IP Solutions Basics

What's new in this release

The following table highlights the features introduced in this release. Refer to the OSS Advanced Feature Guide for more information about new features in this release.

Note: The terms Passport and PVG have been re-branded in conjunction with the new Nortel Networks' brand simplified naming format. Passport is now referred to as the Nortel Networks Multiservice Switch, and PVG is now Media Gateway 7480/15000.

Table 1
SN07 IP features (Sheet 1 of 25)

Feature descriptions
CS 2000 features **A00003487 -- Tri-modal provisioning, logs, and OMs (UA-IP)** This feature implements support for both a UA-AAL1 and Universal Access - IP (UA-IP) configuration within a single CS 2000 call server. It also supports interworking between the UA-AAL1 and UA-IP configurations in a multi-bearer network configuration. Connectivity between the two bearer networks is accomplished using IW-SPM bridges. The CS 2000 call server has been modified to support both the ATM AAL1 and the IP-based IW SPM at the same time. For more detailed information of this feature, refer to Trimodal network configuration on page 43. **A00003506 - H.248 PTS development (PT-IP)** This SN07 activity provides PTS trunking capabilities for the Succession Call Server 2000 (CS 2000). Specifically, this activity provides incoming, outgoing, and two-way interconnections from a North American End Office (EO), Access Tandem (AT), or InterExchange Carrier (IEC) to the Public Switch Telephone Network (PSTN). **A00003662 -- Trimodal Call Server bridge maintenance (PT-IP-UA-IP)**

Table 1
SN07 IP features (Sheet 2 of 25)

Feature descriptions
This feature enables Trimodal Call Server configurations to support ATM and IP as external bearer fabrics at the same time. Bridge Maintenance should be able to manage the bridges so that ENET-ATM, ENET-IP and ATM-IP connections can be realized. To realize ATM to IP bridging, two bridges will be inserted in the call. One bridge will provide the ENET-ATM connection and the other one will provide the ENET-IP connection. These two bridges will then be connected at the ENET providing the ATM to IP end to end path. **A00003698 -- Razor gateway requirements for trunking (PT-IP)** This feature provides an extension to the existing CALLTRAK/TRMTRACE functionality found on the Core. Currently there is not a way to initiate a Termtrace to capture incoming SIP based calls. This shortcoming is addressed by this feature via functionality delivered to the Core, GWC, and the Session Server network elements. **A00003711 -- CS 2000 support for Gateway Inter Machine Trunk (GWIMT) on Passport Voice Gateway (PT-IP)** This activity provides a limited set of gateway services on the long distance application of the Communication Server 2000 with a partial compliance of ITU-T Recommendation Q.767 Blue Book version signaling protocol and ITU-T Recommendation Q.764 White Book version) (ISUP92) signaling protocol (international use only). This functionality is supported on the IMT GLOBAL trunk agency which are provisioned as gateway trunk agents. This feature supports interworking the gateway trunk agency with a set of supported national long distance signalling agencies. **A00003947 -- Trimodal logs and OMs (PT-IP, UA-IP)**

Table 1
SN07 IP features (Sheet 3 of 25)

Feature descriptions
This activity addresses the OMs, Logs, Traver and Translations components of the trimodal call server. This activity address the following • new office parameter MULTINET_DISPLAY_ACTIVE • new OM groups - IWBMNODE, TRK2NET1, TRK2NET2, OFZ2NET1, OFZ2NET2, DPTOFCP • enhanced DPTNODE OM group • IWBM 800 series log enhancements to display the bridge pool • Translations Enhancements — Conditional PKT selector renamed to “FABRIC” and enhanced to support ATM and IP fabrics. — New BEARNET conditional selector to support criteria checking based on network name. • Traver enhancements — New Traver option BEARNET to input the network name of the incoming trunk agent to support FABRIC and BEARNET conditional selector routing — Traver TRKMEM option is enhanced to derive the originating trunk bearer network/fabric. The bearer network/fabric is used to support FABRIC and BEARNET conditional selector routing
A00004046 -- Echo Cancellation support for Trimodal Call Server 2000 (UA-IP) This activity is responsible for ensuring that ECAN resources can and are allocated appropriately within the Call Server VPN. The goal is to ensure that ECAN resources are always applied in IP networks and are applied according to the selected strategy for AAL1 fabric. This entails implementation of an Edge Strategy for IP Networks and either an Edge or Region strategy for AAL1 networks. Edge Strategy requires that ECAN resources are always allocated at the point of entry into a packet network. Region strategy uses a provisioning model that allows the customer to dictate where ECAN resources should be deployed throughout the network. For more detailed information of this feature, refer to Trimodal network configuration on page 43.
A00004096 -- North America (NA) H.323 Support for Networked Meridian Customer Defined Network (MCDN) Services (PT-IP)

