice quality are;

- Latency
- Packet loss
- Jitter

All gateways in VoIP solutions report these statistics via end-of-call reporting mechanisms specific to the protocol used for MGC-to-MG communication.

### 10.3.3.1 Voice Quality Monitoring in a Live Network

Nortel recommends that network planning focus on achieving the latency, packet loss and jitter metrics required for good quality speech. Network surveillance for voice quality should therefore be focused on the specific metrics measuring network impairments. This can be achieved through monitoring the Quality-of-Service metrics reported by the Gateways at the end of every call. Prior to SN06, this was more of a troubleshooting technique, as the metrics needed to be manually gathered through sniffing the signaling stream. However, in SN06 the metrics are collected by the GWC [through end-of-call stats] and forwarded to the QoS Collector Application (QCA), located on the CMT server. These metrics identify packet loss, latency and jitter. Additionally, a new trunk group based Operational Measurement group is introduced that contains pegs of these same parameters when they cross threshold values defined by the telco. Together, these tools can be used for the purposes of:

- Network engineering
- Trend analysis
- Trouble-shooting network problems
- Service Level Agreement (SLA) validation

### 10.3.3.2 Trunk Group Based Quality of Service OM - TRKQOSOM

A capability introduced in SN06 provides an operational measurement group on the CS2000. The operational measurement values record instances in which QoS threshold values have been exceeded for calls handled by a particular GWC-based TDM trunk group.

The QoS statistics that are included in the OM for each GWC trunk group are packet loss, jitter, and delay (latency). As GWC based trunk calls are released, the QOS statistics for that call are compared to the QoS OM threshold values. If a statistic for the call exceeds the QoS OM threshold value for that statistic, the OM value for that statistic on the GWC based trunk group will increment.

The OM group will contain entries for each GWC-based trunk group datafilled on the CS2000. In order for the trunk group to appear in the OM group, at least one member of the trunk group must be datafilled to reside on a GWC node via table TRKMEM.

Each entry in the OM group will contain a CLLI as well as threshold crossing counters for packet loss, jitter, and delay (latency).

The active registers will contain data for the current reporting interval. The holding registers will contain data for the previous reporting period. The interval for OM peg count transfer from the active to holding registers is controlled by the OM system. Refer to the OM system documentation for details on the available intervals for active to holding transfer.

The following table describes the range of values possible for each QoS OM threshold office parameter datafilled in table OFCVAR.

**Table 81 Establishing QoS Parameters for the Office**

| Parameter | Field | | Range | Units |
|---|---|---|---|---|
| PACKET_QOS_OM_THRESHOLDS | Enabled | | Y/N | |
| | Jitter | | 0 TO 100 | Milliseconds (ms) |
| | Delay | | 0 TO 500 | Milliseconds (ms) |
| | Loss | Whole | 0 TO 9 | % packet loss range from 0 TO 9.999999% |
| | | Fraction | 0 TO 999999 | |

The QOS OM threshold values defined in table OFCVAR will be applied to all GWCs datafilled for the call server. The values may be changed at any time without the need for core/GWC restart.

The threshold values may be set in table OFCVAR by positioning on and changing the appropriate threshold as follows:

```
>table ofcvar
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED

TABLE: OFCVAR

>pos packet_qos_om_threshold
PACKET_QOS_OM_THRESHOLDS              Y  10  40 0    001

>
```

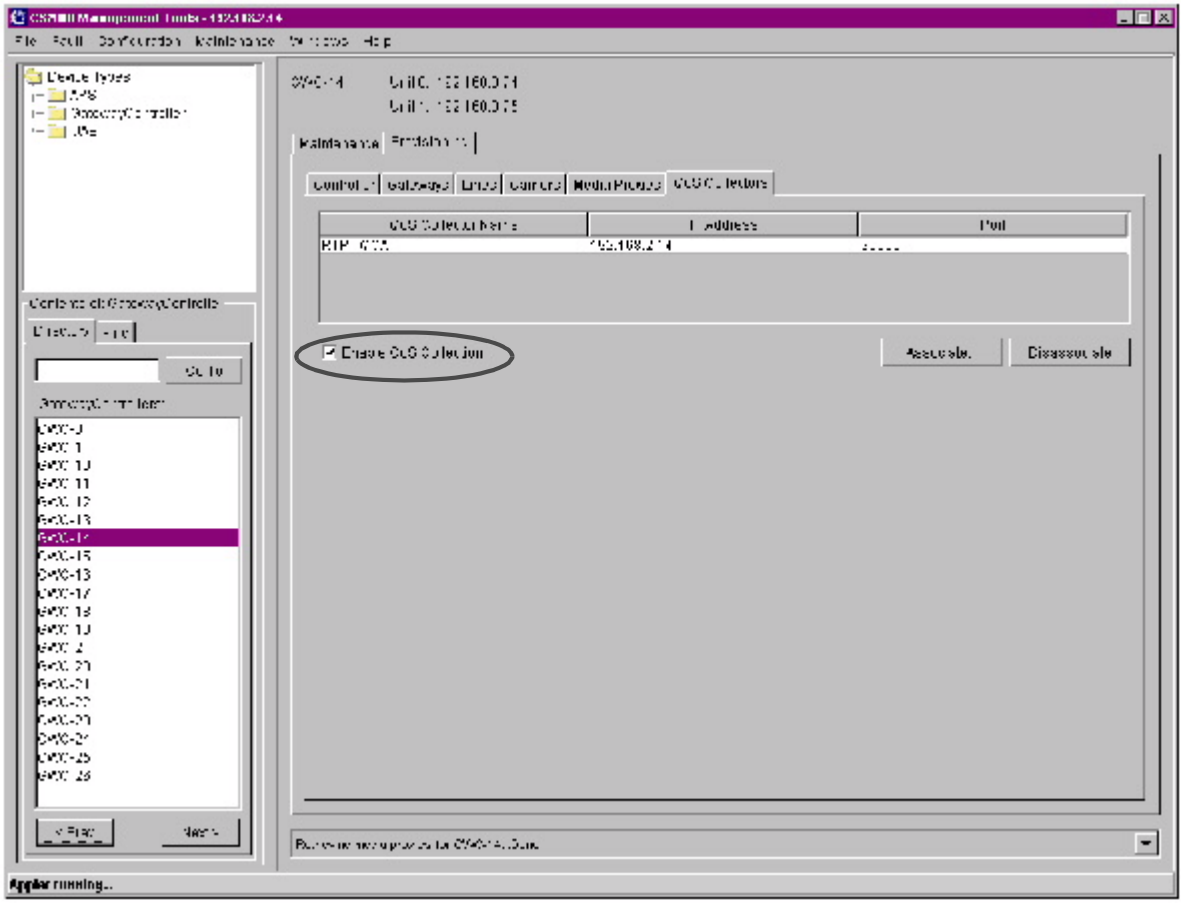
In the above example, the QOS OM threshold reporting was changed such that the reporting is active and the thresholds were set (jitter=10 ms, delay= 40 ms, packet loss= 0.001%).

```
>OMSHOW TRKQOSOM HOLDING
TRKQOSOM

CLASS: HOLDING
START:2003/04/18 09:10:00 FRI; STOP: 2003/04/18 09:15:00 FRI;
SLOWSAMPLES:         3 ; FASTSAMPLES:         30 ;

      KEY (COMMON_LANGUAGE_NAME)

        PKTLOSS     JITTER      DELAY

   227 INET4SS7OG1
0          2          2
   228 INET4SS7OG2
13         0          0
```

To enable the collection of these pegs, the GWC must be provisioned to send this data to the CS2000. The following figure illustrates how this is achieved.

***Note:*** The QoS Collector Application Server does not need to be provisioned in order to receive these pegs, only QoS Collection need be enabled.

**Figure 68 Enabling QoS Collection on the GWC**



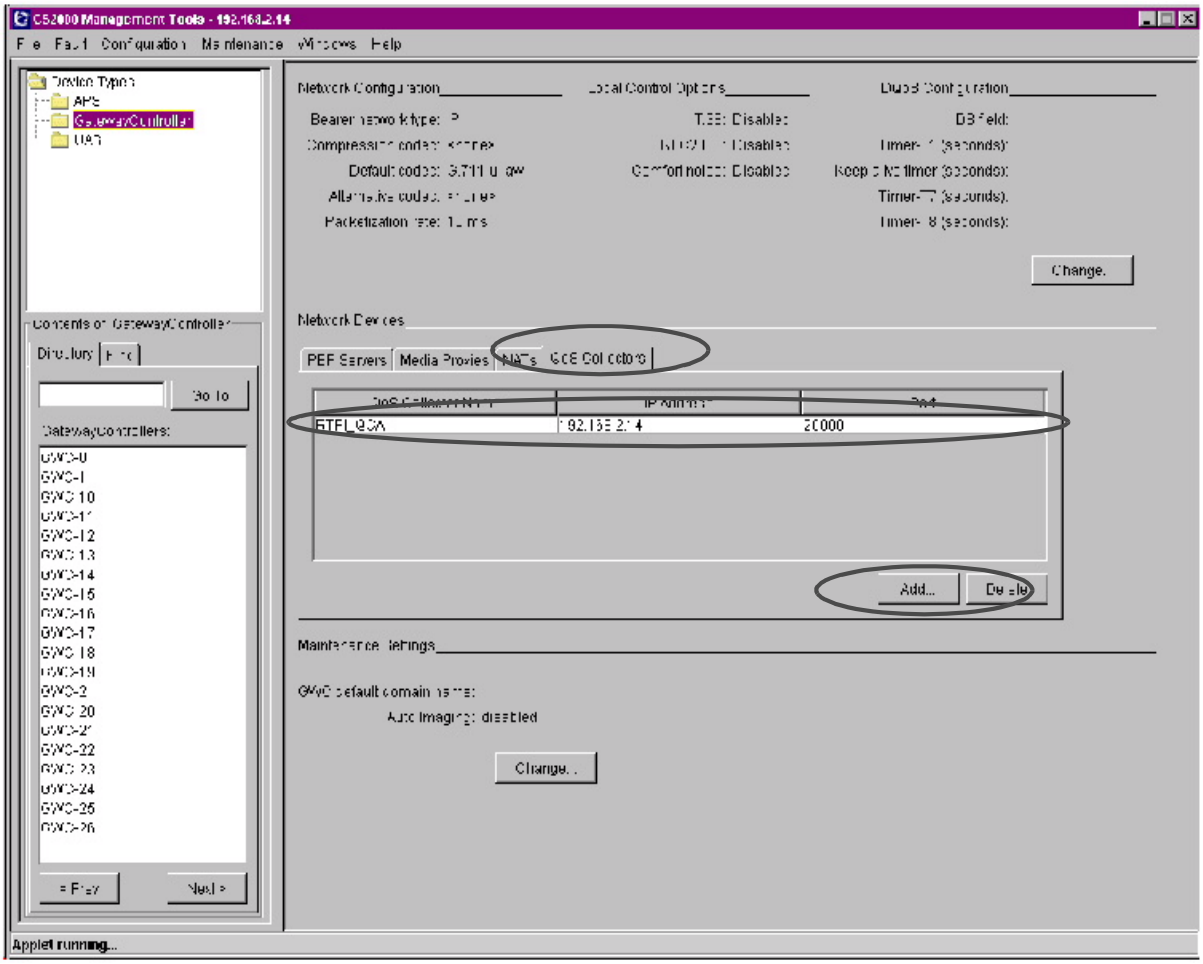

### 10.3.3.3 QoS Collector Application

QoS reports are delivered from the GWC to the QoS collector application (QCA). QoS reports are correlated to applicable billing records with a correlation ID (CID). Each CID references a set of QoS report pairs. Applicable AMA billing records contain zero or more CIDs, thus referencing zero or more QoS report pairs. Each GWC can have up to two links to different QCAs, each receiving identical information. The QCA stores the QoS reports in XML format to be offloaded by the OSS for processing

The QoS Collector Application must be datafilled in CMT, and individual GWCs must enable QoS record collection. Only 2 QoS Collectors can be datafilled. In the CS2000 Management Tools GUI (formerly PTM), select "Gateway Controller" under "Device Types". Then, under "Network Devices", select the "QoS Collectors" tab. Here, you will click "Add". You will be prompted for the following:

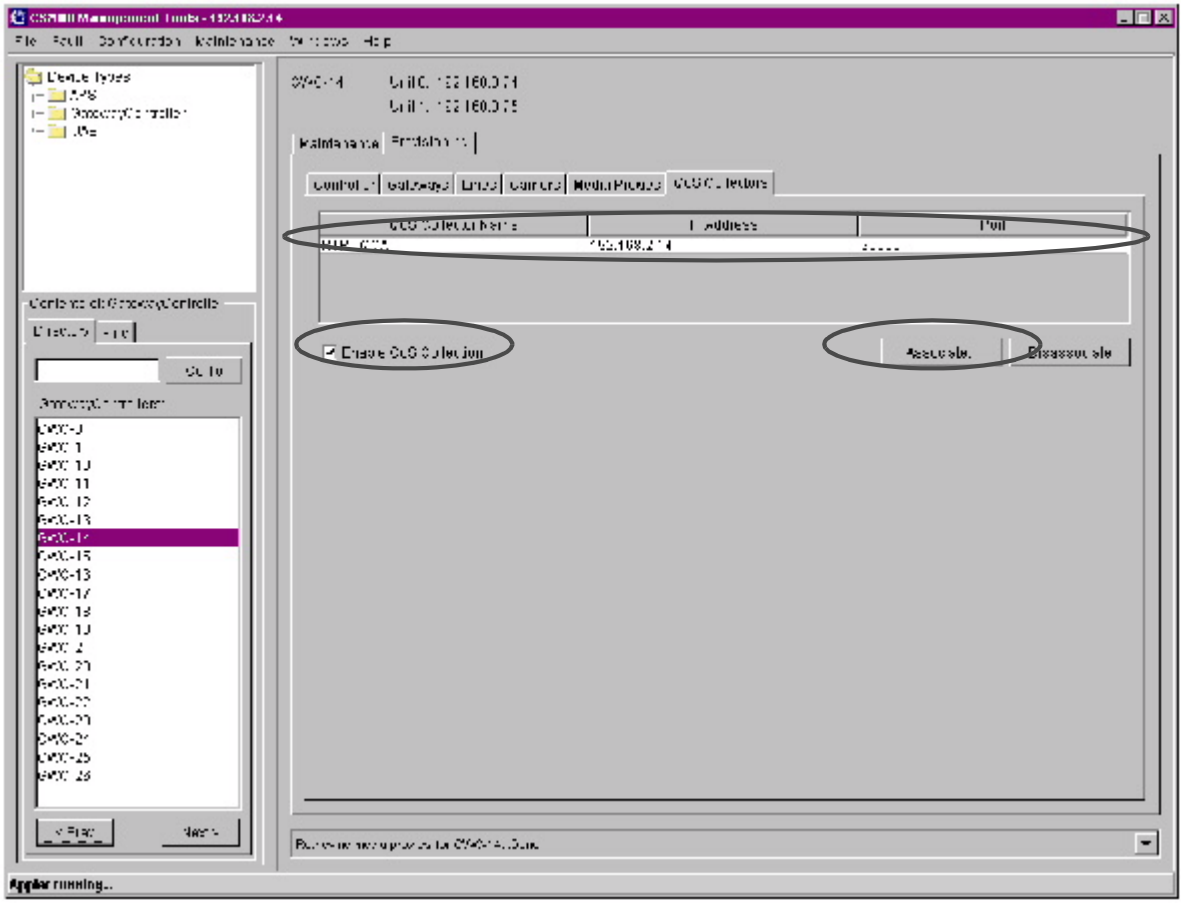
- QoS Collector Name: Give a name for the collector
- IP Address: The address of your SESM server.
- Port: The port number of your QoS Collector.

**Figure 69 Provisioning the QCA Server within the CMT**




Next, QoS record collection must be enabled on each GWC. Select a GWC, and click on its Provisioning tab. Then, select the "QoS Collectors" tab. Click the "Associate" button, and select the Qos Collector. Then, check "Enable QoS Collection".

**Figure 70 Associating the GWC to the QCA Server**



The QCA records are stored in XML format. The following XML tags correspond to the QoS parameters of interest:
Latency - `<averagePacketLatency>`

Packet Loss - `<inboundLostPacketCount>` and `<inboundPacketCount>`

$$\left(\frac{inboundLostPacketCount}{inboundPacketCount}\right) \times 100 = PacketLoss$$

Jitter - `<packetDelayVariation>`

To enable the Core to populate the billing records with Correlation IDs, the following tuple must be set in table AMAOPTS

TABLE: AMAOPTS

RECORD_QOS ON

Each Billing record corresponds to two QoS Records, one for each half-call. All three records have the same correlation ID. In the following examples, the correlation ID is highlighted in red. In the QCA record, the correlation ID is in hexadecimal, while it is in Binary Coded Decimal (BCD) in the billing record. The following example shows how to convert the BCD number to its hexadecimal representation, using the data from the sample records.

096 016 024 124 016 = 60 10 18 7C 10

164 068 133 061 000 = A4 44 85 3D 00

Sample SDM Billing Record:

Record data:

---

RDW 00630000

HEX_ID aa

STRUCTURE_CODE 40510C

CALL_CODE 006C

SENSOR_TYPE 036C

SENSOR_ID 0000000C

RECORD_OFFICE_TYPE 036C

RECORD_OFFICE_ID 0000000C

DATE 30410C

TIMING_INDICATOR 00000C

STUDY_INDICATOR 0200000C

ANSWER 0C

SERVICE_OBSERVED 0C

OPERATOR_ACTION 0C

SERVICE_FEATURE 000C

SIG_DIGITS_NEXT_FIELD 010C

ORIGINATING_OPEN_DIGITS_1 08602120279C

ORIGINATING_OPEN_DIGITS_2 FFFFFFFFFF

ORIGINATING_CHARGE_INFO FFFF

DOMESTIC_INTL_INDICATOR 9C

SIG_DIGITS_NEXT_FIELD 007C

TERMINATING_OPEN_DIGITS_1 00003120779C

TERMINATING_OPEN_DIGITS_2 FFFFFFFFFF

CONNECT_TIME 1152445C

ELAPSED_TIME 000000133C

Subrecord data:

---

MODULE_CODE_ID 612C

GENERIC_CONTEXT_ID 8006600C

DIGITS_DIALED_1_EUR 096016024124016C

DIGITS_DIALED_2_EUR 164068133061000C

Subrecord data:

---

MODULE_CODE_ID 000C

Sample QoS Record:

<IPDR>
<StartTime>1970-01-01T00:00:00.000Z</StartTime>
<EndTime>1970-01-01T00:00:00.000Z</EndTime>
<timeZoneOffset>0</timeZoneOffset>
<callCompletionCode>CC</callCompletionCode>
<originalDestinationId></originalDestinationId>
<hostName>GWC12@RTP4</hostName>
<subscriberId>aaln/10@GWC12_OrigGW27.rtp4.net</subscriberId>
<uniqueCallId>6010187c10a444853d00</uniqueCallId>
<ipAddress>10.127.147.28</ipAddress>
<portNumber>2427</portNumber>
<seqNum>5446</seqNum>
<averagePacketLatency>0</averagePacketLatency>
<inboundByteCount>0</inboundByteCount>
<outboundByteCount>0</outboundByteCount>
<inboundPacketCount>0</inboundPacketCount>
<outboundPacketCount>0</outboundPacketCount>
<inboundLostPacketCount>0</inboundLostPacketCount>
<packetDelayVariation>0</packetDelayVariation>
</IPDR>

```
Record:
Start Time       = 1970-01-01T00:00:00.000Z
End Time         = 1970-01-01T00:00:00.000Z
TimeZone Offset  = 0
Call Comp Code   = CC
Orig Dest Id     =
Host name        = GWC1@RTP4
Subscriber id    = aaln/1@cg1131.rtp4.net
Correlation Id   = 4d006531001cbeb9a601
IP Address       = 10.129.129.30
Port Number      = 2427
Sequence Number  = 1576
Latency          = 15
Octets Received  = 141036
Octets Sent      = 141220
Packets Received = 1533
Packets Sent     = 1535
Packets Lost     = 0
Jitter           = 0
```

```
Record:
Start Time       = 1970-01-01T00:00:00.000Z
End Time         = 1970-01-01T00:00:00.000Z
TimeZone Offset  = 0
Call Comp Code   = CC
Orig Dest Id     =
Host name        = GWC24@RTP4
Subscriber id    = STS/11/0/3/VT15/1/1/3/17@PVG3809
Correlation Id   = 4c00732d4091cdb9a601
IP Address       = 172.16.203.4
Port Number      = 2944
Sequence Number  = 184139
Latency          = 0
Octets Received  = 122720
Octets Sent      = 122000
Packets Received = 1534
Packets Sent     = 1525
Packets Lost     = 0
Jitter           = 0
```

In addition, network management systems can be used to monitor frame/packet discard on any of the router ports.

### 10.3.3.4 Nortel Product Test Voice Quality Verification

When used in the context of packet networks, Quality of Service (QoS) refers not to voice quality, but to mechanisms intended for bandwidth management and optimization of service quality. Examples of QoS mechanisms include call admission control, queue management and packet classification, traffic shaping techniques, and QoS protocols such as diff-serv, RSVP, and MPLS. The acceptability of voice quality varies depending on the users expectation of the particular service; for instance, users expect better quality from local wireline than from cellular. Several standards exist for measuring QoS (quality of service) and VQ (voice quality) and many white papers have been written on why one standard is better than another (http://e2e.ca.nortel.com/thorpe/). In brief:

ITU-T G.107

This Recommendation is based on the use of the E-Model, which estimates the perceived voice quality. The E-Model calculates a metric called Transmission Rating (R) with a range of 0 to 100. R takes into account all factors known to contribute to telephony conversation quality, including distortion, delay, echo, and listening levels, as well as any interactions between these factors. R is more difficult to measure than PESQ-LQ because the E-Model requires a number of input parameters to compute the final value. A major advantage of using the E-Model R as the quality metric is the abil-

ity to do predictive modeling in advance of building the system, and then measuring R for the system to compare to the predicted value.

The E-Model and R-Factor are the basis of the Nortel voice quality test program.

ITU-T P.800.

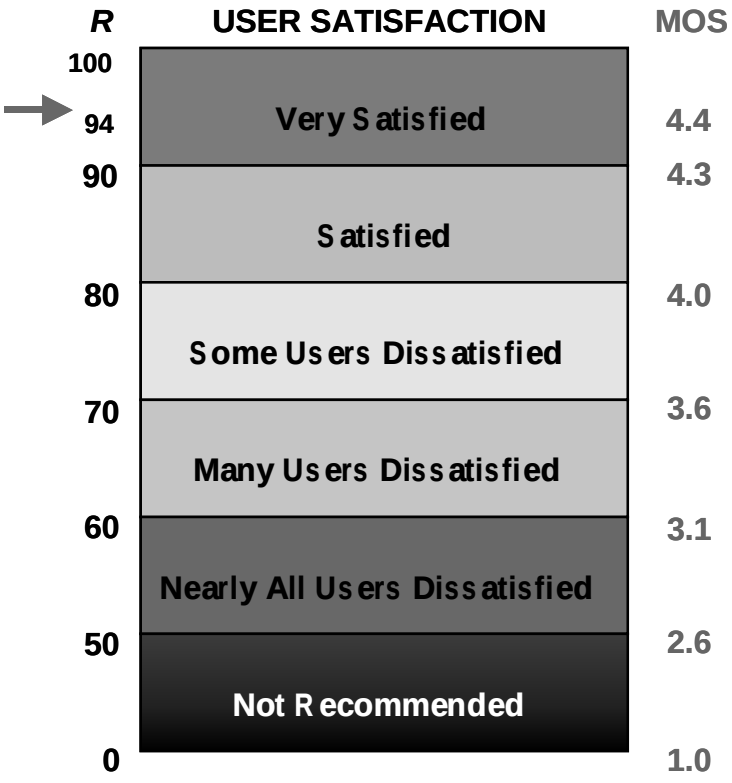
This recommendation describes accepted methodology for conducting subjective Mean Opinion Score (MOS) testing. Listeners rate speech samples on a five-category scale, ranging from Bad (1) to Excellent (5). Using the associated numerical values, ratings given to each test case by each listener are averaged to obtain a mean, ie., the MOS. The absolute MOS for any test case depends on the full set of conditions tested in the session as well as the parameter values used in defining a particular condition. MOS tests are very good at comparing the quality of conditions tested in the same session, but are not as useful for comparing quality across different studies where different sets of conditions have been included (such as might be done by different vendors). Subjective methods are time-consuming and labor-intensive, and so are not generally used for design and verification testing.

ITU-T P.861

This Recommendation describes an objective method for estimating the subjective quality of telephone-band (300-3400 Hz) speech codecs. The measurement algorithm ignores echo and delay. It cannot factor out temporal shifts where silence is added or removed. The range is from 0 (best) to 5 (worst). P.861 has been replaced by P.862

ITU-T P.862 This Recommendation describes the current standard objective estimator of subjective speech quality. Similar to P.861, the method addresses only distortion, ignoring signal level, echo, and delay. Its main advantage over P.861 is in removing temportal shifts in silent periods before it calculates the difference in the input and output signals to estimate the distortion. The range of the raw PESQ score is -0.5 to 4.5. This raw score is sometimes called PESQ MOS, although the transformed value called PESQ-LQ is better correlated with subjective MOS.

TIA TSB116 provides the following comparison:


R
USER SATISFACTION
MOS
100
94
90
80
70
60
50
0
Very Satisfied
Satisfied
Some Users Dissatisfied
Many Users Dissatisfied
Nearly All Users Dissatisfied
Not Recommended
4.4
4.3
4.0
3.6
3.1
2.6
1.0

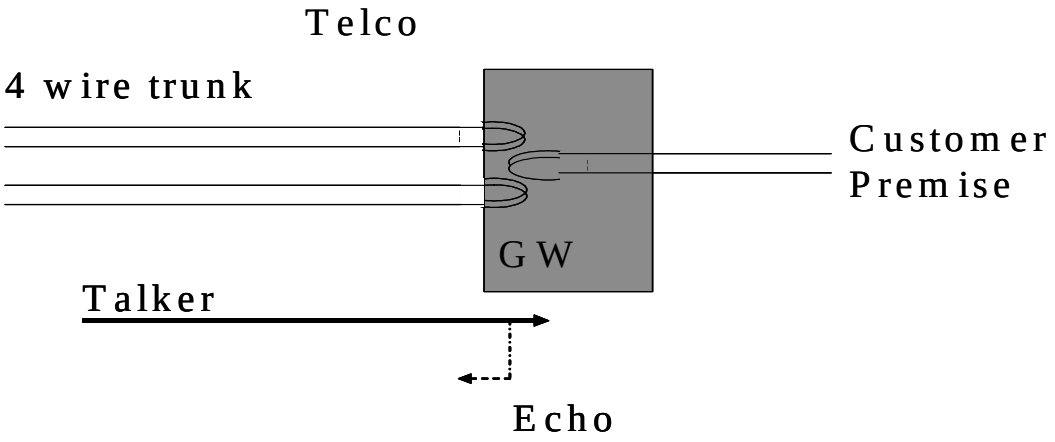
# 11.0 ECHO & Network Loss Plan

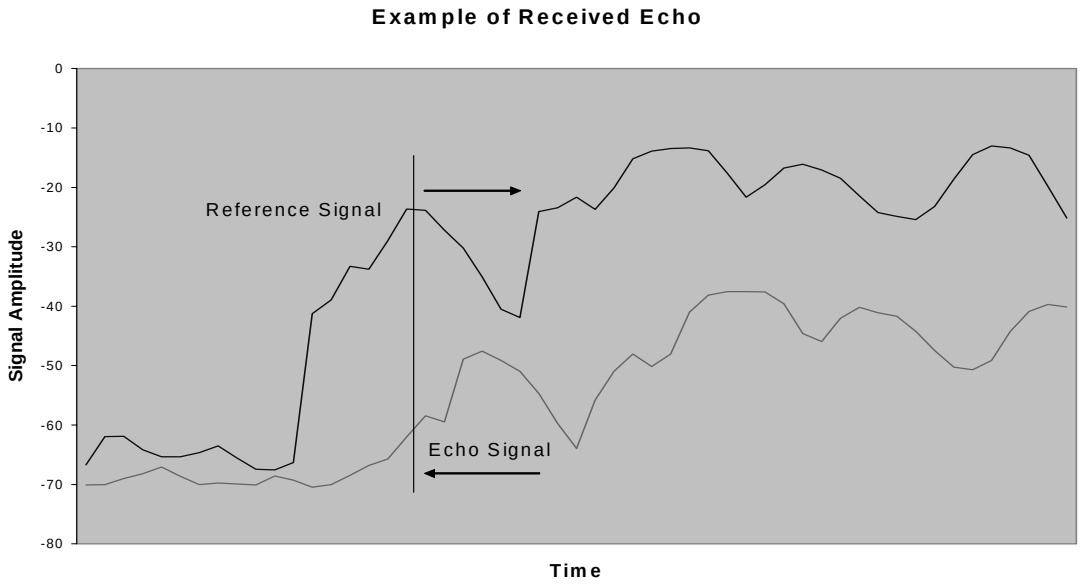
## 11.1 Type of Echo

The most common types of echo are Acoustic and Hybrid.

**Acoustic echo** is often cause by poor voice coupling between the ear piece and the microphone which is usually the quality factor of the handset. You can also get acoustic echo due to reflections of the voice on the surrounding elements back to the microphone. Since acoustic echo is hard to cancel out, importance is needed in selecting a quality handset.

**Hybrid echo** is generated as voice crosses the 4 wire to 2 wire hybrid connection in a network. The connection between the phone (customer premise) and the local exchange carrier is carried over a 2 wire. The trunk connection between a local exchange carrier and a long distance/ Toll carrier is over 4 wire. This is where reflection occurs and a portion of the send signal is reflected back as echo.






Different means exist which attempts to eliminate or reduce echo. These are; attenuation, echo suppressors and echo cancellers.

**Attenuation**; A common method used by LEC and IP Line gateway devices. The basis in Network Loss Plan planning.

**Echo Suppressors**; Defined in ITU-T G.164. Not often used outside of hand free sets and not efficient. These attempt to create a one way speech path by adding excessive attenuation in the send path when speech is detected in the receive path. Many problems can occur with echo suppressors such as muffling of the voice.

**Echo Cancellers**; Defined in ITU-T G.165 and G.168. The intent here is to have the canceller read the voice in one direction and subtract an estimated echo from the return path thus removing the echo.

The best performance is often achieved when both a properly engineered loss plan is used in conjunction with echo cancellers.

## 11.2 Echo due to delay

Where echo is more noticeable is when the delay between the gateways increases. Echo can be noticed in as little as 25 msec of latency when ECAN or loss plans are not applied. In an IP environment where jitter buffers are required, these automatically add to the network delay, and because of this, the echo that is present in all calls becomes more noticeable. Each IP voice gateway typically adds an additional 10 msec or 20 msec of network delay depending on it's jitter buffer size above the codec and gateway processing delays.

## 11.3 Loss and level plans for voice gateways

**Table 82 IP Gateway Loss per Standards**

| Standard | A/D (TX) Attenuation | D/A (RX) Attenuation |
|---|---|---|
| TIA 912 Pan European | 5 | 10 |
| TIA 912 North American | 0 | 9 |
| Packet Cable | 2** | 4** |
| Bellcore GR 909 | 2 | 4 |

**Note: An ECR is open with CableLabs to revise the loss plan recommendation for small IP line gateways. The PacketCable specification will reflect the new values. Refer to ECR emta-r-02221. The MTA loss plan values listed below are subject to change.

**Table 83 Loss Plan & ECAN Characteristics**

| Gateway | Fixed / Configurale | I/C (A/D) Attenuation | O/G (D/A) Attenuation | ECAN Supported | ERL dB | Tail ms |
|---|---|---|---|---|---|---|
| I/W SPM | Configurable | Uses CS2K MNIPPARM Range -6,+6 | | G.168 | | 128 |
| PVG VSP2 | Configurable | Range 0-6 | | G.168 | | 32 |
| PVG VSP3 | Configurable | Range 0-6 | | G.168 | 55 | 128 |

When discussing loss plans, positive values are losses and negative values are gains UNLESS value is quoted as gain and not attenuation. When discussing gains, positive values amplifies the signal and negative values attenuate the signal.

The customer along with the Nortel engineering group should study the customer network and ensure that a proper loss plan is implemented within these recommendation. Depending on the types of gateway present in the network, different values may need to be implemented. Failure to implement the proper loss plan will cause voice quality issues.

**Table 84 ITU-T G.101 Recommended SLR & RLR**

| | SLR (Includes loop lost) | RLR (Includes loop lost) |
|---|---|---|
| Digital Set | 8 dB | 2 dB |

**Table 84 ITU-T G.101 Recommended SLR & RLR**

| | SLR (Includes loop lost) | RLR (Includes loop lost) |
|---|---|---|
| Analog Set (Long loop - up to 2.5 km) | 11 dB | -3 db |
| Analog Set - 600 ohm (Short loop) | 8 dB | -6 dB |

**Table 85 Jitter Buffer Characteristics**

| Gateway | Jitter Buffer Adaptive / Static | Jitter Buffer Defaults | Jitter Buffer Range | Settable |
|---|---|---|---|---|
| I/W SPM | Adaptive | 0/100 | 0/300 | Table MNIPPARM |
| PVG VSP2 | Fixed | 10/100 | 10/100 | CLI |
| PVG VSP3 | Adaptive | 5/100 | 5/100 | CLI |

## 11.4 Passport 7480 & 15000 Voice Gateway's (PVG7K & PVG15K)

The PVG utilizes a software ECAN which cancels echoes at the edges of the network to maintain toll quality voice and to prevent echoes from travelling across the network. The PVG15K/PVG7K VSP2 can support two lengths of tail delay for echo cancellation. A 32-milliseconds tail delay is available on the VSP2 and a choice of 32- or 48-milliseconds tail delay is available on the VSP2 for switched PVG using ATM or IP. If the echo canceller detects echo outside of its capabilities, the canceller will turn off. The PVG15K VSP3 supports both a 64 msec tail delay and a 128 msec tail delay.

When the tail delay is larger than 32-millieseconds (VSP2) or 128-milliseconds (VSP3), then an external device is required to cancel echo and the field ECSTAT in table TRKSGRP should be set to

EXTERNAL.

By default, the PVG should always be configured with ECAN on (*echoCancellation attribute set to g165Mode*). The CS2K controls whether or not ECAN should be applied via the SS7 Signalling & Aspen messages.

***Note:*** It is recommended not to use *g164Mode* (VSP2-only), but rather *g165Mode* for the *echoCancellation* attribute.

The following describes how ECAN behaves functionally based on settings in an office.

In the forward direction:

If the ECSTAT field of table TRKSGRP is INTERNAL, then ecan will be turned on if the *NatureofConnection* field in the incoming IAM indicates that no ecan has been enabled at the adjacent office. The ACM forwarded back to this office will indicate that the CS2K has enabled ecan and the connection control message to the PVG will enable ecan for the call.

If the ECSTAT field of table TRKSGRP is EXTERNAL, the ACM will also indicate the *NatureofConnection* field as ecan enabled, but the connection control message to the PVG will turn off ecan. Here it is assumed that there is an external device to handle echo.

In the backwards direction:

If the ECSTAT field of table TRKSGRP is INTERNAL, then the outgoing IAM will indicate the *NatureofConnection* field has echo enabled and echo will be on at the PVG (since it is provisioned at the brag/bragS component). However, when the ACM coming back from the adjacent office in the *NatureofConnection* field indicates that ecan has been enabled, the connection control message sent to the PVG will disable ecan at the PVG for this call.

If the ECSTAT field of table TRKSGRP is EXTERNAL, again the IAM will indicate the *NatureofConnection* field has echo enabled but the connection control message to the PVG will turn off ecan. Again, here it is assumed that there is an external device to handle echo.

For trunk groups that have a mix of legacy and packet trunks, it is suggested that the customer create two subgroup indices in table TRKSGRP, one for packet and one for legacy. Then apply these appropriately to the trunk group field SGRP in table TRKGRP.

The following illustrates how to utilize the PVG15000's ability to cancel echo via provisioning in table TRKSGRP.

TYPE OF ECSTAT IS ECHO_EQUIP_STATUS

ECSTAT: INTERNAL

TYPE IS AB_CONTROL_TYPE {ACTIVEA,NONE}

ABCNTL: NONE

Example: TRKSGRP

LDBLSS7IC 0 DS1SIG C7UP 2W N N **INTERNAL NONE** Q764 TLRH 0 ISUP $ NIL CIC

The CS2K will then inform the PVG Trunk Gateway via the Aspen Modify Connection wether or not to apply ECAN based on it being applied or not on the previous segment. It uses the NATURE OF CONNECTION from the IAM and ACM SS7 messages to carry this information. When the SS7 message reports ISUP_NO_HALF_ECHO_SUP (ECAN not previously applied), it informs the GW via the E: parameter to apply ECAN on the PVG.

GWC: 01:21:17:11.46  CC: 18:13:31:27.81  Message 10 [sent]

MDCX 16194 ASPEN 2.1

C: callid

Z: PVG4206.DS3_20.7.1

I: 3

M: sendrecv

L: e:on

For PRI calls on the PVG, ECAN is always applied.

## 11.5 Interworking SPM

Starting in SN06, the IW-SPM supports ECAN with delay tails up to 128-milliseconds.

The following is an example of the data fill.

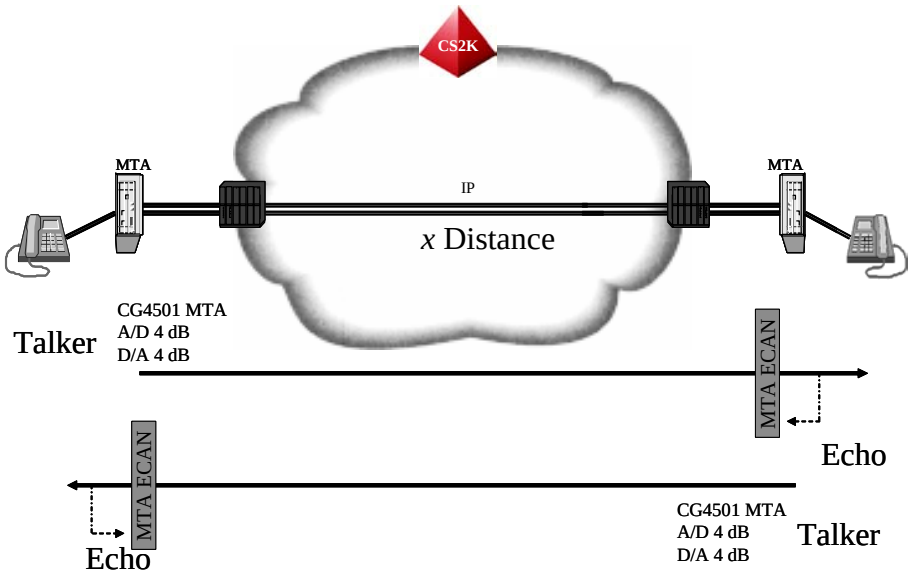
>TABLE MNIPPARM
.
.
.

ECAN: DISABLE
>enable
ECHOLOSS:
>6
ECHOTAIL:
>32

# 11.6 Call Types & TERL examples

## 11.6.1 IP Line to IP Line

The echo cancellation in the MTA provides an 8 millisecond echo tail and 28dB of echo loss. In accordance with ITU-T G.168, the MTA has a non-linear mode, which provides additional processing. This mode can be independently enabled/disabled.



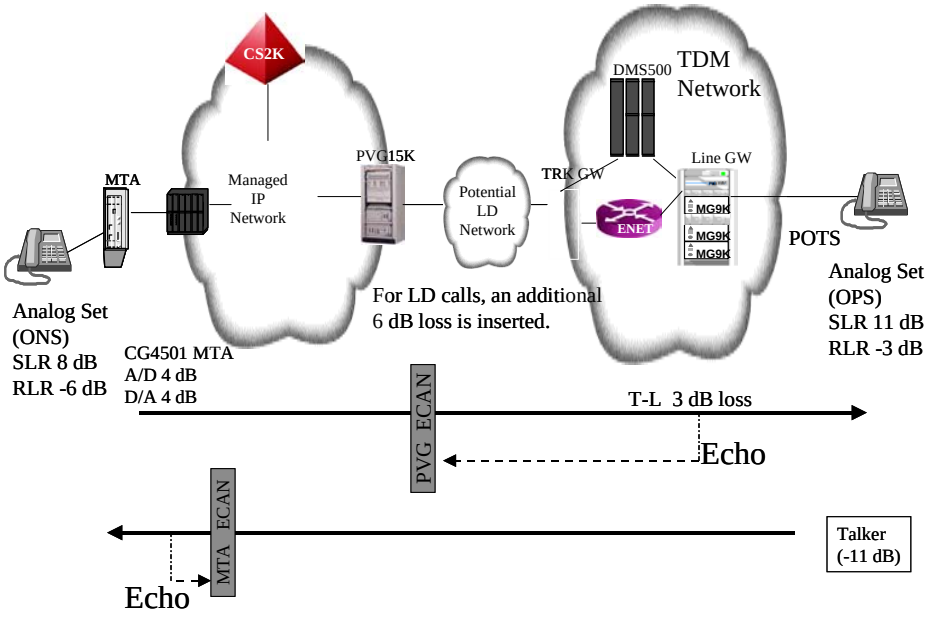

The CG4501 provides 4 dB of attenuation in the send and 4 dB attenuation in the receive direction. The echo canceller provides an additional 20 dB.

The echo heard by the talker equals SLR + MTA A/D + ECAN ERL + MTA D/A + RLR

thus, for a 600 ohm short loop set, TERL would provide a 30 dB attenuation. Assuming the talker's loudness level is -11 dBm, the echo amplitude reflecting towards the talker would be at -41 dBm (Talker Echo Loudness Rating -TELR).

With ECAN disabled on the MTA, the TERL would be equal to 24 dB due to the Hybrid ERL specification at 14 dB. We can conclude that we clearly see better attenuation of the reflected signal when ECAN is used with a loss plan.

### 11.6.2 IP Line to a TDM Line

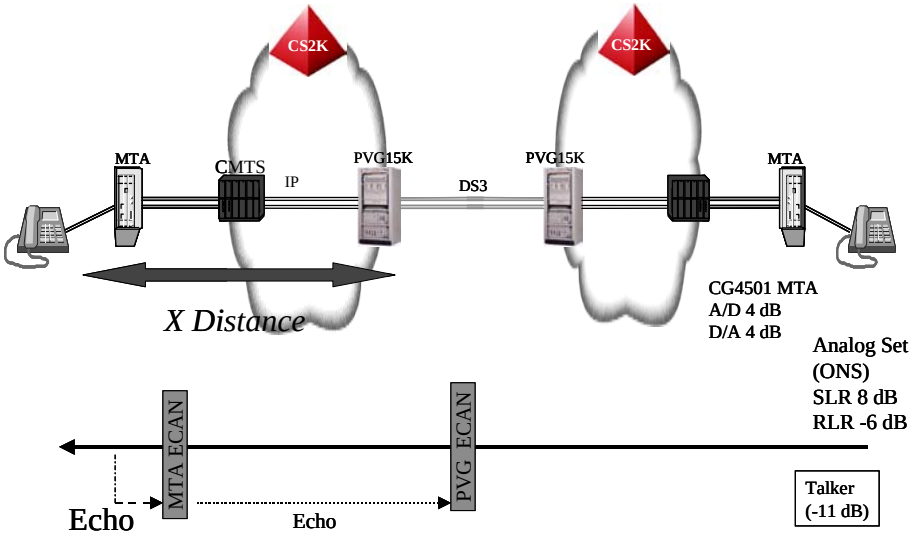



The PVG ECAN along with the loss plan will protect the IP Subscriber from echo. The MTA ECAN along with the loss plan will protect the PSTN subscriber from echo. Trunk groups between the IP network and PSTN network should be provisioned with the ECSTAT parameter set to EXTERNAL in table TRKSGRP in the Call Server.

The TERL for the IP subscriber calling a PSTN user within the same LATA would be 68 dB (Assuming a 55dB attenuation in the PVG ECAN). The TERL for the PSTN subscriber calling an IP subscriber within the same LATA would be 31 dB (Assuming the MTA ECAN Attenuation of 20 dB). If these calls are routed over an LD network, the IP to PSTN subscriber would have a TERL of 74 dB and the PSTN to IP subscriber would have a TERL of 37 dB since the local office applies an additional 6 dB of loss on a T-T call.

In order for the PVG7K/PVG15K VSP2 ECAN to remove 100% of the echo, the reflected signal from the Hybrid 4-2 wire conversion in the LCM must be below -26dBm and the latency between the LCM and the PVG15K must be less than 32 msec. If the signal is above -26 dBm, the ECAN will still work, however, a potential small burst of echo may be heard at the beginning while the ECAN converges. In this example, the reflected signal is at -26dBm for Intra LATA calls and -32 dBm for calls going thought a LD Tandem network assuming a talker loudness of -11 dBm. With the use of VSP3, this is not an issue and the PVG provides a tail of 64 msec.

### 11.6.3 IP Line to a IP Line via a PVG15K TDM Network




In this case, the PVG should not apply echo cancellation. Since the MTA (or any IP gateway) support ECAN, both MTAs (IP Gateways) should apply echo cancellation and the network is considered echo free. However, since the call server is unaware if the local line gateway supports ECAN, the SS7 message will inform the PVG to apply ECAN. The only way to force ECAN on the PVG to be disabled would be to set the ECSTAT parameter to UNEQ for the trunk group between the two PVG which will cause the SS7 message to send a CRCX message with e:0ff to turn off the ECAN in the PVG. By default, it is recommended to leave the ECAN on the PVG since double ECAN does not cause any voice degradation issues.

## 11.7 Basic understanding of Telco Loss Plans

The standards provide a reference for Telco operators to engineering their network in a conforming manner to be able to interwork together. TSB122A - Voice Gateway Loss and Level Plan Guidelines provides the following recommendation for network loss plans.

Call processing determines where the system implements the pad value. The subscriber cannot control this process. If the connection involves a line, the operating company normally sets the pad in the line card in the receive direction.

For the IAW and IAC solution, the IP line gateway is configured with a fixed attenuation and call processing cannot control the pad value based on the call type. It is therefor recommended to provision the lines as PKNIL. PKNIL represent the a Packet Line, short loop with NIL pad control in table PADDATA.

For an End Office Telco, it is important that a 6dB loss is added on any incoming call in from the packet network.

For the UA (AAL1/IP) solution, call processing makes use of the PADDATA values and sends these to the gateway. The pad group (PADGRP) defined as PKLNL (Packet Line Long) is recommended for the MG9K subtending lines. This includes both H.248 lines, and AAL1 lines served by the ABI DS-512 interface. Legacy line to packet line or packet trunk calls should be configured with 6 dB loss pad in table PADDATA. Refer to the table below for additional PADDATA settings.

To create new pad groups, you can add the groups as keys in fields PADGRP1 and PADGRP2 of table PADDATA. To use pad groups as line or trunk data, make sure the pad groups are in table PADDATA. Tables LNINV, TRKGRP, CONF3PR and CONF6PR can then use the above pad group.

An example follows for some of the recommended PADGROUP values. The following table is not a complete set on interworking and is included for illustration purposes only. The L represent a loss and a G represents a gain.