Table 1
SN07 IP features (Sheet 4 of 25)

Feature descriptions
This feature addresses the development associated with providing the CS 2000 switch the ability to support a specified set of MCDN services for its hosted gateway lines (i.e., CICM and Mediatrix 1104) within a carrier hosted H.323 network. **A00004872 -- Services Support for the Universal Access-Internet Protocol Solution (UA-IP)** This activity provides support for the following services in the UA-IP solution • Automatic Call Distribution Observe (ACD OBS) • Automatic Call Distribution Emergency Key, Emergency Key Backup (ACD EMK) • Camp-on for MDC lines (MBSCAMP) • Music on Hold (LMOH, KSMOH, pre-recorded music announcement on hold for ACD) • Executive Busy Override/Executive Busy Override Exempt (EBO/EBX) • Directed Call pick-up Barge In (DCBI) **SAM21 SC features** **A00003601 -- SAM21 SN05/SN06 to SN07 In-service upgrade (IAC, PT-IP, UA-IP)** Since the SAM21 Platform operates in a high availability configuration with two shelf controllers (one active and one standby), in-service upgrades are possible by first upgrading the standby shelf controller, then SWACTing to enable the upgraded shelf controller to be the active shelf controller. This also allows the other shelf controller to be upgraded. Once complete, both shelf controllers are upgraded to the current release without incurring any downtime or impact to Call Processing. **A00003603 - Critical outage prevention and memory recovery (IAC, PT-IP, UA-IP)** Prior to this feature, normal behavior for a SC when it become too unhealthy to provide service was to automatically switch activity to it mate. This created problems if the mate SC was also to unhealthy to provide service. This feature adds the functionality that if the mate shelf controller is determined to be unhealthy for a long period of time, that it be locked and unlocked to freshen the system. **GWC features**

Table 1
SN07 IP features (Sheet 5 of 25)

Feature descriptions
A00003459 -- SSC re-architecture (IAC, UA-IP) This feature contains the following design components: • adds a new alarm for a Succession SYSB line • generates a new log when the above alarm is raised or cleared • adds a new PM sublevel for LGRP • causes an alarm to be raised when there are LGRPs in SYSB state **A00003481 -- PacketCable compliancy (IAC)** Prior to SN07, the GWC software was submitted to PacketCable CertWave 26 (CW26) to test compliancy to the NCS (Network Call Signaling), DQOS (Dynamic Quality of Service), and Security Specifications. Nortel received PacketCable qualification for these protocols. The main purpose of this feature is to incorporate the work done for this qualification testing into the SN07 GWC stream. It will also address upcoming changes to these specifications to maintain PacketCable Compliance. **A00003575 -- GWC security productization (IAC)** IP Security (IPSec) capability is available in SN07 for the following GWC line profiles: • SMALL_LINENA • SMALL_LINEINTL **A00003576 -- TGCP security (IAC)** This feature enables the IP Security (IPSec) capability for the following GWC trunking profiles: • TRUNKNA • TRUNKINTL This feature enables the IPSec provisioning panel on the CS 2000 GWC Manager GUI. **A00003767 -- IP ABI PPVM robustness and message loss alarms (UA-IP)** This activity introduces SCTP (Stream Control Transmission Protocol) for messaging transport between a Succession GWC (gateway controller) and MG 9000 ABI (DS-512) cards. SCTP is used for three of the Nortel proprietary protocols: PPVM (XPM supervision), CSM (Channel Supervision Message), and DS-512 link maintenance.

Table 1
SN07 IP features (Sheet 6 of 25)

Feature descriptions
A00004922 -- DMS-250 N449 PRI Enhancements - GWC (PT-IP) This feature covers the functionalities required to support the following N449 Primary Rate Interface (PRI) enhancements: • Support of CodeSet 0 (CS0) parameterized Network Specific Facilities Information Element (NSF IE) with Out-Of-Band (OOB) data in Facility message. • Support of CS6 Facility IE, Billing IE, and Item IE in Facility message. • Support of CS0 and CS7 User-to-User Information (UUI) if present in PRI Disconnect message. **Session Server features** **A00003277 -- Session Server OM Subsystem (PT-IP)** Like other Call Server platforms, the Session Server Manager records operational measurements (OMs) for various performance related data items. The OM subsystem for the Session Server is similar to the OM subsystem on the Core but is different in some aspects. The majority of OMs pegged in SN07 are directly related to the SIP Gateway application. Also, OMs that are pegged can be viewed via a command line user interface (CLUI) after using secure shell (SSH) to login to the Session Server Manager. **A00003281 -- SIP on Session Server Call Audit (PT-IP)** The Session Server Manager platform provides a secondary call auditing capability for cleaning up stranded calls and reclaiming any call processing resources on the Session Server Manager not associated with valid calls. During normal operation, Session Server Manager calls will be cleaned up properly on call takedown or when a maintenance action results in calls being ended. The call audit assures that the calls are not left up indefinitely due to some type of lost message or other error condition. Session Server Manager calls are audited in two directions. One audit is between the Session Server Manager and the DPT GWC associated with the call. A second audit is between the Session Server Manager and the remote SIP server associated with the call. Calls are terminated whenever any of three components (Session Server Manager, DPT GWC, or remote SIP server) do not recognize the call being audited. **A00003933 -- CS 2000 - Session Server Manager: SCS 2000 -- SIP Gateway application (PT-IP)**

Table 1
SN07 IP features (Sheet 7 of 25)

Feature descriptions
This activity delivers an RFC 3261 Compliant Interface (the Session Server Manager) for the CS 2000 enabling open interoperability with call servers, application servers, and proxy servers using the Session Initiation Protocol (SIP). **A00004005 -- Nortel Carrier Grade Linux (NCGL) platform Session Server (PT-IP)** The purpose of this design is to create a highly available base platform for delivery of multiple applications. The Session Server consists of a Network Equipment-Building System (NEBS) Level 3 compliant hardware platform plus a software framework and architecture for developing Carrier Grade applications and services. In the SN07 release, the architecture for the Session Server will consist of a mated pair of Services Application Module- eXtreme Thin Server (SAM-XTS) with a configuration similar to that of gateway controller. The units consists of an active and inactive unit. Each unit is in reality a fully functional Session Server that is interconnected via a gigabit ethernet LAN. Each server provides processor capacity, local disk storage, and high-bandwidth network connectivity. The Session Server can be configured to use the Integrated Element Manager System (Integrated EMS) between the customer operation LAN and the CS 2000 LAN, or it can be configured without the Integrated EMS. **A00004271 -- SIP Application Server SOC (PT-IP)** This activity implements a mechanism to control the maximum number of SIP/SIPT calls that utilize the Session Server platform when the far end is a non-CS 2000, referred to here as an Application Server. A usage SOC, CS2B0009, is implemented to limit these types of calls. **A00004414 -- SIP Call Server SOC (PT-IP)** This activity implements a mechanism to control the maximum number of SIP/SIPT calls that utilize the Session Server platform when the far end is another CS 2000. A usage SOC, CS2B0008, is implemented to limit these types of calls. **Media Server 2020 features** **A00003918 -- Audiocodes APS09 integration (IAC, PT-IP, UA-IP)**

Table 1
SN07 IP features (Sheet 8 of 25)

Feature descriptions
This feature involves a number of security related features to secure the APS client / server communication link and encryption of various user and system account passwords in the database. **A00003919 -- Audiocodes Media Server integration (IAC, PT-IP, UA-IP)** This feature will aim to integrate the Simple Network Time Protocol standard into the AMS in order to meet the requirements of our customers. This client will periodically query a NTP server, and then use the result to update the system clock on the AMS. **A00004873 - MS 2000 CLUI Enhancements (UA-IP)** This features enhances the existing MS 2000 Series Node CLUI. The following new functionality will be added to the MS 2000 CLUI: • Ability to configure MS 2020 device • Force Lock of a Device • Ability to change the SNMP Community Strings **USP features** **A00003485 - ISUP 200,000 Ports Trunk Support (PT-IP)** This feature increases the limit on the size of table C7TRKMEM for a standalone SSP from 165,000 tuples to a maximum of 200,000 tuples. The constraints which will allow table C7TRKMEM to realize an increased maximum number of tuples from 165,000 to 200,000 are: • Switch is a stand-alone SSP • Universal Signaling Platform **A00004020 -- USP Java GUI Introduction to Succession (PT-IP)** This feature introduces support for a Java based USP GUI application for the USP9.0 Succession release. This feature enables users to run the USP GUI without a central PC running Citrix mainframe. This feature also integrates the USP Java GUI with Integrated EMS and the CS 2000 Management Tools. **A00004951 -- New hardware support (PT-IP)**