**Table 86 MG9K PADDATA Recommendation**

**Table 0-45**

| PADGRP1 | PADGRP2 | PAD 1to2 | PAD 2to1 |
|---|---|---|---|
| PKLNL | STDLN | 6L | 6L |
| PKLNL | PKLNL | 0 to 6L | 0 to 6L |
| PKLNL | PPHONE | 6L | 6L |
| PKLNL | ELO | 0 | 6L |
| PKLNL | TLA | 0 | 6L |
| PKLNL | PRA | 0 | 6L |
| PKLNL | CONF | 0 | 6L |
| PKLNL | TPOS | 0 | 6L |
| PKLNL | ETLS | 0 | 6L |
| PKLNL | ETLL | 0 | 6L |
| PKLNL | TLD | 0 | 6L |
| PKLNL | IAO | 0 | 6L |
| PKLNL | LCO | 0 | 6L |
| PKLNL | CPOS | 0 | 6L |
| PKLNL | DAVLN | 0 | 6L |
| PKLNL | PRAC | 0 | 6L |
| PKLNL | NPDGP | 0 | 6L |
| PKLNL | LRLM | 6L | 6L |

**Table 87 Definition of Standard Pad Group Keys**

**Table 0-46**

| Pad Group | Description |
|---|---|
| STDLN | standard line |
| UNBAL | unbalanced line |
| PKLNL | packet line long |
| PKNIL | packet line short loop with NIL pad control |
| PPHONE | P-phone |
| ELO | POTS interoffice trunk |

**Table 0-46**

| Pad Group | Description |
|---|---|
| TLA | POTS toll connectiong trunk (TCT) to toll trunk |
| CONF | conference circuit |
| TPOS | Traffic Operator Position System (TOPS) position |
| ETLS | POTS end office trunk (short distance) |
| ETLL | POTS end office trunk (long distance) |
| TLD | POTS TCT to toll trunk (digital) |
| IAO | plain ordinary telephone (POTS) intraoffice trunk |
| LCO | POTS collocated step-by-step (SXS) trunk |
| CPOS | centralized automatic message accounting (CAMA) position |
| DAVLN | data above voice line |
| PRAC | primary node access (PRA) |
| NPDGP | no pad group |
| LRLM | remote line module (RLM) |

The following table is out of the TSB122-A specification and is included for illustration only. It shows the expected loss plan values between various call types.

**Table 88 Voice Gateway Loss PLan**

V3

| | | | A | B | C | D | E | F | G | H |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | ONS | OPS | DGS | WAN | DAL | FXO | FXD | ATT |
| | | Loss | ↑ | ↑ | ↑ | ↑ | ↑ | ↑ | ↑ | ↑ |
| 1 | ONS | → | 6 | 3 | 0 | 0 | 3 | 0 | 3 | 3 |
| 2 | OPS | → | 3 | 0 | -3 | -3 | 0 | 0 | 0 | 3 |
| 3 | DGS | → | 9 | 6 | 0 | 0 | 0 | 0 | 3 | 3 |
| 4 | WAN | → | 9 | 6 | 0 | 0 | 0 | 0 | 3 | 3 |
| 5 | DAL | → | 9 | 6 | 0 | 0 | 0 | 3 | 3 | 3 |
| 6 | FXO | → | 0 | 0 | -9 | -6 | -3 | 0 | 0 | 0 |
| 7 | FXD | → | 3 | 0 | -6 | -3 | -3 | 0 | 0 | 0 |
| 8 | ATT | → | 3 | 0 | -3 | -3 | -3 | 0 | 0 | 0 |

**Table 89 Port Definition**

| Voice Gateway Port Designation | Port Definition | PBX or CO Port Designation |
|---|---|---|
| ONS | Analog **On** Premise **S**tation (analog telephone on a short loop) | ONS |
| OPS | Analog **O**ff **P**remise **S**tation (analog telephone on a long loop; can be via an analog CO) | OPS |
| DGS | **D**igital **S**tation (digital telephone) | DGS |
| WAN | **W**ide **A**rea **N**etwork (IP connection) | - |
| DAL | **D**igital **A**ccess **L**ine (digital connection to a digital CO) | DAL |
| FXO | **F**oreign E**x**change **O**ffice (analog connection to an analog CO) | AAL(A) |
| FXD | **F**oreign E**x**change **D**igital (digital connection to an analog CO) | AAL(D) |
| ATT | **A**nalog **T**ie **T**runk (private analog network connection to a gateway or a PBX) | ATT |

## 11.8 Effects of Echo cancellers on FAX calls

First,we need to understand how a fax call works.

- Detect dial tone
- Send digits
- Calling fax sends a 1100 Hz tone
- Receiving fax sends a 2100 Hz tone (~3 secs)
- Receiving fax sends pre-image handshake sequence
- Data rate, resolution, compression, image size,....
- Line testing event message
- Image transmission
- Post image handshake
- Message confirmation

To avoid data corruption, you can configure Passport PVG15K to disable echo cancellation when it detects 2100 Hz tones. If you set the echoCancellation attribute to g164Mode, the system disables echo cancellation when it detects 2100 Hz tones. If you set the echoCancellation attribute to g165Mode, the system disables echo cancellation when it detects 2100 Hz tones with phase reversals. For g164Mode, echo cancellation is re-enabled after 3 seconds of silence in both directions is detected. For g165Mode, echo cancellation is re-enabled when 150- to 350-milliseconds of silence in both directions is detected. If you set the echoCancellation attribute to alwaysOn, the system will not disable echo cancellation for any calls, regardless of the presence of tones. This setting can cause call connection problems for some modems.

# 12.0 Security

## 12.1 System Topology, Strategy Definition and Assumptions

Succession solutions network elements require a secure connectivity for call signaling, OAM&P (Operations, Administration, Maintenance, and Provisioning) messaging, and bearer path.

This section provides the information required to design a security strategy and protect the overall system from malicious users. The main focus of this strategy will be on the Communication Server Local Area Network (CS-LAN) and the Media Gateway sites. In addition, guidelines will be given on protecting the customer Corporate network and the Enterprise network (for line solutions). The Chapters that will address these networks are the following:

- CS-LAN protection - Securing the CS-LAN in Chapter 12.6.
- Media Gateway site protection - Securing the Media Gateway Site in Chapter 12.10.
- Customer Corporate network protection - Securing the Customer's Corporate Network in Chapter 12.8.

Nortel Networks' strategy is primarily based on a packet filtering strategy that will protect the critical elements of the Succession solutions. To achieve this, it is necessary to identify the unique identifiers that characterize each component and the flows originating from each component. These identifiers are:

- IP addresses and/or subnet information.
- Protocols.
- TCP/UDP Port number.

In particular, the document stresses the protection of the following devices:

- Call Processing and Billing.
  - XA-Core.
  - GWC.
  - SC.
  - SDM.
  - USP.
- Media Gateways.
  - PVGs/APGs.
  - IW-SPMs.
  - UAS.
- OAM&P Systems.

Nortel Networks recommends that the threetwo logical blocks above (Call Processing and Billing, Media Gateways, and OAM&P Systems) be assigned their own VLANs. As shown below, segregating the CS-LAN in VLANs increases the overall security.

Through the entire document, the following assumptions are used:

- All Call Processing and Billing network elements are located in the same subnet (Call Processing subnet).
- All OAM&P servers are located in the same subnet. This is different from the Call Processing subnet (the OAM&P subnet).

- One subnet for each of the types of CS-LAN based gateways (i.e., one for UAS, one for PVGs/APGs, one for IW-SPMs) is created. These are the Media Gateway subnets.
- All the subnets above are connected to the same router/Layer 3 switch (Passport 8600).
- The NOC and the OSS are considered as a unique entity with access to the CS-LAN through its own subnet.
- All OAM&P GUIs are located in the NOC/OSS.
- In-band management is used, unless otherwise specifically recommended.

In addition, this section will help to provide the information required to fill a Customer Interaction security questionnaire. The CI session is fundamental to obtain a detailed description on all the physical locations of all the network elements. These sessions should be used to identify the customer requirements on which the insecure/untrusted portions of the network are. In addition, during these meetings it is also important to include any customer-specific application in the overall filtering strategy.

### 12.1.1 Isolation of the CS-LAN Logical Blocks via VLANs

Nortel Networks recommends separating Call Processing and Billing, Media Gateways, and OAM&P elements in threetwo different port-based VLANs. This is because in port-based VLANs each VLAN is completely separated from each other (and in their own broadcast domain).

Because of the Passport 8600 architecture, each packet is analyzed independently of the precedent and allows complete traffic isolation. In addition, the Passport 8600 can be configured to discard untagged traffic on tagged ports or tagged traffic on untagged ports.

### 12.1.2 Routing Security

#### 12.1.2.1 Routing Policies

Added security can be achieved by tuning the overall routing processes of the Succession system. Nortel Networks recommends using route policies to selectively announce the CS-LAN subnets, and blocking the propagation of some of these subnets to the rest of the network.

It is strongly recommended limiting the announcement of the CS-LAN Call Processing subnet to the rest of the Succession network whenever it is possible.

#### 12.1.2.2 Routing Protocol Protection

It is possible that some areas of a customer routed network are or cannot be trusted. In such situations, since malicious users might potentially create routing black holes, Nortel Networks recommends protecting the OSPF updates with an MD5 key on each interface connected to a non-trusted router, according to RFC2178 (OSPF cryptographic authentication with the MD5 algorithm).

### 12.1.3 Traffic Filtering

It is very important to guarantee that only authorized devices can communicate with the Succession elements. Traffic filtering is used to control access to Succession elements and insure that only authorized traffic can reach them. As it will be seen below, traffic filtering is enabled at the demarcation points between trusted and not trusted networks.

The most efficient way of designing an effective traffic filtering strategy is to have in mind the overall system topology and the traffic flows that are present in the system. The document addresses the above statement by:

- Identifying all network elements.
- Identifying locations of all network elements.
- Identifying the logical communication flows between all network elements.
- Identifying which protocols are used for this communication.
- Identifying which devices are allowed to communicate with each other.
- Identifying the IP addresses and/or subnets for all devices.

It is also very important to identify which networks/subnet/domains are trusted and which ones are considered a security risk. Nortel Networks will always assume that traffic filtering will be applied at the ingress ports that might carry untrusted/insecure traffic.

Throughout this document, **all the flows** that will be initiated and terminated inside the following subnets will always be considered **trusted:**

- The CS-LAN Call Processing subnet
- The CS-LAN OAM&P subnet
- The CS-LAN Media Gateway subnets (if present)

Again, Nortel Networks assumes that these three subnets are all located off the same router/Layer 3 switch (Passport 8600). Therefore, it is not necessary to filter at the ingress ports that subtend these subnets.

Throughout this document, **all the flows** that will traverse or are initiated from the following subnets will always be considered **untrusted:**

- The remote Media Gateway subnets, **with the exception of the PVGs/APGs.** Please note that Nortel Networks recommends that the PVGs/APGs be considered trusted since they are not accessible by end-users.
- The customer's Corporate Network subnet **(please note that not all customers will consider this domain as untrusted)**

Figure 71 shows the trusted and untrusted networks by using different colors (see the legend of that figure). In the generalized topology for IP-based Succession solutions (as shown in Figure 71), given the fact that IPSec is not supported in SN06, it is required that packet filtering take place in the following network elements:

- The CS-LAN Router – This will protect the CS-LAN (Call Processing and billing, OAM&P and the UAS/MGs if present at this location). In addition, it filters NOC/OSS traffic if it transits through insecure networks. Please note that the NOC/OSS might have a direct physical connection into CS-LAN Router. Traffic filtering policies do not change.
- The Media Gateway Router – This will protect the MGs.

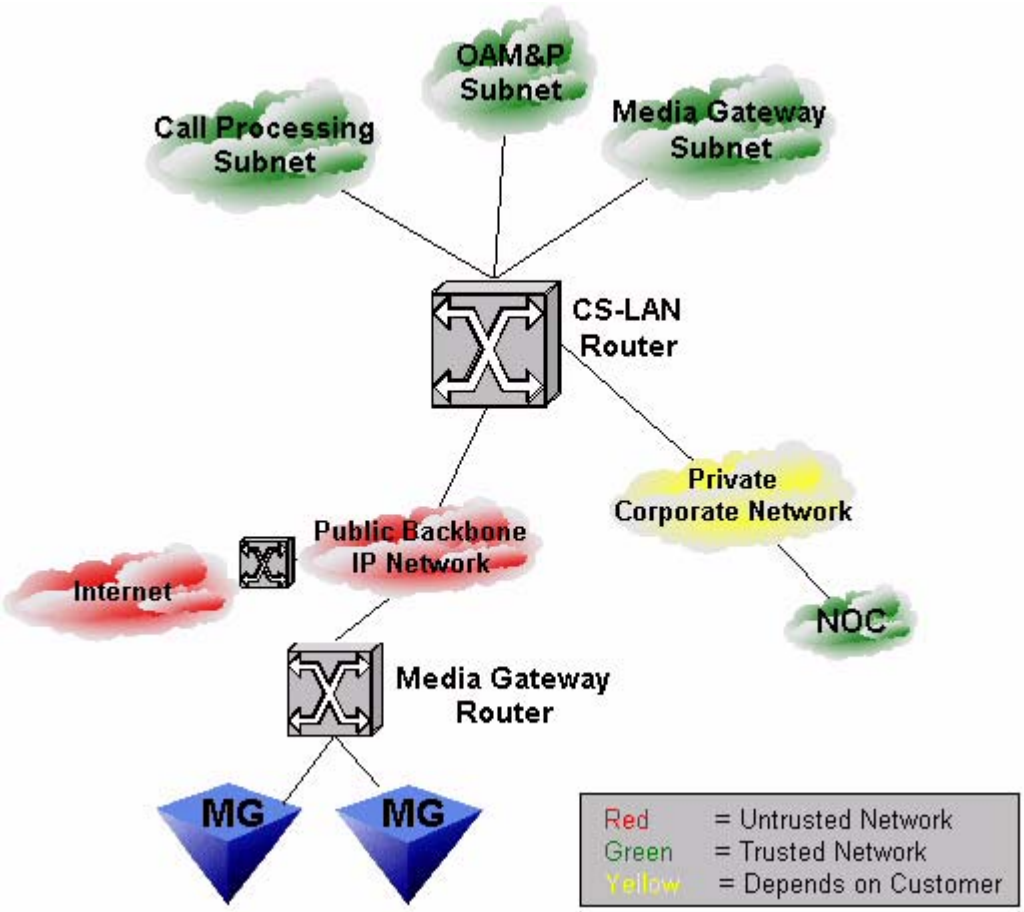



**Figure 71 Succession IP high-level network diagram**

### 12.1.3.1 Traffic Filtering Limitations

It is important to remember that traffic filtering does not guarantee total protection. The main limitations are:

- IP addressing spoofing – The filtering policies described in sections 12.7 and 12.9 will mitigate (though not completely eliminate) IP address spoofing.
- DoS attacks (both single and distributed) using allowed traffic flows. Please see below for more details on how to minimize IP packet spoofing.

It is to note that traffic filtering will be also used for the Succession releases where IPSec is supported. This powerful combination will offer a better protection to the key Succession elements from Denial of Service (DoS) attacks.

#### 12.1.3.2 Minimizing Spoofing Attacks

Using a strong anti-spoofing policy greatly decreases the risks for Denial of Service (DoS) attacks. Therefore, the indirect anti-DoS strategy recommended in this section is built on blocking all unauthorized traffic. This is achieved by throttling traffic filtering on the router/switch closest to the possible source of attacks so that stopping spoofed IP packets would be easier.

Spoofed IP packets should be stopped by configuring the Passport 8600 to ensure that only IP packets containing the correct source IP address are forwarded.

The basic idea of anti-spoofing protection is to have a filter rule/configuration assigned to the interface facing the non-trusted network, which examines the source address of all outside packets crossing that interface. If that address does not belong to the external site/domain as assigned by the network administrator, the packet should be dropped.

It is particularly important that this strategy is applied throughout the Succession network, especially at the external connections to all non-trusted sites/domains. By denying all invalid source IP addresses, the chances of a spoofed DOS attack are greatly minimized.

It is strongly recommended that for the Integrated Access Cable (IAC) and Integrated Access Wireline (IAW) solutions, most of the DoS-related filtering should be performed at the Media Gateways site where the end-subscribers access the network.

### 12.1.4 Protocol Stacks

Table 90 shows the protocols used in the network element communication flows that are described in the packet filtering sections (See “Securing the CS-LAN” on page 284. and See “Securing the Media Gateway Site” on page 294.). Note that this stack is a representation of actual protocol encapsulation used in Succession solutions, not true ISO layers.

**Table 0-47**

| Upper Layer Protocol | UDP | TCP | SCTP |
|---|---|---|---|
| Bootp/DHCP | X | | |
| MGCP/H.248 | X | | |
| TFTP | X | | |
| PPVM | X | | |
| SNMP | X | | |
| NFS | X | | |
| TFTP | X | | |
| SNMP | X | | |
| SNMP Trap | X | | |
| DNS | X | | |

**Table 0-47**

| Upper Layer Protocol | UDP | TCP | SCTP |
|---|---|---|---|
| NTP | X | | |
| MDS | X | | |
| FTS | X | | |
| FTS Audit | X | | |
| FTP | | X | |
| Telnet | | X | |
| HTTP | | X | |
| HTTPS | | X | |
| FMIP | | X | |
| RMI | | X | |
| OSSGate | | X | |
| CORBA | | X | |
| Citrix | | X | |
| Tomcat | | X | |
| TomcatSSL | | X | |
| X11 | | X | |
| Q.931 | | | X |
| SSH | | X | |
| M3UA | | | X |
| Sync Manager | | X | |
| MDM Alarms | | X | |
| PAM | | X | |
| Version Port | | X | |
| VRL Look-up | | X | |

**Table 90 Protocol Stacks**

## 12.2 Network Elements

### 12.2.1 Call processing elements

Several network elements comprise the CS2000 complex. These elements are the following:

- XA-Core
- Gateway Controller Cards
- Shelf Controllers
- SDM
- USP

### 12.2.2 Media Gateways

The Media Gateways can be divided into the following groups:

- trunk gateways (i.e., PVGs)

The exceptions to this division is the Universal Audio Server (UAS)

#### 12.2.2.1 Passport Voice Gateway (PVG) and Anchor Packet Gateway (APG)

The security strategy for PVGs is more complex than the other Media Gateways because of the possibility of being located in different parts of the network: the CS-LAN or a Media gateway Site.

Three different types of traffic flows will be directed to the PVGs:

- Call Processing
  - Aspen 2.1 on UDP port 2427.
  - H.248 on UDP port 2944.
  - Q.931 PRI signaling over SCTP.
- Bearer - variable UDP ports, depending on VSP2 and VSP3s
- OAM&P – TBD.

Please note that the Call Processing port is configurable.

##### 12.2.2.1.1 UDP Ports for Bearer Flows

The following table shows the default port ranges for bearer flows in both VSP2 and VSP3s. Throughout the rest of the document, this table will be refererenced when discussing PVG flows and filtering.

**Table 0-48**

| Card Type | RTP range (Even ports) | RTCP range (Odd ports) | T.38 range |
|---|---|---|---|
| VSP 2 | 49152 – 55150 | 49153 – 55151 | N/A |
| VSP 3 | 49152 - 56576 | 49153-56577 | 58112 - 64768 |

**Table 91 PVGs Bearer Ranges**

In addition, please note that, even if the UDP port ranges can be configurable, Nortel Network does not recommend changing the default values. The customer should contact Nortel Networks if network requirements will force them to change these values.

It is important to notice that, even if a wide range of UDP ports need to be opened on a firewall or a router with traffic filtering functions, the security risk is minimal since the source IP address is also filtered. This means that only traffic coming from the IP addresses of the Media Gateways will be

accepted.

In addition, with VSP2s and IP-over-AAL5 VSP3s, there is a separation of traffic (Call Processing, Bearer and OAM, if present) at Layer 2 since different PVCs are used for these flows. Such separation also adds additional security. Please note that the same strategy can be applied in MPLS networks.

**Please note that the udpPortBase must be 49152 if a Gigabit Ethernet VSP3 is used.**

#### 12.2.2.2 IW-SPM

The IW-SPM will be located in the CS-LAN and will communicate with PVGs and other IW-SPMs for DPT. The current UDP port range is as follows:

- Bearer - UDP ports 30000-34031 (even numbers for RTP and odd numbers for RTCP).

Please note that currently only the even numbers are used (for RTP streams). RTCP is not supported in SN06.

#### 12.2.2.3 Universal Audio Server (UAS)

Three different types of traffic flows will be directed to the UAS:

- Call Processing - UDP port 2427.
- Bearer - See Table 92 below.
- OAM&P – TCP port 23 for Telnet, UDP port 161 for SNMP and TCP/UDP ports 5631-5632 for pcAnywhere.

The following table shows the default port ranges for bearer flows in the UAS. Throughout the rest of the document, this table will be refererenced when discussing UAS flows and filtering.

**Table 0-49**

| RTP range (Even ports) | RTCP range (Odd ports) |
|---|---|
| 30000-30240 | 30000-30241 |

**Table 92 UAS Bearer Ranges**

Please note that the UDP port range used for bearer has always 240 ports. The initial value of 30000 is configurable and if another value is selected, the range needs to be modified accordingly.

### 12.2.3 OAM&P network elements

There are many network element managers, including clients and servers that may be connected to the CS LAN. The traffic flows originating from or going to these OAM&P network elements might need to be secured if they are transiting an insecure or untrusted network.

The following are all the generic OAM&P elements:

- Call Management Tools (CMT)
- SDM
- SAM21 Element Manager

- UAS Audio Provisioning Server (APS)
- UAS Element Manager Server
- USP EM
- Optional Generic Servers (TFTP, FTP, NTP, DNS, DHCP, KDC, DCE)
- Network Management System (optionally in CS-LAN)
- PMDM (PVGPP15K Element Manager)
- CM/CMTS EM Server (only for IAC)

It is important to remember that the PVGs/APGs can be managed in-band or out-of-band. The most secure and recommended approach is the out-of-band management since the Management interface would have an IP address on a diffrent addressing plane from the rest of the system. Nevertheless, for completeness and management flexibility, the in-band flows are shown in the OAM tables later in this section.

Please keep in mind that the same can be applicable to other third party gateways or CMTSs.

### 12.2.4 Operations Support System (OSS) / Network Operations Center (NOC)

The Operations Support Systems (OSS) and the Network Operations Center (NOC) are both OAM&P networks and they are not typically directly connected to the CS-LAN.

## 12.3 Packet Filtering and Security on the Passport 8600

### 12.3.1 Introduction and General Concepts

The CS-LAN router/Layer 3 switch (Passport 8600) has the task of filtering all incoming traffic to provide added security.

IP filters apply to all routed IP packets to be forwarded through the routing switch on specified ingress ports. The filters are applied to the switch ingress ports with a default action to forward or drop. All packets not matching any filter are forwarded or dropped, depending on the port's default action.

Filters are assigned to sets and then applied to a port using filter sets. Actions are assigned when applying a filter set to a port. The actions of individual filters can overwrite the default actions of the port.

As mentioned above, each filter has an action mode associated with it, which determines whether packets matching this filter are forwarded through the switch. Each filtered port on the Passport 8000 Series switch has a default action of forward or drop associated with it. When the filtering action mode matches the port default action, the port default action is taken. When the port default action is drop, a packet is forwarded only if a matching filter was set with an action mode of forward. If a single match occurs with an action mode of forward, it does not matter how many matching filters are found with an action mode of drop; the frame is forwarded. That is, if a packet matches multiple filters and any one of them has an action mode of forward, the packet is forwarded. When the port mode is set to forward, a packet is dropped only if a matching filter is found with a drop action mode. Again if a single match occurs with a drop action, it does not matter how many matching filters have forwarding actions; the packet is dropped. If a packet matches multiple filters and any one

of them has an action mode of drop, the packet is dropped.

Each filter set defines the conditions that must match for inclusion in the filter set and also the actions that should be performed when a match is made.

Filtering actions include

- Forward
- Forward to next hop
- Drop
- Prioritize
- Mirror
- Stop-on-match

Two types of filters can be applied: Source/Destination filters or global filters.

#### 12.3.1.1 Source and Destination Filters

Source filters must specify a source IP address and mask, and they may optionally specify a destination IP address and mask. Destination filters must specify a destination IP address and mask, and they may optionally specify a source IP address and mask. The minimum mask length is 8 bits. A source or destination filter can cause the following actions to be applied to a packet that matches the filter record:

- Forward the packet when the filter is applied with a forward action
- Drop the packet when the filter is applied with a drop action
- Mirror the packet to the defined mirror port
- Match the DS field
- Modify the DS code point (only on DiffServ access ports as shown in the Chapter related to QoS)
- Modify IEEE 802.1p

#### 12.3.1.2 Global Filters

Global filters can specify a source IP address and mask, a destination IP address and mask, both of these, or neither of these. Global filters have the following characteristics:

- No minimum or maximum mask length exists.
- Up to eight global filters can be applied on any given set of eight 10/100 Mb/s ports or one 1000 Mb/s port, each of which can accommodate eight global filters.

### 12.3.2 Summary of filter characteristics on the Passport 8600

Filters on the Passport 8000 Series switches have the following characteristics and requirements:

- Up to 3071 filter IDs can be defined among all ports or on a single port, including source/destination and global filters.
- Up to 200 filter sets can be defined for source/destination filters, while up to 100 filter sets can be defined for global filters.
- A collection of source/destination filters is defined in a set (not exceeding thirty-two per set), and the set is applied to a port or group of ports. Multiple sets can be assigned to any given port but the maximum number of source/destination sets that can be enabled on a given port set is thirty-two.

- A collection of global filters is defined in a global set (not exceeding eight per set), and the set is applied to a port or group of ports. Multiple sets may be applied to a given port or set of ports, but the maximum number of global filters that can be enabled on a given port set is eight.
- Filter counters are maintained for all active filters. Each time an active filter is “hit” by a packet, its counter is incremented by one. These counters are maintained chassis-wide and may be viewed or reset administratively at any time.

The following table contains a summary of the value of the most significant parameters in the configuration of traffic filtering on the Passport 8600.

**Table 0-50**

| Parameter | Value/Range |
|---|---|
| Filter IDs | 3071 (including global and source/destination filters) |
| Range of Global Filters Set IDs | 1 to 100 |
| Number of Global Filters per Set | Maximum 8 |
| Number of Global Filters | Maximum 8 per group of eight 10/100 Mb/s ports or one 1000 Mb/s port |
| Range of Source/Destination Filters Set IDs | 300 to 1000 |
| Number of Filters per Source/Destination Set | Maximum 32 |
| Number of sets per port (any type) | Maximum 32 |
| Number of filters per port | Maximum 1024 (32 * 32) |
| Number of characters in a filter name | 15 |

**Table 93 Summary of Filter Parameters**

For more details on the subject, Nortel Networks recommends the reader to read [Networking].

### 12.3.3 Capacity Engineering on Filtered Ports

A typical Succession solution requires several traffic filters (between 40 and 60, on average) on any interface facing a potentially untrusted network, depending on the customer requirements and security strategy.

The majority of traffic in Succession solutions uses UDP as a Layer 4 protocol. In addition, the packet sizes for both Media and Signaling streams are much smaller than traditional data streams (the average Media packet size is around 160 Bytes).

Therefore, to avoid any potential issues, it is strongly recommended to engineer the capacity of all filtered links at 50% capacity. If more capacity is needed, more Ethernet links can be added to the physical link and create a logical trunk (MLT).

### 12.3.4 Important Information on Configuring Filtering Features

The following paragraphs describe the configuration of important features that are needed for Succession.

#### 12.3.4.1 Enabling ARP Traffic

The Passport 8600 Switch needs to accept and process ARP traffic on *port-based* VLANs when the default port action is set to ***drop***. To permit ARP traffic, the network administrator must use the command line interface to do the following:

- Configure a user-defined protocol-based VLAN for ARP EtherType (byprotocol usrDefined 0x0806)
- Set the ports with a default port action of DROP

Then these ports need to be added to the VLAN as static members. Finally, the port Default VLAN ID needs to be set to the correct port-based VLAN where the ARPs will be processed.

#### 12.3.4.2 Configuring a Range of UDP Ports

The following steps describe how to configure UDP port ranges (i.e., allow all traffic between UDP port X and port X+Y). Two filters need to be configured:

- The first filter will drop all traffic with UDP ports smaller than UDP port X. The option "***Stop on Match***" is set to "**True**".
- The second filter will forward traffic with UDP ports smaller than UDP port X+Y. The option "***Stop on Match***" is set to "**True**".
- The port action must be set to drop.

### 12.3.5 Securing the Management of the Passport 8600

The Passport 8600 can be managed via several services. To optimize security, by default, the SSH, FTP, rlogin, Telnet and TFTP daemons are disabled. Nortel Networks recommends that the customers manually enable only the required services. The HTTP server allows only read parameters (read only mode) and can also be disabled.

Please note that a chassis reboot is currently required for a service change to take effect. With release 3.3, this requirement will be lifted and any change in the state of these daemons (rlogin, TFTP, Telnet, FTP) will not require a chassis reboot for the change to take effect (i.e., dynamic change).

Access policy commands allow the network administrator to control management access by setting policies for services to prevent or allow access to the switch. If management access to the switch is permitted, the administrator can specify which hosts or networks can access the switch through which services.

Nortel Networks recommends defining the network stations and/or networks that are explicitly allowed to access the switch or network stations that are explicitly forbidden to access the switch. For each service the network administrator can also specify the level of access, such as read-only or read/write/all. For more details, please see [Management].

Access policies define *who* can access the switch management functions remotely. To enable access services (i.e., how the switch management functions are accessed), please use the **flags** or **config bootconfig flags** command.

For a detailed guide on configuring SSH on the Passport 8600, please see the “28.0 Appendix: Management via SSH” on page 443.

### 12.3.6 Layer 2 Filtering on the Passport 8600

On the Passport 8600, it is possible to set individual ports to discard packets that originate from a MAC address or are going to a MAC address that is not known to the switch.

This feature is configured on a per port basis with the following command:

- config ethernet <slot/port> unknown-mac-discard <options>

The number of MAC addresses can be specified:

config ethernet <slot/port > unknown-mac-discard max-mac-count <max MAC count> with an value in a range from 0 to 2048

The way the switch learns these addresses can be:

- manually (statically)
  - config ethernet <slot/port > unknown-mac-discard add-allow-mac <mac>. In that case, the MAC addresses are saved in the config file and restored following a switch reboot.
- dynamically
  - config ethernet <slot/port > unknown-mac-discard autolearn <enable|disable>

The way that MAC addresses are learned in this way can be:

- in one shot (**config ethernet <slot/port > unknown-mac-discard autolearn-mode one-shot**). The switch learns the addresses until the table maximum is reached. Entries are never aged out.
- in continuous mode (**config ethernet <slot/port > unknown-mac-discard autolearn-mode continuous**). MAC addresses are never aged out.

After learning some addresses, the process can be enabled/disabled by the following command:

- config ethernet <slot/port > unknown-mac-discard lock-autolearn-mac <enable|disable>

A MAC address can be removed from the list:

- config ethernet <slot/port > unknown-mac-discard remove-allow-mac <mac>

In case of a violation, the port can be partitioned (disabled) if the option is specified:

- config ethernet <slot/port > unknown-mac-discard violation-downport <enable|disable>

To bring the port back up, the selected port must be manually enabled, or the switch must be rebooted.

## 12.4 Packet Filtering and Security on Juniper Routers

To be added later.

## 12.5 Packet Filtering and Security on the Passport 15000

To be added later.

## 12.6 Securing the CS-LAN

The previous sections provided the information that is needed to build a topological representation of the network elements. This information will be used in this chapter to compile a detailed list of the filtering rules required to protect the end-to-end system.

These rules will indicate **only** the traffic streams that need to be permitted to have a functional Voice-over-Packet system. To simplify the document, **only these rules will be included.** Please note that the customer might have other specific flows that need to be allowed. These requirements need to be gathered during the Customer Interaction Sessions.

To simplify the filtering policy tables the "**SRC. IP Address Range**" and "**Dest. IP Address Range**" can be meant as a range of IP addresses, as a subnet or as individual IP addresses.

Please note that Nortel Networks assumes that the Call Processing subnet and the OAM&P subnet are both located in the CS-LAN. It is also assumed that intra-subnet traffic is trusted. This assumption is applicable also for CS-LAN based Media Gateways when present.

It is also important to note that in the filtering tables no assumptions are made on which device is the connection "initiator". Some packet filtering implementations also require this aspect to be included into the security policy configuration. At this time, Nortel Networks believes that none of the present packet filtering devices supports this functionality.

In addition, for the solutions that require it, two PVG "objects" are shown in the filtering rules: CS-LAN PVGs and Remote PVGs. This was done so that security filters could also be applied more easily to a de-centralized Media Gateway site. Please note that an APG is equivalent to a CS-LAN PVG when it is located in the CS-LAN and equivalent to a remote PVG when it is not located in the CS-LAN.

A special attention should be given to ICMP. This protocol is very useful to debug network connectivity issues but it introduces several security risks involving DoS attacks. Because of this reason, Nortel Networks recommends that ICMP flows should not be allowed from untrusted networks into the CS-LAN.

The CS-LAN Router takes care of filtering out all non-allowed traffic. Filters should require both ports and IP address to match before admitting traffic. For the best protection against Denial of Service (DoS) or unauthorized flows, multi-field filtering is recommended. The router will perform the following tasks:

- Allow all intra CS-LAN Call Processing subnet traffic without any filtering.
- Allow all intra CS-LAN OAM&P subnet traffic without any filtering.
- Allow all intra CS-LAN MG subnet traffic without any filtering.
- Allow all inter CS-LAN traffic without any filtering.
- Allow all signaling traffic streams coming from the Media Gateways. Please note that both CS-LAN and Remote based PVGs are shown.
- Allow bearer traffic between the UAS and all Media Gateways. Please note that both CS-LAN and Remote based PVGs are shown.

- Allow bearer traffic between Media Gateways. Please note that PVGs might be located in the CS-LAN. If this is the case, they are labeled “CS-LAN PVG”. Otherwise, they will be labeled “Remote PVGs”.
- Allow bearer traffic between Media Gateways and the Media Portals that are CS-LAN based.
- Allow OAM&P traffic streams coming from the proper managed element and going to the correspondent Element Manager.
- Allow OAM&P traffic streams coming from NOC and going to the OAM&P subnet.
- Allow management traffic (SNMP, SSH, telnet, TFTP) between the Network Management System and the routers/switches (i.e., Passport 8600, Juniper) based on source/destination IP addresses.
- Mark all the flows with their correspondent DSCP.

Please note that Nortel Networks recommends allowing all NOC traffic going to the Call Processing or Media Gateway subnets only if it is through the OAM&P subnet in CS-LAN. This means that an operator needs to run an Element Manager (EM) GUI and connect to the EM server in the OAM&P subnet in CS-LAN. The EM server will then connect to the managed element. This recommendation guarantees a more secure connectivity.

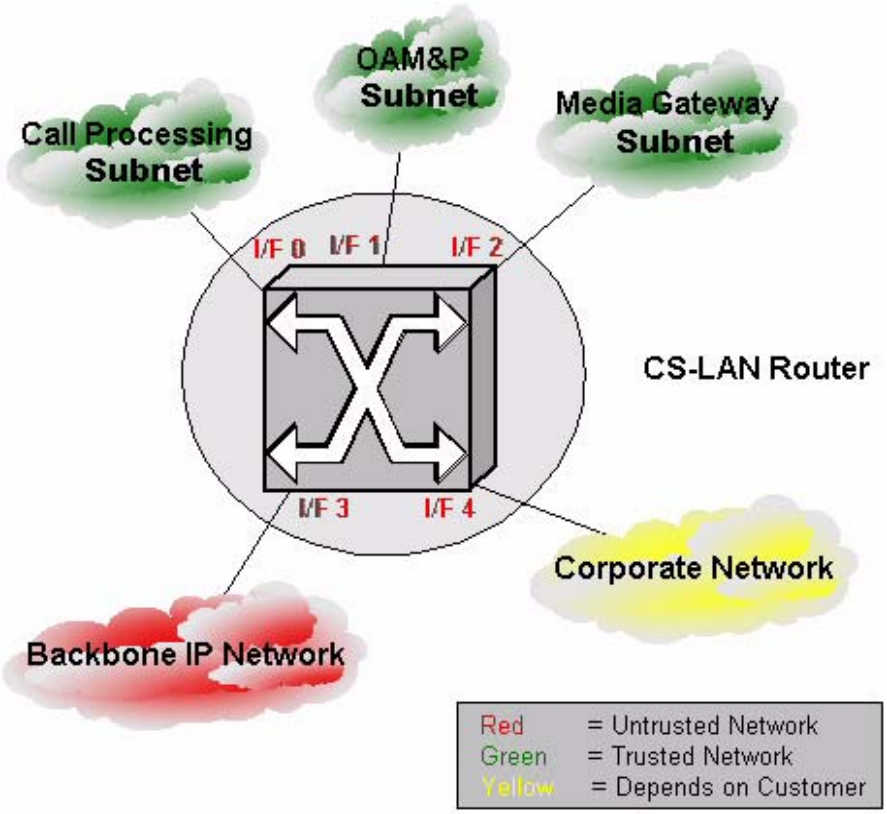



**Figure 72 Filtering interfaces on the CS-LAN Router**

Figure 72 above shows a logical view of all the interfaces in the CS-LAN. In particular, the diagram shows the logical interfaces where traffic filtering needs to be enabled.

- Interfaces 3 and 4 (I/F3 and I/F4) will filter traffic flows that are coming from potentially untrusted networks.
- Interfaces 0, 1, and 2 (I/F0, I/F1 and I/F2) will mark (or re-mark) packets with the correct DSCP. These interfaces receive trusted traffic.

Please note that in a Layer 3 switch a logical interface typically includes several physical ports that are configured in the same VLAN.

## 12.7 Packet Filtering Rules on the CS-LAN Router

This Chapter describes the filtering rules required in the CS-LAN Router for Succession solution. All incoming flows to the CS-LAN are listed in functional groups on each of untrusted ingress interfaces.

The Chapter structure will be describing the following points for all Succession solutions:

- Call Processing flows that can be common to all Succession solutions (in Table 94)
- Bearer flows that can be common to all Succession solutions (in Table 95)
- OAM&P flows that can be common to all Succession solutions (in Table 94 and Table 97)

It will then describe the following points for the Packet Trunking solution:

- Bearer flows that are specific to the Packet Trunking Succession solution (in Table 99)

### 12.7.1 Flow Analysis of Traffic Ingressing the CS-LAN

If we reference Figure 72 and Chapter 12.6, the filters derived from the flows in Table 94, Table 95 and Table 96 will be applied on interface IF/3. The filters in Table 97 will be applied on interface IF/4.

#### 12.7.1.1 Common Signaling Flows

Table 94 describes all the Call Processing and Billing flows (common to all solutions) that must be allowed. Please note that, with CS2000-1 and CS2000-2 VRDNs, Nortel Networks means the VRDNs of two different offices.

In addition, the DPT to VRDN and DPT-to-DPT flows can be either using UDP or SCTP as a Layer 4 protocol. If SCTP is used, the packet filtering functions of the router/firewall needs to support SCTP or user defined Layer 4 protocols. The protocol number for SCTP is 132.

Finally, if a USP is shared across multiple CS2000, then the traffic filtering elements needs to allow all flows coming from GWCs in CS2000-1 and going to the USP.

**Table 0-51**

| Src. IP Address Range | Dest. IP Address Range | Protocol | Source Port Range | Destination Port Range |
|---|---|---|---|---|
| CS2000-1 DPT GWC | CS2000-2 DPT GWC | SIP over UDP or<br>SIP over SCTP | 22541<br>N/A for SCTP | 5060<br>N/A for SCTP |
| CS2000-1 GWC | CS2000-2 USP | M3UA over SCTP | N/A | N/A |

**Table 94 CS-LAN Router - Call Processing Flows**

It is important to notice that the source port for signaling flows coming from third party gateways might be different from 2427. The system integrator should check the gateway documentation to avoid signaling traffic being dropped.

### 12.7.1.2 Common Bearer Flows

Table 95 describes all the Voice Media (Bearer) flows (common to all solutions) that must be allowed.

**Table 0-52**

| Src. IP Address Range | Dest. IP Address Range | Protocol | Src. Port Ranges | Dest. Port Range |
|---|---|---|---|---|
| Remote PVG | UAS | RTP | See Table 91 | See |
| | | RTCP | See Table 91 | See |
| Remote PVG/APG | CS-LAN PVG/APG | RTP | See Table 91 | See Table 91 |
| | | RTCP | See Table 91 | See Table 91 |
| | | T.38 | See Table 91 | See Table 91 |

**Table 95 CS-LAN Router - Voice Media (Bearer) Common Flows**

### 12.7.1.3 Common OAM&P Flows

Table 96 describes all the OAM&P flows (common to all solutions) that must be allowed. Please note that the PMDM might not be located in the OAM&P subnet but in the NOC. In such cases, this rule needs to be applied to the correct interface.

**Table 0-53**

| Src. IP Address Range | Dest. IP Address Range | Protocol | Source Port Range | Destination Port Range |
|---|---|---|---|---|
| Remote PVG/APG | PMDM | Telnet | 23 | 1024 - 65535 |
| | | SNMP | 161 | 1024 - 65535 |
| | | SNMP Trap | 1024 – 65535 | 162 |
| | | FTP | 1024 – 65535 | 20-21 |
| | | Secure FTP | 1024 – 65535 | 2374 (TCP) |
| | | FMIP | Configurable TCP Ports | 1024 – 65535 |
| | | NTP | 123 | 123 |

**Table 96 CS-LAN Router - OAM&P Common Flows**

It is important to notice that the source port for SNMP traps might be also 162. The system integrator should check the network element documentation to avoid SNMP traffic being dropped.

Table 97 describes all the flows between OAM&P subnet and NOC/OSS (common to all solutions) that must be allowed. The filters described in this table are applied to interface I/F4. It is important to remember that these filters might not be necessary if the customer considers these flows trusted or if the NOC is directly connected to the CS-LAN. It is also important to note that this connectivity might not be through the CS-LAN router but through another router in the customer's corporate network. The customer corporate security might require that traffic filtering be implemented in such a router. In addition, some customer's corporate security might require a firewall to protect the CS-LAN from unauthorized traffic streams coming from the NOC/OSS. Finally, in some other implementation, tunneling devices can be used to add extra security (i.e., Contivity). Therefore, the rules shown in Table 97 might be applied to different interfaces or different devices depending on customer requirements. In addition, please in mind that the network services (i.e., NTP and DNS) might be located in the CS-LAN and therefore no filtering might be required.

**Table 0-54**

| Src. IP Address Range | Dest. IP Address Range | Protocol | Source Port Range | Destination Port Range |
|---|---|---|---|---|
| NOC/OSS | USP EM | Citrix | 1024 - 65535 | 1494, 1024 - 65535 |
| NOC/OSS | PMDM | Telnet | 1024 - 65535 | 23 |
| | | FTP | 1024 - 65535 | 20-21 |
| | | FTP client | 20-21 | 1024 - 65535 |
| | | NTP | 123 | 123 |
| | | HTTP | 1024 - 65535 | 8080 |
| | | PAM | Configurable | Configurable |
| | | X11 | 1024 - 65535 | 6000 - 6003 |
| | | MDM Alarms | 1024 - 65535 | 3197 (configurable) |

**Table 0-54**

| Src. IP Address Range | Dest. IP Address Range | Protocol | Source Port Range | Destination Port Range |
|---|---|---|---|---|
| NOC/OSS | CMT | SSH | 1024 - 65535 | 22 |
| | | CORBA | 1024 - 65535 | 2001 and 1024-65535 |
| | | HTTP | 1024 - 65535 | 80 |
| | | HTTPS | 1024 - 65535 | 443 |
| | | OSSGate | 1024 - 65535 | 10023 and 11023 |
| | | Tomcat | 1024 - 65535 | 8080 |
| | | TomcatSSL | 1024 - 65535 | 8443 |
| | | FTP | 1024 - 65535 | 20-21 |
| | | Telnet | 1024 - 65535 | 23 |
| | | SNMP | 1024 – 65535 | 161 |
| | | SNMP Trap | 162 | 1024 – 65535 |
| | | FTP over SSH PORT FWD. | 1024 - 65535 | 9999 |
| | | Version Port | 1024 - 65535 | 24482 |
| | | VRL Look-up | 1024 - 65535 | 24484 |
| | | DNS | 53 | 53 |
| | | NTP | 123 | 123 |
| | | PAM | Configurable | Configurable |
| NOC/OSS | Router/Switch | SNMP | 1024 - 65535 | 161 |
| | | SNMP Trap | 162 | 1024 - 65535 |
| | | Telnet | 1024 - 65535 | 23 |
| | | SSH | 1024 - 65535 | 22 |

**Table 0-54**

| Src. IP Address Range | Dest. IP Address Range | Protocol | Source Port Range | Destination Port Range |
|---|---|---|---|---|
| NOC/OSS | SDM | Telnet | 1024 - 65535 | 23 |
| | | FTP | 20-21 | 1024 - 65535 |
| | | FTP | 1024 - 65535 | 20-21 |
| | | SSH | 1024 - 65535 | 22 |
| | | NTP | 123 | 123 |
| | | DNS | 53 | 1024 - 65535 |
| | | DCE Resolution | 1024 - 65535 | 135 |
| | | DCE RPC | 1024 - 65535 | Configurable |
| | | SCC2 Adapter | Configurable | Configurable |
| | | GR740/EAD AS | 1024 - 65535 | 9550-9556 |
| | | UTA | 1024 - 65535 | 7701 |
| | | OMDD | 1024 - 65535 | 7100 |
| | | TL1 | 1024 - 65535 | 6008 |
| | | AFT | 1024 - 65535 | 30000 |

**Table 97 CS-LAN Router - NOC/OSS flows**

It is important to notice that the source port for SNMP traps might also be 162. The system integrator should check the network element documentation to avoid SNMP traffic being dropped.

### 12.7.1.3.1 Explicit Deny Rule for traffic to the USP RTCs

In the cases in which the Service Provider Corporate network is not considered trusted, it is strongly recommended blocking all traffic originating in the Corporate network with the USP RTCs as a destination. Such a filter would be applied on I/F 4 and would use the IP addresses of the RTCs with an explicit action of **drop**.

**Table 0-55**

| Src. IP Address Range | Dest. IP Address Range | Protocol | Source Port Range | Destination Port Range | Action |
|---|---|---|---|---|---|
| All | RTCs | N/A | N/A | N/A | DROP |

**Table 98 Explicit Deny Rule for RTCs**

#### 12.7.1.4 Packet Trunking Specific Information

This Chapter describes all the flows that specific to the Packet Trunking solution. The following tables show a detailed description of the overall flows.

Please note that the IW-SPM is located in the Media Gateway subnet in the CS-LAN.

##### 12.7.1.4.1 Bearer Flows for Packet Trunking

Table 99 describes all the Bearer flows that are specific to Packet Trunking.