Table 1
SN07 IP features (Sheet 9 of 25)

Feature descriptions
This feature introduces support for the new PP5 card to replace the CEx (Computing Engine, NTST11xx) and LEx (Link Engine, NTST10xx) cards as required for component obsolescence issues and to meet H/W cost issues. The PP5 includes a new PMC disk to replace the NTST12CA SCSI disk. Support is included for a mix of 1GB PP4 and 1GB/3GB PP5 cards in the same shelf plus a mix of PP5 link cards with the previous LE2, LE3, and LE4 cards. **A00005029 -- USP client GUI (IAC, PT-IP)** This feature provides a graphical user interface (GUI) capable of running on multiple operating system platforms in a Windows based environment. The GUI has provisions for administering, monitoring and reporting on the Universal Signaling Point (USP). The GUI delivered by this feature is a replacement for the GUI provided with previous software releases and includes and expands upon the functionality and usability provided by the previous GUI version. **Media Gateway 15000 features** **DS3 interfaces between Media Gateway 15000 and MG 9000 (UA-IP)** The UA-IP solution now supports DS3 connectivity to the Nortel Networks Media Gateway 15000 Core using a channelized OC3 interface and a fiber network that multiplexes/demultiplexes DS3 traffic. Nodal Provisioning templates are available to provision the DS3 interface for connectivity between a Media Gateway 15000 and a Media Gateway 9000 over the fiber network. **Recurring fan alarms for Media Gateway 15000 (UA-IP)** After an initial processor control alarm is raised with a severity of MAJOR for a single fan failure, that alarm is repeated once every eight hours until the condition is cleared. After the alarm has been raised three times, the severity is changed to CRTITICAL. The alarm repetition can be turned ON or OFF (base Media Gateway 15000 default is OFF). • For Succession Networks, this attribute is set to ON, by means of nodal provisioning (NP) templates. • Other Media Gateway 15000 users can leave this attribute OFF, in which case the fan alarm is not repeated. This alarm no longer provides warning of a high shelf temperature.

Table 1
SN07 IP features (Sheet 10 of 25)

Feature descriptions
Temperature alarms for Media Gateway 15000 (UA-IP) **Fabric temperature** Formerly, when fabric temperature rose above 65 degrees C, a processor control WARNING alarm of type EQUIPMENT was generated. The severity of this alarm has been changed from WARNING to MAJOR. The type of this alarm has been changed from EQUIPMENT to ENVIRONMENTAL. **Shelf temperature** Formerly, when the shelf temperature rose above 70 degrees C, a WARNING alarm was generated. A new Media Gateway 15000 processor control system alarm code has been added to provide warning of a high shelf temperature condition. The severity of this alarm is CRITICAL, since there may be limited time before the fabric reaches 72 degrees C and shuts itself off. **Standardized configurations and nodal provisioning (NP) templates for Multiservice Switch 15000 and Media Gateway 15000 (UA-IP)** Standard configurations are defined for Media Gateway 15000 equipment in the UA-IP solution, and supported through nodal provisioning (NP) templates. Nodal Provisioning (NP) templates simplify the initial commissioning in a UA-IP Succession solution and minimize operator error in applying Media Gateway 15000 equipment attributes. **New performance measurements (PMs) for Multiservice Switch 15000 (UA-IP)**

Table 1
SN07 IP features (Sheet 11 of 25)