**Table 0-56**

| Src. IP Address Range | Dest. IP Address Range | Protocol | Src. Port Ranges | Dest. Port Range |
|---|---|---|---|---|
| Remote PVG | IW-SPM | RTP | See Table 91 | 30000-34031 (Even ports) |
| | | RTCP | See Table 91 | 30000-34031 (Odd ports) |
| Remote IW-SPM | IW-SPM | RTP | 30000-34031 (Even ports) | 30000-34031 (Even ports) |
| | | RTCP | 30000-34031 (Odd ports) | 30000-34031 (Odd ports) |

**Table 99 CS-LAN Router - Flows Specific to Packet Trunking**

## 12.8 Securing the Customer's Corporate Network

In many deployments, it is possible that the edge between the CS-LAN and the customer's Corporate network is protected by firewalls. In addition, all traffic entering the NOC might also be monitored by firewalls.

If this is the case, it is necessary to allow OAM&P traffic between the CS-LAN OAM&P subnet and the OAM&P clients residing in the NOC.

A special attention should be given to ICMP. This protocol is very useful to debug network connectivity issues but it introduces several security risks involving DoS attacks. Because of this reason, Nortel Networks recommends that ICMP flows should not be allowed from untrusted networks into the Corporate Network.

## 12.9 Packet Filtering Rules for Protecting the Corporate Network

This Chapter describes the filtering rules required in the Corporate firewalls for Succession solution. All incoming flows to the Corporate network are listed in detail.

The Chapter structure will be describing the following points for all Succession solutions:

- OAM&P flows that can be common to all Succession solutions (in Table 100)

### 12.9.1 Flow Analysis of Traffic Ingressing the Corporate Network

The following tables show all the flows that need to be allowed through the customer's firewalls.

**Table 0-57**

| Src. IP Address Range | Dest. IP Address Range | Protocol | Source Port Range | Destination Port Range |
|---|---|---|---|---|
| USP EM | NOC/OSS | Citrix | 1494, 1024 - 65535 | 1024 - 65535 |
| PMDM | NOC/OSS | Telnet | 23 | 1024 - 65535 |
| | | FTP | 20-21 | 1024 - 65535 |
| | | FMIP (???) | ???? | ???? |
| | | FTP client | 1024 - 65535 | 20-21 |
| | | NTP | 123 | 123 |
| | | HTTP | 80 | 1024 - 65535 |
| | | PAM | Depends | Depends |
| | | X11 | 6000 - 6003 | 1024 - 65535 |
| | | MDM Alarms | 3197 (configurable) | 1024 - 65535 |

**Table 0-57**

| Src. IP Address Range | Dest. IP Address Range | Protocol | Source Port Range | Destination Port Range |
|---|---|---|---|---|
| CMT | NOC/OSS | SSH | 22 | 1024 - 65535 |
| | | CORBA | 2001 and 1024-65535 | 1024 - 65535 |
| | | HTTP | 80 | 1024 - 65535 |
| | | HTTPS | 443 | 1024 - 65535 |
| | | OSSGate | 10023 and 11023 | 1024 - 65535 |
| | | Tomcat | 8080 | 1024 - 65535 |
| | | TomcatSSL | 8443 | 1024 - 65535 |
| | | FTP | 20-21 | 1024 - 65535 |
| | | Telnet | 23 | 1024 - 65535 |
| | | SNMP | | |
| | | SNMP Trap | | |
| | | FTP over SSH PORT FWD. | 9999 | 1024 - 65535 |
| | | Version Port | 24482 | 1024 - 65535 |
| | | VRL Look-up | 24484 | 1024 - 65535 |
| | | DNS | 53 | 53 |
| | | NTP | 123 | 123 |
| | | PAM | Configurable | Configurable |
| Router/Switch | NOC/OSS | SNMP | 161 | 1024 - 65535 |
| | | SNMP Trap | 1024 - 65535 | 162 |
| | | Telnet | 23 | 1024 - 65535 |
| | | SSH | 22 | 1024 - 65535 |

**Table 0-57**

| Src. IP Address Range | Dest. IP Address Range | Protocol | Source Port Range | Destination Port Range |
|---|---|---|---|---|
| SDM | NOC/OSS | Telnet | 23 | 1024 - 65535 |
| | | FTP | 1024 - 65535 | 20-21 |
| | | FTP | 20-21 | 1024 - 65535 |
| | | SSH | 22 | 1024 - 65535 |
| | | NTP | 123 | 123 |
| | | DNS | 1024 - 65535 | 53 |
| | | DCE Resolution | 135 | 1024 - 65535 |
| | | DCE RPC | Configurable | 1024 - 65535 |
| | | SCC2 Adapter | Configurable | Configurable |
| | | GR740/EAD AS | 9550-9556 | 1024 - 65535 |
| | | UTA | 7701 | 1024 - 65535 |
| | | OMDD | 7100 | 1024 - 65535 |
| | | TL1 | 6008 | 1024 - 65535 |
| | | AFT | 30000 | 1024 - 65535 |

**Table 100 Common CS-LAN to NOC Flows - Corporate Firewalls**

## 12.10 Securing the Media Gateway Site

The Media Gateway Site is the location where the Media Gateways are located. It could include both large trunk (PVGs) and/or line gateways or it can contain only one of the two types.

Traffic filtering on the Media Gateway router is typically the first line of defense for the CS-LAN. Specifically, by using IP addresses and TCP/UDP ports, it needs to:

- Allow all signaling traffic between the GWC and the Media Gateways.
- Allow all bearer traffic from the Media Gateways to the UAS.
- Allow all bearer traffic from local Media Gateways to remote Media Gateways
- Allow OAM&P traffic streams coming from the proper managed element and going to the correspondent Element Manager.

The above rules will be applied to Interfaces 1 and 2 (I/F 1 and I/F 2) in Figure 73.

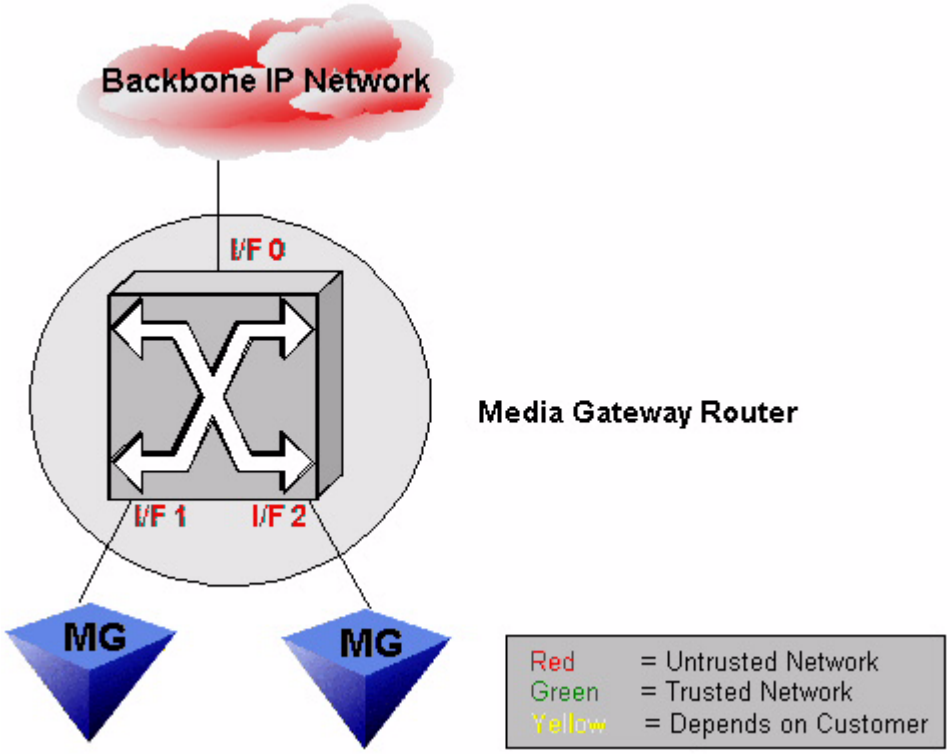



**Figure 73 The Media Gateway Router**

In addition to these, other filtering rules need to be applied to protect the Media Gateways from potential attacks coming from the untrusted Backbone IP Network (see Figure 73). This set of rules will be applied to Interface 0 (I/F 0).

Figure 73 above shows a logical view of all the interfaces in the Media Gateway site. In particular, the diagram shows the logical interfaces where traffic filtering needs to be enabled.

- Interface 0 (I/F 0) will filter traffic flows that are coming from potentially untrusted networks.
- Interfaces 1 and 2 (I/F1 and I/F2) are connected to the Media Gateways and will only allow selected flows. In addition, at these interfaces packets will be marked (or re-mark) with the correct DSCP.

Please note that in a Layer 3 switch a logical interface typically includes several physical ports that are configured in the same VLAN.

As for the CS-LAN, a special attention should be given to ICMP. This protocol is very useful to debug network connectivity issues but it introduces several security risks involving DoS attacks. Because of this reason, Nortel Networks recommends that ICMP flows should not be allowed from untrusted networks into the Media Gateway subnets.

### 12.10.1 Anti-Spoofing

The Media Gateway site router is the network element that can help significantly to stop Spoofing attacks before they reach the Succession components. Since this router is the closest to the possible source of attacks, stopping spoofed IP packets and block all unauthorized traffic is easier here. It is important to notice that using a strong anti-spoofing policy greatly decreases the risks for Denial of Service (DoS) attacks.

### 12.10.2 TFTP Flows

Please note that TFTP flows offer a unique challenge in a traffic filtering strategy. The main reason is because after the initial request on UDP port 69 on the server, the server chooses a random chosen port number for the rest of the connection. Without the use of IPSec, this kind of connection presents an interesting challenge to the network administrator. Nortel Networks recommends using a TFTP server that allows a flexible configuration so that a certain range of UDP ports can be selected. This would minimize the number of ports that should be open on the filtering elements.

## 12.11 Packet Filtering Rules on the Media Gateway Site Router

This Chapter will explore in details all the flows that need to be allowed through a packet-filtering device. First the flows common to all solutions will be identified; then Nortel Networks will describe the flows that are specific to particular solutions. The packet filtering rules that are needed can be therefore derived very easily from the necessary flows.

The Chapter structure describes several points for all Succession solutions. If we reference Figure 73 and Chapter 12.10, for all interfaces connected to the Backbone (I/F 0) and to the Media Gateways (I/F 1 and I/F 2), it will describe:

- Call Processing flows that can be common to all Succession solutions (in Table 101 and Table 104)
- Bearer flows that can be common to all Succession solutions (in Table 102 and Table 105)
- OAM&P flows that can be common to all Succession solutions (in Table 103 and Table 106)

It will then describe the following points for the Packet Trunking solution:

- Bearer flows that are specific to the Packet Trunking Succession solution (in Table 107 and Table 108)

### 12.11.1 Flows Analysis for Traffic Ingressing the Media Gateway Site

#### 12.11.1.1 Flows on Interface 0

Table 101, Table 102 and Table 103 summarize all the flows that need to be accepted on the interface(s) to the Backbone IP Network (see Figure 73). This interface is I/F 0.

#### 12.11.1.1.1 Common Signaling Flows

Table 101 shows all the Call Processing flows that are common to all solutions.

**Table 0-58**

| Src. IP Address Range | Dest. IP Address Range | Protocol | Src. Port Ranges | Dest. Port Range |
|---|---|---|---|---|
| GWC | Local PVG/APG | ASPEN 2.1 | 2427 | 2427 |
| | | H.248 | 2944 | 2944 |
| | | Q.931 | N/A | N/A |

**Table 101 Media Gateway Site – Call Processing Common Flows on I/F 0**

It is important to notice that the source port for signaling flows coming from third party gateways might be different from 2427. The system integrator should check these values in the gateway documentation to avoid signaling traffic being dropped.

#### 12.11.1.1.2 Common Bearer Flows

Table 102 shows all the Voice Media (Bearer) flows that are common to all solutions.

**Table 0-59**

| Src. IP Address Range | Dest. IP Address Range | Protocol | Src. Port Ranges | Dest. Port Range |
|---|---|---|---|---|
| UAS | Local PVG/APG | RTP | See | See Table 91 |
| | | RTCP | See | See Table 91 |
| Remote PVG/APG | Local PVG/APG | RTP | See Table 91 | See Table 91 |
| | | RTCP | See Table 91 | See Table 91 |
| | | T.38 | See Table 91 | See Table 91 |

**Table 102 Media Gateway Site – Voice Media (Bearer) Common Flows on I/F 0**

### 12.11.1.1.3 Common OAM&P Flows

Table 103 shows all the OAM&P flows that are common to all solutions.

**Table 0-60**

| Src. IP Address Range | Dest. IP Address Range | Protocol | Src. Port Range | Dest. Port Range |
|---|---|---|---|---|
| PMDM | Local PVG/APG | Telnet | 1024 - 65535 | 23 |
| | | SNMP | 1024 - 65535 | 161 |
| | | SNMP Trap | 162 | 1024 - 65535 |
| | | FTP | 20-21 | 1024 - 65535 |
| | | Secure FTP | 2374 (TCP) | 1024 - 65535 |
| | | FMIP | Configurable TCP Ports | 1024 - 65535 |
| | | NTP | 123 | 123 |

**Table 103 Media Gateway Site – OAM&P Common Flows on I/F 0**

It is important to notice that the source port for SNMP traps might also be 162. The system integrator should check this value in the network element documentation to avoid SNMP traffic being dropped.

### 12.11.1.2 Flows on Interfaces 1 and 2

Table 104, Table 105 and Table 106 summarize all the flows that need to be accepted on the interface(s) to the Media gateways (see Figure 73). These interfaces are I/F 1 and I/F 2.

### 12.11.1.2.1 Common Signaling Flows

Table 104 shows all the Call Processing flows that are common to all solutions.

**Table 0-61**

| Src. IP Address Range | Dest. IP Address Range | Protocol | Src. Port Ranges | Dest. Port Range |
|---|---|---|---|---|
| Local PVG/APG | GWC | ASPEN 2.1 | 2427 | 2427 |
| | | H.248 | 2944 | 2944 |
| | | Q.931 | N/A | N/A |

**Table 104 Media Gateway Site – Call Processing Common Flows on I/F 1 and 2**

It is important to notice that the source port for signaling flows coming from third party gateways might be different from 2427. The system integrator should check these values in the gateway documentation to avoid signaling traffic being dropped.

#### 12.11.1.2.2 Common Bearer Flows

Table 105 shows all the Voice Media (Bearer) flows that are common to all solutions.

**Table 0-62**

| Src. IP Address Range | Dest. IP Address Range | Protocol | Src. Port Ranges | Dest. Port Range |
|---|---|---|---|---|
| Local PVG/APG | UAS | RTP | See Table 91 | See |
| | | RTCP | See Table 91 | See |
| Local PVG/APG | Remote PVG/APG | RTP | See Table 91 | See Table 91 |
| | | RTCP | See Table 91 | See Table 91 |
| | | T.38 | See Table 91 | See Table 91 |

**Table 105 Media Gateway Site – Voice Media (Bearer) Common Flows on I/F 1 and 2**

#### 12.11.1.2.3 Common OAM&P Flows

Table 106 shows all the OAM&P flows that are common to all solutions.

**Table 0-63**

| Src. IP Address Range | Dest. IP Address Range | Protocol | Src. Port Range | Dest. Port Range |
|---|---|---|---|---|
| Local PVG/APG | PMDM | Telnet | 23 | 1024 - 65535 |
| | | SNMP | 161 | 1024 - 65535 |
| | | SNMP Trap | 1024 - 65535 | 162 |
| | | FTP | 1024 - 65535 | 20-21 |
| | | Secure FTP | 1024 – 65535 | 2374 (TCP) |
| | | FMIP | 1024 - 65535 | Configurable TCP Ports |
| | | NTP | 123 | 123 |

**Table 106 Media Gateway Site – OAM&P Common Flows on I/F 1 and 2**

It is important to notice that the source port for SNMP traps might also be 162. The system integrator should check this value in the network element documentation to avoid SNMP traffic being dropped.

### 12.11.2 Packet Trunking Specific Information

This Chapter describes all the flows that specific to the Packet Trunking IP solution. The following tables show a detailed description of the flows needed to build the filtering.

### 12.11.2.1 Flows on Interface 0

#### 12.11.2.1.1 Bearer Flows for Packet Trunking

All the filters described in Table 107 summarize all the Voice Media (Bearer) flows that need to be accepted on the interface(s) to the Backbone IP Network (see Figure 73). This interface is I/F 0.

**Table 0-64**

| Src. IP Address Range | Dest. IP Address Range | Protocol | Src. Port Ranges | Dest. Port Range |
|---|---|---|---|---|
| IW-SPM | Local PVG | RTP | 30000-34031 (Even ports) | See Table 91 |
| | | RTCP | 30000-34031 (Odd ports) | See Table 91 |

**Table 107 Media Gateway Site – Flows Specific to Packet Trunking on I/F 0**

### 12.11.2.2 Flows on Interfaces 1 and 2

#### 12.11.2.2.1 Bearer Flows for Packet Trunking

Table 108 summarizes all the flows that need to be accepted on the interface(s) to the Media Gateways (see Figure 73). These interfaces are I/F 1 and I/F 2.

**Table 0-65**

| Src. IP Address Range | Dest. IP Address Range | Protocol | Src. Port Ranges | Dest. Port Range |
|---|---|---|---|---|
| Local PVG | IW-SPM | RTP | See Table 91 | 30000-34031 (Even ports) |
| | | RTCP | See Table 91 | 30000-34031 (Odd ports) |

**Table 108 Media Gateway Site - Flows Specific to Packet Trunking on I/F 1 and 2**

# 13.0 Quality of Service (QoS)

QoS is a necessary strategy in multi-service networks to guarantee the best service to all the applications. As shown in the following Sections, Nortel Networks recommend the following techniques:

- DiffServ in routed networks.
- 802.1p in switched layer 2 networks **(To be added later).**
- MPLS EXP using DiffServ PSCs in MPLS-based networks **(To be added later).**

DiffServ (as described in RFC3246, RFC247 and RFC2597) specifies the following code points:

**Table 0-66**

| **DS PHB** | **DiffServ Code Point** | | | | |
|---|---|---|---|---|---|
| **EF** | '101110' | | | | |
| **AF[Y][X]** | Class 1 | Class 2 | Class 3 | Class 4 | Drop Precedence |
| | '001010' (AF11) | '010010' (AF21) | '011010' (AF31) | '100010' (AF41) | Low |
| | '001100' (AF12) | '010100' (AF22) | '011100' (AF32) | '100100' (AF42) | Medium |
| | '001110' (AF13) | '010110' (AF23) | '011110' (AF33) | '100110' (AF43) | High |
| | Y = Class Number<br>X = Drop Precedence (discard priority), 1=lowest, 3=highest | | | | |
| **DF** | '000000' | | | | |

**Table 0-67**

| **CS** | '111000' (CS7) | '110000' (CS6) | '101000' (CS5) | '100000' (CS4) | '011000' (CS3) | '010000' (CS2) | '001000' (CS1) | '000000' (CS0) |
|---|---|---|---|---|---|---|---|---|

**Table 109 IETF DSCPs**

It is typically recommended that all network elements pre-mark their traffic according to their class category. A detail description of the flows and their DSCP can be found in Sections 13.4 and 13.5.

If the elements are unable to mark packets with the appropriate DSCP value or the elements are not trusted, then the re-marking **must** be performed on DS edge node.

## 13.1 Nortel Networks Service Classes (NNSC)

Nortel Networks has created standardized default QoS behaviors for its product in the form of end-to-end network service classes. These are called Nortel Networks Service Classes (NNSC).

The following paragraphs give a high-level overview of these classes. Table 110 shows an example of the NNSC.

**Table 0-68**

| Traffic Category | Example Application | NNSC | DSCP in NNSC |
|---|---|---|---|
| **Network Control** | Critical Alarms | Critical | CS7 |
| | Routing, Billing, Critical OAM | Network | CS6 |
| **Interactive** | VoIP, Interactive Gaming | Premium | EF or CS5[1] |
| | Video Conferencing | Platinum | AF41, AF42, AF43, CS4 |
| **Responsive** | Streaming audio/video | Gold | AF31, AF32, AF33, CS3 |
| | Client/Server transactions | Silver | AF21, AF22, AF23, CS2 |
| **Timely** | E-mail | Bronze | AF11, AF12, AF13, CS1 |
| | Best Effort | Standard | DF |

**Table 110 Examples of the NNSCs with 8 Classes**

It should be noted that Succession solutions that support IP Telephony, priority data and best effort data services only require a subset of the Nortel Networks Service Classes. For such solutions above, four NNSCs MUST be supported as summarized in Table 111. Additional service classes (NNSCs) **MAY** be supported in the Managed IP Network for additional services/applications like video conferencing, streaming video services and various differentiated data services.

**Table 0-69**

| Traffic Category | NNSC | DSCP | Example Application |
|---|---|---|---|
| Network Control | Network | CS7, CS6 | Critical Alarms, heartbeats, Routing, Critical OAM |
| Interactive | Premium | EF, CS5 | IP Telephony (voice G.711 and compressed, DTMF Tones, voice-band data, clear-channel data, lawful intercept, signaling between GW/phone and call server) |
| Timely | Bronze | AF11, AF12, AF13, CS1 | Non-critical OAM&P, Priority data, Billing |
| | Standard | DF (=CS0) | Best effort or unclassified data |

**Table 111 Examples of the NNSCs with 4 Classes**

### 13.1.1 Critical Class

The Critical NNSC is used only for network-to-network device communications within an administrative domain (i.e., critical heartbeats between nodes).

Network devices should premark their packets with CS7 DSCP to receive Critical NNSC treatment. An example of the Critical NNSC includes VRRP heartbeats.

### 13.1.2 Network Class

The Network NNSC is used for communications between network devices within one administrative domain (i.e., routing protocols, ICMP) if Critical NNSC is not supported as well for control and signaling communication between administrative domains (i.e., SIP-T, DNS, DHCP/BootP, RSVP). Network devices should premark their packets with CS6 DSCP to receive the Network NNSC edge-to-edge treatment.

### 13.1.3 Premium Class

This class is intended for support of telephony service over IP networks. It is **required** that the end equipment (voice media gateways, IP phones and call servers) set the DSCP as indicated below:

- EF = Voice data (bearer traffic)
- CS5 = Telephony signaling between media gateways and call server. Also T.38 encoded fax calls

### 13.1.4 Platinum Class

The Platinum NNSC is used for Interactive Video (Video Conferencing) and Interactive Gaming. Packets marked with Assured Forwarding 4 (AF4) or Class Selector 4 (CS4) belong to this NNSC.

### 13.1.5 Gold Class

The Gold NNSC is **recommended** for streaming audio and video. Packets marked with Assured Forwarding 3 (AF3) or Class Selector 3 (CS3) belong to this NNSC.

### 13.1.6 Silver Class

The Silver NNSC is **used** for fast response for TCP and HTTP short lived flows (i.e., interactive TCP traffic, eCommerce). Packets marked with Assured Forwarding 2 (AF2) or Class Selector 2 (CS2) belong to this NNSC.

### 13.1.7 Bronze Class

The Bronze NNSC is **used** for long-lived TCP, and HTTP flows (E-Mail, Priority data, non-critical OAM&P). Packets marked with Assured Forwarding 1 (AF1) or Class Selector 1 (CS1) belong to this NNSC.

### 13.1.8 Standard Class

The Standard NNSC is used for all traffic that has not been characterized into one of the other supported NNSC in the DS network domain. Packets marked with DSCP value ‘000 000’ (or any other DSCP value that is not mapped to the supported classes described above) must be mapped to the Standard NNSC.

## 13.2 DiffServ in Succession

Since a general discussion of DiffServ has been completed, the rest of the QoS sections will focus on the guidelines required for Succession IP solutions. In particular, Nortel Networks will explore in detail how to classify and mark all the logical flows. Further down in the document, the logical flows will be examined and classified one-by-one.

### 13.2.1 Flow Classification

The first step is to group the logical flow types. The groups are:

- Voice Media (bearer traffic)
- Voice Signaling, and Call Control and T.38 Fax.
- OAM&P.

Table 112 illustrates the different applications for each flow and shows the DSCP for the three types.

**Table 0-70**

| Flow Type | Network Elements | NNSC | Application | DSCP |
|---|---|---|---|---|
| Voice Signaling (Control) | MG - MGC | Premium | H.248 | CS5 |
| | Carrier MGC - Carrier MGC | Network | SIP-T (IP solutions only) | CS6 |
| Critical OAM&P | OAM&P Servers - MG | Network | DHCP, BootP, high priority OAM | CS6 |
| Non-Critical OAM&P | OAM&P Servers - MG | Bronze | FTP, HTTP | AF11 |
| Non-Critical OAM&P | OAM&P Servers - MG | Bronze | SNMP, Billing record transfers, TFTP | CS1 |

**Table 112 Default DSCP**

### 13.2.2 Mapping to Queues

All the service classes defined above need to be mapped to the internal queues of the routers in the DS domain for optimal servicing. Nortel Networks recommends network elements that support 8 queues. However, this is not always possible, especially in a multi-vendor network.

#### 13.2.2.1 Queues in the Passport 8600

Since the router that is primarily used for the CS-LAN and for aggregating Media Gateway sites is the Passport 8600, Table 113 shows this mapping for all the Succession logical flows. Please note that the Passport 8600 supports eight queues.

**Table 0-71**

| Traffic Type | Code Points | | Class name | Queue Number |
|---|---|---|---|---|
| Network control | CS7 | 111000 | Network | 7 |
| Critical OAM | CS6 | 110000 | Network | 7 |
| VoIP Signaling | CS5 | 101000 | Premium | 6 |
| VoIP Bearer | EF | 101110 | Premium | 6 |
| Priority IP Data | AF41 | 100010 | Platinum | 5 |
| Priority IP Data | AF31 | 011010 | Gold | 4 |

**Table 0-71**

| Traffic Type | Code Points | | Class name | Queue Number |
|---|---|---|---|---|
| Priority IP Data | AF21 | 010010 | Silver | 3 |
| Non-Critical OAM | CS1 | 001010 | Bronze | 2 |
| Priority IP Data | AF11 | 001000 | Bronze | 2 |
| Best Effort Data | DF | 000000 | Standard | 1 |
| Best Effort Data | CS0 | 000000 | Standard | 1 |

**Table 113 Mapping to Queues in the 8600**

### 13.2.2.2 Queues in Junipers Routers

The other routers that might be present in Succession solutions are typically Junipers M-Series routers. Table 114 shows the mapping of NNSC to queues for all the Succession logical flows. Please note that Juniper routers support only four queues. In addition, it is strongly recommended not to mix data with voice in the same queue.

**Table 0-72**

| Traffic Type | CoS Code Points | DSCP | Juniper Forwarding Class | NNSC | Queue Number |
|---|---|---|---|---|---|
| Network control | 111 | 111000 | Network-control | Network | 3 |
| OAM | 110 | 110000 | Network-control | Network | 3 |
| Signaling | 101 | 101000 | Expedited-forwarding | Premium | 2 |
| Bearer | 101 | 101110 | Expedited-forwarding | Premium | 2 |
| Priority IP Data | 011 | 001010 | Assured-forwarding | Bronze | 1 |
| Priority IP Data | 010 | 001000 | Assured-forwarding | Bronze | 1 |
| Best Effort Data | 000 | 000000 | Best-effort | Standard | 0 |

**Table 114 Mapping to Queues in Juniper**

### 13.2.2.3 Queues in the BPS

Another network element that can be present in a Succession solution is the BPS 2000, used in the IAW solutions. Table 115 describes the default DSCP, QoS class, IEEE 802.1p, and egress queue assignment for packets in each traffic class.

**Table 0-73**

| Incoming or re-marked DSCP | QoS class | Outgoing 802.1p user Priority |
|---|---|---|
| CS7 | Critical | 7 |
| CS6 | Network | |
| EF, CS5 | Premium | 6 |
| AF41, AF42, AF43, CS4 | Platinum | 5 |
| AF31, AF32, AF33, CS3 | Gold | 4 |
| AF21, AF22, AF23, CS2 | Silver | 3 |
| AF11, AF12, AF13, CS1 | Bronze | 2 |
| DE, CS0 | Standard | 0 |

**Table 115 Mapping to Queues in BPS2000**

### 13.2.2.4 Queues in the Passport 15000

To be added later.

## 13.3 QoS on the Passport 8600

Filtering is the methodology that is used to implement QoS on the Passport 8600. The Passport 8600 uses an internal value, called “Internal QoS” that correlates the mapping between all QoS strategies.

On the Passport 8600, all the ports that are connected to Succession network elements are **Access** ports. The ports that are connected to other routers and/or switches are considered **Core** ports.

A port can receive the following types of traffic:

- Tagged and Bridged Traffic
- Tagged and Routed Traffic
- Untagged and Bridged Traffic
- Untagged and Routed Traffic

The following paragraphs will explore the behavior of both Access and Core ports when receiving

the above types of traffic.

### 13.3.1 DiffServ Access Port

The DiffServ access element is at the edge of the DS network and classifies traffic by marking it with the appropriate DSCP and assigning it to the internal QoS level based on the filters and traffic policies that are enabled. The traffic filters allow setting criteria for identifying a micro flow or an aggregate flow by matching on multiple fields in the IP packet.

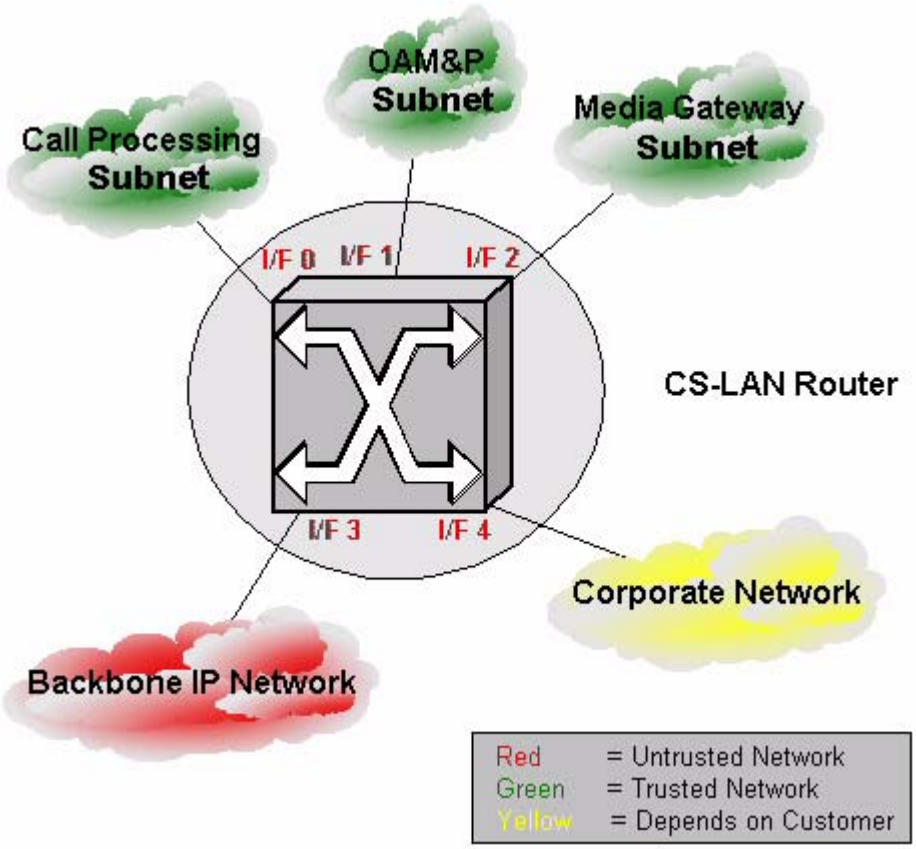



**Figure 74 CS-LAN Router**

If the reader refers to the network diagram in Figure 74 , Interfaces 0, 1 and 2 (I/F 0, I/F 1 and I/F 2) are Access ports.

An Access port, when receiving the four types of traffic as described above, will behave according

to Table 116..

**Table 0-74**

| Type of traffic | Ingress | Egress |
|---|---|---|
| Tagged and bridged | Use Tag-to-QoS mapping to map the IEEE 802.1p bits to a QoS level, if no global filter is present. With global filter, re-mark IEEE 802.1p bits with filter value only if the filter value is higher.<br>Preserve DSCP. | Use the QoS-to-Tag mapping to reset the IEEE 802.1p bits based on the QoS level.<br>Use the QoS-to-DSCP mapping to set the DSCP, if no filter is present. Otherwise, re-mark DSCP to filter DSCP. |
| Tagged and routed | Reset DSCP to zero, and use traffic filters to set the new DSCP. Use the DSCP-to-QoS mapping to map the new DSCP to a QoS level.<br>Ignore IEEE 802.1p bits. | Use the QoS-to-Tag mapping to reset the IEEE 802.1p bits based on the QoS level. |
| Untagged and bridged | If a global filter is used, set the new DSCP according to that filter. Assign QoS level based on highest QoS level in the DSCP mapping or port, VLAN, or MAC address. | Use the QoS-to-DSCP mapping to reset the DSCP. |
| Untagged and routed | Reset DSCP to zero, and use traffic filters to set the new DSCP. Use the DSCP-to-QoS mapping to map the new DSCP to a QoS level. | No action is performed. |

**Table 116 DiffServ Access Point Behavior**

### 13.3.2 DiffServ Core Port

The DiffServ core port does not change packet classification or marking done in the DiffServ access port. The core port preserves the DSCP or IEEE 802.1p bit marking of all incoming packets and uses these markings to assign the packet to an internal queue.

If the reader refers to the network diagram in Figure 74 , Interfaces 3 and 4 (I/F 3 and I/F 4) are Core ports.

A Core port, when receiving the four types of traffic as described above, will behave according to Table 117.

For more detailed information on the way this classification is implemented in the Passport 8600, please see [Networking].

**Table 0-75**

| Type of traffic | Ingress | Egress |
|---|---|---|
| Tagged and bridged | Place the packet in the QoS queue based on the DSCP-to-QoS mapping. Ignore the IEEE 802.1p bits. | No action is performed. |

**Table 0-75**

| Type of traffic | Ingress | Egress |
|---|---|---|
| Tagged and routed | Place the packet in the QoS queue based on the DSCP-to-QoS mapping. Ignore the IEEE 802.1p bits. | Use the QoS-to-Tag mapping to reset the IEEE 802.1p bits based on the QoS level. |
| Untagged and bridged | Place the packet in the QoS queue based on the DSCP-to-QoS mapping. | No action is performed. |
| Untagged and routed | Place the packet in the QoS queue based on the DSCP-to-QoS mapping. | No action is performed. |

**Table 117 DiffServ Core Port Behavior**

## 13.4 QoS in the CS-LAN Router (Passport 8600)

The CS-LAN router/Layer 3 switch (Passport 8600) has also the task of marking the packets originating from all devices that do not mark already the DSCP according to the quality of service that they require. This marking is done based on the guidelines of section 13.2.

### 13.4.1 Common Flows

As previously discussed, the filters that perform marking will be applied on logical interfaces I/F 0, 1 and 2, as shown in Figure 75 .

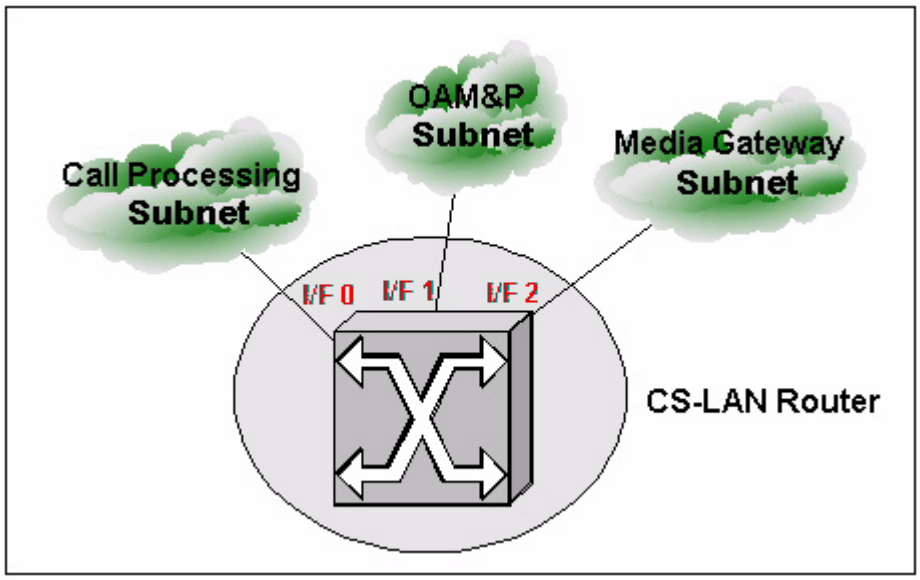



**Figure 75 QoS in the CS-LAN**

Please note that in a Layer 3 switch a logical interface typically includes several physical ports that are configured in the same VLAN.

The following tables group all the flows originating from the same logical subnet of the CS-LAN (Call

Processing, OAM&P and Media Gateway) and a DSCP based on their NNSC (see section 13.2 for more details) is assigned to each of them.

### 13.4.1.1 QoS for Call Processing Elements

Table 118 illustrates all the flows that originate from the Call Processing subnet. These flows are common for all solutions. The traffic filters derived from the flows described in Table 118 will be applied on interface I/F 0.

**Table 0-76**

| Src. IP Address Range | Dest. IP Address Range | Protocol | Source Port Range | Destination Port Range | DSCP |
|---|---|---|---|---|---|
| GWC | XA-Core | All | N/A | N/A | CS6 |
| GWC | SDM | All | N/A | N/A | CS6 |
| GWC | UAS | All | N/A | N/A | CS5 |
| GWC (Unit 0) | GWC (Unit 1) | All | N/A | N/A | CS6 |
| GWC | GWC | All | N/A | N/A | CS6 |
| GWC | CMT | All | N/A | N/A | CS1 |
| CS2000-1 DPT GWC | CS2000-2 DPT GWC | All | N/A | N/A | CS6 |
| GWC | USP | All | N/A | N/A | CS6 |
| XA-Core | GWC | All | N/A | N/A | CS5 |
| SDM | SC | All | N/A | N/A | CS6 |
| SDM | GWC | All | N/A | N/A | CS6 |
| USP | GWC | All | N/A | N/A | CS6 |
| SC | SDM | All | N/A | N/A | CS6 |
| SC | CMT | All | N/A | N/A | CS1 |

**Table 118 QoS in the CS-LAN - Call Processing Subnet Flows**

### 13.4.1.2 QoS for Voice Media Elements

Table 119 illustrates all the flows that originate from the Media Gateway subnet in the CS-LAN. These flows are common for all solutions. The traffic filters derived from the flows described in Table 119 will be applied on interface I/F 2.

**Table 0-77**

| Src. IP Address Range | Dest. IP Address Range | Protocol | Source Port Ranges | Destination Port Range | DSCP |
|---|---|---|---|---|---|
| UAS | CMT | All | N/A | N/A | CS1 |
| UAS | All PVGs/APG | All | N/A | N/A | EF |

**Table 0-77**

| Src. IP Address Range | Dest. IP Address Range | Protocol | Source Port Ranges | Destination Port Range | DSCP |
|---|---|---|---|---|---|
| UAS | GWC | All | N/A | N/A | CS5 |
| CS-LAN PVG | UAS | All | N/A | N/A | EF |
| CS-LAN PVG/APG | GWC | All | N/A | N/A | CS5 |
| CS-LAN PVG/APG | Remote PVGs/APGs | T.38 | 58112 – 64768 | 58112 – 64768 | CS5 |
| | | All | N/A | N/A | EF |
| CS-LAN PVG/APG | PMDM | All | N/A | N/A | CS1 |

**Table 119 QoS in the CS-LAN - Media Gateway Subnet Flows**

### 13.4.1.3 QoS for OAM&P Elements

Table 120 illustrates all the flows that originate from the OAM&P subnet in the CS-LAN. These flows are common for all solutions. The traffic filters derived from the flows that are described in Table 120 will be applied on interface I/F 1.

**Table 0-78**

| Src. IP Address Range | Dest. IP Address Range | Protocol | Source Port Ranges | Destination Port Range | DSCP |
|---|---|---|---|---|---|
| SDM | NOC/OSS | Telnet | 23 | 1024 - 65535 | CS1 |
| | | DNS | 1024 - 65535 | 53 | CS6 |
| | | All | N/A | N/A | AF11 |
| PMDM | All PP15Ks | All | N/A | N/A | CS1 |
| | | FTP | 20-21 | 1024 - 65535 | AF11 |
| PMDM | NOC/OSS | Telnet | 23 | 1024 - 65535 | CS1 |
| | | All | N/A | N/A | AF11 |
| CMT | GWC | All | N/A | N/A | CS1 |
| CMT | SC | All | N/A | N/A | CS1 |
| CMT | UAS | All | N/A | N/A | CS1 |
| CMT | NOC/OSS | Telnet | 23 | 1024 - 65535 | CS1 |
| | | DNS | 1024 - 65535 | 53 | CS6 |
| | | All | N/A | N/A | AF11 |

**Table 120 QoS in the CS-LAN - OAM&P Subnet Flows**

### 13.4.2 Packet Trunking Specific Flows

This Section describes all the flows that are specific to the Packet Trunking IP solution. The following tables show a detailed description of the filtering rules that are required.

Table 121 describes all the Bearer flows that are specific to Packet Trunking IP. The traffic filters described in Table 121 will be applied on interface I/F 2.

**Table 0-79**

| Src. IP Address Range | Dest. IP Address Range | Protocol | Src. Port Ranges | Dest. Port Range | DSCP |
|---|---|---|---|---|---|
| IW-SPM | All PVGs | All | N/A | N/A | EF |
| IW-SPM | All IW-SPMs | All | N/A | N/A | EF |

**Table 121 QoS in the CS-LAN - Media Gateway Subnet Flows Specific to Packet Trunking**

## 13.5 QoS on the Media Gateway Site Router

### 13.5.1 Introduction and Common Flows

The Media Gateway Site router/Layer 3 switch has also the task of marking the packets originating from devices that do not mark already the DSCP according to the quality of service that they require. This marking is done based on the guidelines of Section 13.2.

As previously discussed, the filters that perform marking will be applied on logical interfaces I/F 1 and 2, as shown in Figure 76 below.

Please note that in a Layer 3 switch a logical interface typically includes several physical ports that are configured in the same VLAN.

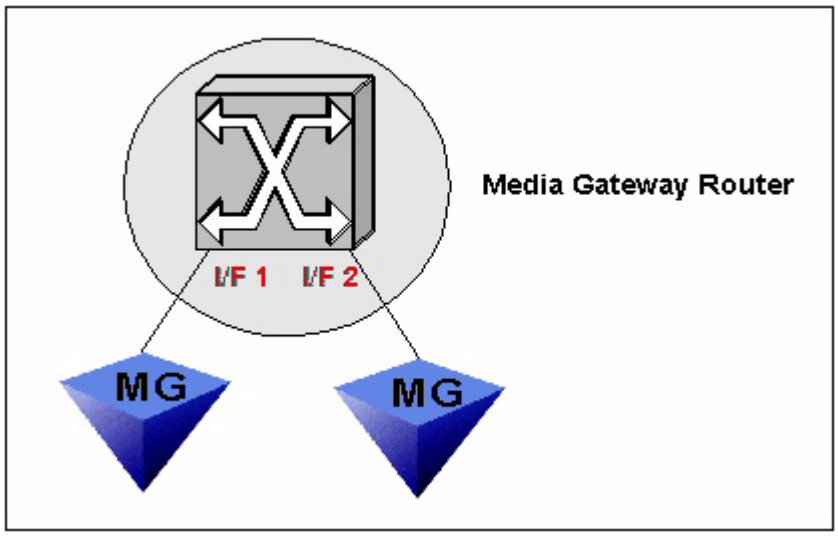



**Figure 76 QoS in the Media Gateway Router**

The following tables show the VoIP flows and a DSCP based on their NNSC (see Section 13.2 for more details) is assigned to each of them.

Table 122 illustrates all the common flows that originate from the Media Gateway site. The traffic filters derived from the flows described in Table 122 will be applied on interfaces I/F 1 and 2.

**Table 0-80**

| Src. IP Address Range | Dest. IP Address Range | Protocol | Src. Port Ranges | Dest. Port Range | DSCP |
|---|---|---|---|---|---|
| PVG | GWC | All | N/A | N/.A | CS5 |
| PVG | UAS | All | N/A | N/.A | EF |
| PVG | All PVGs/APGs | All | N/A | N/A | EF |
| | | T.38 | 58112 – 64768 | 58112 – 64768 | CS5 |
| PVG | PMDM | All | N/A | N/A | AF11 |

**Table 122 QoS in the Media Gateway Router – Common Flows**

## 13.5.2 Packet Trunking Specific Flows

This Section describes all the flows that are specific to the Packet Trunking IP solution. The following tables show a detailed description of the flows that leave the Media Gateways site.

All the filters described in Table 123 will be applied to interfaces I/F 1 and 2.

**Table 0-81**

| Src. IP Address Range | Dest. IP Address Range | Protocol | Src. Port Ranges | Dest. Port Range | DSCP |
|---|---|---|---|---|---|
| PVG | IW-SPM | All | N/A | N/A | EF |

**Table 123 QoS in the Media Gateway Router – Flows Specific to Packet Trunking**

# 14.0 Network Time (NTP) & Clock Synchronization

Unlike the TDM network, common clock synchronization of all elements is not required. Clock synchronization is required for SS7 gateways and synchronization of the DS0 channels on T1/E1 carriers.

The Network Time Protocol, specified in RFC 1305, is the most widely used protocol for network elements clock synchronization. The Simple Network Time Protocol, specified in RFC 1769, is a simplified access strategy for servers and clients that do not require the degree of accuracy that NTP provides. An NTP Server serves time to clients and an NTP Client gets time responses from an NTP server or servers and uses this information to calibrate their clock. Time Of Day is derived from the NTP source.

It is recommended to have a minimum of 2 NTP servers in the OAM CS-LAN where all routers and gateways acting as NTP clients synchronize from. These 2 NTP servers should synchronize off of A MINIMUM OF 2 independent customer provided Stratum 1 clock source (such as the Symmetricom NTS-150 server) with 3 servers recommended when possible. The NTPd can run on any reliable server such as the Sun E250 used by PMDM, a Netra 1400 (SSPFS) and the SDM since it is a lightweight application. The 2 NTP Stratum 1 servers should not be co-located, should be powered from two different sources, and redundant routes to them should be available to avoid any single point of failure.

The following guideline applies to elements directly connected to the CS LAN (i.e., the Passport 8600) that utilize the SDM's NTP Server capabilies..

***Note:*** A network element's NTP client should use the SDM address that is in the VLAN in which the NTP client resides. For example, the SAM21 SC NTP client resides in the CALLP VLAN, therefore it should use the SDM address that is configured in the CALLP VLAN.

***Note:*** The instructions for setting up NTP across the various elements is for reference and should be confirmed with the component IM (Installation Manual). These methods include additional information on how to manage and set timezones.

## 14.1 XA-Core Call Server

For offices not equipped with an ENET or no peripherals subtending an ENET, setting the tuple to Master Internal in table SYNCCLK is recommended. For offices with peripherals subtending the ENET, the Message Switch can be synchronize to an external source based on local requirements in order to align the DS0's and setting the tuple in table SYNCLK to Master External, or, synchronization can be retrieved from a dedicated pair of DS0's and setting the tuple in table SYNCCLK to Slave.

The TOD (Time of Day) is provide on XA-Core by the redundant OC3 CMIC packlet located on the XA-Core shelf. These provide a 10 msec reference used by Call Processing, Billing, maintenance and time stamped events. Also, the SuperNode internally generates the office clock reference for the rest of the system in accordance with Stratum II, Stratum 2.5, or Stratum III standards when equipped with an external frame. Stratum I requires the Master Reference Frequency frame, Stratum II requires the Remote Oscillator shelf in an IOE frame equipped with the Stratum II circuit packs and Stratum III capability has been built into the Supernode XA-Core. The TOD can also be synchronized from an external NTP server.

This is achieved by setting tuple SNTP_CLIENT in table OFCENG to Y and using the NTPCI CIBINCOM to start (startntp) and set the TOD to the NTP time (settimetontp) and query the TOD (querynntptime). Table DSTTABLE can also be provisioned to provide automatic switch to Daylight saving time.

The XA-Core will use the IP address from table EXNDINV and port 123 to send an NTP query to the SDM and listens on port 9701 for the response. When the TOD drifts or becomes unavailable, a SOS log is generated on the core.

## 14.2 CS2Kc (Compact) / Storm

The compact CS2K requires two NTP sources configured via the SAM21EM Shelf Controller provisioning panel. The SAM21 shelf provides clocking to both the 3PC and Storm cards. This time reference is used to for Time Of Day on the switch by call processing, maintenance and billing software.

Succession SAM21 Manager > Configuration > Add/Modify > SAM21 Network Element

- **a.** Primary NTP
- **b.** Secondary NTP
- **c.** Timezone Offset.

## 14.3 IW-SPM

The IW-SPM receives it's time of day from the CS2K. For Hybrid offices using the Interworking SPM, clock synchronization is require and this can be achieved by setting the CLOCK-TAB-KEY in table SYNCCLK to Master External and use an external composite clock (usually via a GPS clock system connected to the MS NT9X54 clock card) in order to provide synchronization to trunk gateways subtending the ENET. The composite clock provides a 64KHz clock reference in order to align the trunk gateway T1's and does not use UTC.

The Sync Resource Module (Sync RM), NTLX44AA, provides an alternative timing and synchronization interface for the Spectrum Peripheral Module (SPM), Interworking SPM (**IW SPM ATM only**), or MG4000. A Sync RM receives clocking information via DS1 twisted pairs from a BITS DS-1 timing reference. Each Sync RM has four DS1 inputs (two available for test purposes) and two DS1 outputs; two inputs are dedicated as separate BITS clock inputs, the other two inputs are available for monitor/test equipment. The Sync RM selects the best of the two input timing references and using a Digital Frequency-Locked Loop with a Direct Digital Synthesis (DDS) engine driven by a Stratum 3E oscillator, creates a disciplined 8 KHz output reference signal. The disciplined output reference signal is tracked to each Common Equipment Module (CEM) in the SPM shelf. The CEM uses this reference signal to transmit the phase/frequency control information to the MS, which, in turn, distributes this BITS synchronized clock to the other system components, for use in timing all synchronous carriers.

If optional Sync RM is provisioned, one NTLX44AA Sync RM circuit pack is required in each of two IW SPM ATM. The Sync RM pack must be provisioned in slot 6 of the lower shelf only.

## 14.4 Gateway Controllers & Shelf Controllers in SAM21 shelf

The GWC and SC require a NTP clock reference in order to provide it with Time-Of-Day reference used for time stamping events. The NTP source is independent and not required for call processing. Each GWC and SC will have a T42 parameter set in the bootptab file when provisioned.

Primary and secondary NTP servers are provisioned in the SAM21EM Shelf Controller provisioning panel. If left blank, the IP address is defaulted to the CS2K Management tools server.

## 14.5 Passport 8600

The PP8600 can make use of an NTP server for Time-Of-Day. This is used for the timestamp reference on log reports only and performs no synchronization. Multiple NTP servers can be configured via the NTP level in the PP8600. It is recommended to use 3 NTP servers. It is important that each server being used for synchronization runs the same stratum level. Timezone are also supported and configured as part of the bootconfig.

Example on how to configure an NTP server

:# config ntp server create 47.142.86.27

:# config ntp server create 47.142.86.210

To configure a timezone and DST

# config bootconfig tz info

tz dst-end M10.4.0/0200

tz dst-name "edt"

tz dst-offset 60

tz dst-start M4.1.0/0200

tz offset-from-utc 300

tz name "est"

TIMEZONE=est:edt:300:M4.1.0/0200:M10.4.0/0200:60

To Monitor the NTP stats

:# show ntp server stat

## 14.6 Universal Audio Server

The UAS NTP is built on top of Windows Net Time. The NTP time can be provisionned at the DOS prompt and at the GUI for the CG6000 node config.

> NET TIME /SETNTP:"IP_Address_of_server_1  IP_Address_of_server_2"

> NET TIME /QUERYSNTP

## 14.7 CS2K Management Tool server (SSPFS, SESM, APS, NPM & LMM/TMM)

A time zone and NTP server is configured during the SSPFS platform configuration steps via the cli ntp_conf option. This time is then used for all applications running on top of SSPFS.

## 14.8 SDM (CS2E)

It is recommended to run a NTP server on the SDM. The SDM can act as a server or a peer. It also uses NTP for logging. NTP on the SDM is not required for billing records. If DTE [DCE Distributed Time Service] is installed and running, it will need to be decommissioned for NTP to work. The NTP can be configured via the sdmconfig ntp level and monitored via the sdmmtc ntp level.

```
# sdmconfig

# step <Network Time Protocol>

# add   < server > < description, hostname, IP address >

% Attempting to remove components: dts_cl

To Monitor

# sdmmtc ntp
```

## 14.9 LPP/FLPP/FLIS SS7 gateways

Where DS0 interfaces are employed, a master timing reference is required. The preferred method is to use a Timing Supply Generator (TSG), also known as Signal Reference Distribution (SRD), which supplies all equipment with the required timing signal. For reliability, the components of the TSG are fully duplicated with hot standby capability. In an SSP/SP office, the TSG can be an inexpensive type, of low Stratum standard, without impacting reliability of the CCS7 links. The Stratum standard of the TSG does not have to agree with the Stratum standard of the SSP/SP office. The TSG is to be supplied by the telco.

## 14.10 USP & USP-Compact IP SS7 Signalling Gateway

The USP/ USP-Compact blade requires an 8 kHz timing signal for synchronization of the T1 or E1 signal. The timing signal is used for clocking of the outgoing data stream. The timing signal may be obtained by:

- Loop timing: where the timing is derived from the incoming data signal and used to drive the outgoing data stream.
- External timing: where an 8 kHz reference signal is brought in via the 2nd RJ45 input on the mpmc8260. The external timing input should come from DS1 or DS30 BITS source and should provide a stratum 3 or stratum 3E reference

The USP / USP-Compact uses the time received from the SNTP server for the time stamping of Logs and system events. As there is no billing or accounting resident on the USP-Compact, the need for time of day precision is not as exacting as nodes within the network that have those func-

tions. The USP-Compact expects to receive UTC time from the server. Time Zone information is provisioned at the USP-Compact GUI. The USP-Compact applies the Time Zone information to the UTC time received from the SNTP server to derive the current local time. Only a single SNTP server IP address is expected or supported for use by the USP-Compact for TOD synchronization.
Using the Administration Panel, choose “Set Date/ Time” and enable SNTP.

## 14.11 PVG Trunk Gateways (Passport 15000 Voice Gateway)

The PVG15K requires synchronization on the trunk in order to minimize slips. The Clocking Source attribute in the PVG is set to local by default and requires an external clock source which is synchronized with the telephony network. This source can be provided by a GPS clock system. Alternatively, the Clocking Source can be retrieved by dedicating a DS0 as a timing link when the other end is able to provide a reliable timing source.

The PVG15K also makes use of NTP for Time of Day. If you do not specify a network time server, Passport automatically attempts to synchronize with the PMDM workstation. You can also configure up to 10 NTP servers using the add Time Server and set Time Server commands in the PVG.

## 14.12 PMDM & Various other EM clients

PMDM supports both a client NTP and running a server. Various other EM clients running on Sun servers or workstations usually support running either a client or server NTP application.

Example of a NTP server running on a Sun Ultra80 (47.142.86.210)

%% type “man xntpd” for more information

ctxip% more /etc/inet/ntp.conf

# NTP server configuration for RTP4. ## Synchronized off of 3 main servers. ##

server ntp-rtp-3-us-nortel.com

server ntp-rtp-1.us.nortel.com

server ntp-rtp-2.us.nortel.com

driftfile /var/ntp/ntp.drift

statsdir /var/ntp/ntpstats/

# access control

restrict default nomodify nopeer

# completly trust your own machine

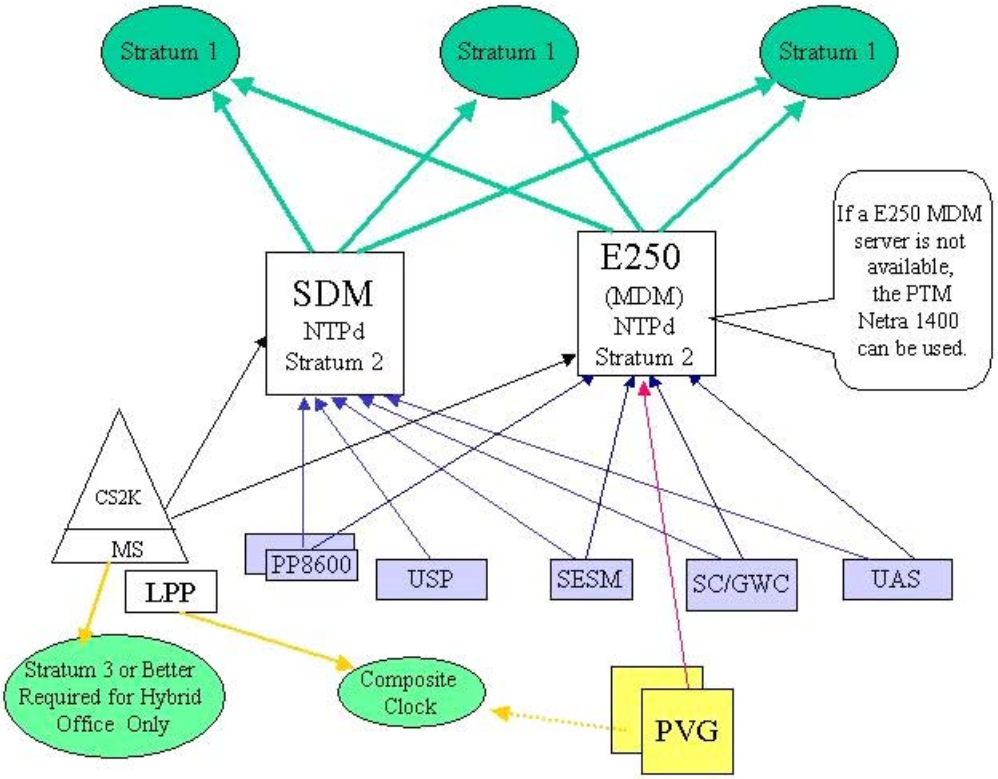
restrict 47.142.86.210  # restrict local host

restrict 127.0.0.1  # local host loopback

## 14.13 Summary

| NEs | NTP Server Capable | NTP Client Supported | Number of NTP sources possible | Primary NTP source | Secondary NTP source | Alternate Secondary NTP source | Secure NTP supported | Proposed Base Time Zone | NTP Sync rate |
|---|---|---|---|---|---|---|---|---|---|
| XA-Core | No | Yes | 1 | SDM | N/A | N/A | | Local | 5 min |
| UAS | No | Yes | 2+ | SDM | Netra1400 | N/A | Yes | Local | 45min/8hrs |
| USP | No | Yes | 1 | SDM | N/A | N/A | No | Local | 5 min |
| GWC | No | Via SAM21 | 2 | SDM | Netra1400 | MDM | | Local | init/24 hrs |
| MG9K | No | Yes | 1 | SDM | Netra1400 | MDM | No | Local | 10 min |
| PP8600 | No | Yes | 2+ | SDM | Netra1400 | MDM | Yes | Local | 15 min |
| SAM21 SC | Yes | Yes | 2 | SDM | Netra1400 | MDM | Yes | (Local) | At init |
| IP IW SPM | No | No | (Core) | XA-Core | N/A | N/A | N/A | Local | N/A |
| MG4K | No | No | (Core) | XA-Core | N/A | N/A | N/A | Local | N/A |
| Storm | No | Yes | 3 | SDM | Netra1400 | MDM | | Local | |
| 3PC | No | Yes | 2 | SDM | Netra1400 | MDM | | Local | |
| PP7000/15000 | No | Yes | 10 | MDM | backup MDM | backup MDM | | Local | |
| | | | | | | | | | |
| **EMSs** | | | | | | | | | |
| SDM (Platform) | Yes | Yes | 3+ | Cust NTP | Cust NTP | Cust NTP | Yes | Local | 64-10024 sec |
| SSPFS (Netra1400 CMT Platform) | Yes | Yes | 1(3) | Cust NTP | Cust NTP | Cust NTP | Yes | Local | |
| SSPFS (MG9k EM/Mid-tier) | No | Yes | 1(3) | SDM | Netra1400 | | Yes | Local | |
| MDM, MDP (Platform) | Yes | Yes | | Cust NTP | Cust NTP | Cust NTP | | UTC | |

NTP servers should be setup for unicast messaging between element client and server.


Stratum 1
Stratum 1
Stratum 1
SDM
NTPd
Stratum 2
E250
(MDM)
NTPd
Stratum 2
If a E250 MDM server is not available, the PTM Netra 1400 can be used.
CS2K
MS
LPP
PP8600
USP
SESM
SC/GWC
UAS
Stratum 3 or Better Required for Hybrid Office Only
Composite Clock
PVG

# 15.0 Element Distance Limitations

The capacity and performance results discussed in this document are based on distance limitations between elements located in and between the Hub, the Trunk Gateways Site, and CS-LAN. Some of these distance limitations, which are based on communications media and port/line speeds, are captured in Table 124. Note that some distance limitations remain ambiguous due to the variety of configurations possible for the different communications media available for a particular solution.

**Table 124 Distance Limitations for Network Elements**

| **Element A** | Element **B** | Communications **Medium** | Port/Line **Speed** | Distance **Limitation** |
|---|---|---|---|---|
| VRRP Passport 8600 (Master) | VRRP Passport 8600 (Slave) | 100 BaseT Fast Ethernet<br>• CAT5<br><br>Gigabit Ethernet<br>• Single mode 10 microns<br>• Multi-mode 62.5 microns<br>• Multi-mode 50 microns | 100 Mbps<br><br>1 Gbps | 100 meters<br><br>5 km<br>275 meters<br>550 meters |
| CS-LAN Passport 8600 | XA-Core, UAS, GWC, SDM | 100 BaseT Fast Ethernet<br>• CAT5 | 100 Mbps | 100 meters |
| CS-LAN Passport 8600 | Compact 3PC & Storm | 100 BaseT Fast Ethernet<br>• CAT5 | 100 Mbps | 100meters |
| Compact 3PC | Compact 3PC | Multimode fiber 62.5 microns | 1 Gbps | 275 meters |
| CS-LAN Passport 8600 | OAM&P Platforms | 100 BaseT Fast Ethernet, Gigabit Ethernet, or remoted | Depends on medium chosen | Depends on medium chosen |
| CS-LAN Passport 8600 | Co-located Trunk Gateway Site with M40 router | Gigabit Ethernet<br>• Single mode 10 microns<br>• Multi-mode 62.5 microns<br>• Multi-mode 50 microns | 1 Gbps | 5 km<br>275 meters<br>550 meters |

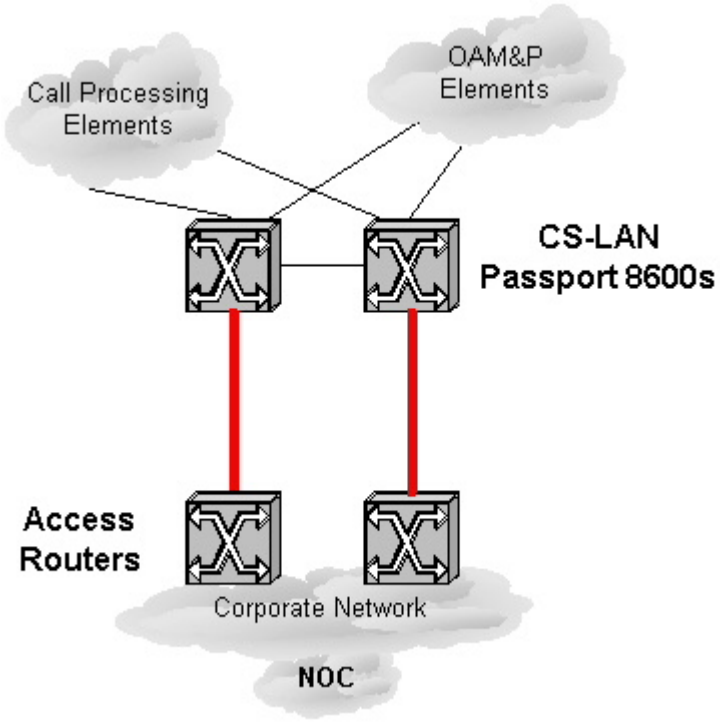
**Table 124 Distance Limitations for Network Elements**

| | | | | |
|---|---|---|---|---|
| CS-LAN<br>Passport 8600 | Core Router and/or Remote Trunk Gateway Site | Gigabit Ethernet<br>• Single mode 10 microns<br>• Multi-mode 62.5 microns<br>• Multi-mode 50 microns | 1 Gbps | 5 km<br>275 meters<br>550 meters |

# 16.0 Connectivity with Remote Network Operations Center (NOC)

This section describes the logical connectivity between the CS-LAN and the customer's Corporate Network (see Figure 77).

**Figure 77 Typical CS-LAN Configuration**




## 16.1 Connectivity via a pair of existing Access Routers: No VPN

If the OAM&P subnet and the NOC are in the same addressing domain, an end-to-end connection can be established directly, typically exploiting the customer's Corporate Network.

This is required because, for an improved security, the NOC should not communicate directly with the Call Processing the Media Gateway subnets. Instead, the NOC should only communicate with the OAM&P servers that then exploit the knowledge that the Passport 8600 has of the other subnets to connect to the Call Processing elements. In addition, a routing strategy needs to be enabled on the CS-LAN routers (Passport 8600) to be sure that they know how to reach the NOC in the Corporate Network. This can be obtained with dynamic routing. This solution will be discussed below.

It is important to note that the recommended configuration requires redundant Access Routers with dual links, in addition to the standard dual Passport 8600 configuration in the CS-LAN. The Access Routers should also be multi-homed to two distribution Routers in the customer's Corporate Network to avoid a single point of failure.

### 16.1.1 Dynamic Routing

Dynamic routing is the recommended option. It is suggested to configure a VLAN on each of the CS-LAN routers (Passport 8600) for the sole scope of interfacing logically with one of the access

routers of the Corporate Network. For this reason, it is suggested to use the same addressing scheme that the customer currently uses to interconnect routers in its Corporate Network.

The routing information for reaching the NOC is obtained by enabling a dynamic routing protocol on the interfaces that are connected to the customer's Access network. In addition, the access routers should redistribute the OAM&P subnet into the IGP running in the Corporate Network. This will guarantee end-to-end connectivity between the NOC and the CS-LAN.

Please note that the CS-LAN routers (Passport 8600) support both RIP and OSPF. Nortel Networks strongly recommends the use of OSPF for a faster fail-over.

In such a configuration, for security reasons, it is recommended not to redistribute the Call Processing subnet (and Media Gateway subnet, if present for IP Succession solutions) into the IGP of the Corporate Network. This can be achieved easily on the Passport 8600 via policy routing. Alternatively, this function can be also be implemented on the Access Routers.

### 16.1.2 Static Routing

Static routing is an alternative way to connect the Corporate Network to the CS-LAN. Given the more complex provisioning and the possibility of black-holes, it is not the recommended solution and it should only be used when dynamic routing cannot be used.

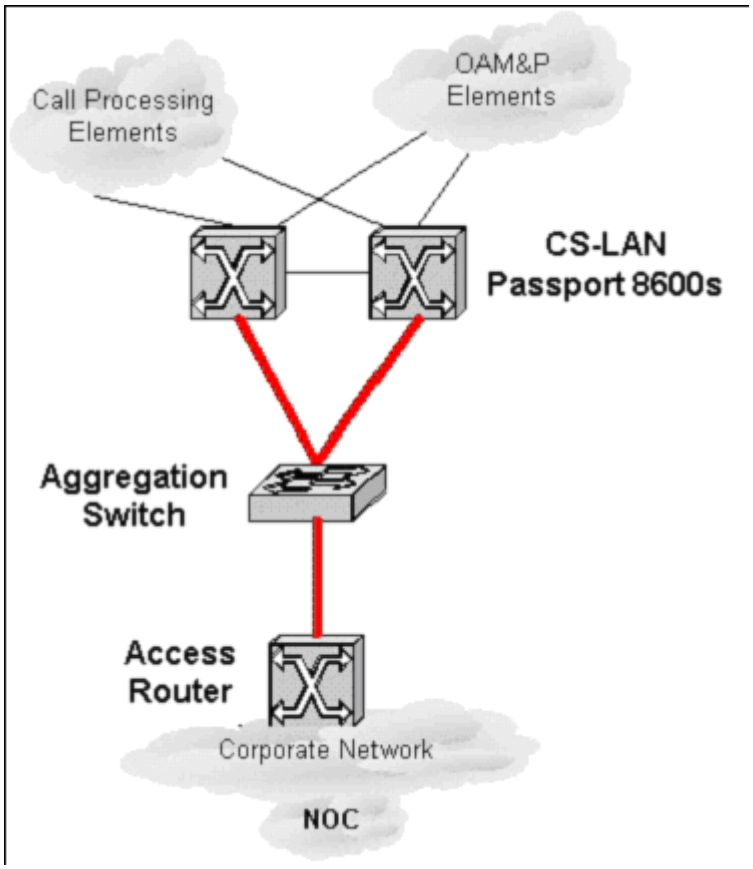
To optimize the fail-over times and the overall performance, the following guidelines should be observed:

- In case not already present, a VLAN/subnet should be created (with a 30 bit subnet mask) and assigned to the MLT interfaces. Creating an interface that does not belong to the Call Processing or OAM&P VLAN is meant for optimizing the Layer 3 fail-over mechanism needed for the second static route on the two Passports 8600 to become active if the link to the Aggregation Switch were to fail.
- Two VLANs/subnets (one per Passport 8600) should be created and assigned to the interfaces toward the corporate network. This VLAN would typically be assigned to a subnet with a netmask of 255.255.255.252.
- The MLT across the two 8600s is not assigned to the VLANs on the two Passport 8600s used to connect to the Access Routers.
- Spanning tree is disabled on the two 8600s ports going to the Access Routers.
- Two default routes are configured on Passport 8600-1. The first default route points to Access Router-1 as the next hop with a cost of 10. The second default route points to the Passport 8600-2 as the next hop with a cost of 15. With such a configuration, if the link between 8600-1 and Access Router-1 fails, the first default route is removed from the routing table and the second default route takes effect. Therefore all routed traffic still can exit the CS-LAN OAM&P subnet via Passport 8600-2.
- Two default routes are configured on Passport 8600-2. The first default route points to the Access Router-2 as the next hop with a cost of 10. The second default route points to the Passport 8600-1 as the next hop with a cost of 15. With such a configuration, if the link between 8600-2 and Access Router-2 fails, the first default route is removed from the routing table and the second default route takes effect. Therefore all routed traffic still can exit the CS-LAN OAM&P subnet via Passport 8600-1.
- A static route is configured on each Access Router that points to Passport 8600-1 and 8600-2 respectively as a next hop to reach the OAM&P subnet in the CS-LAN.

## 16.2 Connectivity via a single Access Router: No VPN

In rare cases, because of the extra cost, some customers might only have one Access Router at the edge of the corporate network. This topology is shown below in Figure 78.

**Figure 78 Single Router Configuration**




In such a configuration, the Aggregation Switch aggregates the two links coming from the two Passport 8600s and switches traffic to the Access Router.

This configuration is not recommended unless absolutely necessary because It is easy to see that such topology has two single point of failures (the Access Router and the Aggregation Switch). Again, a routing strategy needs to be enabled on the CS-LAN routers (Passport 8600) to be sure that they know how to reach the NOC in the Corporate Network. The two possible configurations are described below.

### 16.2.1 Dynamic Routing

Dynamic routing is the recommended option. It is suggested to configure a VLAN on the CS-LAN routers (Passport 8600) for the sole scope of interfacing logically with the access router of the Corporate Network. For this reason, it is suggested to use the same addressing scheme that the customer currently uses to interconnect routers in its Corporate Network.

The routing information for reaching the NOC is obtained by enabling a dynamic routing protocol on

the interfaces that are connected to the customer's Access network. In addition, the access routers should redistribute the OAM&P subnet into the IGP running in the Corporate Network. This will guarantee end-to-end connectivity between the NOC and the CS-LAN.

Please note that the CS-LAN routers (Passport 8600) support both RIP and OSPF. Nortel Networks strongly recommends the use of OSPF for a faster fail-over.

In such a configuration, for security reasons, it is recommended not to redistribute the Call Processing subnet (and Media Gateway subnet, if present for IP Succession solutions) into the IGP of the Corporate Network. This can be achieved easily on the Passport 8600 via policy routing. Alternatively, this function can be also be implemented on the Access Routers.

### 16.2.2 Static Routing

Static routing is an alternative way to connect the Corporate Network to the CS-LAN. Given the more complex provisioning and the possibility of black-holes, it is not the recommended solution and it should only be used when dynamic routing cannot be used.

To optimize the fail-over times and the overall performance, the following guidelines should be observed:

- In case not already present, a VLAN/subnet should be created (with a 30 bit subnet mask) and assigned to the MLT interfaces. Creating an interface that does not belong to the Call Processing or OAM&P VLAN is meant for optimizing the Layer 3 fail-over mechanism needed for the second static route on the two Passports 8600 to become active if the link to the Aggregation Switch were to fail.
- A VLAN/subnet should be created and assigned to the interfaces toward the corporate network. This VLAN would typically be assigned to a subnet with a netmask of 255.255.255.248. A VRRP instance is created on this VLAN facing the Access Router.
- The MLT across the two 8600s is not assigned to the VLAN on the two Passport 8600s used to connect to the Aggregation Switch. Therefore the VRRP multicast communication between the master and backup 8600s is forced to happen through the Aggregation Switch.
- Spanning tree is disabled on the two 8600s ports going to the Aggregation Switch. It is also disabled on the Aggregation Switch and the Access Router.
- The three ports on the Aggregation Switch that are used by the system (two ports going to the 8600s and one port going to the Access Router) need to be removed from the default VLAN and assigned to a new VLAN.
- Two default routes are configured on Passport 8600-1. The first default route points to the Access Router as the next hop with a cost of 10. The second default route points to the Passport 8600-2 as the next hop with a cost of 15. With such a configuration, if the link between 8600-1 and the Aggregation Switch fails, the first default route is removed from the routing table and the second default route takes effect. Therefore all routed traffic still can exit the CS-LAN OAM&P subnet via Passport 8600-2.
- Two default routes are configured on Passport 8600-2. The first default route points to the Access Router as the next hop with a cost of 10. The second default route points to the Passport 8600-1 as the next hop with a cost of 15. With such a configuration, if the link between 8600-2 and the Aggregation Switch fails, the first default route is removed from the routing table and the second default route takes effect. Therefore all routed traffic still can exit the CS-LAN OAM&P subnet via Passport 8600-1.
- A static route is configured on the Access Router that points to the VRRP address of the Passport 8600s as a next hop to reach the OAM&P subnet in the CS-LAN.

## 16.3 Remote Access via Contivity

It is important to have a remote access strategy to be able to connect to the CS-LAN. This strategy can be used for remote access from the NOC or from Nortel Networks' technical support.

To achieve this, two ways of interconnecting securely the CS LAN and the NOC/OSS exist. Both require the use of IPSec tunneling and the use of a tunneling device (i.e., the Contivity line in the case of Nortel Networks portfolio).

### 16.3.1 Logical Separation between CS-LAN subnets

Before examining the tunneling strategies, let's review the reachability and the connectivity of the CS LAN. Figure 79 shows the typical CS LAN configuration.

- The blue lines represent the elements connected to VLAN 1 (Call processing elements).
- The red lines represent the elements connected to VLAN 2 (OAM&P elements).
- The green lines represent the elements connected to VLAN 3 (Gateway elements, if present).

***Note:*** The NOC/OSS access to the CS-Lan has its own VLAN. See section "2.0 CS-LAN Common Components and Subnet Configuration" on page 25.

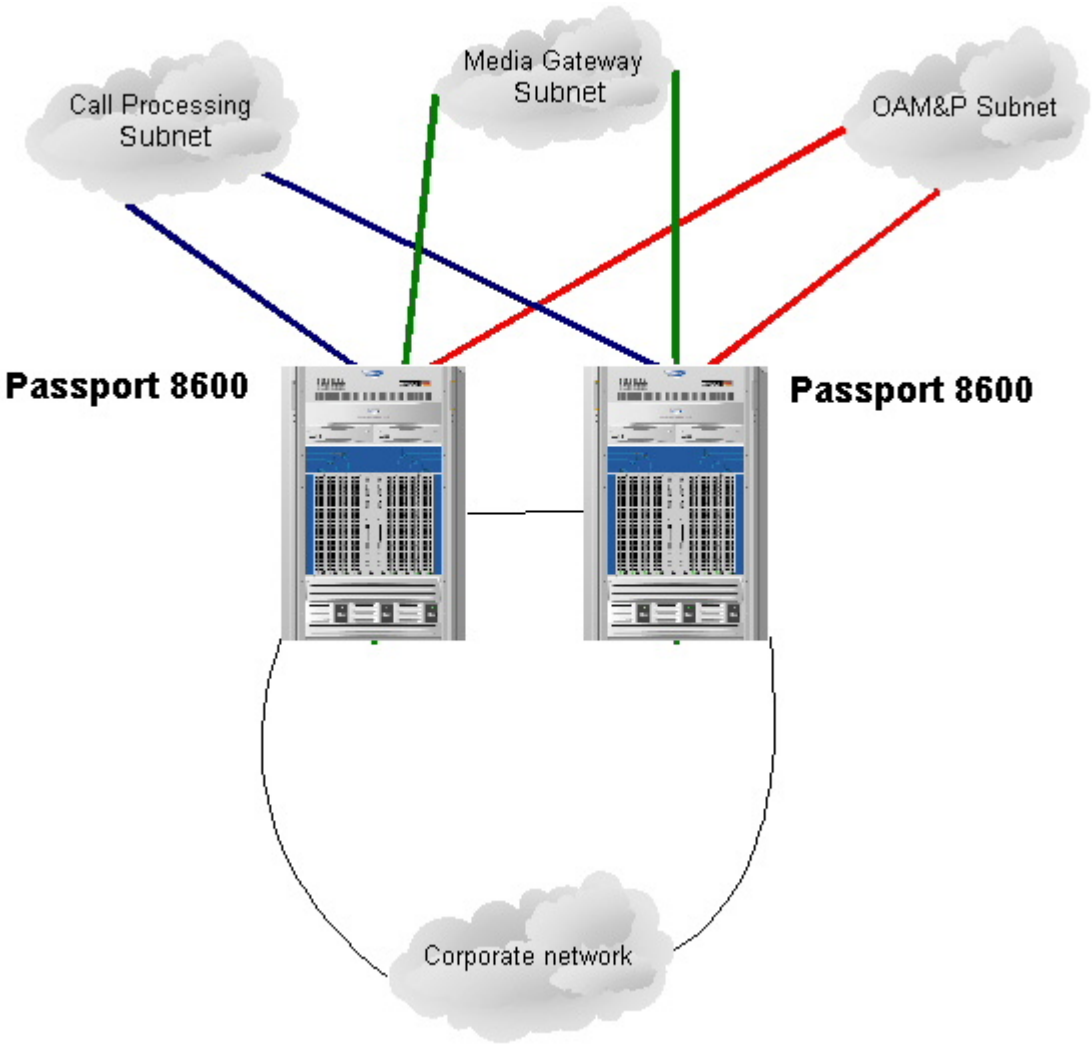
The traffic streams belonging to the different VLANs are completely separated and protected from each other.

In addition, since the Passport 8600s are the default gateways for all the CS LAN elements, each device in VLAN 1 can reach each element in VLAN 2 and 3; each device in VLAN 2 can reach each element in VLAN 1 and 3; each device in VLAN 3 can reach each element in VLAN 2 and 1. The Passport 8600 routes the inter-VLAN traffic, allowing seamless connectivity.

This means that any OAM&P client residing in the corporate network can talk with the OAM&P server in the CS LAN with no issues (see Figure 79). The OAM&P server then has perfect connectivity to the Call Processing elements via the Passport 8600.

What an OAM&P client cannot do from the corporate network is communicating directly with the Call Processing elements because these elements reside in a subnet that uses private addresses. The following Chapters will describe how to obtain this type of connectivity by using VPN gateways (Nortel Networks Contivity Series) and VPN clients.

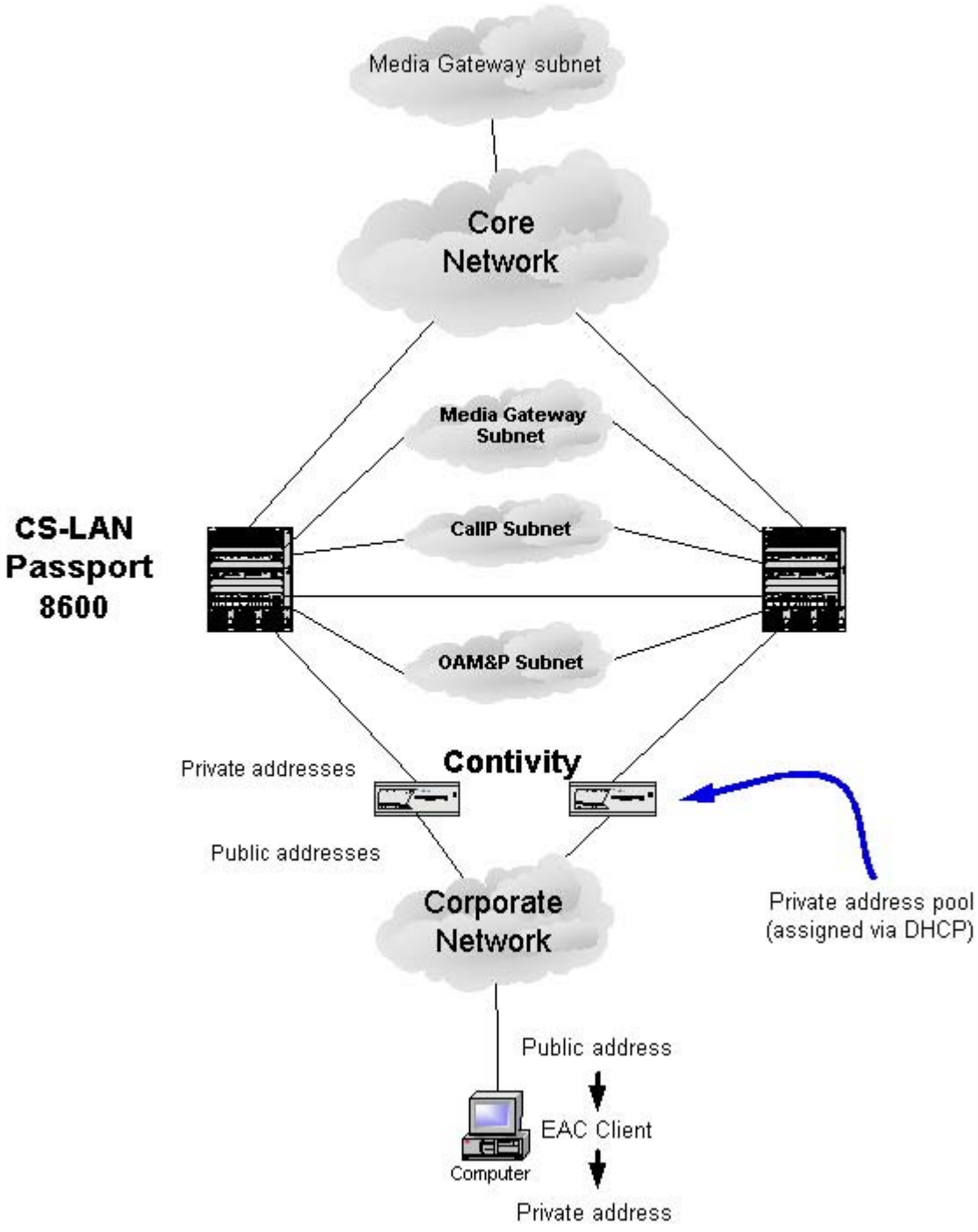
**Figure 79 VLAN Separation in the CS-LAN**




### 16.3.2 End-user to Branch Tunnel

An End-user to Branch tunnel allows an operator to connect to the CS-LAN subnet by using only an IPSec client, therefore minimizing the hardware required in the NOC/OSS.

**Figure 80 End-User to Branch Tunnel**




When the client is run, an authentication process (via username and password, via RADIUS or via Digital Certificates) takes place and an IP address in the private realm is assigned to the client if the user is authorized. At the same time, the routing table of the client machine is updated with the private domain routes and has full knowledge of the CS-LAN. This configuration is show in Figure 80.

For a better security, the following recommendations are suggested:

- Usage of strong passwords with frequent mandatory changes.
- Usage of a SecureID strategy as an option for providing stronger authentication if tunneling from untrusted location.
- Usage of the Contivity packet filtering/firewalling features to restrict all flows coming through the tunnel.

### 16.3.3 Branch to Branch Tunnel

An IPSec Branch-to-Branch tunnel allows a VPN to be built between the CS LAN subnets and NOC/OSS by using four (for redundancy) tunneling devices (i.e., Contivity series).

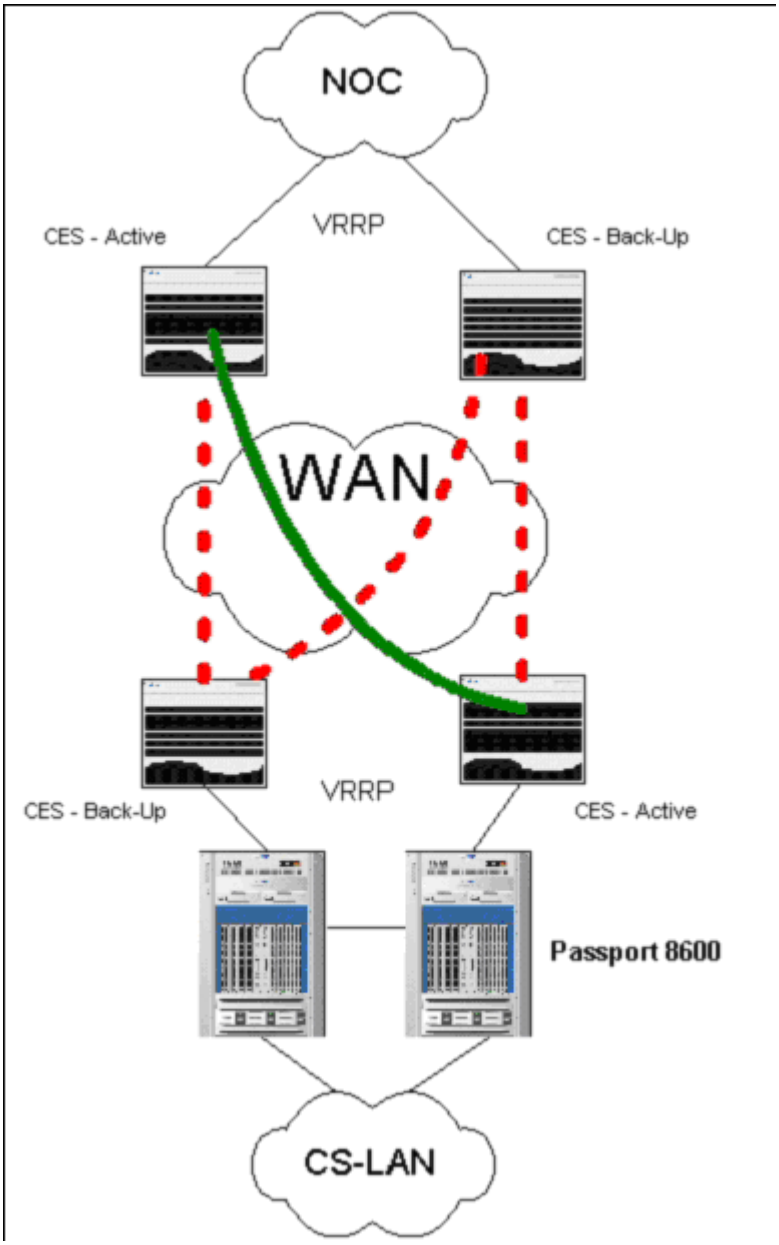
Figure 81 illustrates this network scenario. In such topology VRRP is the protocol used to guarantee LAN redundancy and provide a permanent default gateway to the CS LAN devices and, possibly, to the NOC/OSS devices.

WAN redundancy is achieved by using OSPF. Four logical links (obtained via IPSec branch-to-branch tunnels) interconnects the Contivities. OSPF is running with different OSPF metrics on the tunnels and only one tunnel at a time is used to forward traffic (the one with lower cost). If the active Contivity goes down, OSPF will reconverge and all traffic will be rerouted to the former back-up Contivity.

Again, for a better security, the following recommendations are suggested:

- Usage of the Contivity packet filtering/firewalling features to restrict all flows coming through the tunnel.

**Figure 81 Branch-to-Branch Tunnel**



# 17.0 Appendix: CS-LAN Cabling Guidelines

Nortel Networks recommends that the following cabling guidelines be taken into consideration in order to minimize any cabling issues during the installation of this CS2K Solution. We have verified that when these guidelines are followed, the IP message loss in the CS-LAN can be better than 1 in 109.

- Use High quality pre-manufactured CAT5 cabling.
- Verify all cables with a cable tester before installation.
- Maintain at least 2ft distance between RF/AC cabling and the Ethernet cabling.
- Keep Ethernet cabling away from EMF generating devices, i.e. fans.

Below are some troubleshooting tips to consider if any cabling issues arise while installing this CS2K Solution.

In regards to reducing noise on Ethernet lines:

- Move data cables away from possible sources of interference. See ANSI/EIA/TIA-569, Commercial Building Standards for Telecommunications Pathways and Spaces, which provides guidelines for separating data cables from common sources of noise.
- Move interference sources away from data cabling. Change the location of microwave ovens, copiers, etc., if possible.
- Install a better grade of cable. If you are using UTP, install Category 5, even if the application only requires Category 3.
- Maintain cable pair twist up to the point of termination. Category 5, for example, requires that twists be maintained to within 13 mm (0.5 in.) of the point of termination.
- Make sure there are no split pairs.
- Maintain separate cross-connects for voice and data.

In regards to cable integrity:

- Too Short - Verified via a cable tester, usually indicates an open or short somewhere in the cable.
- Too Long - Make sure the Ethernet cables do not exceed the 100m maximum length limitations.

# 18.0 Appendix: Configuring the Passport 8600

The Passport 8600 is a routing switch that allows both Layer 2 and Layer 3 functionality in a single box. This capability provides varying configuration options based on the desired functionality. The following sections outline simple Management IP address assignment as well as Layer 3 configuration and may be used as a starting guideline.

The Passport 8600s used for this configuration, was equipped with the following switch modules:

**Table 0-82**

| Qty | Module description | Slot # |
|---|---|---|
| 1 | 8691SF Switch Fabric Module | 5 |
| 2 | 8632TXE Module | 1,2 |

**Table 125 Passport 8600 Switch Modules in Example**

***Note:*** The slot assignment used in this example is not to be interpreted as a guideline for which slot to use. If such a guideline is found in the installation method, it should be followed

Prior to any configuration attempts you need to connect to the switch. Since the switch does not have an IP address yet, you need to use the Console Serial Port on the 8691SF module to access it. A laptop or PC with a terminal emulator application such as HyperTerminal, and a serial cable with two female DB-9 connectors are required for this connection. Use the serial cable to connect the PC through its serial port/com to the Passport 8600 Console Serial Port.

**Use the following settings when you set up your serial port:**

9600 bps,

8 data bits,

no parity,

one stop bit,

and none for flow control.

**Table 0-83**

| Note: For further details on configuring the PP8600, refer to the documentation located here: http://worcester.us.nortel.com/Products/p8600/ |
|---|

## 18.1 Setting the Runtime and Configuration File Choices

It is required for the reliability of the system that the primary, secondary, and tertiary runtime and configuration file choices be set appropriately. The choices for the locations of the files can be:

- in flash memory
- on the pcmcia card
- on a remote database server

Use the following commands to set the file choices:

config bootconfig choice <boot-choice> image-file <filename>

config bootconfig choice <boot-choice> config-file <filename>

where:

<boot-choice> specifies which boot choice {primary|secondary|tertiary}

<filename> specifies the filename, a.b.c.d:<file> | /pcmcia/<file> | /flash/<file>

i.e.config bootconfig choice primary config-file "/flash/config.cfg"

config bootconfig choice primary image-file "/flash/p80a3120.img"

## 18.2 Assigning an IP Address to the Management Port

You must assign an IP address to the Management port before you can use it for out-of-band management.

Use the following command to assign an IP address:

config bootconfig net mgmt ip <ipaddr/mask>

where:

<ipaddr/mask> specifies the IP address and mask of the Management port.

i.e.config bootconfig net mgmt ip 47.108.0.158/255.255.240.0

**Note:** The preferred route for managing the switch is to use the Management port.

## 18.3 Assigning a Default Gateway to the Management Port

A default gateway is required to provide proper routing for the Management Port.

**Use the following command to assign a default gateway:**

config bootconfig net mgmt route net <value> <ipaddr>

where:

<value> specifies the IP address of the destination network

<ipaddr > specifies the default gatewayís IP address.

i.e.config bootconfig route net 47.0.0.0 47.108.0.10

## 18.4 Setting Access Privileges to the Switch

Five distinct levels of access privileges can be set for Telnet users.

Use the following command to set the CLI access privileges:

config cli password <access> <username> [<password>]

where:

<access> specifies one of five levels of access (rwa, rw, l3, l2, ro)

<username> specifies the login name of the user

[<password>] specifies the password of the user.

i.e.config cli password ro guest temp

Use the following commands to set the Device Manager access privileges:

config sys set snmp community <ro|rw|l1|l2|l3|rwa> <commstr>

where:

<ro|rw|l1|l2|l3|rwa> specifies the community {ro|l1|l2|l3|rw|rwa}

<commstr> specifies the input community string {string length 1..1536}

i.e.config sys set snmp community rwa manager

## 18.5 Enabling Telnet Access to the Switch

After the switch has been configured with an IP address, you may want to enable Telnet access to provide remote management capabilities. To enable or disable Telnet access, you set flags from the boot monitor CLI. You can access the boot monitor CLI while the switch is booting.

To set up Telnet access follow these instructions:

While the switch is booting, press any key to interrupt the auto-boot process.

Enable or disable Telnet access using the command:

flags telnetd <true|false>

where:

true enables Telnet access.

false disables Telnet access.

i.e. flags telnetd true

## 18.6 Saving the Management IP Configuration

In order for the Passport 8600 to save the Management IP address information you have to save the bootconfig configuration.

Use the following command to save the bootconfig:

save bootconfig [file <filename>]

where:

[file <filename>] specifies an optional filename for the bootconfig file. Use this option if you wish to save under a different name.

Default is boot.cfg.

i.e.save bootconfig

## 18.7 Layer 3 Switch Configuration

This section discusses how to use the Command Line Interface (CLI) configure the switch as a layer 3 device (routing) with Two VLANs and Static Routes- where needed as the Routing Protocol. More likely OSPF will be used in the future and its configuration will be documented at a later time.

**Table 0-84**

| |
|---|
| Note: Although the Nortel Networks Device Manager can also be used to configure the Passport 8600, CLI commands are used in this section to facilitate explaining the configuration procedures. |

### 18.7.1 Add IP addressing information to VLAN 1

Due to our specific lab requirements, in this configuration, VLAN 1 is the Public side LAN, therefore a standard CORWAN address is assigned to the VLAN.

**Note:** Please refer to the IP addressing section for optional IP addressing schemes.

**Use the following command to create an IP address on VLANs:**

config vlan <vid> ip create <ipaddr/mask>

where:

<vid> specifies a unique VLAN identifier (numbered 1 to 4095)

<addr/mask> specifies the IP address and mask for the VLAN

i.e.config vlan 1 ip create 47.142.86.41/255.255.255.0

### 18.7.2 Add Ethernet ports to VLAN 1

In this configuration ports 1/1 through 1/32 were assigned to VLAN 1.

**Use the following command to assign Ethernet ports on VLANs:**

config vlan <vid> ports add <ports>

where:

<vid> specifies a unique VLAN identifier (numbered 1 to 4095)

<ports> specifies the ports to be assigned to the VLAN {slot/port[-slot/port][,...]}

i.e.config vlan 1 ports add 1/1-1/32

### 18.7.3 Add IP addressing information to VLAN 2

In this configuration, VLAN 2 is the Private side LAN, therefore a Private address is assigned to the VLAN.

**Note:** Please refer to the IP addressing section for optional IP addressing schemes.

Use the following command to create an IP address on VLANs:

config vlan <vid> ip create <ipaddr/mask>

where:

<vid> specifies a unique VLAN identifier (numbered 1 to 4095)

<addr/mask> specifies the IP address and mask for the VLAN

i.e.config vlan 2 ip create 10.16.0.1/255.255.255.0

### 18.7.4 Add Ethernet ports to VLAN 2

In this configuration ports 2/1 through 2/32 were assigned to VLAN 2.

Use the following command to assign Ethernet ports on VLANs:

config vlan <vid> ports add <ports>

where:

<vid> specifies a unique VLAN identifier (numbered 1 to 4095)

<ports> specifies the ports to be assigned to the VLAN {slot/port[-slot/port][,...]}

i.e.config vlan 2 ports add 2/1-2/32

### 18.7.5 VRRP Setup

As per above, 10.16.0.1 is the default gateway for devices subtending VLAN 2. In order to maintain this default gateway during VRRP failover 10.16.0.1 needs to become the IP address of the VRRP virtual interface.

Use the following commands to setup VRRP on VLAN 2:

config vlan <vid> ip vrrp <vrid> address <ipaddr>

where:

<vid> specifies a unique VLAN identifier (numbered 1 to 4095)

<vrid> specifies the virtual router id (numbered 1 to 255)

<ipaddr> specifies IP address of the virtual interface

i.e.config vlan 2 ip vrrp 2 address 10.16.0.1

config vlan <vid> ip vrrp <vrid> priority <prio>

where:

<prio> specifies the port VRRP priority value (numbered 1 to 254)

i.e.config vlan 2 ip vrrp 2 priority 50(virtual router #2)

config vlan <vid> ip vrrp <vrid> backup-master <enable|disable>

i.e.config vlan 2 ip vrrp 2 backup-master enable

### 18.7.6 OSPF Routing

OSPF needs to be enabled on all the Passport 8600 boxes and on all the required VLANs in order to dynamically route traffic throughout the network. Additionally Autonomous System Boundary Router needs to be enabled on any box that needs to announce its static IP routes throughout the network.

Use the following commands to configure OSPF on the box:

config ip ospf admin-state enable

config ip ospf as-boundary-router enable

Use the following commands to configure OSPF on VLAN 2:

config vlan 2 ip ospf enable

config vlan 2 ip ospf metric 1(for GigE interfaces)

config vlan 2 ip ospf metric 10(default for 100 BaseT interfaces)

After further testing, additional OSPF area configuration details will be included in a later release of this document.

## 18.8 Saving your configuration

**Use the following command to save the bootconfig:**

save config [file <filename>]

where:

[file <filename>] specifies an optional filename for the config file. Use this option if you wish to save under a different name.

Default is config.cfg.

i.e.save config

## 18.9 Special Notes

### 18.9.1 Spanning Tree Protocol (STP)

Spanning Tree Protocol is enabled by default on all the Passport 8600 ports. Therefore, it is very important to check the Spanning Tree state of the PP8600 interfaces to ensure that STP is disabled by default unless otherwise explicitly stated in these guidelines.

Use the following command to check the STP on Ethernet ports:

config ethernet <ports> stg <sid> info

where:

<ports> specifies the ports to check for STP {slot/port[-slot/port][,...]}

<sid> specifies a spanning tree id {1..25}

i.e.config ethernet 1/5 stg 1 info

Use the following command to disable STP on Ethernet ports:

config ethernet <ports> stg <sid> stp <parameter>
where:

<ports> specifies the ports to disable STP {slot/port[-slot/port][,...]}

<sid> specifies a spanning tree id {1..25}

<parameter> enable or disable STP {enable|disable}

i.e.config ethernet 1/5 stg 1 stp disable

### 18.9.2 Proxy ARP

For the devices which are configured as their own gateway, you might need to turn on Proxy ARP on the VLAN that they are connected to. This will allow the VLAN to act as a Proxy for any ARP requests coming from the connected devices.

Use the following command to enable Proxy ARP on a VLAN:

config vlan <vid> ip proxy <parameter>

where:

<vid> specifies a unique VLAN identifier (numbered 1 to 4095)

<parameter> enable or disable Proxy {enable|disable}

i.e.config vlan 1 ip proxy enable

### 18.9.3 Multi-Link Trunk (MLT)

In order to facilitate robustness on the VRRP link between the redundant PP8600s, MLT needs to be configured using ports on multiple modules, thereby, ensuring that no single point of failure will disrupt the VRRP communication.

In this configuration ports 1/34 and 2/34 were configured in an MLT 1

Use the following command to configure MLT:

config mlt <mid> create

config mlt <mid> perform-tagging enable

config mlt <mid> add ports <ports>

where:

<mid> specifies the mlt id {1..32}

<ports> specifies the ports in the multi-link trunk

i.e.config mlt 10 create

config mlt 10 perform-tagging enable

config mlt 10 add ports 1/34,2/34

## 18.10 Upgrading the Passport 8600

The Passport 8600 facilitates hitless image upgrades to its Switching Fabrics (SFs) when it is setup in a redundant VRRP configuration with another Passport 8600. For a detailed, step-by-step description on how to do a hitless upgrade of the software loads on the PP8600, refer to the Succession CS2K PP8600 Software Upgrade Procedure documentation.

# 19.0 Appendix: SN06.2 PP8600 Port Setting and Connectivity Requirements

Table 126 summarizes the number of IP addresses and PP8600 port speed/mode settings for the elements in the CS-LAN. For more details consult the Succession Engineering Guidelines.

***Note:*** STP is disabled for all ports unless specified.

***Note:*** Bold items are new to SN06.2 release

**Table 126 CS-LAN IP Addressing and Port Settings Summary**

| ELEMENT | SUBNET | # OF IP ADDRs | PP8600 PORT SPEED and MODE | SPECIAL NOTES |
|---|---|---|---|---|
| PP8600 | OAM, CallP, UAS Bearer, Portal-Int, Portal-Ext, MLT, OOB | 19 | N/A | 2 PP8600 chassis.<br>3 IP addresses per VLAN, 2 for MLT and 2 for OOB<br>OOB IP address for NMI since it is routable a port |
| SDM | OAM & CallP | 3 | Auto-neg = TRUE<br>100BT - Full | 2 ethernet (1 per subnet)<br>1 DS-512 (XA-Core only) |
| SESM - N1400 | OAM | 3 | Auto-neg = TRUE<br>100BT - Full | 1 multipathing for the server;<br>2 physical (1 per link for heartbeat) |
| **SESM - N240 Simplex** | **OAM** | **3** | **Auto-neg = TRUE<br>100BT - Full** | **1 multipathing for the server;<br>2 physical (1 per link for heartbeat) - Using bge1 & bge3** |
| **SESM - N240 Duplex** | **OAM** | **3** | **Auto-neg = TRUE<br>100BT - Full** | **1 Logical for the 2 servers;<br>1 physical per N240;<br><br>bge1 of server 0 to PP8600-0<br>bge3 of server 0 to PP8600-1<br>bge1 of server 1 to PP8600-1<br>bge3 of server 1 to PP8600-0<br><br>bge0 & bge2 used for Interconnect** |
| **IEMS - V100** | **OAM** | **3** | **Auto-neg = TRUE<br>100BT - Full** | **1 multipathing for the server;<br>2 physical (1 per link for heartbeat)** |
| **IEMS- N240 Simplex** | **OAM** | **3** | **Auto-neg = TRUE<br>100BT - Full** | **1 multipathing for the server;<br>2 physical (1 per link for heartbeat) - Using bge1 & bge3** |
| GWC | CallP | 4 | Auto-neg = TRUE<br>100BT - Half | 2 physical; 2 logical; Last byte of active IP address must be divisible by 4 |
| SC | CallP | 4 | Auto-neg = True<br>100BT - Full | 2 physical; 2 logical; Last byte of active IP address must be divisible by 4 |
| XA-Core/ HIOPs | CallP | 6 | Auto-neg = TRUE<br>100BT - Full | 2 logical (host); 2 etherlink (1 per card); 2 maintenance (1 per card) |

| ELEMENT | SUBNET | # OF IP ADDRs | PP8600 PORT SPEED and MODE | SPECIAL NOTES |
|---|---|---|---|---|
| UAS | UAS Bearer & CallP | 9 | Auto-neg = TRUE<br>100BT - Full | For a 3 domain configuration w/ 2 CG6Ks each:<br>1 per CG6K card; 1 per CPU card |
| **AMS - 120 ports** | **CallP** | **1** | **Auto-neg = TRUE<br>100BT - Full** | **1 IP address floats to active port** |
| **AMS - 240 ports** | **CallP** | **2** | **Auto-neg = TRUE<br>100BT - Full** | **1 IP address per 120 ports node - Both IP addresses operate off the same physical interface and float to active port** |
| USP | OAM & CallP | 4 | Auto-neg = TRUE<br>100BT - Full | # of IP addresses depends on the # of IPS7 cards. The two RTCs each require an OAM IP address, and each IPS7 card requires a CallP IP address. Minimal configuration with 2 IPS7 cards would require 4 IP addresses |
| 3PC Call Server | CallP | 10 | Auto-neg = TRUE<br>100BT - Full | Last octet of the active call processing IP address must be divisible by 8 |
| STORM Blades | CallP | 2 | Auto-neg = TRUE<br>100BT - Full | one IP address per STORM blade |
| **Storm IA - XTS Servers** | **CallP** | **2** | **Auto-neg = TRUE<br>100BT - Full** | **One IP address per SAM-XTS.<br>One SMLT for each XTS Server<br>One port on each PP8600/SMLT** |
| USP-Lite | CallP | 4 | Auto-neg = FALSE<br>100BT-Half | The pair of cards use 4 contiguous IP addresses starting at a divisible by 4 boundary. |
| PVG - ATM | VSP Bearer<br>VSP Signalling<br>VSP PRI | 6 | External Clocking | 1 Port per VSP2/VSP3, 3 VCC<br>2 Ip addresses per VCC ( /30 subnet)<br>Applies to OC3 and OC12<br>1 port per MDA on PP8600 |
| PVG - GigE (VSP Face plate) | PVG Subnet | 12 | Auto-neg = TRUE | 1 subnet per PVG shelf - 4+4 VSP3 configuration<br>3 IP addresses per VSP (Bearer, Signalling, PRI) |
| **PVG - GigE (4 port GigE)** | | | | **Info provided in future updates** |

# 20.0 Appendix: Configuration details for PVG to Juniper

## 20.1 PVG15K

The following lists the set of commands required to provision a single VSP (inserted in slot 7), while provisioning a redundant configuration through two ATM FPs (inserted in slots 4 and 5) to redundant Juniper Mx serires. This list does not include any standard PVG provisioning.

```
##
## Configure Line Automatice Protection Swithing
##
add Laps/1
set Laps/1 workingLine Lp/4 Sonet/0, protectionLine Lp/5 Sonet/0, mode bidirectional, revertive
no
add Lp/4 Sonet/0
set Lp/4 Sonet/0 lineAutomaticProtectionSwitch Laps/1
add Lp/5 Sonet/0
set Lp/5 Sonet/0 lineAutomaticProtectionSwitch Laps/1
add Laps/1 Sts/0
set Laps/1 Sts/0 applicationFramerName AtmIf/400
```

***Note:*** Laps mode must be set to bidirectional since Juniper only supports bidirectional mode.

```
##
## Create the ATM interface and add Laps to it
##
add AtmIf/400
set AtmIf/400 interfaceName Laps/1 Sts/0

##
## Configure the VSP (Nsta component) Media Gateway Voice services
##
add Nsta/7 Vgs Ctrl/mediaGateway
set Nsta/7 Vgs Ctrl/mediaGatewayipAddress 172.16.209.2
add Nsta/7 Vgs Ctrl/mediaGateway spvcap
set Nsta/7 Vgs Ctrl/mediaGateway SpvcAp atmServiceCategory nrtVariableBitRate
set Nsta/7 Vgs Ctrl/mediaGateway SpvcAp pcr 800, scr 400, mbs 110
set Nsta/7 Vgs Ctrl/mediaGateway SpvcAp addressToCall
!45613512123400002F000000020020480D019000, remoteVpiVci 0.700
```

```
##
## Configure the VSP (Nsta component) PRI Signaling Gateway Voice services
##
add Nsta/7 Vgs Ctrl/signalingGateway
set Nsta/7 Vgs Ctrl/signalingGateway ipAddress 172.16.209.6
add Nsta/7 Vgs Ctrl/signalingGateway SctpPort/9900
add Nsta/7 Vgs Ctrl/signalingGateway SpvcAp
set Nsta/7 Vgs Ctrl/signalingGateway SpvcAp atmServiceCategory nrtVariableBitRate
set Nsta/7 Vgs Ctrl/signalingGateway SpvcAp pcr 450, scr 210, mbs 60
set Nsta/7 Vgs Ctrl/signalingGateway SpvcAp addressToCall
!45613512123400002F000000020020480D019000 ,remoteVpiVci 0.701

##
## Configure the VSP (Nsta component) Bearer Voice services
##
add Nsta/7 Vgs IpMConn
set Nsta/7 Vgs IpMConn ipAddress 172.16.209.10
add Nsta/7 Vgs IpMConn SpvcAp
set Nsta/7 Vgs IpMConn SpvcAp atmServiceCategory rtVariableBitRate
set Nsta/7 Vgs IpMConn SpvcAp pcr 336000, scr 336000, mbs 1
set Nsta/7 Vgs IpMConn SpvcAp addressToCall
!45613512123400002F000000020020480D019000 ,remoteVpiVci 0.710
```

***Note:*** The address to call subcomponent of the spvcap is the NSAP address of the ATM interface were the Laps Sts is attached to, i.e. AtmIf/400 interfaceName Laps/1 Sts/0

## 20.2 Juniper M40-A

```
##
## Configure Distributed APS on the ATM inteface attached to the PVG
##
[edit interfaces at-6/2/0]
description "D-APS Working Circuit connection to RTP4_PVG41-4/0";
clocking external;
sonet-options {
   aps {
      working-circuit PVG41;
      neighbor 172.30.242.17;
   }
}
```

```
##
## The working/protect circuit has to match the correct LP, Sonet provisioned
##

atm-options {
   vpi 0 {
      maximum-vcs 1200;
   }
}

##
## Configure Logical Units on the ATM interface with PVG VSP subnets
##

unit 3 {
   description PVG4107_Ctrl/MG;
   encapsulation atm-snap;
   vci 0.700;
   inverse-arp;
   family inet {
      address 172.16.209.1/30;
   }
}
unit 4 {
   description PVG4107_Ctrl/SG;
   encapsulation atm-snap;
   vci 0.701;
   inverse-arp;
   family inet {
      address 172.16.209.5/30;
   }
}
unit 5 {
   description PVG4107_IpmCon;
   encapsulation atm-snap;
   vci 0.710;
   inverse-arp;
   family inet {
      address 172.16.209.9/30;
   }
```

```
}

##
## Add the PVG facing interfaces to OSPF as Passive interfaces
##

protocols {
   ospf {
     area 0.0.0.0 {
          interface at-6/2/0.3 {
             passive;
          }
          interface at-6/2/0.4 {
             passive;
          }
          interface at-6/2/0.5 {
             passive;
          }
}
```

## 20.3 Juniper M40-B

***Note:*** The configuration in the alternate M40 is identical to the primary one with the exception of the Distributed APS section.

```
[edit interfaces at-6/2/0]
description "D-APS Protection Circuit connection to RTP4_PVG41-5/0";
clocking external;
sonet-options {
   aps {
      protect-circuit PVG41;
      neighbor 172.30.242.18;
   }
}
atm-options {
   vpi 0 {
      maximum-vcs 1200;
   }
```

```
}
```

***Note:*** The logical unit numbers do not have to match, but the vci and the IP addresses must be identical to the primary configuration

```
unit 3 {
   description PVG4107_Ctrl/MG;
   encapsulation atm-snap;
   vci 0.700;
   inverse-arp;
   family inet {
      address 172.16.209.1/30;
   }
}
unit 4 {
   description PVG4107_Ctrl/SG;
   encapsulation atm-snap;
   vci 0.701;
   inverse-arp;
   family inet {
      address 172.16.209.5/30;
   }
}
unit 5 {
   description PVG4107_IpmCon;
   encapsulation atm-snap;
   vci 0.710;
   inverse-arp;
   family inet {
      address 172.16.209.9/30;
   }
}
```

***Note:*** The OSPF configuration on M40-B is equal to M40-A

# 21.0 Appendix: Configuration details for PVG to PP8600

## 21.1 PVG15K

The following lists the set of commands required to provision a single VSP2 (inserted in slot 10), while provisioning a redundant configuration through two ATM FPs (inserted in slots 2 and 3) to redundant PP8600s. This list does not include any standard PVG provisioning.

```
a artg

a atmif/20
a atmif/20 uni

a atmif/30
a atmif/30 uni

s atmif/20 endToEndLoopback on
s atmif/30 endToEndLoopback on

a atmif/20 uni addr/45160000000000000F000000000020480D100220, primary
a atmif/20 uni addr/45160000000000000F000000000020480D100220, primary term

a atmif/30 uni addr/45160000000000000F000000000020480D100220, alternate
a atmif/30 uni addr/45160000000000000F000000000020480D100220, alternate term

s nsta/10 vgs ctrl/mg spvcap rVpiVci 0.90
s nsta/10 vgs ctrl/sg spvcap rVpiVci 0.91
s nsta/10 vgs ipmconn spvcap rVpiVci 0.100
s nsta/10 vgs ctrl/mg spvcap addresstocall !45160000000000000F000000000020480D100220
s nsta/10 vgs ctrl/sg spvcap addresstocall !45160000000000000F000000000020480D100220
s nsta/10 vgs ipmconn spvcap addresstocall !45160000000000000F000000000020480D100220
```

## 21.2 Passport 8600s

The following is a set of minimum commands for setting up PVG15K interconnecting PVCs on the redundant PP8600s. This list does not include standard Passport 8600 configuration.

```
#
# VLAN CONFIGURATION
#
vlan 602 create byport 1 name "PVG42-vsp06-mg"
```

```
vlan 602 ports remove 1/1-1/8,2/1-2/48,3/1-3/48,4/1-4/48,7/2-7/8,8/1-8/8,9/1-9/8,10/1-10/8
member portmember
vlan 602 ports add 7/1 member portmember
vlan 602 ip create 172.16.228.1/255.255.255.252 mac_offset 2
vlan 602 ip igmp mrdisc mrdisc-enable disable
vlan 606 create byport 1 name "PVG42-vsp06-sg"
vlan 606 ports remove 1/1-1/8,2/1-2/48,3/1-3/48,4/1-4/48,7/2-7/8,8/1-8/8,9/1-9/8,10/1-10/8
member portmember
vlan 606 ports add 7/1 member portmember
vlan 606 ip create 172.16.228.5/255.255.255.252 mac_offset 4
vlan 606 ip igmp mrdisc mrdisc-enable disable
vlan 610 create byport 1 name "PVG42-vsp06-ipmconn"
vlan 610 ports remove 1/1-1/8,2/1-2/48,3/1-3/48,4/1-4/48,7/2-7/8,8/1-8/8,9/1-9/8,10/1-10/8
member portmember
vlan 610 ports add 7/1 member portmember
vlan 610 ip create 172.16.228.9/255.255.255.252 mac_offset 6
vlan 610 ip igmp mrdisc mrdisc-enable disable

#
# PORT CONFIGURATION - PHASE II
#
atm 7/1 stg 1 stp disable

#
# OSPF CONFIGURATION
#
ip ospf admin-state enable
ip ospf as-boundary-router enable
ip ospf router-id 172.30.242.1
ip ospf enable

#
# IP ROUTE POLICY CONFIGURATION
#
ip route-policy "_rpsOsAcpt" seq 21845 create
ip route-policy "_rpsOsAcpt" seq 21845 enable
ip route-policy "_rpsOsAcpt" seq 21845 action permit
ip route-policy "_rpsLocalOs" seq 21845 create
ip route-policy "_rpsLocalOs" seq 21845 enable
ip route-policy "_rpsLocalOs" seq 21845 action permit
ip route-policy "_rpsStaticOs" seq 21845 create
ip route-policy "_rpsStaticOs" seq 21845 enable
```

```
ip route-policy "_rpsStaticOs" seq 21845 action permit
ip route-policy "_rpsRipOs" seq 21845 create
ip route-policy "_rpsRipOs" seq 21845 disable
ip route-policy "_rpsRipOs" seq 21845 action permit
ip route-policy "BlockRoutes" seq 10 create
ip route-policy "BlockRoutes" seq 10 enable
ip route-policy "BlockRoutes" seq 10 action deny
ip route-policy "BlockRoutes" seq 10 match-network "RTPI-47.142.116.0"

#
# IP REDISTRIBUTION CONFIGURATION
#
ip ospf redistribute rip create
ip ospf redistribute rip route-policy "_rpsRipOs"
ip ospf redistribute rip enable
ip ospf redistribute static create
ip ospf redistribute static route-policy "_rpsStaticOs"
ip ospf redistribute static enable
ip ospf redistribute direct create
ip ospf redistribute direct route-policy "_rpsLocalOs"
ip ospf redistribute direct enable
```

***Note:*** An alternative to the IP Route Policy and the Redistribution of Local routes configuration would be to configure the vsp VLAN interfaces as Passive OSPF interfaces. There is an advantage by using Passive interfaces where only those interfaces would be announced in OSPF route advertisements and not all the local subnets.

```
#
# ATM CONFIGURATION
#
atm 7/1 state enable
atm 7/1 clock-source loop-timed
atm 7/1 name "PVG42-vsp"
atm 7/1 pvc create 6.2
atm 7/1 pvc f5-oam 6.2 enable send 1 retry 1 up 1 down 1 trap enable
atm 7/1 pvc create 6.6
atm 7/1 pvc f5-oam 6.6 enable send 1 retry 1 up 1 down 1 trap enable
atm 7/1 pvc create 6.10
atm 7/1 pvc f5-oam 6.10 enable send 1 retry 1 up 1 down 1 trap enable
```

```
atm 7/1 pvc 1483 ip create 602 6.2 172.16.228.2 enable 1
atm 7/1 pvc 1483 ip create 606 6.6 172.16.228.6 enable 1
atm 7/1 pvc 1483 ip create 610 6.10 172.16.228.10 enable 1
atm 7/2 state disable
atm 7/2 name "Open"
atm 7/3 state disable
atm 7/3 name "Open"
atm 7/4 state disable
atm 7/4 name "Open"
```

The redundant Passport 8600 is configured identical to this configuration.

# 22.0 Appendix: Configuration details for PVG to PP8600 using Gigabit Ethernet

## 22.1 PVG15000

The following lists the set of commands required to provision a single VSP3 (inserted in slot 6), and 4 Port OC3/STM-1 ch TDM card (inserted in slot 13). The VSP3 is interconnected to the Dual Passport 8600s through the Gigabit Ethernet ports off the VSP3 faceplate. Although not all the TDM provisioning is listed here, sufficient portions of the TDM provisioning is provided as a guide for completeing the provisioning.

***Note:*** This list does not include any standard PVG provisioning.

st prov

add Sw Lpt/VSP3

set Sw Lpt/VSP3 featureList vgsipgige

add Shelf Card/6

set Shelf Card/6 cardType 2pGeMmSrVsp3

add Lp/6

set Lp/6 mainCard Shelf Card/6,spareCard !,logicalProcessorType Sw Lpt/VSP3

add Lp/6 Vsp

add Lp/6 Vsp GigE/0

add Lp/6 Vsp GigE/1

add Nsta/6

set Lp/6 Vsp linkToApplication Nsta/6

set Nsta/6 linkToServer Lp/6 Vsp

add Nsta/6 Vgs

set Nsta/6 Vgs hostname PVG006

add Nsta/6 Vgs IpIf

set Nsta/6 Vgs IpIf defaultRouterAddress 192.168.9.1,subnetMask 255.255.255.0

add Nsta/6 Vgs Ctrl/mediaGateway

set Nsta/6 Vgs Ctrl/mediaGateway ipAddress 192.168.9.8
add Nsta/6 Vgs Ctrl/mediaGateway UdpPort/2427
set Nsta/6 Vgs Ctrl/mediaGateway UdpPort/2427 linkToApplication Nsta/6 Vgs Vgcp
add Nsta/6 Vgs Vgcp
set Nsta/6 Vgs Vgcp udpPortConnection Nsta/6 Vgs Ctrl/mediaGateway UdpPort/2427

add Nsta/6 Vgs IpMConn
set Nsta/6 Vgs IpMConn ipAddress 192.168.9.16,udpPortBase 49152

add Nsta/6 Vgs Ctrl/signalingGateway
set Nsta/6 Vgs Ctrl/signalingGatewayipAddress 192.168.9.12
add Nsta/6 Vgs Ctrl/signalingGateway SctpPort/9900
add Nsta/6 Vgs Iua
set Nsta/6 Vgs Ctrl/signalingGateway SctpPort/9900 linkToApplication Nsta/6 Vgs Iua
set Nsta/6 Vgs Iua sctpPortConnection Nsta/6 Vgs Ctrl/signalingGateway SctpPort/9900

add Nsta/6 Vgs BragS/0

add Nsta/6 Vgs BragS/1
add Nsta/6 Vgs BragS/1 Q921
set Nsta/6 Vgs BragS/1 Q921 dChanTimeslot 24,side user

add Sw Lpt/OC3TDM
set Sw Lpt/OC3TDM featureList aal1ces

add Shelf card/13
set Shelf card/13 cardtype 4pOC3ChSmIr

add Lp/13
set Lp/13 maincard shelf card/13

add -s Lp/13 Sonet/0 Sts/0 vt1dot5/1,1 ds1 chan/0 tc
add -s Lp/13 Sonet/0 Sts/0 vt1dot5/1,2 ds1 chan/0 tc
add -s Lp/13 Sonet/0 Sts/0 vt1dot5/1,3 ds1 chan/0 tc

add -s Lp/13 Sonet/0 Sts/0 vt1dot5/1,4 ds1 chan/0 tc
add -s Lp/13 Sonet/0 Sts/0 vt1dot5/2,1 ds1 chan/0 tc
add -s Lp/13 Sonet/0 Sts/0 vt1dot5/2,2 ds1 chan/0 tc
add -s Lp/13 Sonet/0 Sts/0 vt1dot5/2,3 ds1 chan/0 tc
add -s Lp/13 Sonet/0 Sts/0 vt1dot5/2,4 ds1 chan/0 tc
add -s Lp/13 Sonet/0 Sts/0 vt1dot5/3,1 ds1 chan/0 tc
add -s Lp/13 Sonet/0 Sts/0 vt1dot5/3,2 ds1 chan/0 tc
add -s Lp/13 Sonet/0 Sts/0 vt1dot5/3,3 ds1 chan/0 tc
add -s Lp/13 Sonet/0 Sts/0 vt1dot5/3,4 ds1 chan/0 tc
add -s Lp/13 Sonet/0 Sts/0 vt1dot5/4,1 ds1 chan/0 tc
add -s Lp/13 Sonet/0 Sts/0 vt1dot5/4,2 ds1 chan/0 tc
add -s Lp/13 Sonet/0 Sts/0 vt1dot5/4,3 ds1 chan/0 tc
add -s Lp/13 Sonet/0 Sts/0 vt1dot5/4,4 ds1 chan/0 tc
add -s Lp/13 Sonet/0 Sts/0 vt1dot5/5,1 ds1 chan/0 tc
add -s Lp/13 Sonet/0 Sts/0 vt1dot5/5,2 ds1 chan/0 tc
add -s Lp/13 Sonet/0 Sts/0 vt1dot5/5,3 ds1 chan/0 tc
add -s Lp/13 Sonet/0 Sts/0 vt1dot5/5,4 ds1 chan/0 tc
add -s Lp/13 Sonet/0 Sts/0 vt1dot5/6,1 ds1 chan/0 tc
add -s Lp/13 Sonet/0 Sts/0 vt1dot5/6,2 ds1 chan/0 tc
add -s Lp/13 Sonet/0 Sts/0 vt1dot5/6,3 ds1 chan/0 tc
add -s Lp/13 Sonet/0 Sts/0 vt1dot5/6,4 ds1 chan/0 tc
add -s Lp/13 Sonet/0 Sts/0 Vt1dot5/7,1 ds1 chan/0 tc
add -s Lp/13 Sonet/0 Sts/0 Vt1dot5/7,2 ds1 chan/0 tc
add -s Lp/13 Sonet/0 Sts/0 Vt1dot5/7,3 ds1 chan/0 tc
add -s Lp/13 Sonet/0 Sts/0 Vt1dot5/7,4 ds1 chan/0 tc

add -s Lp/13 Sonet/0 Sts/1 Vt1dot5/1,1 ds1 chan/0 tc
add -s Lp/13 Sonet/0 Sts/1 Vt1dot5/1,2 ds1 chan/0 tc
add -s Lp/13 Sonet/0 Sts/1 Vt1dot5/1,3 ds1 chan/0 tc
add -s Lp/13 Sonet/0 Sts/1 Vt1dot5/1,4 ds1 chan/0 tc
add -s Lp/13 Sonet/0 Sts/1 Vt1dot5/2,1 ds1 chan/0 tc
add -s Lp/13 Sonet/0 Sts/1 Vt1dot5/2,2 ds1 chan/0 tc
add -s Lp/13 Sonet/0 Sts/1 Vt1dot5/2,3 ds1 chan/0 tc
add -s Lp/13 Sonet/0 Sts/1 Vt1dot5/2,4 ds1 chan/0 tc

add -s Lp/13 Sonet/0 Sts/1 Vt1dot5/3,1 ds1 chan/0 tc
add -s Lp/13 Sonet/0 Sts/1 Vt1dot5/3,2 ds1 chan/0 tc
add -s Lp/13 Sonet/0 Sts/1 Vt1dot5/3,3 ds1 chan/0 tc
add -s Lp/13 Sonet/0 Sts/1 Vt1dot5/3,4 ds1 chan/0 tc
add -s Lp/13 Sonet/0 Sts/1 Vt1dot5/4,1 ds1 chan/0 tc
add -s Lp/13 Sonet/0 Sts/1 Vt1dot5/4,2 ds1 chan/0 tc
add -s Lp/13 Sonet/0 Sts/1 Vt1dot5/4,3 ds1 chan/0 tc
add -s Lp/13 Sonet/0 Sts/1 Vt1dot5/4,4 ds1 chan/0 tc
add -s Lp/13 Sonet/0 Sts/1 Vt1dot5/5,1 ds1 chan/0 tc
add -s Lp/13 Sonet/0 Sts/1 Vt1dot5/5,2 ds1 chan/0 tc
add -s Lp/13 Sonet/0 Sts/1 Vt1dot5/5,3 ds1 chan/0 tc
add -s Lp/13 Sonet/0 Sts/1 Vt1dot5/5,4 ds1 chan/0 tc
add -s Lp/13 Sonet/0 Sts/1 Vt1dot5/6,1 ds1 chan/0 tc
add -s Lp/13 Sonet/0 Sts/1 Vt1dot5/6,2 ds1 chan/0 tc
add -s Lp/13 Sonet/0 Sts/1 Vt1dot5/6,3 ds1 chan/0 tc
add -s Lp/13 Sonet/0 Sts/1 Vt1dot5/6,4 ds1 chan/0 tc
add -s Lp/13 Sonet/0 Sts/1 Vt1dot5/7,1 ds1 chan/0 tc
add -s Lp/13 Sonet/0 Sts/1 Vt1dot5/7,2 ds1 chan/0 tc
add -s Lp/13 Sonet/0 Sts/1 Vt1dot5/7,3 ds1 chan/0 tc
add -s Lp/13 Sonet/0 Sts/1 Vt1dot5/7,4 ds1 chan/0 tc

add -s Lp/13 Sonet/0 Sts/2 Vt1dot5/1,1 ds1 chan/0 tc
add -s Lp/13 Sonet/0 Sts/2 Vt1dot5/1,2 ds1 chan/0 tc
add -s Lp/13 Sonet/0 Sts/2 Vt1dot5/1,3 ds1 chan/0 tc
add -s Lp/13 Sonet/0 Sts/2 Vt1dot5/1,4 ds1 chan/0 tc
add -s Lp/13 Sonet/0 Sts/2 Vt1dot5/2,1 ds1 chan/0 tc
add -s Lp/13 Sonet/0 Sts/2 Vt1dot5/2,2 ds1 chan/0 tc
add -s Lp/13 Sonet/0 Sts/2 Vt1dot5/2,3 ds1 chan/0 tc
add -s Lp/13 Sonet/0 Sts/2 Vt1dot5/2,4 ds1 chan/0 tc
add -s Lp/13 Sonet/0 Sts/2 Vt1dot5/3,1 ds1 chan/0 tc
add -s Lp/13 Sonet/0 Sts/2 Vt1dot5/3,2 ds1 chan/0 tc
add -s Lp/13 Sonet/0 Sts/2 Vt1dot5/3,3 ds1 chan/0 tc
add -s Lp/13 Sonet/0 Sts/2 Vt1dot5/3,4 ds1 chan/0 tc
add -s Lp/13 Sonet/0 Sts/2 Vt1dot5/4,1 ds1 chan/0 tc

add -s Lp/13 Sonet/0 Sts/2 Vt1dot5/4,2 ds1 chan/0 tc
add -s Lp/13 Sonet/0 Sts/2 Vt1dot5/4,3 ds1 chan/0 tc
add -s Lp/13 Sonet/0 Sts/2 Vt1dot5/4,4 ds1 chan/0 tc
add -s Lp/13 Sonet/0 Sts/2 Vt1dot5/5,1 ds1 chan/0 tc
add -s Lp/13 Sonet/0 Sts/2 Vt1dot5/5,2 ds1 chan/0 tc
add -s Lp/13 Sonet/0 Sts/2 Vt1dot5/5,3 ds1 chan/0 tc
add -s Lp/13 Sonet/0 Sts/2 Vt1dot5/5,4 ds1 chan/0 tc
add -s Lp/13 Sonet/0 Sts/2 Vt1dot5/6,1 ds1 chan/0 tc
add -s Lp/13 Sonet/0 Sts/2 Vt1dot5/6,2 ds1 chan/0 tc
add -s Lp/13 Sonet/0 Sts/2 Vt1dot5/6,3 ds1 chan/0 tc
add -s Lp/13 Sonet/0 Sts/2 Vt1dot5/6,4 ds1 chan/0 tc
add -s Lp/13 Sonet/0 Sts/2 Vt1dot5/7,1 ds1 chan/0 tc
add -s Lp/13 Sonet/0 Sts/2 Vt1dot5/7,2 ds1 chan/0 tc
add -s Lp/13 Sonet/0 Sts/2 Vt1dot5/7,3 ds1 chan/0 tc
add -s Lp/13 Sonet/0 Sts/2 Vt1dot5/7,4 Ds1 chan/0 tc

...
...
...

add -s Lp/13 Sonet/3 Sts/2 Vt1dot5/1,1 Ds1 chan/0 tc
add -s Lp/13 Sonet/3 Sts/2 Vt1dot5/1,2 Ds1 chan/0 tc
add -s Lp/13 Sonet/3 Sts/2 Vt1dot5/1,3 Ds1 chan/0 tc
add -s Lp/13 Sonet/3 Sts/2 Vt1dot5/1,4 Ds1 chan/0 tc
add -s Lp/13 Sonet/3 Sts/2 Vt1dot5/2,1 Ds1 chan/0 tc
add -s Lp/13 Sonet/3 Sts/2 Vt1dot5/2,2 Ds1 chan/0 tc
add -s Lp/13 Sonet/3 Sts/2 Vt1dot5/2,3 Ds1 chan/0 tc
add -s Lp/13 Sonet/3 Sts/2 Vt1dot5/2,4 Ds1 chan/0 tc
add -s Lp/13 Sonet/3 Sts/2 Vt1dot5/3,1 Ds1 chan/0 tc
add -s Lp/13 Sonet/3 Sts/2 Vt1dot5/3,2 Ds1 chan/0 tc
add -s Lp/13 Sonet/3 Sts/2 Vt1dot5/3,3 Ds1 chan/0 tc
add -s Lp/13 Sonet/3 Sts/2 Vt1dot5/3,4 Ds1 chan/0 tc
add -s Lp/13 Sonet/3 Sts/2 Vt1dot5/4,1 Ds1 chan/0 tc
add -s Lp/13 Sonet/3 Sts/2 Vt1dot5/4,2 Ds1 chan/0 tc

add -s Lp/13 Sonet/3 Sts/2 Vt1dot5/4,3 Ds1 chan/0 tc
add -s Lp/13 Sonet/3 Sts/2 Vt1dot5/4,4 Ds1 chan/0 tc
add -s Lp/13 Sonet/3 Sts/2 Vt1dot5/5,1 Ds1 chan/0 tc
add -s Lp/13 Sonet/3 Sts/2 Vt1dot5/5,2 Ds1 chan/0 tc
add -s Lp/13 Sonet/3 Sts/2 Vt1dot5/5,3 Ds1 chan/0 tc
add -s Lp/13 Sonet/3 Sts/2 Vt1dot5/5,4 Ds1 chan/0 tc
add -s Lp/13 Sonet/3 Sts/2 Vt1dot5/6,1 Ds1 chan/0 tc
add -s Lp/13 Sonet/3 Sts/2 Vt1dot5/6,2 Ds1 chan/0 tc
add -s Lp/13 Sonet/3 Sts/2 Vt1dot5/6,3 Ds1 chan/0 tc
add -s Lp/13 Sonet/3 Sts/2 Vt1dot5/6,4 Ds1 chan/0 tc
add -s Lp/13 Sonet/3 Sts/2 Vt1dot5/7,1 Ds1 chan/0 tc
add -s Lp/13 Sonet/3 Sts/2 Vt1dot5/7,2 Ds1 chan/0 tc
add -s Lp/13 Sonet/3 Sts/2 Vt1dot5/7,3 Ds1 chan/0 tc
add -s Lp/13 Sonet/3 Sts/2 Vt1dot5/7,4 Ds1 chan/0 tc

add -s Aal1Ces/0001 interfacename Lp/13 Sonet/0 Sts/0 Vt1dot5/1,1 Ds1 chan/0
add -s Aal1Ces/0002 interfacename Lp/13 Sonet/0 Sts/0 Vt1dot5/1,2 Ds1 chan/0
add -s Aal1Ces/0003 interfacename Lp/13 Sonet/0 Sts/0 Vt1dot5/1,3 Ds1 chan/0
add -s Aal1Ces/0004 interfacename Lp/13 Sonet/0 Sts/0 Vt1dot5/1,4 Ds1 chan/0

add -s Aal1Ces/0005 interfacename Lp/13 Sonet/0 Sts/0 Vt1dot5/2,1 Ds1 chan/0
add -s Aal1Ces/0006 interfacename Lp/13 Sonet/0 Sts/0 Vt1dot5/2,2 Ds1 chan/0
add -s Aal1Ces/0007 interfacename Lp/13 Sonet/0 Sts/0 Vt1dot5/2,3 Ds1 chan/0
add -s Aal1Ces/0008 interfacename Lp/13 Sonet/0 Sts/0 Vt1dot5/2,4 Ds1 chan/0

add -s Aal1Ces/0009 interfacename Lp/13 Sonet/0 Sts/0 Vt1dot5/3,1 Ds1 chan/0
add -s Aal1Ces/0010 interfacename Lp/13 Sonet/0 Sts/0 Vt1dot5/3,2 Ds1 chan/0
add -s Aal1Ces/0011 interfacename Lp/13 Sonet/0 Sts/0 Vt1dot5/3,3 Ds1 chan/0
add -s Aal1Ces/0012 interfacename Lp/13 Sonet/0 Sts/0 Vt1dot5/3,4 Ds1 chan/0

add -s Aal1Ces/0013 interfacename Lp/13 Sonet/0 Sts/0 Vt1dot5/4,1 Ds1 chan/0
add -s Aal1Ces/0014 interfacename Lp/13 Sonet/0 Sts/0 Vt1dot5/4,2 Ds1 chan/0
add -s Aal1Ces/0015 interfacename Lp/13 Sonet/0 Sts/0 Vt1dot5/4,3 Ds1 chan/0
add -s Aal1Ces/0016 interfacename Lp/13 Sonet/0 Sts/0 Vt1dot5/4,4 Ds1 chan/0

add -s Aal1Ces/0017 interfacename Lp/13 Sonet/0 Sts/0 Vt1dot5/5,1 Ds1 chan/0
add -s Aal1Ces/0018 interfacename Lp/13 Sonet/0 Sts/0 Vt1dot5/5,2 Ds1 chan/0
add -s Aal1Ces/0019 interfacename Lp/13 Sonet/0 Sts/0 Vt1dot5/5,3 Ds1 chan/0
add -s Aal1Ces/0020 interfacename Lp/13 Sonet/0 Sts/0 Vt1dot5/5,4 Ds1 chan/0

add -s Aal1Ces/0021 interfacename Lp/13 Sonet/0 Sts/0 Vt1dot5/6,1 Ds1 chan/0
add -s Aal1Ces/0022 interfacename Lp/13 Sonet/0 Sts/0 Vt1dot5/6,2 Ds1 chan/0
add -s Aal1Ces/0023 interfacename Lp/13 Sonet/0 Sts/0 Vt1dot5/6,3 Ds1 chan/0
add -s Aal1Ces/0024 interfacename Lp/13 Sonet/0 Sts/0 Vt1dot5/6,4 Ds1 chan/0

add -s Aal1Ces/0025 interfacename Lp/13 Sonet/0 Sts/0 Vt1dot5/7,1 Ds1 chan/0
add -s Aal1Ces/0026 interfacename Lp/13 Sonet/0 Sts/0 Vt1dot5/7,2 Ds1 chan/0
add -s Aal1Ces/0027 interfacename Lp/13 Sonet/0 Sts/0 Vt1dot5/7,3 Ds1 chan/0
add -s Aal1Ces/0028 interfacename Lp/13 Sonet/0 Sts/0 Vt1dot5/7,4 Ds1 chan/0

add -s Aal1Ces/0029 interfacename Lp/13 Sonet/0 Sts/1 Vt1dot5/1,1 Ds1 Chan/0
add -s Aal1Ces/0030 interfacename Lp/13 Sonet/0 Sts/1 Vt1dot5/1,2 Ds1 Chan/0
add -s Aal1Ces/0031 interfacename Lp/13 Sonet/0 Sts/1 Vt1dot5/1,3 Ds1 Chan/0
add -s Aal1Ces/0032 interfacename Lp/13 Sonet/0 Sts/1 Vt1dot5/1,4 Ds1 Chan/0

add -s Aal1Ces/0033 interfacename Lp/13 Sonet/0 Sts/1 Vt1dot5/2,1 Ds1 Chan/0
add -s Aal1Ces/0034 interfacename Lp/13 Sonet/0 Sts/1 Vt1dot5/2,2 Ds1 Chan/0
add -s Aal1Ces/0035 interfacename Lp/13 Sonet/0 Sts/1 Vt1dot5/2,3 Ds1 Chan/0
add -s Aal1Ces/0036 interfacename Lp/13 Sonet/0 Sts/1 Vt1dot5/2,4 Ds1 Chan/0

add -s Aal1Ces/0037 interfacename Lp/13 Sonet/0 Sts/1 Vt1dot5/3,1 Ds1 Chan/0
add -s Aal1Ces/0038 interfacename Lp/13 Sonet/0 Sts/1 Vt1dot5/3,2 Ds1 Chan/0
add -s Aal1Ces/0039 interfacename Lp/13 Sonet/0 Sts/1 Vt1dot5/3,3 Ds1 Chan/0
add -s Aal1Ces/0040 interfacename Lp/13 Sonet/0 Sts/1 Vt1dot5/3,4 Ds1 Chan/0

add -s Aal1Ces/0041 interfacename Lp/13 Sonet/0 Sts/1 Vt1dot5/4,1 Ds1 Chan/0
add -s Aal1Ces/0042 interfacename Lp/13 Sonet/0 Sts/1 Vt1dot5/4,2 Ds1 Chan/0

add -s Aal1Ces/0043 interfacename Lp/13 Sonet/0 Sts/1 Vt1dot5/4,3 Ds1 Chan/0
add -s Aal1Ces/0044 interfacename Lp/13 Sonet/0 Sts/1 Vt1dot5/4,4 Ds1 Chan/0

add -s Aal1Ces/0045 interfacename Lp/13 Sonet/0 Sts/1 Vt1dot5/5,1 Ds1 Chan/0
add -s Aal1Ces/0046 interfacename Lp/13 Sonet/0 Sts/1 Vt1dot5/5,2 Ds1 Chan/0
add -s Aal1Ces/0047 interfacename Lp/13 Sonet/0 Sts/1 Vt1dot5/5,3 Ds1 Chan/0
add -s Aal1Ces/0048 interfacename Lp/13 Sonet/0 Sts/1 Vt1dot5/5,4 Ds1 Chan/0

add -s Aal1Ces/0049 interfacename Lp/13 Sonet/0 Sts/1 Vt1dot5/6,1 Ds1 Chan/0
add -s Aal1Ces/0050 interfacename Lp/13 Sonet/0 Sts/1 Vt1dot5/6,2 Ds1 Chan/0
add -s Aal1Ces/0051 interfacename Lp/13 Sonet/0 Sts/1 Vt1dot5/6,3 Ds1 Chan/0
add -s Aal1Ces/0052 interfacename Lp/13 Sonet/0 Sts/1 Vt1dot5/6,4 Ds1 Chan/0

add -s Aal1Ces/0053 interfacename Lp/13 Sonet/0 Sts/1 Vt1dot5/7,1 Ds1 Chan/0
add -s Aal1Ces/0054 interfacename Lp/13 Sonet/0 Sts/1 Vt1dot5/7,2 Ds1 Chan/0
add -s Aal1Ces/0055 interfacename Lp/13 Sonet/0 Sts/1 Vt1dot5/7,3 Ds1 Chan/0
add -s Aal1Ces/0056 interfacename Lp/13 Sonet/0 Sts/1 Vt1dot5/7,4 Ds1 Chan/0

add -s Aal1Ces/0057 interfacename Lp/13 Sonet/0 Sts/2 Vt1dot5/1,1 Ds1 Chan/0
add -s Aal1Ces/0058 interfacename Lp/13 Sonet/0 Sts/2 Vt1dot5/1,2 Ds1 Chan/0
add -s Aal1Ces/0059 interfacename Lp/13 Sonet/0 Sts/2 Vt1dot5/1,3 Ds1 Chan/0
add -s Aal1Ces/0060 interfacename Lp/13 Sonet/0 Sts/2 Vt1dot5/1,4 Ds1 Chan/0

add -s Aal1Ces/0061 interfacename Lp/13 Sonet/0 Sts/2 Vt1dot5/2,1 Ds1 Chan/0
add -s Aal1Ces/0062 interfacename Lp/13 Sonet/0 Sts/2 Vt1dot5/2,2 Ds1 Chan/0
add -s Aal1Ces/0063 interfacename Lp/13 Sonet/0 Sts/2 Vt1dot5/2,3 Ds1 Chan/0
add -s Aal1Ces/0064 interfacename Lp/13 Sonet/0 Sts/2 Vt1dot5/2,4 Ds1 Chan/0

add -s Aal1Ces/0065 interfacename Lp/13 Sonet/0 Sts/2 Vt1dot5/3,1 Ds1 Chan/0
add -s Aal1Ces/0066 interfacename Lp/13 Sonet/0 Sts/2 Vt1dot5/3,2 Ds1 Chan/0
add -s Aal1Ces/0067 interfacename Lp/13 Sonet/0 Sts/2 Vt1dot5/3,3 Ds1 Chan/0
add -s Aal1Ces/0068 interfacename Lp/13 Sonet/0 Sts/2 Vt1dot5/3,4 Ds1 Chan/0

add -s Aal1Ces/0069 interfacename Lp/13 Sonet/0 Sts/2 Vt1dot5/4,1 Ds1 Chan/0
add -s Aal1Ces/0070 interfacename Lp/13 Sonet/0 Sts/2 Vt1dot5/4,2 Ds1 Chan/0
add -s Aal1Ces/0071 interfacename Lp/13 Sonet/0 Sts/2 Vt1dot5/4,3 Ds1 Chan/0
add -s Aal1Ces/0072 interfacename Lp/13 Sonet/0 Sts/2 Vt1dot5/4,4 Ds1 Chan/0

add -s Aal1Ces/0073 interfacename Lp/13 Sonet/0 Sts/2 Vt1dot5/5,1 Ds1 Chan/0
add -s Aal1Ces/0074 interfacename Lp/13 Sonet/0 Sts/2 Vt1dot5/5,2 Ds1 Chan/0
add -s Aal1Ces/0075 interfacename Lp/13 Sonet/0 Sts/2 Vt1dot5/5,3 Ds1 Chan/0
add -s Aal1Ces/0076 interfacename Lp/13 Sonet/0 Sts/2 Vt1dot5/5,4 Ds1 Chan/0

add -s Aal1Ces/0077 interfacename Lp/13 Sonet/0 Sts/2 Vt1dot5/6,1 Ds1 Chan/0
add -s Aal1Ces/0078 interfacename Lp/13 Sonet/0 Sts/2 Vt1dot5/6,2 Ds1 Chan/0
add -s Aal1Ces/0079 interfacename Lp/13 Sonet/0 Sts/2 Vt1dot5/6,3 Ds1 Chan/0
add -s Aal1Ces/0080 interfacename Lp/13 Sonet/0 Sts/2 Vt1dot5/6,4 Ds1 Chan/0

add -s Aal1Ces/0081 interfacename Lp/13 Sonet/0 Sts/2 Vt1dot5/7,1 Ds1 Chan/0
add -s Aal1Ces/0082 interfacename Lp/13 Sonet/0 Sts/2 Vt1dot5/7,2 Ds1 Chan/0
add -s Aal1Ces/0083 interfacename Lp/13 Sonet/0 Sts/2 Vt1dot5/7,3 Ds1 Chan/0
add -s Aal1Ces/0084 interfacename Lp/13 Sonet/0 Sts/2 Vt1dot5/7,4 Ds1 Chan/0

...
...
...

add -s Aal1Ces/0309 interfacename Lp/13 Sonet/3 Sts/2 Vt1dot5/1,1 Ds1 Chan/0
add -s Aal1Ces/0310 interfacename Lp/13 Sonet/3 Sts/2 Vt1dot5/1,2 Ds1 Chan/0
add -s Aal1Ces/0311 interfacename Lp/13 Sonet/3 Sts/2 Vt1dot5/1,3 Ds1 Chan/0
add -s Aal1Ces/0312 interfacename Lp/13 Sonet/3 Sts/2 Vt1dot5/1,4 Ds1 Chan/0

add -s Aal1Ces/0313 interfacename Lp/13 Sonet/3 Sts/2 Vt1dot5/2,1 Ds1 Chan/0
add -s Aal1Ces/0314 interfacename Lp/13 Sonet/3 Sts/2 Vt1dot5/2,2 Ds1 Chan/0
add -s Aal1Ces/0315 interfacename Lp/13 Sonet/3 Sts/2 Vt1dot5/2,3 Ds1 Chan/0
add -s Aal1Ces/0316 interfacename Lp/13 Sonet/3 Sts/2 Vt1dot5/2,4 Ds1 Chan/0

add -s Aal1Ces/0317 interfacename Lp/13 Sonet/3 Sts/2 Vt1dot5/3,1 Ds1 Chan/0
add -s Aal1Ces/0318 interfacename Lp/13 Sonet/3 Sts/2 Vt1dot5/3,2 Ds1 Chan/0
add -s Aal1Ces/0319 interfacename Lp/13 Sonet/3 Sts/2 Vt1dot5/3,3 Ds1 Chan/0
add -s Aal1Ces/0320 interfacename Lp/13 Sonet/3 Sts/2 Vt1dot5/3,4 Ds1 Chan/0

add -s Aal1Ces/0321 interfacename Lp/13 Sonet/3 Sts/2 Vt1dot5/4,1 Ds1 Chan/0
add -s Aal1Ces/0322 interfacename Lp/13 Sonet/3 Sts/2 Vt1dot5/4,2 Ds1 Chan/0
add -s Aal1Ces/0323 interfacename Lp/13 Sonet/3 Sts/2 Vt1dot5/4,3 Ds1 Chan/0
add -s Aal1Ces/0324 interfacename Lp/13 Sonet/3 Sts/2 Vt1dot5/4,4 Ds1 Chan/0

add -s Aal1Ces/0325 interfacename Lp/13 Sonet/3 Sts/2 Vt1dot5/5,1 Ds1 Chan/0
add -s Aal1Ces/0326 interfacename Lp/13 Sonet/3 Sts/2 Vt1dot5/5,2 Ds1 Chan/0
add -s Aal1Ces/0327 interfacename Lp/13 Sonet/3 Sts/2 Vt1dot5/5,3 Ds1 Chan/0
add -s Aal1Ces/0328 interfacename Lp/13 Sonet/3 Sts/2 Vt1dot5/5,4 Ds1 Chan/0

add -s Aal1Ces/0329 interfacename Lp/13 Sonet/3 Sts/2 Vt1dot5/6,1 Ds1 Chan/0
add -s Aal1Ces/0330 interfacename Lp/13 Sonet/3 Sts/2 Vt1dot5/6,2 Ds1 Chan/0
add -s Aal1Ces/0331 interfacename Lp/13 Sonet/3 Sts/2 Vt1dot5/6,3 Ds1 Chan/0
add -s Aal1Ces/0332 interfacename Lp/13 Sonet/3 Sts/2 Vt1dot5/6,4 Ds1 Chan/0

add -s Aal1Ces/0333 interfacename Lp/13 Sonet/3 Sts/2 Vt1dot5/7,1 Ds1 Chan/0
add -s Aal1Ces/0334 interfacename Lp/13 Sonet/3 Sts/2 Vt1dot5/7,2 Ds1 Chan/0
add -s Aal1Ces/0335 interfacename Lp/13 Sonet/3 Sts/2 Vt1dot5/7,3 Ds1 Chan/0
add -s Aal1Ces/0336 interfacename Lp/13 Sonet/3 Sts/2 Vt1dot5/7,4 Ds1 Chan/0

### For each Aal1Ces, it’s Aep addressToCall must be set to the ATM address of the BasicRate-GroupServer for that service (ISUP,PRI)

### Issue the following command

d Nsta/6 Vgs BragS/0<---------- Assume BragS/0 was used for ISUP

### The following is a sample output from a PVG

8> d nsta/6 vgs brags/0

```
Nsta/6 Vgs BragS/0
  localAddress = 45972555123400000F000000010020480D556000
  tdmLogLaw    = autoConfigured
  bufferSize   = 50 msec
  packetDelayVariationTolerance = 20 msec
  lossIntegrationPeriod        = 5 seconds
  ingressGain                  = 0 dB
  egressGain                   = 0 dB
  echoCancellation             = g165Mode
  minimumEchoReturnLoss        = 6 dB
  echoCancelComfortNoiseGeneration = enabled
  echoCancellationTailLength       = autoConfigure msec
  defaultVoiceRate                 = 64kG711
  tone2100Rate                     = 64kG711
  silenceDetectionHangOverTime     = 200 msec
  silenceSuppression               = disabled
  silenceSuppressionThreshold      = -40 dBm0
  signalingType                    = unsignaled
  toneset                          = canadaUsa
  minimumDtmfPowerLevel            = -27 dBm0
  digitTransport                   = relay
  vbdTransport                     = useTone2100RateIfNegotiated
ok          2002-10-21 09:47:39.37
```

### Assign the Aep address to call given by the above command

```
add Aal1Ces/1 Aep
set Aal1Ces/1 Aep addressToCall 45972555123400000F000000010020480D556000
```

### The above command needs to be repeated for each Aal1Ces/x Aep that is going to run ISUP
### Now for PRI set up
### Issue the following command

```
d Nsta/6 Vgs BragS/1<---------- Assume BragS/1 was used for PRI
```

### The following is a sample output from a PVG

```
8> d Nsta/6 Vgs BragS/1
```

```
Nsta/6 Vgs BragS/1
  localAddress = 45972555123400000F000000010020480D556001
  tdmLogLaw    = autoConfigured
  bufferSize   = 50 msec
  packetDelayVariationTolerance = 20 msec
  lossIntegrationPeriod        = 5 seconds
  ingressGain                  = 0 dB
  egressGain                   = 0 dB
  echoCancellation             = g165Mode
  minimumEchoReturnLoss        = 6 dB
  echoCancelComfortNoiseGeneration = enabled
  echoCancellationTailLength       = autoConfigure msec
  defaultVoiceRate                 = 64kG711
  tone2100Rate                     = 64kG711
  silenceDetectionHangOverTime     = 200 msec
  silenceSuppression               = disabled
  silenceSuppressionThreshold      = -40 dBm0
  signalingType                    = unsignaled
  toneset                        = sameAsVgs
  minimumDtmfPowerLevel            = -27 dBm0
  digitTransport                 = relay
  vbdTransport                     = useTone2100RateIfNegotiated
ok          2002-10-21 09:48:44.40
```

add Aal1Ces/2 Aep

set Aal1Ces/2 Aep addressToCall 45972555123400000F000000010020480D556001

### The above command needs to be repeated for each Aal1Ces/x Aep that is going to run PRI

## 22.2 Passport 8600s

The following is a set of minimum commands for setting up PVG15000 interconnecting a VSP3 via Gigabit Ethernet on the redundant PP8600s.

***Note:*** This list does not include standard Passport 8600 configuration.

Passport 8600-00

```
#
# MLT CONFIGURATION
#
mlt 1 create
mlt 1 perform-tagging enable
```

```
mlt 1 add ports 9/1,10/1

#
# VLAN CONFIGURATION
#
vlan 13 create byport 1 color 2
vlan 13 add-mlt 1
vlan 13 ports add 8/3-8/8,9/1,10/1 member portmember
vlan 13 ip create 192.168.9.2/255.255.255.0 mac_offset 7
vlan 13 ip igmp mrdisc mrdisc-enable disable
vlan 13 ip ospf interface-type passive
vlan 13 ip ospf enable
vlan 13 ip vrrp 13 address 192.168.9.1
vlan 13 ip vrrp 13 enable

#
# OSPF CONFIGURATION
#
ip ospf admin-state enable
ip ospf as-boundary-router enable
ip ospf router-id 172.30.244.2
ip ospf enable
ip ospf area 13.13.13.13 create
ip ospf interface 192.168.9.2 area 13.13.13.13
ip ospf interface 172.30.244.2 area 13.13.13.13

#
# IP ROUTE POLICY CONFIGURATION
#

ip route-policy "drop_corwan" seq 1 create
ip route-policy "drop_corwan" seq 1 enable
ip route-policy "drop_corwan" seq 1 action deny
ip route-policy "drop_corwan" seq 1 match-protocol ospf
ip route-policy "drop_corwan" seq 1 match-network "corwan"
ip route-policy "drop_corwan" seq 1 set-metric-type type2
ip route-policy "_rpsStaticOs" seq 5555 create
ip route-policy "_rpsStaticOs" seq 5555 enable
ip route-policy "_rpsStaticOs" seq 5555 action permit
ip route-policy "_rpsLocalOs" seq 5555 create
ip route-policy "_rpsLocalOs" seq 5555 enable
```

```
ip route-policy "_rpsLocalOs" seq 5555 action permit

#
# IP REDISTRIBUTION CONFIGURATION
#

ip ospf redistribute static create
ip ospf redistribute static route-policy "_rpsStaticOs"
ip ospf redistribute static enable
ip ospf redistribute direct create
ip ospf redistribute direct route-policy "_rpsLocalOs"
ip ospf redistribute direct enable
```

***Note:*** An alternative to the IP Route Policy and the Redistribution of Local routes configuration would be to configure the vsp VLAN interfaces as Passive OSPF interfaces. There is an advantage by using Passive interfaces where only those interfaces would be announced in OSPF route advertisements and not all the local subnets.

Passport 8600-01

```
#
# MLT CONFIGURATION
#

mlt 1 create
mlt 1 perform-tagging enable
mlt 1 add ports 9/1,10/1

#
# VLAN configuration
#

config vlan 13 create byport 1 color 2
config vlan 13 add-mlt 1
config vlan 13 ports add 8/3-8/8,9/1,10/1 member portmember
config vlan 13 ip create 192.168.9.3/255.255.255.0 mac_offset 7
config vlan 13 ip igmp mrdisc mrdisc-enable disable
config vlan 13 ip ospf interface-type passive
config vlan 13 ip ospf enable
```

```
config vlan 13 ip vrrp 13 address 192.168.9.1
config vlan 13 ip vrrp 13 priority 50
config vlan 13 ip vrrp 13 enable

#
# OSPF CONFIGURATION
#

ip ospf admin-state enable
ip ospf as-boundary-router enable
ip ospf router-id 172.30.244.6
ip ospf enable
ip ospf area 13.13.13.13 create
ip ospf interface 192.168.9.3 area 13.13.13.13
ip ospf interface 172.30.244.6 area 13.13.13.13

#
# IP ROUTE POLICY CONFIGURATION
#

ip route-policy "drop_corwan" seq 1 create
ip route-policy "drop_corwan" seq 1 enable
ip route-policy "drop_corwan" seq 1 action deny
ip route-policy "drop_corwan" seq 1 match-protocol ospf
ip route-policy "drop_corwan" seq 1 match-network "corwan"
ip route-policy "drop_corwan" seq 1 set-metric-type type2
ip route-policy "_rpsStaticOs" seq 5555 create
ip route-policy "_rpsStaticOs" seq 5555 enable
ip route-policy "_rpsStaticOs" seq 5555 action permit
ip route-policy "_rpsLocalOs" seq 5555 create
ip route-policy "_rpsLocalOs" seq 5555 enable
ip route-policy "_rpsLocalOs" seq 5555 action permit

#
# IP REDISTRIBUTION CONFIGURATION
#

ip ospf redistribute static create
ip ospf redistribute static route-policy "_rpsStaticOs"
ip ospf redistribute static enable
ip ospf redistribute direct create
```

```
ip ospf redistribute direct route-policy "_rpsLocalOs"
ip ospf redistribute direct enable
```

***Note:*** An alternative to the IP Route Policy and the Redistribution of Local routes configuration would be to configure the vsp VLAN interfaces as Passive OSPF interfaces. There is an advantage by using Passive interfaces where only those interfaces would be announced in OSPF route advertisements and not all the local subnets.

# 23.0 Appendix: Configuration details for M2K to PP8600

## 23.1 M2K

The following is a sample .ini file retrieved from a 8-span M2K utilizing PRI on Megaco protocol interconnected to Dual Passport 8600s:

```
;***************
;** Ini File **
;***************

;board: TrunkPack 1610
;serial Number: 223856
;slot Number: 31
;Software Version: 4.20.108.9
;------------------------------


[SYSTEM Params]

SYSLOGSERVERIP = 47.142.158.47
ENABLESYSLOG = 1

[BSP Params]

TDMBUSMASTERSLAVESELECTION = 1
TDMBUSLOCALREFERENCE = -1
INIFILEVERSION = 100

[Analog Params]


[ControlProtocols Params]

GATEWAYNAME = "DS1"
ENDPOINTNAME = "/"
TRUNKNAME = "/0"
MGCPCOMPATIBILITYPROFILE = 20
PROVISIONEDCALLAGENTSPORTS = 2944, 2944, 2944, 2944, 2944, 2944, 2944, 2944,
2944, 2944
MGCONTROLPROTOCOLTYPE = 2
```

[MGCP Params]

CALLAGENTIP = 172.18.18.32
CALLAGENTPORT = 2944

[MEGACO Params]

KEEPALIVEENABLED = 1
MEGACOTRUNKIDOFFSET = 1
PHYSTERMNAMEPATTERN = 'DS1/0*/*'
LOGICALRTPTERMPATTERN = 'DS1RTP/*'
LOGICALATMTERMPATTERN = 'DS1ATM/*'
EP_NUM = 1
EP_MIN_0 = 0
EP_MIN_1 = 0
EP_MIN_2 = 0
EP_MIN_3 = 24
EP_MIN_4 = 0
EP_MAX_0 = 9
EP_MAX_1 = 0
EP_MAX_2 = 0
EP_MAX_3 = 0
EP_MAX_4 = 0
RTP_NUM_0 = 1
RTP_NUM_1 = 0
ATM_NUM_0 = 1
ATM_NUM_1 = 0

[PSTN Params]

TDMBUSPSTNAUTOCLOCKENABLE = 1
PROTOCOLTYPE = 28
CLOCKMASTER = 1
TERMINATIONSIDE_0 = 1
TERMINATIONSIDE_1 = 1
TERMINATIONSIDE_2 = 1
TERMINATIONSIDE_3 = 1
TERMINATIONSIDE_4 = 1
TERMINATIONSIDE_5 = 1
TERMINATIONSIDE_6 = 1
TERMINATIONSIDE_7 = 1

TERMINATIONSIDE_8 = 1
TERMINATIONSIDE_9 = 0
TERMINATIONSIDE_10 = 0
TERMINATIONSIDE_11 = 0
TERMINATIONSIDE_12 = 0
TERMINATIONSIDE_13 = 0
TERMINATIONSIDE_14 = 0
TERMINATIONSIDE_15 = 0
FRAMINGMETHOD_0 = 0
FRAMINGMETHOD_1 = 0
FRAMINGMETHOD_2 = 0
FRAMINGMETHOD_3 = 0
FRAMINGMETHOD_4 = 0
FRAMINGMETHOD_5 = 0
FRAMINGMETHOD_6 = 0
FRAMINGMETHOD_7 = 0
FRAMINGMETHOD_8 = 1
FRAMINGMETHOD_9 = 1
FRAMINGMETHOD_10 = 1
FRAMINGMETHOD_11 = 1
FRAMINGMETHOD_12 = 1
FRAMINGMETHOD_13 = 1
FRAMINGMETHOD_14 = 1
FRAMINGMETHOD_15 = 1
LINECODE_0 = 0
LINECODE_1 = 0
LINECODE_2 = 0
LINECODE_3 = 0
LINECODE_4 = 0
LINECODE_5 = 0
LINECODE_6 = 0
LINECODE_7 = 0
LINECODE_8 = 2
LINECODE_9 = 2
LINECODE_10 = 2
LINECODE_11 = 2
LINECODE_12 = 2
LINECODE_13 = 2
LINECODE_14 = 2
LINECODE_15 = 2
ISDNOUTCALLSBEHAVIOR_0 = 16384

ISDNOUTCALLSBEHAVIOR_1 = 16384
ISDNOUTCALLSBEHAVIOR_2 = 16384
ISDNOUTCALLSBEHAVIOR_3 = 16384
ISDNOUTCALLSBEHAVIOR_4 = 16384
ISDNOUTCALLSBEHAVIOR_5 = 16384
ISDNOUTCALLSBEHAVIOR_6 = 16384
ISDNOUTCALLSBEHAVIOR_7 = 16384
ISDNOUTCALLSBEHAVIOR_8 = 0
ISDNOUTCALLSBEHAVIOR_9 = 0
ISDNOUTCALLSBEHAVIOR_10 = 0
ISDNOUTCALLSBEHAVIOR_11 = 0
ISDNOUTCALLSBEHAVIOR_12 = 0
ISDNOUTCALLSBEHAVIOR_13 = 0
ISDNOUTCALLSBEHAVIOR_14 = 0
ISDNOUTCALLSBEHAVIOR_15 = 0
IUAINTERFACEID_0 = 696
IUAINTERFACEID_1 = 720
IUAINTERFACEID_2 = 744
IUAINTERFACEID_3 = 768
IUAINTERFACEID_4 = 792
IUAINTERFACEID_5 = 816
IUAINTERFACEID_6 = 840
IUAINTERFACEID_7 = 864
IUAINTERFACEID_8 = -1
IUAINTERFACEID_9 = -1
IUAINTERFACEID_10 = -1
IUAINTERFACEID_11 = -1
IUAINTERFACEID_12 = -1
IUAINTERFACEID_13 = -1
IUAINTERFACEID_14 = -1
IUAINTERFACEID_15 = -1
Q931RELAYMODE = 3

[Voice Engine Params]

ENABLECONTINUITYTONES = 1
ENABLECONTINUITYTEST = 1
DTMFTRANSPORTTYPE = 2
DJBUFMINDELAY = 150
FLASHHOOKPERIOD = 700

[WEB Params]

[H323 Params]

ISFASTCONNECTUSED = 1
IPDIFFSERV = 46
APPLICATIONPROFILE = -1

[SCTP Params]

[VXML Params]

## 23.2 Passport 8600s

The following is a set of minimum commands for setting up M2K interconnection on redundant PP8600s. This list does not include standard Passport 8600 configuration.

### PP8600-0

```
#
# VLAN CONFIGURATION
#
vlan 422 create byport 1 name "Audiocode"
vlan 422 add-mlt 1
vlan 422 ports remove 1/1-1/7,2/1-2/33,3/1-3/48,4/1-4/39,4/42-4/48,9/1-9/8,10/1,10/5 member portmember
vlan 422 ports add 1/8,2/34,4/40-4/41 member portmember
vlan 422 qos-level 6
vlan 422 ip create 172.20.1.2/255.255.255.192 mac_offset 6
vlan 422 ip vrrp 22 address 172.20.1.1
vlan 422 ip vrrp 22 backup-master enable
vlan 422 ip vrrp 22 enable
#
# PORT CONFIGURATION - PHASE II
#
ethernet 4/40 enable-diffserv true
ethernet 4/40 access-diffserv true
ethernet 4/40 name "M2K00&M2K01-primary"
ethernet 4/40 ip traffic-filter create
ethernet 4/40 ip traffic-filter add set 304
```

```
ethernet 4/40 ip traffic-filter default-action forward
ethernet 4/40 ip traffic-filter enable
ethernet 4/40 stg 1 stp disable
ethernet 4/41 enable-diffserv true
ethernet 4/41 access-diffserv true
ethernet 4/41 name "M2K02-primary"
ethernet 4/41 ip traffic-filter create
ethernet 4/41 ip traffic-filter add set 304
ethernet 4/41 ip traffic-filter default-action forward
ethernet 4/41 ip traffic-filter enable
ethernet 4/41 stg 1 stp disable
```

**PP8600-1**

```
#
# VLAN CONFIGURATION
#
vlan 422 create byport 1 name "Audiocode"
vlan 422 add-mlt 1
vlan 422 ports remove 1/1-1/7,2/1-2/33,3/1-3/48,4/1-4/39,4/42-4/48,10/1,10/5 member
portmember
vlan 422 ports add 1/8,2/34,4/40-4/41 member portmember
vlan 422 qos-level 6
vlan 422 ip create 172.20.1.3/255.255.255.192 mac_offset 9
vlan 422 ip vrrp 22 address 172.20.1.1
vlan 422 ip vrrp 22 backup-master enable
vlan 422 ip vrrp 22 enable
#
# PORT CONFIGURATION - PHASE II
#
ethernet 4/40 enable-diffserv true
ethernet 4/40 access-diffserv true
ethernet 4/40 name "M2K00&M2K01-alternate"
ethernet 4/40 ip traffic-filter create
ethernet 4/40 ip traffic-filter add set 304
ethernet 4/40 ip traffic-filter default-action forward
ethernet 4/40 ip traffic-filter enable
ethernet 4/40 stg 1 stp disable
ethernet 4/41 enable-diffserv true
ethernet 4/41 access-diffserv true
ethernet 4/41 name "M2K02-alternate"
ethernet 4/41 ip traffic-filter create
```

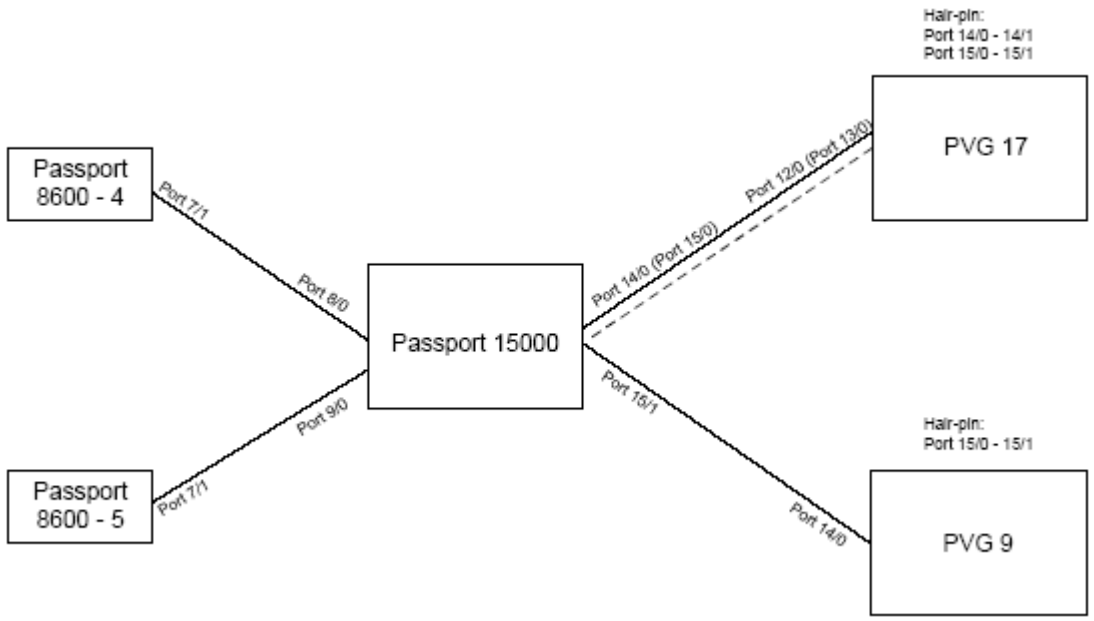
ethernet 4/41 ip traffic-filter add set 304
ethernet 4/41 ip traffic-filter default-action forward
ethernet 4/41 ip traffic-filter enable
ethernet 4/41 stg 1 stp disable

# 24.0 Appendix: PVG VR - Passport 8600

## 24.1 Sample Setup

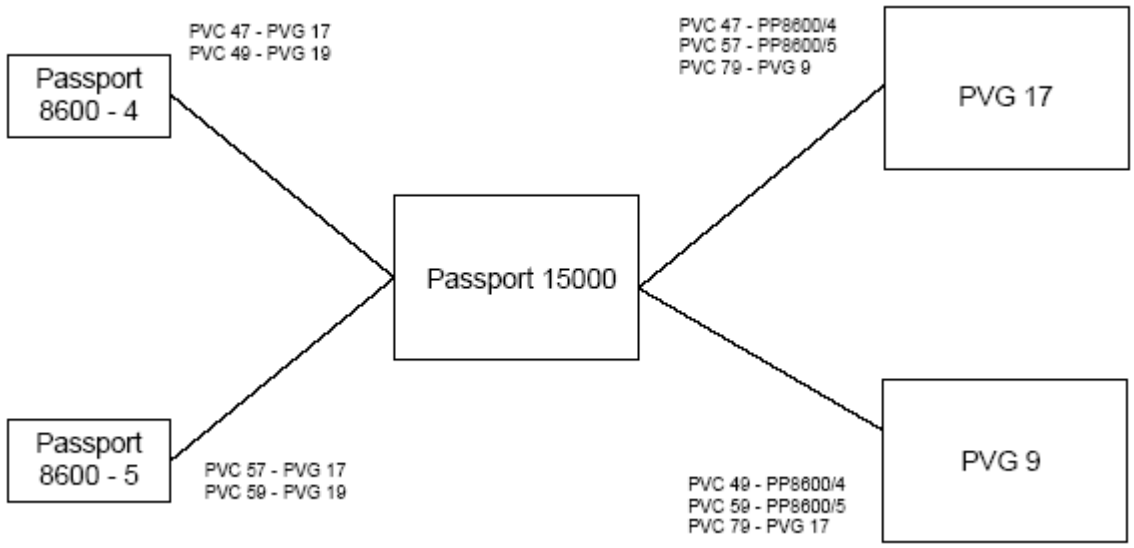
### 24.1.1 Physical Connection

**Figure 82 Physical Connection**



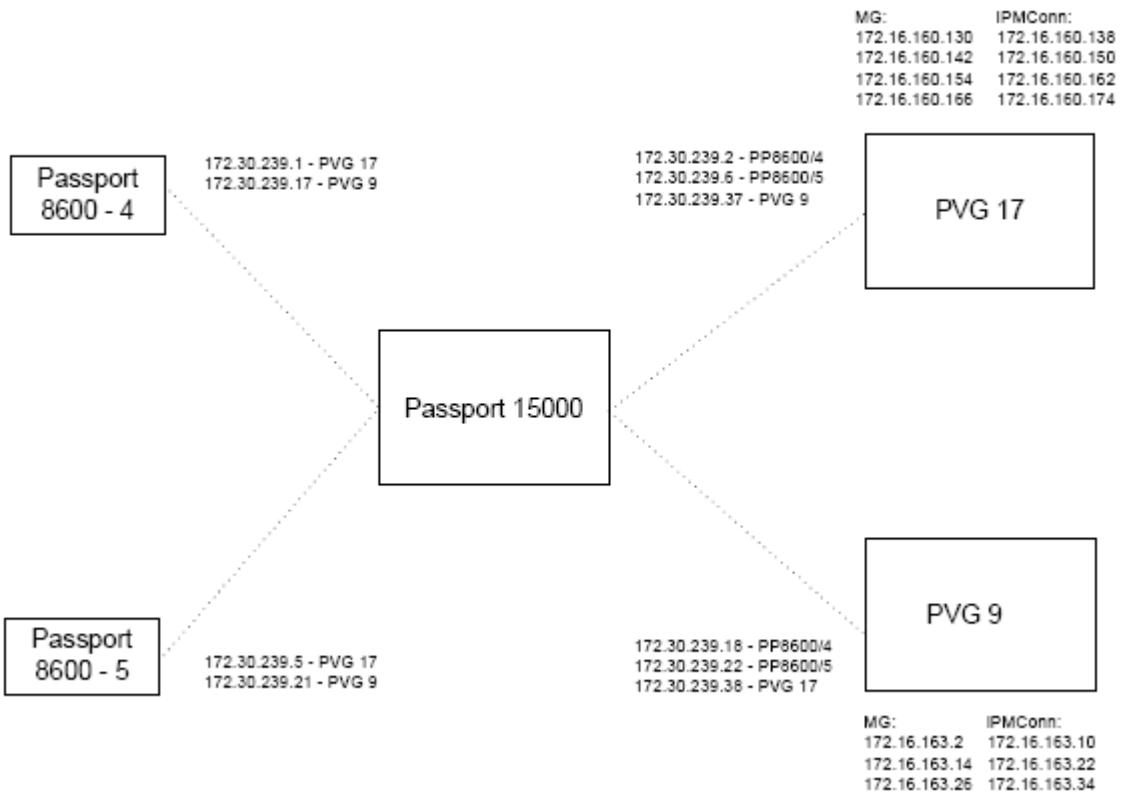

### 24.1.2 ATM VCCs

**Figure 83 VCCs Connection**




### 24.1.3 A.3 IP Address Scheme

**Figure 84 IP Address**




## 24.2 Working Configuration

### 24.2.1 PVG VR Hairpin Specific Configuration

The following lists the set of commands required to provision a single PVG VR using hairpin. There are one VSP (inserted in slot 2) and four ATM 4-port OC12 card in slot 12 - 15. Redundant uplink to Passport 15000 is done by the ATM FPs in slots 12 and 13. Due to the limited number of 4p OC12 cards, we didn't set up LAPS to protect hairpin. However, to achieve the maximum redundancy, LAPS is required. The following configuration does not include any standard PVG provisioning.

This section tries to avoid the overlapped information with PVG VRAP configuration. Thus, we only show those commands which are unique to PVG VR Hairpin setup. For common information, please refer to Section 24.2.3:

We use PVG 17 as the example.

#

# Set up Hairpin Port

#

```
add -s lp/14 sonet/0 sts/0 cell

add -s lp/14 sonet/1 sts/0 cell

set lp/14 sonet/0 clockingSource module

set lp/14 sonet/1 clockingSource module

set lp/14 sonet/0 sts/0 concat 12

set lp/14 sonet/1 sts/0 concat 12

add -s atmif/140 interfaceName lp/14 sonet/0 sts/0

add -s atmif/141 interfaceName lp/14 sonet/1 sts/0


add -s atmif/140 pnni[1]


#

# Set up ATM OAM F5

#

set atmif/140 oamSegmentBoundary yes

set atmif/140 endToEndLoopback on

set atmif/141 oamSegmentBoundary yes

set atmif/141 endToEndLoopback on


#

# Set up VCCs on the Hairpin

#

add -s atmif/140 pnni
```

1. Instead of PNNI, UNI component can be used too. The goal is to give a system-assigned ATM address to the port in order to support SPVC.

```
add -s atmif/141 vcc/0.42 nep

add -s atmif/141 vcc/0.52 nep

set atmif/141 vcc/0.42 vcd tm txTrafficDescType 6

set atmif/141 vcc/0.42 vcd tm txTrafficDescParm 1 1200 2 600 3 160

set atmif/141 vcc/0.42 vcd tm atmServiceCategory nrtvbr


set atmif/141 vcc/0.52 vcd tm txTrafficDescType 6

set atmif/141 vcc/0.52 vcd tm txTrafficDescParm 1 608832 2 608832 3 1

set atmif/141 vcc/0.52 vcd tm atmServiceCategory rtvbr


#

# Set up VSP for ISUP Signaling

#

add nsta/2 vgs

set nsta/2 vgs hostname pp172

set nsta/2 vgs defaultPacketLogLaw mulaw


add -s nsta/2 vgs ctrl/mg spvcap

set nsta/2 vgs ctrl/mg ipAddress 172.16.160.130

set nsta/2 vgs ctrl/mg spvcap addressToCall !47525450490000F000110000000020480D008C00[2]

set nsta/2 vgs ctrl/mg spvcap remotevpivci 0.42

set nsta/2 vgs ctrl/mg spvcap pcr 1200
```

2. This is the ATM address of PNNI/UNI interface. This address can be viewed by executing "l atmif/* pnni addr/*" or "l atmif/* uni addr/*" in the operational mode.

```
set nsta/2 vgs ctrl/mg spvcap scr 600

set nsta/2 vgs ctrl/mg spvcap mbs 160


add -s nsta/2 vgs ctrl/mg udpport/2427

add -s nsta/2 vgs vgcp

set nsta/2 vgs vgcp udpPortConnection Nsta/2 Vgs Ctrl/mediaGateway UdpPort/2427


#

# Set up VSP for Bearer

#

add -s nsta/2 vgs ipmconn spvcap

set nsta/2 vgs ipmconn ipAddress 172.16.160.138

set nsta/2 vgs ipmconn spvcap addressToCall !47525450490000F000110000000020480D008C00[3]

set nsta/2 vgs ipmconn spvcap remotevpivci 0.52

set nsta/2 vgs ipmconn spvcap pcr 608832

set nsta/2 vgs ipmconn spvcap scr 608832

set nsta/2 vgs ipmconn spvcap mbs 1


add -s nsta/2 vgs brags/0

set nsta/2 vgs brags/0 tdmLogLaw mulaw


#

# VR Protocol Ports Provisioning for Hairpin Connections
```

3. This is the ATM address of PNNI/UNI interface. This address can be viewed by executing "l atmif/* pnni addr/*" or "l atmif/* uni addr/*" in the operational mode.

```
#
add -s vr/1 ip
set vr/1 virtualRouterProcessor lp/0

add -s vr/1 pp/pvg172_mg ipport log/172.16.160.129 netmask 255.255.255.252
add -s vr/1 pp/pvg172_bearer ipport log/172.16.160.137 netmask 255.255.255.252

add atmmpe/720
add atmmpe/721

set atmmpe/720 linktoprotocolport vr/1 pp/pvg172_mg
set atmmpe/721 linktoprotocolport vr/1 pp/pvg172_bearer

set atmmpe/720 ac/1 atmconnection atmif/141 vcc/0.42 nep
set atmmpe/721 ac/1 atmconnection atmif/141 vcc/0.52 nep

#
# OSPF Provisioning for Hairpin Connections
#
add -s vr/1 ip ospf
add -s vr/1 ip ospf area/13.13.13.13
add -s vr/1 ip ospf stub/13.13.13.13,0
set vr/1 ip ospf area/13.13.13.13 importAsExtern importNoExternal

add -s vr/1 pp/pvg172_mg ipport log/172.16.160.129 ospfif
set vr/1 pp/pvg172_mg ipport log/172.16.160.129 ospfif areaid 13.13.13.13
```

set vr/1 pp/pvg172_mg ipport log/172.16.160.129 ospfif ifType passive

### 24.2.2 PVG VRAP Specific Configuration

The hardware layout used by this  is identical to Section 24.2.1.

This section tries to avoid the overlapped information with PVG VR Hairpin configuration. Thus, we only show those commands which are unique to PVG VRAP. For common section, please refer to Section 24.2.3:

```
#
# Setup IP Port on VR for VRAP
#

add -s vr/1 ip
set vr/1 virtualRouterProcessor lp/0
set vr/1 vpnMode carrier

add -s vr/1 pp/pvg ipport log/172.16.160.129 netmask 255.255.255.252
add -s vr/1 pp/pvg ipport log/172.16.160.137 netmask 255.255.255.252

add vm/0
set vr/1 pp/pvg linktomedia vm/0 if/0



#
# Add VRAP for ISUP Signaling
#

add nsta/2 vgs ctrl/mg vrap
set nsta/2 vgs ctrl/mg ipAddress 172.16.160.130
set nsta/2 vgs ctrl/mg vrap subnetAccessName vr/1 pp/pvg ipport log/172.16.160.129

add -s nsta/2 vgs ctrl/mg udpport/2427
add -s nsta/2 vgs vgcp
set nsta/2 vgs vgcp udpPortConnection nsta/2 Vgs Ctrl/mediaGateway UdpPort/2427
```

```
#
# Add VRAP for Bearer
#

add -s nsta/2 vgs ipmconn vrap
set nsta/2 vgs ipmconn ipAddress 172.16.160.138
set nsta/2 vgs ipmconn vrap subnetAccessName vr/1 pp/pvg ipport log/172.16.160.137

#
# OSPF Provisioning for VRAP Port
#
add -s vr/1 ip ospf
add -s vr/1 ip ospf area/13.13.13.13
add -s vr/1 ip ospf stub/13.13.13.13,0
set vr/1 ip ospf area/13.13.13.13 importAsExtern importNoExternal

add -s vr/1 pp/pvg ipport log/172.16.160.129 ospfif
set vr/1 pp/pvg ipport log/172.16.160.129 ospfif iftype passive
set vr/1 pp/pvg ipport log/172.16.160.129 ospfif areaid 13.13.13.13
```

### 24.2.3 Common Section for PVG VR Hairpin and PVG VRAP Configuration

```
#
# Set up MOD and PNNI
#
set mod nodeprefix 47525450490000F00011000000
add -s artg pnni cfgnode/72
set artg pnni cfgnode/72 peergroupid 4847525450490000F00000000000
check prov
act prov
confirm prov
```

```
#
# Set up UPlink Port (LAPS)
#
add -s lp/12 sonet/0
add -s lp/13 sonet/0
set lp/12 sonet/0 clockingSource module
set lp/13 sonet/0 clockingSource module

add lp/12 eng arc ov
set lp/12 eng arc ov protectedConnectionPoolCapacity 3072
add lp/13 eng arc ov
set lp/13 eng arc ov protectedConnectionPoolCapacity 3072

add -s laps/120 sts/0 cell
set laps/120 workingLine lp/12 sonet/0
set laps/120 protectionLine lp/13 sonet/0
set laps/120 mode bidirectional
set laps/120 sts/0 concat 12

add -s atmif/120 interfaceName laps/120 sts/0

#
# Set up ATM OAM F5
#
set atmif/120 oamSegmentBoundary yes
set atmif/120 endToEndLoopback on
```

```
#
# Set up Timing
#
add lp/0 eds1/0
add ns
set ns primaryreference Lp/0 EDS1/0
set ns secondaryReference lp/12 sonet/0

#
# Set up VCCs on Uplinks
#
add -s atmif/120 vcc/0.47 nep
add -s atmif/120 vcc/0.57 nep
add -s atmif/120 vcc/0.79 nep


set atmif/120 vcc/0.47 vcd tm txTrafficDescType 6
set atmif/120 vcc/0.47 vcd tm txTrafficDescParm 1 4800 2 4800 3 1 [4]
set atmif/120 vcc/0.47 vcd tm atmServiceCategory rtvbr


set atmif/120 vcc/0.57 vcd tm txTrafficDescType 6
set atmif/120 vcc/0.57 vcd tm txTrafficDescParm 1 4800 2 4800 3 1
set atmif/120 vcc/0.57 vcd tm atmServiceCategory nrtvbr
```

4. Assume we have a total of four VSP cards on PVG 17. This VCC aggregates all connect conrol message from all VSPs.

```
set atmif/120 vcc/0.79 vcd tm txTrafficDescType 6

set atmif/120 vcc/0.79 vcd tm txTrafficDescParm 1 304416 2 304416 3 1 [5]

set atmif/120 vcc/0.79 vcd tm atmServiceCategory rtvbr


#

# VR Protocol Ports Provisioning for Uplink Connections

#

add -s vr/1 pp/8600-4 ipport log/172.30.239.2 netmask 255.255.255.252

add -s vr/1 pp/8600-5 ipport log/172.30.239.6 netmask 255.255.255.252

add -s vr/1 pp/pvg9 ipport log/172.30.239.37 netmask 255.255.255.252


add atmmpe/4

add atmmpe/5

add atmmpe/9


set atmmpe/4 linktoprotocolport vr/1 pp/8600-4

set atmmpe/5 linktoprotocolport vr/1 pp/8600-5

set atmmpe/9 linktoprotocolport vr/1 pp/pvg9


set atmmpe/4 ac/1 atmconnection atmif/120 vcc/0.47 nep

set atmmpe/5 ac/1 atmconnection atmif/120 vcc/0.57 nep

set atmmpe/9 ac/1 atmconnection atmif/120 vcc/0.79 nep
```

5. We assume that between PVG 17 and PVG 9, there will be no more than 1008 simultaneous call. The PCR/SCR/MBS values are defined according to the assumption. The real value on the field should be defined based on the expected number of DS0s between PVGs.

```
#
# OSPF Provisioning for Uplink Connections
#
add -s vr/1 pp/8600-4 ipport log/172.30.239.2 ospfif
add -s vr/1 pp/8600-5 ipport log/172.30.239.6 ospfif

set vr/1 pp/8600-4 ipport log/172.30.239.2 ospfif areaid 13.13.13.13
set vr/1 pp/8600-5 ipport log/172.30.239.6 ospfif areaid 13.13.13.13

set vr/1 pp/8600-4 ipport log/172.30.239.2 ospfif hello 1
set vr/1 pp/8600-5 ipport log/172.30.239.6 ospfif hello 1

set vr/1 pp/8600-4 ipport log/172.30.239.2 ospfif rtrdead 4
set vr/1 pp/8600-5 ipport log/172.30.239.6 ospfif rtrdead 4

#
# Static Route Provisioning
#
add -s vr/1 ip static route/0.0.0.0,0.0.0.0,0 nh/172.30.239.1
add -s vr/1 ip static route/0.0.0.0,0.0.0.0,0 nh/172.30.239.5
add -s vr/1 ip static route/172.16.163.0,255.255.255.0,0 nh/172.30.239.38

#
# Static InARP Entry
#
```

add -s vr/1 ip arp host/172.30.239.1,0

add -s vr/1 ip arp host/172.30.239.5,0

set vr/1 ip arp host/172.30.239.1,0 permanentVirtualCircuitNumber 1

set vr/1 ip arp host/172.30.239.5,0 permanentVirtualCircuitNumber 1

### 24.2.4 Configuration Details for Passport 15000

The following lists the set of commands required to provision relayed PVCs on Passport 15000. The following configuration does not include any standard Passport provisioning.

```
#
# Set up LAPS
#
add -s lp/14 sonet/0
add -s lp/15 sonet/0
set lp/14 sonet/0 clockingSource module
set lp/15 sonet/0 clockingSource module

add lp/14 eng arc ov
set lp/14 eng arc ov protectedConnectionPoolCapacity 3072
add lp/15 eng arc ov
set lp/15 eng arc ov protectedConnectionPoolCapacity 3072

add -s laps/140 sts/0 cell
set laps/140 workingLine lp/14 sonet/0
set laps/140 protectionLine lp/15 sonet/0
set laps/140 mode bidirectional
set laps/140 sts/0 concat 12

add -s atmif/140 interfaceName laps/140 sts/0

#
# Set up Timing
```

400

```
#
add lp/0 eds1/0
add ns
set ns primaryreference Lp/0 EDS1/0

#
# Set up ATM OAM F5
#
set atmif/80 oamSegmentBoundary yes
set atmif/80 endToEndLoopback on
set atmif/90 oamSegmentBoundary yes
set atmif/90 endToEndLoopback on
set atmif/140 oamSegmentBoundary yes
set atmif/140 endToEndLoopback on
set atmif/151 oamSegmentBoundary yes
set atmif/151 endToEndLoopback on

#
# Relay PVCs
#
add -s atmif/140 vcc/0.47 nrp
add -s atmif/140 vcc/0.57 nrp
add -s atmif/140 vcc/0.79 nrp

add -s atmif/151 vcc/0.79 nrp
```

```
add -s atmif/80 vcc/0.47 nrp

add -s atmif/90 vcc/0.57 nrp


set atmif/80 vcc/0.47 nrp nexthop atmif/140 vcc/0.47 nrp

set atmif/90 vcc/0.57 nrp nexthop atmif/140 vcc/0.57 nrp


set atmif/140 vcc/0.79 nrp nexthop atmif/151 vcc/0.79 nrp


#

# Size VCCs

#

set atmif/80 vcc/0.47 vcd tm txTrafficDescType 6

set atmif/80 vcc/0.47 vcd tm txTrafficDescParm 1 4800 2 4800 3 1

set atmif/80 vcc/0.47 vcd tm atmServiceCategory rtvbr


set atmif/90 vcc/0.57 vcd tm txTrafficDescType 6

set atmif/90 vcc/0.57 vcd tm txTrafficDescParm 1 4800 2 4800 3 1

set atmif/90 vcc/0.57 vcd tm atmServiceCategory rtvbr


set atmif/140 vcc/0.47 vcd tm txTrafficDescType 6

set atmif/140 vcc/0.47 vcd tm txTrafficDescParm 1 4800 2 4800 3 1

set atmif/140 vcc/0.47 vcd tm atmServiceCategory rtvbr


set atmif/140 vcc/0.57 vcd tm txTrafficDescType 6

set atmif/140 vcc/0.57 vcd tm txTrafficDescParm 1 4800 2 4800 3 1

set atmif/140 vcc/0.57 vcd tm atmServiceCategory rtvbr
```

set atmif/140 vcc/0.79 vcd tm txTrafficDescType 6

set atmif/140 vcc/0.79 vcd tm txTrafficDescParm 1 304416 2 304416 3 1 [6]

set atmif/140 vcc/0.79 vcd tm atmServiceCategory rtvbr

set atmif/151 vcc/0.79 vcd tm txTrafficDescType 6

set atmif/151 vcc/0.79 vcd tm txTrafficDescParm 1 304416 2 304416 3 1

set atmif/151 vcc/0.79 vcd tm atmServiceCategory rtvbr

### 24.2.5 Configuration Details for Passport 8600

Here we only use Passport 8600-5 as an example. The configuration for Passport 8600-4 should be identical.

#

# VLAN CONFIGURATION

#

vlan 57 create byport 1

vlan 57 ports remove 1/1-1/48,2/1-2/48,3/1-3/48,4/1-4/48,7/2-7/4,8/1-8/8,9/1-9/8,10/1-10/8 member portmember

vlan 57 ports add 7/1 member portmember

vlan 57 ip create 172.30.239.5/255.255.255.252 mac_offset 3

vlan 57 ip igmp mrdisc mrdisc-enable disable

vlan 57 ip ospf enable

vlan 57 ip ospf hello-interval 1

vlan 57 ip ospf dead-interval 4

6. We assume that between PVG 17 and PVG 9, there will be no more than 1008 simultaneous call. Thus, the PCR/SCR/MBS values are defined according to the assumption. The real value on the field should be defined based on the expected number of DS0s between PVGs.

vlan 59 create byport 1

vlan 59 ports remove 1/1-1/48,2/1-2/48,3/1-3/48,4/1-4/48,7/2-7/4,8/1-8/8,9/1-9/8,10/1-10/8 member portmember

vlan 59 ports add 7/1 member portmember

vlan 59 ip create 172.30.239.21/255.255.255.252 mac_offset 18

vlan 59 ip igmp mrdisc mrdisc-enable disable

vlan 59 ip ospf enable

vlan 59 ip ospf hello-interval 1

vlan 59 ip ospf dead-interval 4

#

# IP & RIP CONFIGURATION

#

ip static-route create 172.16.160.0/255.255.255.0 next-hop 172.30.239.6 cost 10 preference 100

ip static-route create 172.16.163.0/255.255.255.0 next-hop 172.30.239.22 cost 10 preference 100

#

# OSPF CONFIGURATION

#

ip ospf admin-state enable

ip ospf as-boundary-router enable

ip ospf router-id 172.30.244.6

ip ospf enable

ip ospf area 13.13.13.13 create

ip ospf area 13.13.13.13 stub true

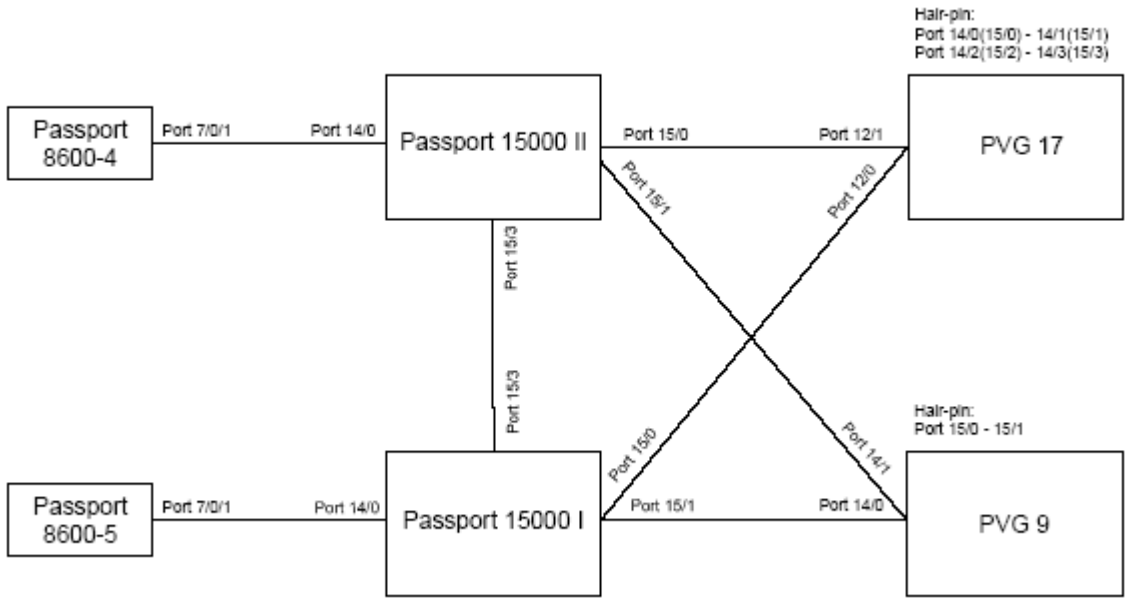
```
ip ospf area 13.13.13.13 import-summaries false
ip ospf interface 172.30.239.5 area 13.13.13.13
ip ospf interface 172.30.239.21 area 13.13.13.13


#
# ATM CONFIGURATION
#
atm 7/1 state enable
atm 7/1 clock-source loop-timed
atm 7/1 pvc create 0.57
atm 7/1 pvc f5-oam 0.57 enable send 1 retry 1 up 1 down 1 trap enable
atm 7/1 pvc create 0.59
atm 7/1 pvc f5-oam 0.59 enable send 1 retry 1 up 1 down 1 trap enable
atm 7/1 pvc 1483 ip create 57 0.57 172.30.239.6 enable 1
atm 7/1 pvc 1483 ip create 59 0.59 172.30.239.22 enable 1
```

# 25.0 Appendix: PVG VR - Passport VR

## 25.1 Lab Setup

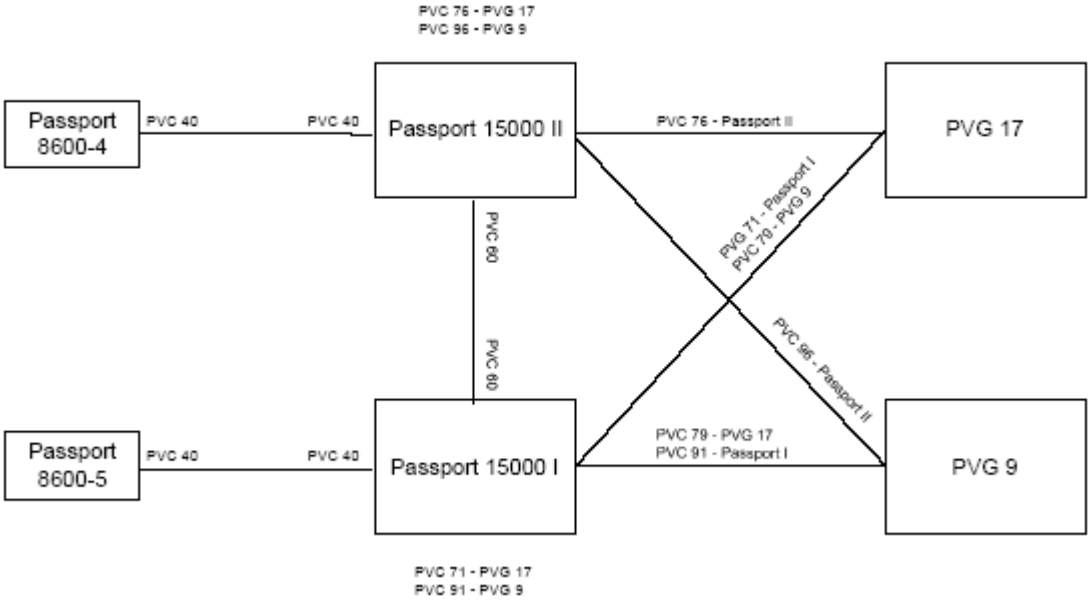
### 25.1.1 Physical Connection

**Figure 85 Physical Connection**



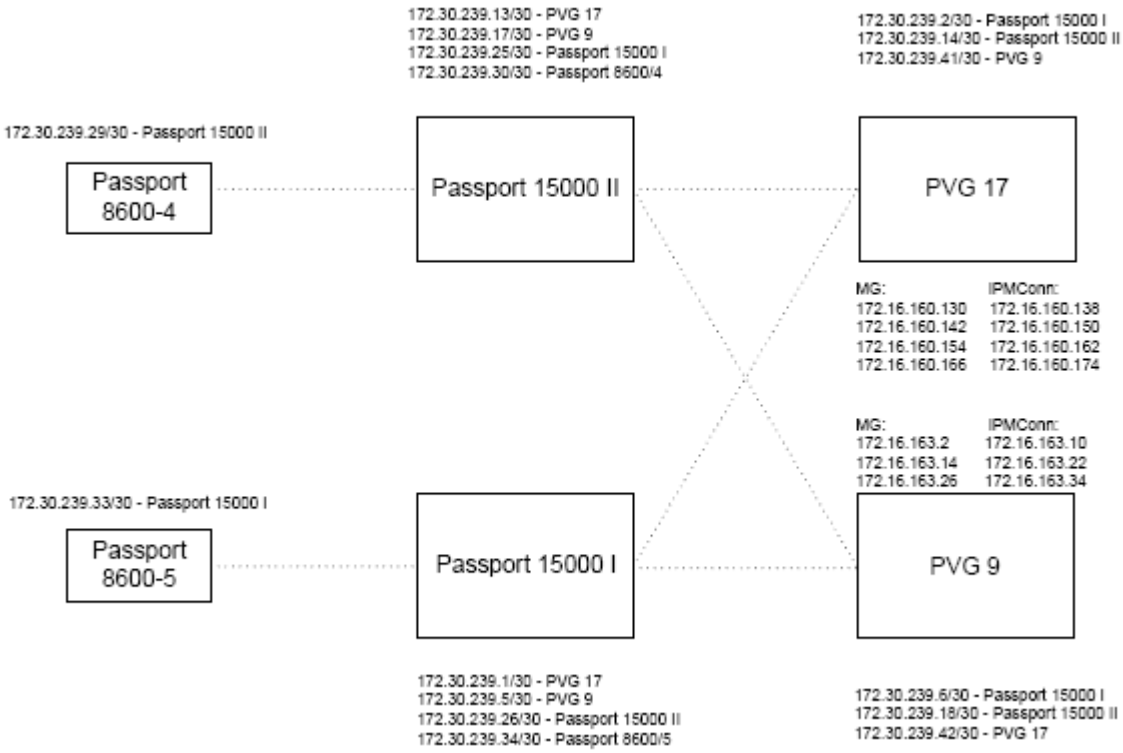

### 25.1.2 ATM VCCs

**Figure 86 ATM VCC Numbering**




### 25.1.3 IP Address Scheme

**Figure 87 IP Address Space**




## 25.2 Working Congifuration

### 25.2.1 Configuration Details for PVG VR

The following lists the set of commands required to provision a single VR with one VSP (inserted in slot 2), while provisioning a redundant hairpin configuration through two ATM FPs (inserted in slots 14 and 15). The following configuration does not include any standard PVG provisioning. Please note that, due to limited number of 4p OC12 cards in the lab, we didn't use LAPS in this case to protect the uplink. However, as we recommend in the engineering guideline, the LAPS is required for any inter-link between Passports and PVGs.

We use PVG 17 as the example.

#

# Set up MOD and PNNI

#

set mod nodeprefix 47525450490000F00011000000

add -s artg pnni cfgnode/72

```
set artg pnni cfgnode/72 peergroupid 4847525450490000F00000000000
check prov
act prov
confirm prov

#
# Set up UPlink Port
#
add -s lp/12 sonet/0 sts/0 cell
add -s lp/12 sonet/1 sts/0 cell
set lp/12 sonet/0 clockingSource module
set lp/12 sonet/1 clockingSource module
set lp/12 sonet/0 sts/0 concat 12
set lp/12 sonet/1 sts/0 concat 12
add -s atmif/120 interfaceName lp/12 sonet/0 sts/0
add -s atmif/121 interfaceName lp/12 sonet/1 sts/0

#
# Set up Hairpin Port (LAPS)
#
add -s lp/14 sonet/0
add -s lp/14 sonet/1
add -s lp/15 sonet/0
add -s lp/15 sonet/1

set lp/14 sonet/0 clockingSource module
```

```
set lp/14 sonet/1 clockingSource module

set lp/15 sonet/0 clockingSource module

set lp/15 sonet/1 clockingSource module


add lp/14 eng arc ov

set lp/14 eng arc ov protectedConnectionPoolCapacity 3072

add lp/15 eng arc ov

set lp/15 eng arc ov protectedConnectionPoolCapacity 3072


add -s laps/140 sts/0 cell

set laps/140 workingLine lp/14 sonet/0

set laps/140 protectionLine lp/15 sonet/0

set laps/140 mode bidirectional

set laps/140 sts/0 concat 12


add -s laps/141 sts/0 cell

set laps/141 workingLine lp/14 sonet/1

set laps/141 protectionLine lp/15 sonet/1

set laps/141 mode bidirectional

set laps/141 sts/0 concat 12


add -s atmif/140 interfaceName laps/140 sts/0

add -s atmif/141 interfaceName laps/141 sts/0


#

# Set up ATM OAM F5
```

```
#
set atmif/120 oamSegmentBoundary yes
set atmif/120 endToEndLoopback on
set atmif/121 oamSegmentBoundary yes
set atmif/121 endToEndLoopback on
set atmif/140 oamSegmentBoundary yes
set atmif/140 endToEndLoopback on
set atmif/141 oamSegmentBoundary yes
set atmif/141 endToEndLoopback on

#
# Set up Timing
#
add lp/0 eds1/0
add ns
set ns primaryreference Lp/0 EDS1/0
set ns secondaryReference lp/12 sonet/0

check prov
act prov
confirm prov

#
# Set up VCCs on the Hairpin
#
```

add -s atmif/140 pnni [7]

add -s atmif/141 vcc/0.42 nep

add -s atmif/141 vcc/0.52 nep

set atmif/141 vcc/0.42 vcd tm txTrafficDescType 6

set atmif/141 vcc/0.42 vcd tm txTrafficDescParm 1 1200 2 600 3 160

set atmif/141 vcc/0.42 vcd tm atmServiceCategory nrtvbr

set atmif/141 vcc/0.52 vcd tm txTrafficDescType 6

set atmif/141 vcc/0.52 vcd tm txTrafficDescParm 1 608832 2 608832 3 1

set atmif/141 vcc/0.52 vcd tm atmServiceCategory rtvbr

#

# Set up VSP for ISUP link

#

add nsta/2 vgs

set nsta/2 vgs hostname pp172

set nsta/2 vgs defaultPacketLogLaw mulaw

add -s nsta/2 vgs ctrl/mg spvcap

set nsta/2 vgs ctrl/mg ipAddress 172.16.160.130

set nsta/2 vgs ctrl/mg spvcap addressToCall !47525450490000F000110000000020480D008C00[8]

set nsta/2 vgs ctrl/mg spvcap remotevpivci 0.42

7. Instead of PNNI, UNI component can be used to assign an ATM address to the port.

8. This is the ATM address of PNNI/UNI interface. This address can be viewed by executing "l atmif/* pnni addr/*" or "l atmif/* uni addr/*" in the operational mode.

```
set nsta/2 vgs ctrl/mg spvcap pcr 1200

set nsta/2 vgs ctrl/mg spvcap scr 600

set nsta/2 vgs ctrl/mg spvcap mbs 160


add -s nsta/2 vgs ctrl/mg udpport/2427

add -s nsta/2 vgs vgcp

set nsta/2 vgs vgcp udpPortConnection Nsta/2 Vgs Ctrl/mediaGateway UdpPort/2427


add -s nsta/2 vgs ipmconn spvcap

set nsta/2 vgs ipmconn ipAddress 172.16.160.138

set nsta/2 vgs ipmconn spvcap addressToCall !47525450490000F000110000000020480D008C00
9

set nsta/2 vgs ipmconn spvcap remotevpivci 0.52

set nsta/2 vgs ipmconn spvcap pcr 608832

set nsta/2 vgs ipmconn spvcap scr 608832

set nsta/2 vgs ipmconn spvcap mbs 1


add -s nsta/2 vgs brags/0

set nsta/2 vgs brags/0 tdmLogLaw mulaw


#

# Set up VCCs on Uplinks

#

add -s atmif/120 vcc/0.71 nep
```

9. This is the system-assigned ATM address of ATMIF/140

add -s atmif/120 vcc/0.79 nep

add -s atmif/121 vcc/0.76 nep

set atmif/120 vcc/0.71 vcd tm txTrafficDescType 6

set atmif/120 vcc/0.71 vcd tm txTrafficDescParm 1 4800 2 4800 3 1 [10]

set atmif/120 vcc/0.71 vcd tm atmServiceCategory rtvbr

set atmif/121 vcc/0.76 vcd tm txTrafficDescType 6

set atmif/121 vcc/0.76 vcd tm txTrafficDescParm 1 4800 2 4800 3 1

set atmif/121 vcc/0.76 vcd tm atmServiceCategory rtvbr

set atmif/120 vcc/0.79 vcd tm txTrafficDescType 6

set atmif/120 vcc/0.79 vcd tm txTrafficDescParm 1 608832 2 608832 3 1 [11]

set atmif/120 vcc/0.79 vcd tm atmServiceCategory rtvbr

#

# VR Protocol Ports Provisioning for Hairpin Connections

#

add -s vr/1 ip

set vr/1 virtualRouterProcessor lp/0

10. We assume a total of four VSP cards are used on PVG 17. This VCC aggregates the connection control messages from all VSPs.

11. We assume that between PVG 17 and PVG 9, there will be no more than 2016 simultaneous call. Thus, the PCR/SCR/MBS values are defined according to the assumption. The real value on the field should be defined based on the expected number of DS0s between PVGs.

```
add -s vr/1 pp/pvg172_mg ipport log/172.16.160.129 netmask 255.255.255.252
add -s vr/1 pp/pvg172_bearer ipport log/172.16.160.137 netmask 255.255.255.252

add atmmpe/720
add atmmpe/721

set atmmpe/720 linktoprotocolport vr/1 pp/pvg172_mg
set atmmpe/721 linktoprotocolport vr/1 pp/pvg172_bearer

set atmmpe/720 ac/1 atmconnection atmif/141 vcc/0.42 nep
set atmmpe/721 ac/1 atmconnection atmif/141 vcc/0.52 nep

#
# VR Protocol Ports Provisioning for Uplink Connections
#
add -s vr/1 pp/passport-i ipport log/172.30.239.2 netmask 255.255.255.252
add -s vr/1 pp/passport-ii ipport log/172.30.239.14 netmask 255.255.255.252
add -s vr/1 pp/pvg9 ipport log/172.30.239.41 netmask 255.255.255.252

add atmmpe/1
add atmmpe/2
add atmmpe/9

set atmmpe/1 linktoprotocolport vr/1 pp/passport-i
set atmmpe/2 linktoprotocolport vr/1 pp/passport-ii
set atmmpe/9 linktoprotocolport vr/1 pp/pvg9
```

```
set atmmpe/1 ac/1 atmconnection atmif/120 vcc/0.71 nep

set atmmpe/2 ac/1 atmconnection atmif/121 vcc/0.76 nep

set atmmpe/9 ac/1 atmconnection atmif/120 vcc/0.79 nep


#

# Static Route Provisioning

#

add -s vr/1 ip static route/0.0.0.0,0.0.0.0,0 nh/172.30.239.1

add -s vr/1 ip static route/0.0.0.0,0.0.0.0,0 nh/172.30.239.13

add -s vr/1 ip static route/172.16.163.0,255.255.255.0,0 nh/172.30.239.42
```

### 25.2.2 Configuration Details for PVG VR with VRAP

This section only shows the configuration which pertains to VRAP. The rest of the configuration will be identical to Section 25.2.1

```
#

# Setup IP Port on VR for VRAP

#


add -s vr/1 ip

set vr/1 virtualRouterProcessor lp/0

set vr/1 vpnMode carrier


add -s vr/1 pp/pvg ipport log/172.16.160.129 netmask 255.255.255.252

add -s vr/1 pp/pvg ipport log/172.16.160.137 netmask 255.255.255.252


add vm/0

set vr/1 pp/pvg linktomedia vm/0 if/0
```

```
#
# Add VRAP for ISUP Signaling
#

add nsta/2 vgs ctrl/mg vrap
set nsta/2 vgs ctrl/mg ipAddress 172.16.160.130
set nsta/2 vgs ctrl/mg vrap subnetAccessName vr/1 pp/pvg ipport log/172.16.160.129

add -s nsta/2 vgs ctrl/mg udpport/2427
add -s nsta/2 vgs vgcp
set nsta/2 vgs vgcp udpPortConnection nsta/2 Vgs Ctrl/mediaGateway UdpPort/2427

#
# Add VRAP for Bearer
#

add -s nsta/2 vgs ipmconn vrap
set nsta/2 vgs ipmconn ipAddress 172.16.160.138
set nsta/2 vgs ipmconn vrap subnetAccessName vr/1 pp/pvg ipport log/172.16.160.137
```

### 25.2.3 Configuration Details for Passport VR

The following lists the set of commands required to provision a single VR on Passport 15000. The following configuration does not include any standard Passport provisioning. Please note that, due to limited number of 4p OC12 cards in the lab, we didn't use LAPS in this case to protect the links between Passport VR and PVG VR. However, as we recommend in the engineering guideline, the LAPS is required.

We only use the connection to/from PVG 17 on Passport 15000 I as the example.The configuration of other PVG connections and another Passport 15000 should be identical.

```
#

# Set up Timing

#
```

```
add lp/0 eds1/0
add ns
set ns primaryreference Lp/0 EDS1/0

#
# Create and Size PVCs
#
add -s atmif/140 vcc/0.40 nep
add -s atmif/150 vcc/0.71 nep
add -s atmif/150 vcc/0.79 nrp
add -s atmif/151 vcc/0.79 nrp
add -s atmif/153 vcc/0.60 nep

set atmif/150 vcc/0.79 nrp nexthop atmif/151 vcc/0.79 nrp

set atmif/140 vcc/0.40 vcd tm txTrafficDescType 6
set atmif/140 vcc/0.40 vcd tm txTrafficDescParm 1 6900 2 6900 3 1[12]
set atmif/140 vcc/0.40 vcd tm atmServiceCategory rtvbr

set atmif/150 vcc/0.71 vcd tm txTrafficDescType 6
set atmif/150 vcc/0.71 vcd tm txTrafficDescParm 1 4800 2 4800 3 1
set atmif/150 vcc/0.71 vcd tm atmServiceCategory rtvbr

set atmif/150 vcc/0.79 vcd tm txTrafficDescType 6
```

12. Assume we have four VSP3 on PVG 17 and 3 VSP2 on PVG 9

```
set atmif/150 vcc/0.79 vcd tm txTrafficDescParm 1 608832 2 608832 3 1
set atmif/150 vcc/0.79 vcd tm atmServiceCategory rtvbr

set atmif/151 vcc/0.79 vcd tm txTrafficDescType 6
set atmif/151 vcc/0.79 vcd tm txTrafficDescParm 1 608832 2 608832 3 1
set atmif/151 vcc/0.79 vcd tm atmServiceCategory rtvbr

set atmif/153 vcc/0.60 vcd tm txTrafficDescType 6
set atmif/153 vcc/0.60 vcd tm txTrafficDescParm 1 1000 2 500 3 220
set atmif/153 vcc/0.60 vcd tm atmServiceCategory rtvbr

#
# Set up ATM OAM F5
#
set atmif/140 oamSegmentBoundary yes
set atmif/140 endToEndLoopback on
set atmif/150 oamSegmentBoundary yes
set atmif/150 endToEndLoopback on
set atmif/151 oamSegmentBoundary yes
set atmif/151 endToEndLoopback on
set atmif/153 oamSegmentBoundary yes
set atmif/153 endToEndLoopback on

#
# VR Protocol Ports Provisioning
#
```

```
add -s vr/1 ip

set vr/1 virtualRouterProcessor lp/0


add -s vr/1 pp/pvg17 ipport log/172.30.239.1 netmask 255.255.255.252

add atmmpe/17

set atmmpe/17 linktoprotocolport vr/1 pp/pvg17

set atmmpe/17 ac/1 atmconnection atmif/150 vcc/0.71 nep


add vr/1 ip ospf area/0.0.0.0

set vr/1 ip ospf area/0.0.0.0 areasummary sendAreaSummary


add -s vr/1 pp/8600-5 ipport log/172.30.239.34 netmask 255.255.255.252

add -s vr/1 pp/area0 ipport log/172.30.239.26 netmask 255.255.255.252


add atmmpe/5

set atmmpe/5 linktoprotocolport vr/1 pp/8600-5

set atmmpe/5 ac/1 atmconnection atmif/140 vcc/0.40 nep


add atmmpe/0

set atmmpe/0 linktoprotocolport vr/1 pp/area0

set atmmpe/0 ac/1 atmconnection atmif/153 vcc/0.60 nep


add vr/1 pp/8600-5 ipport log/172.30.239.34 ospfif

set vr/1 pp/8600-5 ipport log/172.30.239.34 ospfif areaid 0.0.0.0

set vr/1 pp/8600-5 ipport log/172.30.239.34 ospfif hello 1

set vr/1 pp/8600-5 ipport log/172.30.239.34 ospfif rtrdead 4
```

```
add vr/1 pp/area0 ipport log/172.30.239.26 ospfif

set vr/1 pp/area0 ipport log/172.30.239.26 ospfif areaid 0.0.0.0

set vr/1 pp/area0 ipport log/172.30.239.26 ospfif hello 1

set vr/1 pp/area0 ipport log/172.30.239.26 ospfif rtrdead 4


set vr/1 ip ospf asBdrRtrStatus true

add vr/1 ip ospf AreaAggregateEntry/0.0.0.0,summarylink,172.16.160.0,255.255.252.0


#

# Static Route Provisioning

#

add -s vr/1 ip static route/0.0.0.0,0.0.0.0,0 nh/172.30.239.33

add -s vr/1 ip static route/172.16.160.0,255.255.255.0,0 nh/172.30.239.2


#

# Static InARP Entry

#

add -s vr/1 ip arp host/172.30.239.33,0

set vr/1 ip arp host/172.30.239.33,0 permanentVirtualCircuitNumber 1
```

### 25.2.4 Configuration Details for Passport 8600

Here, we only use Passport 8600-5 as an example. The configuration of Passport 8600-4 should be identical.

```
#

# VLAN CONFIGURATION

#
```

vlan 40 create byport 1

vlan 40 ports remove 1/1-1/48,2/1-2/48,3/1-3/48,4/1-4/48,7/2-7/4,8/1-8/8,9/1-9/8,10/1-10/8 member portmember

vlan 40 ports add 7/1 member portmember

vlan 40 ip create 172.30.239.33/255.255.255.252 mac_offset 3

vlan 40 ip igmp mrdisc mrdisc-enable disable

vlan 40 ip ospf enable

vlan 40 ip ospf hello-interval 1

vlan 40 ip ospf dead-interval 4

#

# IP & RIP CONFIGURATION

#

ip static-route create 172.16.160.0/255.255.252.0 next-hop 172.30.239.34 cost 10 preference 100

#

# OSPF CONFIGURATION

#

ip ospf admin-state enable

ip ospf as-boundary-router enable

ip ospf router-id 172.30.244.6

ip ospf enable [13]

#

13. The OSPF interface of 172.16.239.33 doesn't show up here because it is located in Area 0.0.0.0.

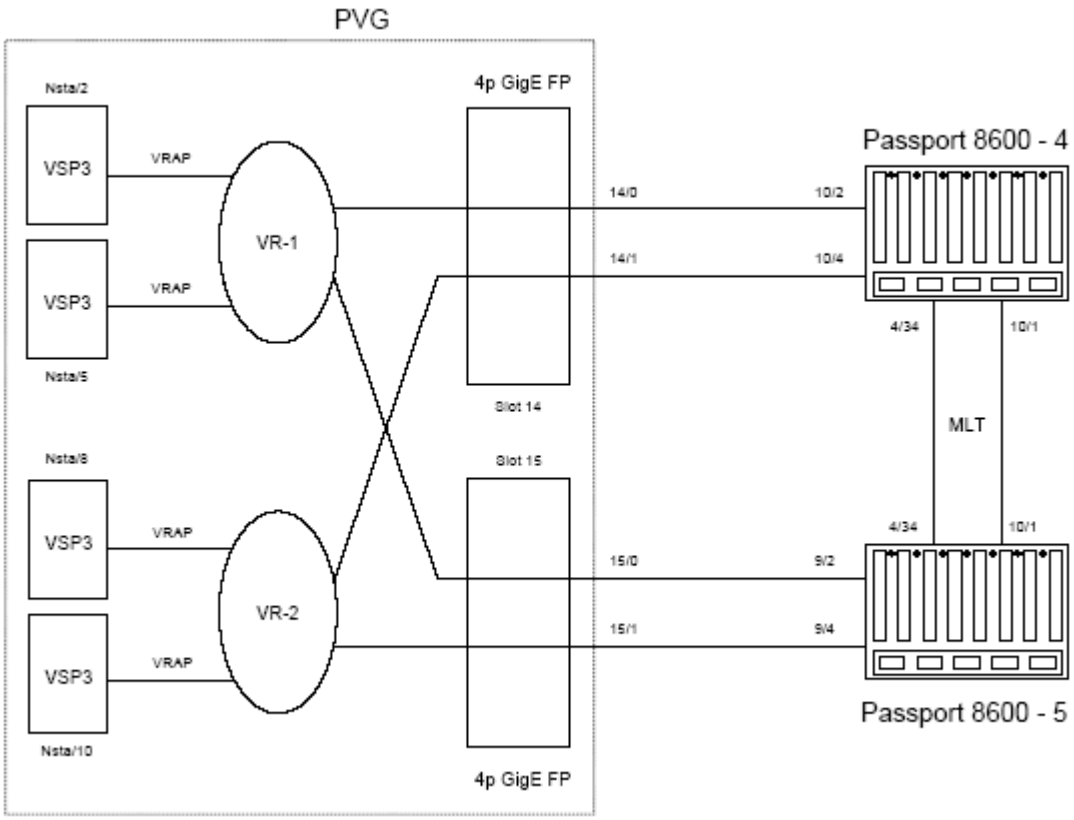
```
# ATM CONFIGURATION
#
atm 7/1 state enable
atm 7/1 clock-source loop-timed
atm 7/1 pvc create 0.40
atm 7/1 pvc f5-oam 0.40 enable send 1 retry 1 up 1 down 1 trap enable
atm 7/1 pvc 1483 ip create 40 0.40 172.30.239.34 enable 1
```

# 26.0 Appendix: PVG VRAP - Passport 8600

## 26.1 Sample Setup

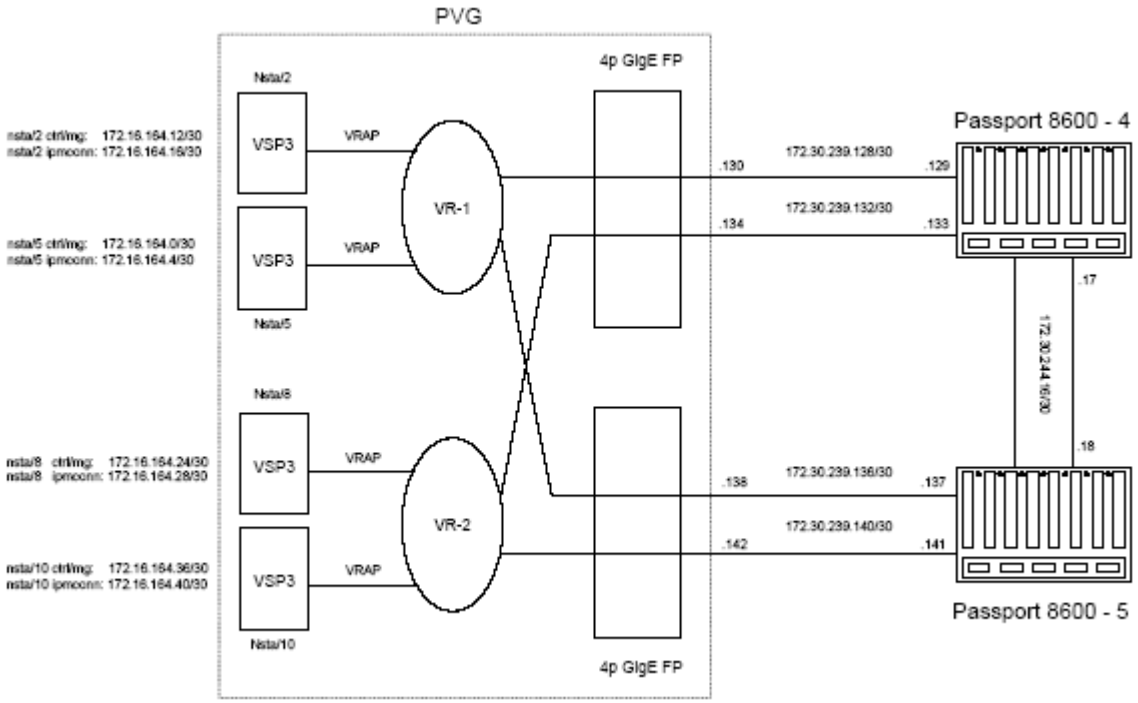
### 26.1.1 Physical Connection

**Figure 88 Physical Connection**



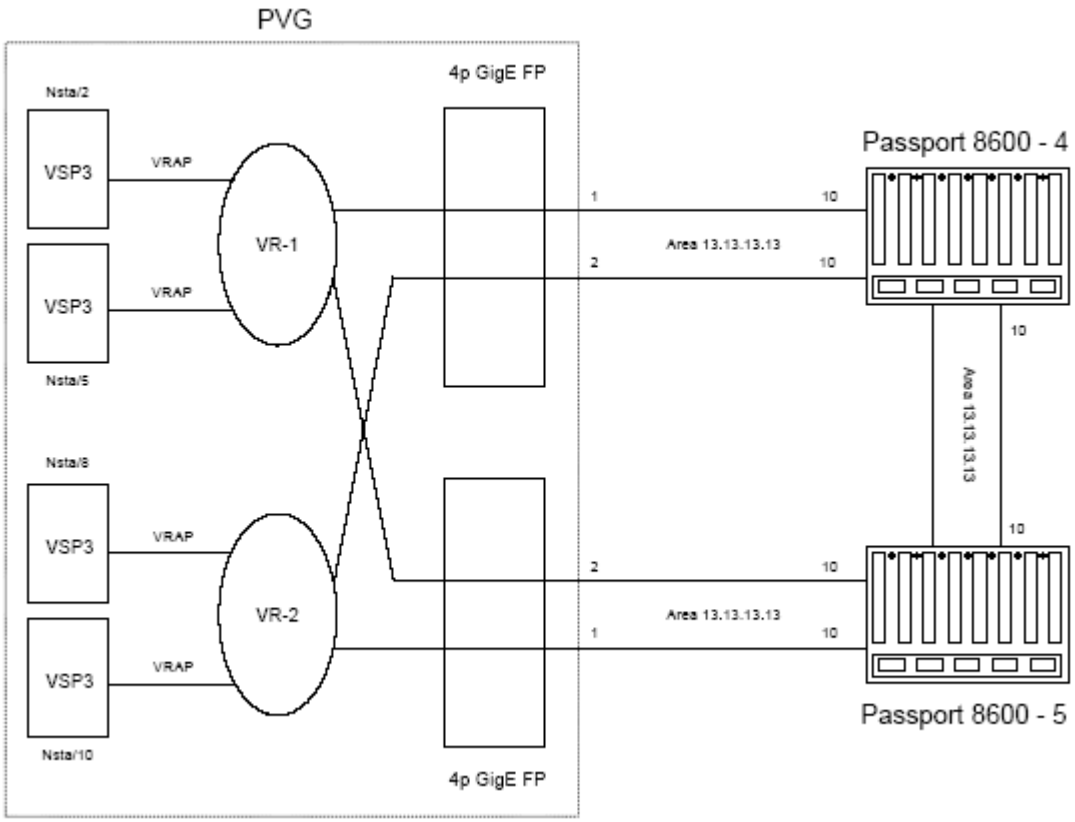

### 26.1.2 IP Address Scheme

**Figure 89 IP Address**




### 26.1.3 OSPF Design

**Figure 90 OSPF Design**




## 26.2 Working Configuration

### 26.2.1 PVG VRAP Specific Configuration

The following lists the set of commands required to provision dual PVG VRs using VRAP. There are four pair of VSPs in slot 2 - 5 and slot 8 - 11. A pair of 4-port OC3 TDM cards are installed in slot 6 and slot 7. Redundant uplinks to dual Passport 8600s are done by two 4-port GigE cards in slots 14 and 15. Due to the limited content of this appendix section, we only use nsta/2 and nsta/8 as example to show the configuration. Please note that the following working configuration does not include any standard PVG provisioning.

```
#
# Add VR for VRAP
#


add -s vr/1 ip
```

```
set vr/1 virtualRouterProcessor lp/0

set vr/1 vpnMode carrier

add vr/1 CustSpec


add -s vr/2 ip

set vr/2 virtualRouterProcessor lp/0

set vr/2 vpnMode carrier

add vr/2 CustSpec

#
# Setup IP Port for VRAP
#


add -s vr/1 pp/pvg ipport log/172.16.164.13 netmask 255.255.255.252

add -s vr/1 pp/pvg ipport log/172.16.164.17 netmask 255.255.255.252


add -s vr/2 pp/pvg ipport log/172.16.164.25 netmask 255.255.255.252

add -s vr/2 pp/pvg ipport log/172.16.164.29 netmask 255.255.255.252


add vm/0

set vr/1 pp/pvg linktomedia vm/0 if/0


add vm/2

set vr/2 pp/pvg linktomedia vm/2 if/0

#
# Add NSTA for VSP Card
```

```
#

add nsta/2 vgs

add nsta/8 vgs

set nsta/2 linktoserver lp/2 vsp

set nsta/8 linktoserver lp/8 vsp

set nsta/2 vgs hostname PVG142

set nsta/8 vgs hostname PVG148

set nsta/2 vgs defaultPacketLogLaw mulaw

set nsta/8 vgs defaultPacketLogLaw mulaw


#
# Provision CTRL/MG for Connection Control
#

add -s nsta/2 vgs ctrl/mg vrap

add -s nsta/8 vgs ctrl/mg vrap

set nsta/2 vgs ctrl/mg ipAddress 172.16.164.14

set nsta/8 vgs ctrl/mg ipAddress 172.16.164.26

set nsta/2 vgs ctrl/mg vrap subnetAccessName vr/1 pp/pvg ipport log/172.16.164.13
```

```
set nsta/8 vgs ctrl/mg vrap subnetAccessName vr/2 pp/pvg ipport log/172.16.164.25


add -s nsta/2 vgs ctrl/mg udpport/2427

add -s nsta/8 vgs ctrl/mg udpport/2427


add -s nsta/2 vgs vgcp

add -s nsta/8 vgs vgcp


set nsta/2 vgs vgcp udpPortConnection nsta/2 Vgs Ctrl/mediaGateway UdpPort/2427

set nsta/8 vgs vgcp udpPortConnection nsta/8 Vgs Ctrl/mediaGateway UdpPort/2427


set nsta/2 vgs ctrl/mg udpport/2427 diffserv 40

set nsta/8 vgs ctrl/mg udpport/2427 diffserv 40



#
# Provision IPMCONN for Media Traffic
#


add -s nsta/2 vgs ipmconn vrap

add -s nsta/8 vgs ipmconn vrap


set nsta/2 vgs ipmconn ipAddress 172.16.164.18

set nsta/8 vgs ipmconn ipAddress 172.16.164.30


set nsta/2 vgs ipmconn vrap subnetAccessName vr/1 pp/pvg ipport log/172.16.164.17
```

```
set nsta/8 vgs ipmconn vrap subnetAccessName vr/2 pp/pvg ipport log/172.16.164.29


#
# Provision BRAGS to Link TDM Trunks
#

add -s nsta/2 vgs brags/0
add -s nsta/8 vgs brags/0

set nsta/2 vgs brags/0 tdmLogLaw mulaw
set nsta/8 vgs brags/0 tdmLogLaw mulaw

#
# Provision GigE Port on 4p GigE FP
#

add lp/14 Ethernet/0
add lp/14 Ethernet/1

add lp/15 Ethernet/0
add lp/15 Ethernet/1

set lp/14 ethernet/0 om type LX
set lp/14 ethernet/1 om type LX

set lp/15 ethernet/0 om type LX
```

set lp/15 ethernet/1 om type LX

add la/140

add la/141

add la/150

add la/151

set la/140 framer interfaceName lp/14 Ethernet/0

set la/141 framer interfaceName lp/14 Ethernet/1

set la/150 framer interfaceName lp/15 Ethernet/0

set la/151 framer interfaceName lp/15 Ethernet/1

add -s vr/1 pp/8600-04 ipport log/172.30.239.130 netmask 255.255.255.252

add -s vr/1 pp/8600-05 ipport log/172.30.239.138 netmask 255.255.255.252

add -s vr/2 pp/8600-04 ipport log/172.30.239.134 netmask 255.255.255.252

add -s vr/2 pp/8600-05 ipport log/172.30.239.142 netmask 255.255.255.252

set vr/1 pp/8600-04 linkToMedia la/140

set vr/1 pp/8600-05 linkToMedia la/150

set vr/2 pp/8600-04 linkToMedia la/141

set vr/2 pp/8600-05 linkToMedia la/151

```
#
# Add OSPF on VR
#

add -s vr/1 ip ospf
add -s vr/1 ip ospf area/13.13.13.13
set vr/1 ip ospf area/13.13.13.13 importAsExtern importexternal
set vr/1 ip ospf area/13.13.13.13 areaSummary sendAreaSummary
set vr/1 ip ospf spareInstance enable

add -s vr/2 ip ospf
add -s vr/2 ip ospf area/13.13.13.13
set vr/2 ip ospf area/13.13.13.13 importAsExtern importexternal
set vr/2 ip ospf area/13.13.13.13 areaSummary sendAreaSummary
set vr/2 ip ospf spareInstance enable

#
# Add VRAP Interface into OSPF
#

add -s vr/1 pp/pvg ipport log/172.16.164.13 ospfif
add -s vr/1 pp/pvg ipport log/172.16.164.17 ospfif

add -s vr/2 pp/pvg ipport log/172.16.164.37 ospfif
add -s vr/2 pp/pvg ipport log/172.16.164.41 ospfif

set vr/1 pp/pvg ipport log/172.16.164.13  ospfif iftype passive
```

```
set vr/1 pp/pvg ipport log/172.16.164.17  ospfif iftype passive

set vr/2 pp/pvg ipport log/172.16.164.37  ospfif iftype passive
set vr/2 pp/pvg ipport log/172.16.164.41  ospfif iftype passive

set vr/1 pp/pvg ipport log/172.16.164.13  ospfif areaid 13.13.13.13
set vr/1 pp/pvg ipport log/172.16.164.17  ospfif areaid 13.13.13.13

set vr/2 pp/pvg ipport log/172.16.164.37  ospfif areaid 13.13.13.13
set vr/2 pp/pvg ipport log/172.16.164.41  ospfif areaid 13.13.13.13

#
# Provision GigE WAN Interface into OSPF
#

add -s vr/1 pp/8600-04 ipport log/172.30.239.130 ospfif
add -s vr/1 pp/8600-05 ipport log/172.30.239.138 ospfif
add -s vr/2 pp/8600-04 ipport log/172.30.239.134 ospfif
add -s vr/2 pp/8600-05 ipport log/172.30.239.142 ospfif

set vr/1 pp/8600-04 ipport log/172.30.239.130 ospfif areaid 13.13.13.13
set vr/1 pp/8600-05 ipport log/172.30.239.138 ospfif areaid 13.13.13.13
set vr/2 pp/8600-04 ipport log/172.30.239.134 ospfif areaid 13.13.13.13
set vr/2 pp/8600-05 ipport log/172.30.239.142 ospfif areaid 13.13.13.13

set vr/1 pp/8600-04 ipport log/172.30.239.130 ospfif hello 1
```

set vr/1 pp/8600-05 ipport log/172.30.239.138 ospfif hello 1

set vr/2 pp/8600-04 ipport log/172.30.239.134 ospfif hello 1

set vr/2 pp/8600-05 ipport log/172.30.239.142 ospfif hello 1

set vr/1 pp/8600-04 ipport log/172.30.239.130 ospfif rtrdead 4

set vr/1 pp/8600-05 ipport log/172.30.239.138 ospfif rtrdead 4

set vr/2 pp/8600-04 ipport log/172.30.239.134 ospfif rtrdead 4

set vr/2 pp/8600-05 ipport log/172.30.239.142 ospfif rtrdead 4

add vr/1 pp/8600-04 ipport log/172.30.239.130 ospfIf tos/0

add vr/1 pp/8600-05 ipport log/172.30.239.138 ospfIf tos/0

add vr/2 pp/8600-04 ipport log/172.30.239.134 ospfIf tos/0

add vr/2 pp/8600-05 ipport log/172.30.239.142 ospfIf tos/0

set vr/1 pp/8600-04 ipport log/172.30.239.130 ospfIf tos/0 tosMetric 1

set vr/1 pp/8600-05 ipport log/172.30.239.138 ospfIf tos/0 tosMetric 2

set vr/2 pp/8600-04 ipport log/172.30.239.134 ospfIf tos/0 tosMetric 2

set vr/2 pp/8600-05 ipport log/172.30.239.142 ospfIf tos/0 tosMetric 1

### 26.2.2 Passport 8600s Specific Configuration

Due to limited hardware in lab environment, GigE ports on a Passport 8600 for PVG connection are located on the same module. In practice, this must be avoided.

Between Passport 8600s, there is a MLT connection. The detail of MLT configuration is skipped. Please refer to Succession CS-LAN section in Engineering Guideline for details.

Also, two Passport 8600s here in the diagram are not ABR. So summarization will not be done on Passport 8600s.

Here, we only use Passport 8600-04 as an example:

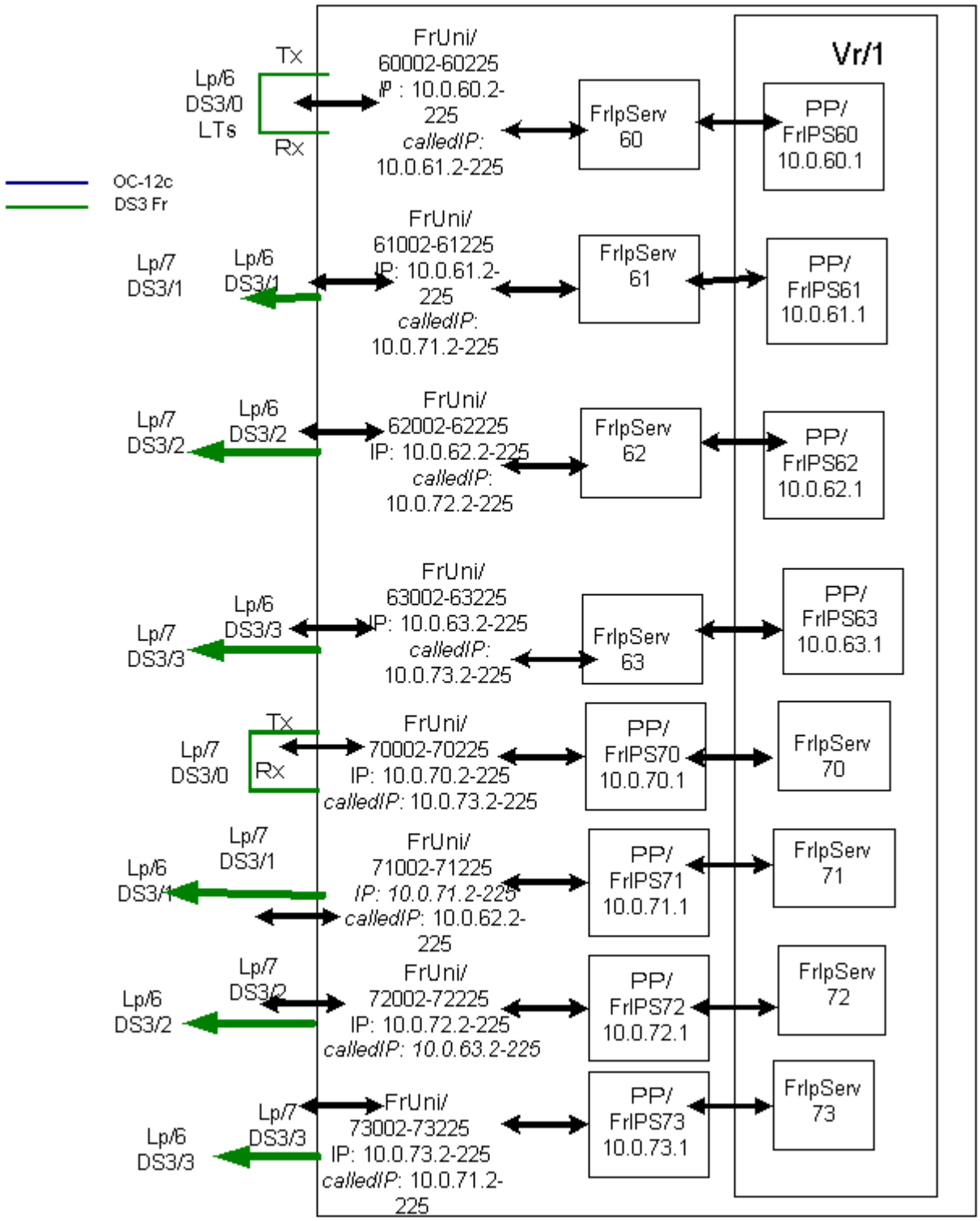
```
#
# VLAN CONFIGURATION
#

vlan 300 create byport 1 name "To-PVG14-VR1"
vlan 300 ports add 10/2 member portmember
vlan 300 ip create 172.30.239.129/255.255.255.252 mac_offset 10
vlan 300 ip ospf enable
vlan 300 ip ospf metric 10
vlan 300 ip ospf hello-interval 1
vlan 300 ip ospf dead-interval 4

vlan 310 create byport 1 name  "To-PVG14-VR2"
vlan 310 ports add 10/4 member portmember
vlan 310 ip create 172.30.239.133/255.255.255.252 mac_offset 14
vlan 310 ip ospf enable
vlan 310 ip ospf metric 10
vlan 310 ip ospf hello-interval 1
vlan 310 ip ospf dead-interval 4

vlan 200 create byport 1 name "To-PP8600-MLT"
vlan 200 add-mlt 1
vlan 200 ports add 4/34,10/1 member portmember
vlan 200 ip create 172.30.244.17/255.255.255.252 mac_offset 6
vlan 200 ip ospf enable
```

```
vlan 200 ip ospf metric 10
vlan 200 ip ospf hello-interval 1
vlan 200 ip ospf dead-interval 4

#
# OSPF CONFIGURATION
#

ip ospf admin-state enable
ip ospf router-id 192.168.223.104
ip ospf enable
ip ospf area 13.13.13.13 create

ip ospf interface 172.30.239.129 area 13.13.13.13
ip ospf interface 172.30.239.133 area 13.13.13.13
ip ospf interface 172.30.244.17 area 13.13.13.13
```

# 27.0 Appendix-Config for PVG to Juniper - with Frame Relay

## 27.1 Sample Setup

**Figure 91 Frame Relay / BNX required Components**


Vr/1
OC-12c
DS3 Fr
Lp/6
DS3/0
LTs
Tx
Rx
FrUni/
60002-60225
IP : 10.0.60.2-225
calledIP:
10.0.61.2-225
FrIpServ
60
PP/
FrIPS60
10.0.60.1
Lp/7
DS3/1
Lp/6
DS3/1
FrUni/
61002-61225
IP: 10.0.61.2-225
calledIP:
10.0.71.2-225
FrIpServ
61
PP/
FrIPS61
10.0.61.1
Lp/7
DS3/2
Lp/6
DS3/2
FrUni/
62002-62225
IP: 10.0.62.2-225
calledIP:
10.0.72.2-225
FrIpServ
62
PP/
FrIPS62
10.0.62.1
Lp/6
DS3/3
Lp/7
DS3/3
FrUni/
63002-63225
IP: 10.0.63.2-225
calledIP:
10.0.73.2-225
FrIpServ
63
PP/
FrIPS63
10.0.63.1
Lp/7
DS3/0
Tx
Rx
FrUni/
70002-70225
IP: 10.0.70.2-225
calledIP: 10.0.73.2-225
PP/
FrIPS70
10.0.70.1
FrIpServ
70
Lp/7
DS3/1
Lp/6
DS3/1
FrUni/
71002-71225
IP: 10.0.71.2-225
calledIP: 10.0.62.2-225
PP/
FrIPS71
10.0.71.1
FrIpServ
71
Lp/7
DS3/2
Lp/6
DS3/2
FrUni/
72002-72225
IP: 10.0.72.2-225
calledIP: 10.0.63.2-225
PP/
FrIPS72
10.0.72.1
FrIpServ
72
Lp/7
DS3/3
Lp/6
DS3/3
FrUni/
73002-73225
IP: 10.0.73.2-225
calledIP: 10.0.71.2-225
PP/
FrIPS73
10.0.73.1
FrIpServ
73

## 27.2 Provisioning Commands

The following lists the set of commands required to provision two 4-port DS3 Ch (inserted in slot 6 & 7). It does not include the provisioning of the Frame Relay / BNX WAN ports. It does not include any standard PVG provisioning.

## Provisioning of the 4-port DS3 Ch FPs to ingress Frame Relay / BNX traffic to the PVG

st prov

set sh ca/6 cardtype 4pds3ch

set sh ca/7 cardtype 4pds3

check, act and commit prov-save and commit prov

## Provisioning of the Module-level components that require a shelf restart

add -s lp/6

add -s lp/7

add sw lpt/Fr

set w lpt/fr fl ip,atmmpe,frameRelayLts,UniPvcBnx

set rtg dpn routing ID 1

set rtg dpn module ID 47

set mod regionid 1

add -s mod vcs

set mod vcs generationmode bothends

set mod vcs networkIdCode 3333

ch, act prov -confirm, save and commit prov (after the Cp reset)

## Adding static routes to forward traffic to the FR WAN ports

-st prov

add -s vr/1 ip static route/0.0.0.0,0.0.0.0,0 nh/172.30.239.9

add -s vr/1 ip static route/0.0.0.0,0.0.0.0,0 nh/172.30.239.13

check, act and commit prov-save and commit prov

## Adding the AtmMpe to the S/W feature of the 4-port OC-12s

st prov

set Sw Lpt/Atm fl atmMpe

check, act and commit prov-save and commit prov

## Adding the Frame Relay IP Service Components and the Protocol Ports for each of those FRIPs

-st prov-

add -s fripserv/60 (and /61, /62, /63)

add -s fripserv/70 (and /71, /72, /73)

set fripserv/60 lp lp/6 (and /61, /62, /63)

set fripserv/70 lp lp/7 (and /71, /72, /73)

add -s vr/1 pp/frips60 ipp log 10.0.60.1 (and /61, /62, /63)

add -s vr/1 pp/frips70 ipp log 10.0.70.1 (and /71, /72, /73)

set vr/1 pp/frips60 ipp log 10.0.60.1 netmask 255.255.255.0 (and /61, /62, /63)

set vr/1 pp/frips70 ipp log 10.0.70.1 netmask 255.255.255.0 (and /71, /72, /73)

check, act and commit prov-save and commit prov

## Adding 1792 Frunis, 224 Frunis per DS3 of the 4-port DS3 Ch. Only 1 Fruni is shown. Other Frunis and ports should be configured similarly. It is recommended to use automated Scripts for this provisioning

-st prov

add -s fruni/601002 bp

set fruni/601002 framer interfacename lp/6 ds3/0 ds1/1 chan/1

set fruni/601002 dna dna 3333147601002

set fruni/601002 bp ipaddress 10.0.60.62

set fruni/601002 bp linktoipserver fripserv/60, trafficPriorityEnabled yes-

set fruni/601002 lmi procedures none, asyncStatusReport on, pvcAlarmsReporting both

set fruni/601002 dna egressaccounting yes

set fruni/601002 numberOfEmissionQs 4

set fruni/6062 ifAdminStatus down

check, act and commit prov-save and commit prov

## Adding 3 DLCIs per FrUni and creating the FR PVCs.It is recommended to use automated Scripts for this provisioning

st prov

add -s Fruni/601002 dlci/101 bnxiwf

set Fruni/601002 dlci/101 bnxiwf calledipaddress 10.0.71.2

```
set Fruni/601002  dlci/101 bnxiwf calleddlci 101
add -s Fruni/601002  dlci/102 bnxiwf
set Fruni/601002  dlci/102 bnxiwf calledipaddress 10.0.71.2
set Fruni/601002  dlci/102 bnxiwf calleddlci 102
add -s Fruni/601002  dlci/103 bnxiwf
set Fruni/601002  dlci/103 bnxiwf calledipaddress 10.0.71.2
set Fruni/601002  dlci/103 bnxiwf calleddlci 102
```

# 28.0 Appendix: Management via SSH

The SSH is a protocol that specifies the way to conduct secure communications over a network via authentication, encryption and the integrity of the data transmitted over the network: The Passport 8600 switch software release 3.2.2 supports both the Secure SHell (SSH) protocol and Secure CoPy (SCP).

The SSH protocol supports the following security features:

- Authentication. This determines in a reliable way to identity the SSH client. During the login process the SSH client is queried for a digital proof of identity.
- Supported authentications are RSA (SSH-1), DSA (SSH-2) and passwords (both SSH-1 and SSH-2).
- Encryption. The SSH server uses encryption algorithms to scramble data and rendered it unintelligible except to the receiver. Supported encryption is 3DES only.
- Integrity. This guarantees that the data is transmitted from the sender to the receiver without any alteration. If any third party captures and modifies the traffic, the SSH server will detect this alteration.

Before enabling SSH services, Nortel Networks recommends disabling the following insecure services: SNMP, TFTP, FTP, Telnet, and rlogin.

Nortel Networks also recommends using the console port to configure the SSH parameters. In addition, when setting the version parameter, Nortel Networks recommends setting the version to SSH v2 only.

## 28.1 SSH Configuration

This chapter will describe the engineering details to configure SSH on the Passport 8600. The third party client that will be used as an example is OpenSSH.

It is important that the 3DES image is loaded before enabling SSH. The 3DES image needs to be copied on the Passport 8600 Switch CPU. Then, the encryption image file needs to be loaded into memory using the following command:

- config load-module 3DES <*filename* >

where ***filename*** is the 3DES image name. For software version 3.2.2, the file is p80c3220.img***.*** The next step is to generate the public and private keys on the client machine and on the server (the Passport 8600). This process is required for each of the authentication methods that the customer plans to use.

If RSA SSH version 1 is the preferred method, than SSH-1 RSA keys are necessary on the client machine. To generate the RSA keys, the command to be executed on the client is: ***ssh-keygen –t rsa1***

Once the keys are generated, they will be saved into the .ssh directory on the client machine. The names of the keys will be “identity” for the private key and “*identity.pub*” for the public key.

The Passport 8600 will automatically generate a RSA public and private server key pair once the SSH server is enabled.

The public part of the key for RSA is stored in /flash/.ssh/rsa_pub.key

If DSA SSH version 2 is the preferred method, than SSH-2 DSA keys are necessary on the client machine. To generate the DSA keys, the command to be executed on the client is: ***ssh-keygen –t dsa***

Once the keys are generated, they will be saved into the ***.ssh*** directory on the client machine. The names of the keys will be *"id.dsa*" for the private key and "*id_dsa.pub*" for the public key.

The Passport 8600 will automatically generate a DSA public and private server key pair once the SSH server is enabled.

The public part of the key for DSA is stored in ***/flash/.ssh/dsa_pub.key***

The next step is to copy the public keys files to from the client machine to the Passport 8600. If TFTP is used to transfer the files, the command to be executed on the Passport 8600 is the following:

- copy <TFTP server address>:/<PATH>/id_dsa.pub/flash/.ssh/<Key name>
  - ***<TFTP server address>*** is the IP address of the TFTP server. ***<PATH>*** is the absolute path for the root directory of the TFTP server.
  - ***<Key name>*** is the file name of the public key that corresponds to the one of the Passport 8600 Access Levels. These names are different for RSA and DSA authentication.

If RSA is used, the following table shows the file names that need to be used for the different access levels:

**Table 0-85**

| Access level | File name |
|---|---|
| RWA | /flash/.ssh/rsa_key_rwa |
| RW | /flash/.ssh/rsa_key_rw |
| RO | /flash/.ssh/rsa_key_ro |
| L3 | /flash/.ssh/rsa_key_rwl3 |
| L2 | /flash/.ssh/rsa_key_rwl2 |
| L1 | /flash/.ssh/rsa_key_rwl1 |

**Table 127 RSA Keys**

If DSA is used, the following table shows the file names in non-IETF format that need to be used for the different access levels:

**Table 0-86**

| Access level | File name in non-IETF format |
|---|---|
| RWA | /flash/.ssh/dsa_key_rwa |
| RW | /flash/.ssh/dsa_key_rw |
| RO | /flash/.ssh/dsa_key_ro |

**Table 0-86**

| | |
|---|---|
| L3 | /flash/.ssh/dsa_key_rwl3 |
| L2 | /flash/.ssh/dsa_key_rwl2 |
| L1 | /flash/.ssh/dsa_key_rwl1 |

**Table 128 DSA Keys**

If DSA is used, the following table shows the file names in IETF format that need to be used for the different access levels:

**Table 0-87**

| Access level | File name in IETF format |
|---|---|
| RWA | /flash/.ssh/dsa_key_rwa_ietf |
| RW | /flash/.ssh/dsa_key_rw_ietf |
| RO | /flash/.ssh/dsa_key_ro_ietf |
| L3 | /flash/.ssh/dsa_key_rwl3_ietf |
| L2 | /flash/.ssh/dsa_key_rwl2_ietf |
| L1 | /flash/.ssh/dsa_key_rwl1_ietf |

**Table 129 DSA Keys in IETF Format**

Example:

copy 47.1.1.1:/TFTPRoot/id_dsa.pub/flash/.ssh/ dsa_key_rwa

## 28.2 Connection to the switch – SSH and SCP

To connect via SSH to the switch, the following command needs to be run:

- ssh -l <username> -v -1 <Passport 8600 IP address>
  - ***<username>*** is the user name.
  - ***<Passport 8600 IP address>*** is the address of the Passport 8600 to connect to.
  - ***V*** is used for the verbose mode.
  - ***-1*** forces the use of protocol version 1.

The SCP command to transfer files to the Passport 8600 is the following:

- scp -v -oProtocol=1 <Filename> <username>@<Passport 8600 IP address>:/flash/<Filename>
  - ***V*** is used for the verbose mode.
  - ***-oProtocol=1*** forces the use of protocol version 1.
  - ***<Filename>*** is name of the file to transfer.
  - ***<username>*** is the user name.

- ***<Passport 8600 IP address>*** is the address of the Passport 8600 to connect to.

Examples:

ssh -l rwa -v -1 172.30.242.10

scp -v -oProtocol=1  config.cfg  rwa@172.30.242.10:/flash/config.cfg

# 29.0 Appendix: Passport 8600 QoS Configuration - To be updated

CS-LAN OAM&P Subnet

- 47.142.86.0/24

CS-LAN Call Processing Subnet

- 172.16.0.0/255.255.240.0

Summary for PVG Subnets

- 172.16.128.0/255.255.128.0

Summary of MTA Subnets

- 10.128.0.0/255.252.0.0

NOC Subnet

- 172.31.0.0/255.255.255.0

VRDN IP addresses

- 192.168.0.148/255.255.255.255
- 172.16.2.20/255.255.255.255

ip traffic-filter create source src-ip 47.142.86.0/255.255.255.0 dst-ip 0.0.0.0/0.0.0.0 id 220

ip traffic-filter filter 220 action mode forward

ip traffic-filter filter 220 action statistic enable

ip traffic-filter filter 220 modify dscp 101110

ip traffic-filter filter 220 modify dscp-enable enable

ip traffic-filter filter 220 modify ieee8021p 7

ip traffic-filter filter 220 modify ieee8021p-enable enable

ip traffic-filter create source src-ip 172.16.128.0/255.255.128.0 dst-ip 10.128.0.0/255.252.0.0 id 212

ip traffic-filter filter 212 action mode forward

ip traffic-filter filter 212 action statistic enable

ip traffic-filter filter 212 modify dscp 101110

ip traffic-filter filter 212 modify dscp-enable enable

ip traffic-filter filter 212 modify ieee8021p 6

ip traffic-filter filter 212 modify ieee8021p-enable enable

ip traffic-filter create source src-ip 172.16.128.0/255.255.128.0 dst-ip 172.16.128.0/255.255.128.0 id 211

ip traffic-filter filter 211 action mode forward

ip traffic-filter filter 211 action statistic enable

ip traffic-filter filter 211 modify dscp 101110

ip traffic-filter filter 211 modify dscp-enable enable

ip traffic-filter filter 211 modify ieee8021p 6

ip traffic-filter filter 211 modify ieee8021p-enable enable

ip traffic-filter create source src-ip 172.16.0.0/255.255.240.0 dst-ip 172.16.128.0/255.255.128.0 id 102

ip traffic-filter filter 102 action mode forward

ip traffic-filter filter 102 action statistic enable

ip traffic-filter filter 102 modify dscp 101110

ip traffic-filter filter 102 modify dscp-enable enable

ip traffic-filter filter 102 modify ieee8021p 6

ip traffic-filter filter 102 modify ieee8021p-enable enable

ip traffic-filter create source src-ip 172.16.128.0/255.255.128.0 dst-ip 172.16.0.0/255.255.240.0 id 210

ip traffic-filter filter 210 action mode forward

ip traffic-filter filter 210 action statistic enable

ip traffic-filter filter 210 modify dscp 101110

ip traffic-filter filter 210 modify dscp-enable enable

ip traffic-filter filter 210 modify ieee8021p 6

ip traffic-filter filter 210 modify ieee8021p-enable enable

ip traffic-filter create source src-ip 172.16.0.0/255.255.240.0 dst-ip 172.16.0.0/255.255.240.0 id 108

ip traffic-filter filter 108 action mode forward

ip traffic-filter filter 108 action statistic enable

ip traffic-filter filter 108 modify dscp 101110

ip traffic-filter filter 108 modify dscp-enable enable

ip traffic-filter filter 108 modify ieee8021p 6

ip traffic-filter filter 108 modify ieee8021p-enable enable

ip traffic-filter create source src-ip 172.16.0.0/255.255.240.0 dst-ip 47.142.86.0/255.255.255.0 id 100

ip traffic-filter filter 100 action mode forward

ip traffic-filter filter 100 action statistic enable

ip traffic-filter filter 100 modify dscp 101110

ip traffic-filter filter 100 modify dscp-enable enable

ip traffic-filter filter 100 modify ieee8021p 7

ip traffic-filter filter 100 modify ieee8021p-enable enable

ip traffic-filter create source src-ip 172.16.0.0/255.255.240.0 dst-ip 172.31.0.0/255.255.255.0 id 98

ip traffic-filter filter 98 action mode forward

ip traffic-filter filter 98 action statistic enable

ip traffic-filter filter 98 modify dscp 101110

ip traffic-filter filter 98 modify dscp-enable enable

ip traffic-filter filter 98 modify ieee8021p 7

ip traffic-filter filter 98 modify ieee8021p-enable enable

ip traffic-filter create source src-ip 172.16.2.20/255.255.255.255 dst-ip 192.168.0.148/255.255.255.255 id 200

ip traffic-filter filter 200 action mode forward

ip traffic-filter filter 200 action statistic enable

ip traffic-filter filter 200 modify dscp 101110

ip traffic-filter filter 200 modify dscp-enable enable

ip traffic-filter filter 200 modify ieee8021p 7

ip traffic-filter filter 200 modify ieee8021p-enable enable

ip traffic-filter set 305 create name "OAM&P"

ip traffic-filter set 305 add-filter 220

ip traffic-filter set 310 create name "CallProcessing"

ip traffic-filter set 310 add-filter 98

ip traffic-filter set 310 add-filter 100

ip traffic-filter set 310 add-filter 102

ip traffic-filter set 310 add-filter 108

ip traffic-filter set 315 create name "VRDN"

ip traffic-filter set 315 add-filter 200

ip traffic-filter set 320 create name "PVG"

ip traffic-filter set 320 add-filter 210

ip traffic-filter set 320 add-filter 211

ip traffic-filter set 320 add-filter 212

ethernet 1/7 enable-diffserv true

ethernet 1/8 enable-diffserv true

ethernet 1/8 access-diffserv true

ethernet 1/8 ip traffic-filter create

ethernet 1/8 ip traffic-filter add set 310

ethernet 1/8 ip traffic-filter default-action forward

ethernet 1/8 ip traffic-filter enable

ethernet 2/1 enable-diffserv true

ethernet 2/1 access-diffserv true

ethernet 2/1 name "OAM"

ethernet 2/1 ip traffic-filter create

ethernet 2/1 ip traffic-filter add set 305

ethernet 2/1 ip traffic-filter default-action forward

ethernet 2/1 ip traffic-filter enable

ethernet 2/2 enable-diffserv true

ethernet 2/2 access-diffserv true

ethernet 2/27 enable-diffserv true

ethernet 2/27 access-diffserv true

ethernet 2/27 name "CallProcessing"

ethernet 2/27 ip traffic-filter create

ethernet 2/27 ip traffic-filter add set 310

ethernet 2/27 ip traffic-filter default-action forward

ethernet 2/27 ip traffic-filter enable

atm 7/1 ip traffic-filter create

atm 7/1 ip traffic-filter add set 320

atm 7/1 ip traffic-filter default-action forward

atm 7/1 ip traffic-filter enable

# 30.0 Appendix: Passport 8600 Traffic Filtering Configuration

CS-LAN OAM&P Subnet

- 47.142.86.0/24

CS-LAN Call Processing Subnet

- 172.16.0.0/255.255.240.0

Summary for PVG Subnets

- 172.16.128.0/255.255.128.0

Summary of MTA Subnets

- 10.128.0.0/255.252.0.0

NOC Subnet

- 172.31.0.0/255.255.255.0

VRDN IP addresses

- 192.168.0.148/255.255.255.255
- 172.16.2.20/255.255.255.255

MTA Subnets

- 10.129.128.0/255.255.128.0
- 10.131.128.0/255.255.128.0
- 10.17.48.0/255.255.255.0
- 10.17.49.0/255.255.255.0

CM Subnets

- 10.17.48.0/255.255.255.0
- 10.10.128.0/255.255.128.0
- 10.10.128.0/255.255.128.0

Network Servers

- 47.142.86.133/255.255.255.255
- 47.142.86.134/255.255.255.255
- 47.142.86.210/255.255.255.255

ip traffic-filter create global src-ip 0.0.0.0/0.0.0.0 dst-ip 0.0.0.0/0.0.0.0 id 54

ip traffic-filter filter 54 action mode forward

ip traffic-filter filter 54 action statistic enable

ip traffic-filter filter 54 match protocol ospf

ip traffic-filter filter 54 name "OSPF"

ip traffic-filter create global src-ip 0.0.0.0/0.0.0.0 dst-ip 47.142.86.210/255.255.255.255 id 1

ip traffic-filter filter 1 action mode forward

ip traffic-filter filter 1 action statistic enable

ip traffic-filter filter 1 match dst-port 123 dst-option equal

ip traffic-filter filter 1 match protocol udp

ip traffic-filter filter 1 name "NTP"

ip traffic-filter create destination dst-ip 172.16.224.0/255.255.224.0 src-ip 10.129.128.0/255.255.128.0 id 12

ip traffic-filter filter 12 action mode drop

ip traffic-filter filter 12 action statistic enable

ip traffic-filter filter 12 match src-port 49152 src-option less

ip traffic-filter filter 12 match protocol udp

ip traffic-filter filter 12 name "BPVGMotMetroA-1"

ip traffic-filter create destination dst-ip 172.16.224.0/255.255.224.0 src-ip 10.129.128.0/255.255.128.0 id 13

ip traffic-filter filter 13 action mode drop

ip traffic-filter filter 13 action statistic enable

ip traffic-filter filter 13 match dst-port 49152 dst-option less

ip traffic-filter filter 13 match protocol udp

ip traffic-filter filter 13 name "BPVGMotMetro-2"

ip traffic-filter create destination dst-ip 172.16.224.0/255.255.224.0 src-ip 10.129.128.0/255.255.128.0 id 14

ip traffic-filter filter 14 action mode forward

ip traffic-filter filter 14 action statistic enable

ip traffic-filter filter 14 match dst-port 51392 dst-option less

ip traffic-filter filter 14 match src-port 49160 src-option less

ip traffic-filter filter 14 match protocol udp

ip traffic-filter filter 14 name "BPVGMotMetro-3"

ip traffic-filter create destination dst-ip 172.16.224.0/255.255.224.0 src-ip 10.131.128.0/255.255.128.0 id 82

ip traffic-filter filter 82 action mode drop

ip traffic-filter filter 82 action statistic enable

ip traffic-filter filter 82 match src-port 49152 src-option less

ip traffic-filter filter 82 match protocol udp

ip traffic-filter filter 82 name "BPVGMotMetroB-1"

ip traffic-filter create destination dst-ip 172.16.224.0/255.255.224.0 src-ip 10.131.128.0/255.255.128.0 id 83

ip traffic-filter filter 83 action mode drop

ip traffic-filter filter 83 action statistic enable

ip traffic-filter filter 83 match dst-port 49152 dst-option less

ip traffic-filter filter 83 match protocol udp

ip traffic-filter filter 83 name "BPVGMotMetroB-2"

ip traffic-filter create destination dst-ip 172.16.224.0/255.255.224.0 src-ip 10.131.128.0/255.255.128.0 id 84

ip traffic-filter filter 84 action mode forward

ip traffic-filter filter 84 action statistic enable

ip traffic-filter filter 84 match dst-port 51392 dst-option less

ip traffic-filter filter 84 match src-port 49160 src-option less

ip traffic-filter filter 84 match protocol udp

ip traffic-filter filter 84 name "BPVGMotMetroB-3"

ip traffic-filter create destination dst-ip 172.16.224.0/255.255.224.0 src-ip 172.16.208.0/255.255.240.0 id 16

ip traffic-filter filter 16 action mode drop

ip traffic-filter filter 16 action statistic enable

ip traffic-filter filter 16 match src-port 49152 src-option less

ip traffic-filter filter 16 match protocol udp

ip traffic-filter filter 16 name "BToPVG-JunPVG-1"

ip traffic-filter create destination dst-ip 172.16.224.0/255.255.224.0 src-ip 172.16.208.0/255.255.240.0 id 17

ip traffic-filter filter 17 action mode drop

ip traffic-filter filter 17 action statistic enable

ip traffic-filter filter 17 match dst-port 49152 dst-option less

ip traffic-filter filter 17 match protocol udp

ip traffic-filter filter 17 name "BToPVG-JunPVG-2"

ip traffic-filter create destination dst-ip 172.16.224.0/255.255.224.0 src-ip 172.16.208.0/255.255.240.0 id 18

ip traffic-filter filter 18 action mode forward

ip traffic-filter filter 18 action statistic enable

ip traffic-filter filter 18 match dst-port 51392 dst-option less

ip traffic-filter filter 18 match src-port 51392 src-option less

ip traffic-filter filter 18 match protocol udp

ip traffic-filter filter 18 name "BToPVG-JunPVG-3"

ip traffic-filter create destination dst-ip 172.16.224.0/255.255.224.0 src-ip 10.17.49.0/255.255.255.0 id 35

ip traffic-filter filter 35 action mode drop

ip traffic-filter filter 35 action statistic enable

ip traffic-filter filter 35 match dst-port 49152 dst-option less
ip traffic-filter filter 35 match protocol udp

ip traffic-filter filter 35 name "BPVGArMetroA-1"

ip traffic-filter create destination dst-ip 172.16.224.0/255.255.224.0 src-ip 10.17.49.0/255.255.255.0 id 36

ip traffic-filter filter 36 action mode forward

ip traffic-filter filter 36 action statistic enable

ip traffic-filter filter 36 match dst-port 51392 dst-option less

ip traffic-filter filter 36 match protocol udp

ip traffic-filter filter 36 name "BUasArMetroA-2"

ip traffic-filter create destination dst-ip 172.16.0.0/255.255.240.0 src-ip 10.127.128.0/255.255.128.0 id 6

ip traffic-filter filter 6 action mode forward

ip traffic-filter filter 6 action statistic enable

ip traffic-filter filter 6 match dst-port 2427 dst-option equal

ip traffic-filter filter 6 match src-port 2427 src-option equal

ip traffic-filter filter 6 match protocol udp

ip traffic-filter filter 6 name "SigHurMetroA"

ip traffic-filter create destination dst-ip 172.16.0.0/255.255.240.0 src-ip 10.129.128.0/255.255.128.0 id 2

ip traffic-filter filter 2 action mode forward

ip traffic-filter filter 2 action statistic enable

ip traffic-filter filter 2 match dst-port 2427 dst-option equal

ip traffic-filter filter 2 match src-port 2427 src-option equal

ip traffic-filter filter 2 match protocol udp

ip traffic-filter filter 2 name "SigMotMetroA"

ip traffic-filter create destination dst-ip 172.16.0.0/255.255.240.0 src-ip 10.129.128.0/255.255.128.0 id 8

ip traffic-filter filter 8 action mode drop

ip traffic-filter filter 8 action statistic enable

ip traffic-filter filter 8 match src-port 49152 src-option less

ip traffic-filter filter 8 match protocol udp

ip traffic-filter filter 8 name "BUasMotMetroA-1"

ip traffic-filter create destination dst-ip 172.16.0.0/255.255.240.0 src-ip 10.129.128.0/255.255.128.0

id 9

ip traffic-filter filter 9 action mode drop

ip traffic-filter filter 9 action statistic enable

ip traffic-filter filter 9 match dst-port 30000 dst-option less

ip traffic-filter filter 9 match protocol udp

ip traffic-filter filter 9 name "BUasMotMetroA-2"

ip traffic-filter create destination dst-ip 172.16.0.0/255.255.240.0 src-ip 10.129.128.0/255.255.128.0 id 10

ip traffic-filter filter 10 action mode forward

ip traffic-filter filter 10 action statistic enable

ip traffic-filter filter 10 match dst-port 30242 dst-option less

ip traffic-filter filter 10 match src-port 49160 src-option less

ip traffic-filter filter 10 match protocol udp

ip traffic-filter filter 10 name "BUasMotMetroA-3"

ip traffic-filter create destination dst-ip 172.16.0.0/255.255.240.0 src-ip 10.131.128.0/255.255.128.0 id 70

ip traffic-filter filter 70 action mode forward

ip traffic-filter filter 70 action statistic enable

ip traffic-filter filter 70 match dst-port 2427 dst-option equal

ip traffic-filter filter 70 match src-port 2427 src-option equal

ip traffic-filter filter 70 match protocol udp

ip traffic-filter filter 70 name "SigMotMetroB"

ip traffic-filter create destination dst-ip 172.16.0.0/255.255.240.0 src-ip 10.131.128.0/255.255.128.0 id 78

ip traffic-filter filter 78 action mode drop

ip traffic-filter filter 78 action statistic enable

ip traffic-filter filter 78 match src-port 49152 src-option less

ip traffic-filter filter 78 match protocol udp

ip traffic-filter filter 78 name "BUasMotMetroB-1"

ip traffic-filter create destination dst-ip 172.16.0.0/255.255.240.0 src-ip 10.131.128.0/255.255.128.0 id 79

ip traffic-filter filter 79 action mode drop

ip traffic-filter filter 79 action statistic enable

ip traffic-filter filter 79 match dst-port 30000 dst-option less

ip traffic-filter filter 79 match protocol udp

ip traffic-filter filter 79 name "BUasMotMetroB-2"

ip traffic-filter create destination dst-ip 172.16.0.0/255.255.240.0 src-ip 10.131.128.0/255.255.128.0 id 80

ip traffic-filter filter 80 action mode forward

ip traffic-filter filter 80 action statistic enable

ip traffic-filter filter 80 match dst-port 30242 dst-option less

ip traffic-filter filter 80 match src-port 49160 src-option less

ip traffic-filter filter 80 match protocol udp

ip traffic-filter filter 80 name "BUasMotMetroB-3"

ip traffic-filter create destination dst-ip 172.16.0.0/255.255.240.0 src-ip 172.16.192.0/255.255.192.0 id 7

ip traffic-filter filter 7 action mode forward

ip traffic-filter filter 7 action statistic enable

ip traffic-filter filter 7 match protocol usrDefined 132

ip traffic-filter filter 7 name "SCTP"

ip traffic-filter create destination dst-ip 172.16.0.0/255.255.240.0 src-ip 172.16.208.0/255.255.240.0 id 3

ip traffic-filter filter 3 action mode forward

ip traffic-filter filter 3 action statistic enable

ip traffic-filter filter 3 match dst-port 2427 dst-option equal

ip traffic-filter filter 3 match src-port 2427 src-option equal

ip traffic-filter filter 3 match protocol udp

ip traffic-filter filter 3 name "SigJunPVG"

ip traffic-filter create destination dst-ip 172.16.0.0/255.255.240.0 src-ip 172.16.208.0/255.255.240.0 id 22

ip traffic-filter filter 22 action mode drop

ip traffic-filter filter 22 action statistic enable

ip traffic-filter filter 22 match src-port 49152 src-option less

ip traffic-filter filter 22 match protocol udp

ip traffic-filter filter 22 name "BUasJunPVG-1"

ip traffic-filter create destination dst-ip 172.16.0.0/255.255.240.0 src-ip 172.16.208.0/255.255.240.0 id 23

ip traffic-filter filter 23 action mode drop

ip traffic-filter filter 23 action statistic enable

ip traffic-filter filter 23 match dst-port 30000 dst-option less

ip traffic-filter filter 23 match protocol udp

ip traffic-filter filter 23 name "BUasJunPVG-2"

ip traffic-filter create destination dst-ip 172.16.0.0/255.255.240.0 src-ip 172.16.208.0/255.255.240.0 id 24

ip traffic-filter filter 24 action mode forward

ip traffic-filter filter 24 action statistic enable

ip traffic-filter filter 24 match dst-port 30242 dst-option less

ip traffic-filter filter 24 match src-port 51392 src-option less

ip traffic-filter filter 24 match protocol udp

ip traffic-filter filter 24 name "BUasJunPVG-3"

ip traffic-filter create destination dst-ip 172.16.0.0/255.255.240.0 src-ip 10.17.49.0/255.255.255.0 id 5

ip traffic-filter filter 5 action mode forward

ip traffic-filter filter 5 action statistic enable

ip traffic-filter filter 5 match dst-port 2427 dst-option equal

ip traffic-filter filter 5 match src-port 2427 src-option equal

ip traffic-filter filter 5 match protocol udp

ip traffic-filter filter 5 name "SigArMetroA"

ip traffic-filter create destination dst-ip 172.16.0.0/255.255.240.0 src-ip 10.17.49.0/255.255.255.0 id 32

ip traffic-filter filter 32 action mode drop

ip traffic-filter filter 32 action statistic enable

ip traffic-filter filter 32 match dst-port 30000 dst-option less

ip traffic-filter filter 32 match protocol udp

ip traffic-filter filter 32 name "BUasArMetroA-1"

ip traffic-filter create destination dst-ip 172.16.0.0/255.255.240.0 src-ip 10.17.49.0/255.255.255.0 id 33

ip traffic-filter filter 33 action mode forward

ip traffic-filter filter 33 action statistic enable

ip traffic-filter filter 33 match dst-port 30242 dst-option less

ip traffic-filter filter 33 match protocol udp

ip traffic-filter filter 33 name "BUasArMetroA-2"

ip traffic-filter create destination dst-ip 172.16.0.0/255.255.240.0 src-ip 172.31.0.0/255.255.255.0 id 26

ip traffic-filter filter 26 action mode forward

ip traffic-filter filter 26 action statistic enable

ip traffic-filter filter 26 name "OAM-Flows"

ip traffic-filter create destination dst-ip 47.142.86.134/255.255.255.255 src-ip 10.10.128.0/255.255.128.0 id 96

ip traffic-filter filter 96 action mode forward

ip traffic-filter filter 96 action statistic enable

ip traffic-filter filter 96 name "MtroA-CM-OAM"

ip traffic-filter create destination dst-ip 47.142.86.134/255.255.255.255 src-ip 10.12.128.0/255.255.128.0 id 97

ip traffic-filter filter 97 action mode forward

ip traffic-filter filter 97 action statistic enable

ip traffic-filter filter 97 name "MtroB-CM-OAM"

ip traffic-filter create destination dst-ip 47.142.86.0/255.255.255.0 src-ip 172.31.0.0/255.255.255.0 id 27

ip traffic-filter filter 27 action mode forward

ip traffic-filter filter 27 action statistic enable

ip traffic-filter filter 27 name "NOC-OAM "

ip traffic-filter create destination dst-ip 172.16.2.0/255.255.255.0 src-ip 192.168.1.0/255.255.255.0 id 4

ip traffic-filter filter 4 action mode forward

ip traffic-filter filter 4 action statistic enable

ip traffic-filter filter 4 name "VRDN-DIPT"

ip traffic-filter create destination dst-ip 47.142.86.133/255.255.255.255 src-ip 10.17.48.0/255.255.255.0 id 56

ip traffic-filter filter 56 action mode forward

ip traffic-filter filter 56 action statistic enable

ip traffic-filter filter 56 name "Flow-CPS"

ip traffic-filter global-set 33 create name "NetworkServices"

ip traffic-filter global-set 33 add-filter 1

ip traffic-filter global-set 33 add-filter 54

ip traffic-filter set 400 create name "Signaling"

ip traffic-filter set 400 add-filter 2

ip traffic-filter set 400 add-filter 3

ip traffic-filter set 400 add-filter 4

ip traffic-filter set 400 add-filter 5

ip traffic-filter set 400 add-filter 6

ip traffic-filter set 400 add-filter 7

ip traffic-filter set 400 add-filter 70

ip traffic-filter set 410 create name "Bearer"

ip traffic-filter set 410 add-filter 8

ip traffic-filter set 410 add-filter 9

ip traffic-filter set 410 add-filter 10

ip traffic-filter set 410 add-filter 12

ip traffic-filter set 410 add-filter 13

ip traffic-filter set 410 add-filter 14

ip traffic-filter set 410 add-filter 16

ip traffic-filter set 410 add-filter 17

ip traffic-filter set 410 add-filter 18

ip traffic-filter set 410 add-filter 22

ip traffic-filter set 410 add-filter 23

ip traffic-filter set 410 add-filter 24

ip traffic-filter set 410 add-filter 32

ip traffic-filter set 410 add-filter 33

ip traffic-filter set 410 add-filter 35

ip traffic-filter set 410 add-filter 36

ip traffic-filter set 410 add-filter 78

ip traffic-filter set 410 add-filter 79

ip traffic-filter set 410 add-filter 80

ip traffic-filter set 410 add-filter 82

ip traffic-filter set 410 add-filter 83

ip traffic-filter set 410 add-filter 84

ip traffic-filter set 420 create name "NOC"

ip traffic-filter set 420 add-filter 26

ip traffic-filter set 420 add-filter 27

ip traffic-filter set 440 create name "M40"

ip traffic-filter set 440 add-filter 50

ip traffic-filter set 440 add-filter 51

ip traffic-filter set 440 add-filter 52

ip traffic-filter set 440 add-filter 53

ip traffic-filter set 450 create name "ArrisCM"

ip traffic-filter set 450 add-filter 56

ip traffic-filter set 460 create name "MotCM-OAM"

ip traffic-filter set 460 add-filter 96

ip traffic-filter set 460 add-filter 97

ethernet 1/2 enable-diffserv true

ethernet 1/2 name "JUNIPER-01"

ethernet 1/2 ip traffic-filter create

ethernet 1/2 ip traffic-filter add set 33

ethernet 1/2 ip traffic-filter add set 400

ethernet 1/2 ip traffic-filter add set 410

ethernet 1/2 ip traffic-filter add set 420

ethernet 1/2 ip traffic-filter add set 440

ethernet 1/2 ip traffic-filter add set 450

ethernet 1/2 ip traffic-filter add set 460

ethernet 1/2 ip traffic-filter default-action drop

ethernet 1/2 ip traffic-filter disable

ethernet 1/2 stg 1 stp disable

# 31.0 References

[1] [RFC 2474] "*Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*", Nichols, K., Blake, S., Baker, F. and D. Black, December 1998.

[2] [RFC 2597] "*Assured Forwarding PHB Group*", J. Heinanen, F. Baker, W. Weiss, J. Wroclawski, June 1999.

[3] [RFC 2598] "*An Expedited Forwarding PHB*", V. Jacobson, K. Nichols, K. Poduri, June 1999.

[4] [Networking] Networking Concepts for the Passport 8000 Series Switch **(**10/2001, Rev A)

[5] [Management] Managing the Passport 8000 Series Switch Using the Command Line Interface Release 3.2 (October 2001, Rev 00)

[6] MD-2000.0173 PVG PRI Backhaul

# 32.0 Glossary

| | |
|---|---|
| **AAL1** | ATM Adaptation Layer 1 |
| **AAL5** | ATM Adaptation Layer 5 |
| **AHT** | Average Hold Time |
| **APG** | Anchor Packet Gateway |
| **APS** | Audio Provisioning Server |
| **APS** | Automatic Protection Switching |
| **ATM** | Asynchronous Transfer Mode |
| **BHCA** | Busy Hour Call Attempts |
| **BHHCA** | Busy Hour Half Call Attempt |
| **CallP** | Call Processing |
| **CCS** | 100 Call Seconds |
| **CHT** | Call Hold Time |
| **CLI** | Common Line Interface |
| **CMTS** | Cable Modem Termination System |
| **CoS** | Class of Service |
| **CP** | Control Processor |
| **CS2K** | Communications Server 2000 |
| **CS-LAN** | Communications Server Local Area Network |
| **CPS2000** | Cornerstone Provisioning System 2000 |
| **DCE** | Distributed Computing Environment |
| **DHCP** | Dynamic Host Configuration Protocol |
| **DNS** | Domain Name Server |
| **DOS** | Denial of Service |
| **DP** | Destination Protection |
| **DSCP** | DiffServ Code Point |
| **EIOP** | Ethernet Input/Output Processor |
| **EM** | Element Manager |
| **GEM** | Gigabit Ethernet Module |
| **GWC** | Gateway Controller |
| **HFC** | Hybrid Fiber Coax |
| **HIOP** | High-Performance Input/Output Processor |
| **IW-SPM** | Interworking SPM |
| **LDAP** | Light-weight Directory Access Protocol |
| **LMM** | Line Maintenance Manager |
| **LTM** | Line Test Manager |
| **MADN** | Multiple Appearance Directory Number |
| **MBS** | Maximum Burst Size |
| **MG** | Media Gateway |
| **MLT** | Multi-link Trunking |
| **MTA** | Multimedia Terminal Adapter |
| **NCS** | Network-based Call Signaling |
| **NMI** | Network Management Interface |

| | |
|---|---|
| **NOC** | Network Operations Center |
| **NPM** | Network Patch Manager |
| **NTP** | Network Time Protocol |
| **OOB** | Out of Band |
| **PCR** | Peak Cell Rate |
| **PSTN** | Public Switched Telephone Network |
| **PTM** | Packet Telephony Manager |
| **PVG** | Packet Voice Gateway |
| **QoS** | Quality of Service |
| **RTP** | Real Time Protocol |
| **SAM16** | Service Application Module – 16 slot |
| **SAM21** | Service Application Module – 21 slot |
| **SAM21EM** | SAM21 Element Manager |
| **SC/SCU** | Shelf Controller/Shelf Controller Unit |
| **SCR** | Sustained Cell Rate |
| **SDM** | Supernode Data Manager |
| **SESM** | Succession Element and Sub-network Manager |
| **SPM** | Spectrum Peripheral Module |
| **TDM** | Time Division Multiplex |
| **TMM** | Trunk Maintenance Manager |
| **UAS** | Universal Audio Server |
| **USP** | Universal Signaling Point |
| **VPN** | Virtual Private Network |
| **VR** | Virtual Router |
| **VRRP** | Virtual Router Reduncy Protocol |
| **VSP** | Voice Services Processor |
| **WAN** | Wide-Area Network |
| **XA-Core** | eXtended Architecture Core |