Feature descriptions
5- and 30-minute performance measurements (PMs) for Succession VoIP Performance measurements (PMs) provide a network-level view that can help recover from network outages and facilitate long range office planning: • Media Gateway 15000 nodes use new PMs to report IP statistics for 4-port Gigabit Ethernet and ATM function processor (FP) cards. • Media Gateway 15000 nodes use new PMs to report voice processing performance of the VSP3 and VSP3-o FP cards. The new VoIP PM record format is backward compatible with the existing 5- and 30-minute PM record format for VoA. **5-minute performance measurement (PM) for shelf temperature** The maximum shelf temperature during a 5 minute interval is now supplied in a new 5-minute PM record. These 5-minute PM records can be monitored by the OSS performance host so that appropriate pro-active action can be taken at the network level. **Preside MDM enhancements for Media Gateway 15000 (UA-IP)**

Table 1
SN07 IP features (Sheet 12 of 25)

Feature descriptions
Preside MDM configuration and engineering for Succession UA-IP solution Configuration and engineering practices for the Succession UA-IP solution comply with those in place for Succession UA-ALL1 and PT-AAL1 solutions. **Management Data Provider (MDP) configuration** Administration and configuration of Management Data Provider (MDP) is simplified through application of existing Preside MDM Administration tool services. **Preside MDM workstation synchronization** VoIP Succession networks include Multiservice Switch 15000 equipment in the packet core and Media Gateway 15000 equipment as a voice gateway. A single pair of Preside MDM workstations can be used to manage both of these network elements in more than one Succession office, thereby reducing the operating cost of a VoIP network. One of the pair of redundant server workstations in the Succession network may have a failure that requires the data on the disk drive to be restored. Once the failed workstation has been recovered, an operator must synchronize the recovered workstation with the operational workstation. The data synchronization procedure is also useful when installing a new redundant Preside MDM workstation, or after upgrading the operating system. **Graphical user interface (GUI) to set Succession release name** You can use a graphical user interface to set the current Succession release name in the Preside MDM toolset menu, and in the shelf comment text field of a Media Gateway 15000. **MG 9000 features** **A00001893 -- MG 9000 Imaging (UA-IP)**

Table 1
SN07 IP features (Sheet 13 of 25)

Feature descriptions
Currently, there is not a concept of imaging a Media Gateway 9000 (MG 9000) device load from the Media Gateway 9000 Manager (MG 9000 Manager) or any other application. This means that after a new load is loaded into a Supercore OC3, ITX, ITP, DS1, or ABI device, each device must then be patched up to date. This process can take hours, days and some times months depending on the size of the office, the number of patches and the maintenance window. This feature will provide a means for the customer to upgrade an MG 9000 Device, patch the device up to date, image the MG 9000 Device load with the patches applied and then upgrade the rest of the devices in the office with the imaged load. This feature will also provide a means for imaging to occur automatically so that after the upgrade, if more patches arrive to the site, the customer can continuously keep a stored, up to date, imaged load. **A00002020 -- ESA Translation Download (UA-IP)** This activity allows the download of information necessary to support Emergency Stand Alone (ESA) call processing across all native (non ABI) lines served by a single MG 9000. The download takes place from the CS2000 core to an MG 9000 Manager. The data is generated by the core at 1:00 AM and stored in a file called ESA_SYSTEM_SD$XML on a device specified by OFCENG parameter ESA_GWDATA_DEVICE. It is then downloaded by the MG 9000 Manager through the SDM. **A00002280 -- BITS Interface on Supercore (UA-IP)** The purpose of the feature is to provide a redundant input to the Building Integrated Time Source (BITS). This signal is used to synchronize the MG 9000 to the rest of the transmission network. The technology and functionality is ported from the Internet Telephony Extender design. The Clock Sync application will automatically provision the clock sync system with the following parameters if no provision data is available upon system initialization: **A00002380 -- ESA for ABI: MG 9000 and XPM (UA-IP)**

Table 1
SN07 IP features (Sheet 14 of 25)

Feature descriptions
This activity provides the ability for the Succession Call Server 2000 (CS2000) to support Emergency Stand Alone calling on the following DMS-100 Legacy Extended Peripheral Modules (XPM) subtending a Media Gateway 9000 (MG 9000): • LGC, LGCI • LTC, LTCI • SMA2 **A00002607 -- ABI XPM Site and MG 9000 Location support (UA-IP)** The purpose of this feature is to provide physical location data to aid in the determination and resolution of ABI XPM out of service conditions and native MG 9000 line troubles on the Core. Currently, these service impacting failures can occur in many different points in the Succession networks. This feature will aid in identifying the failure points detectable by the Core by providing necessary and accurate location data. **A00003486 -- Gateway location information (UA-IP)** The purpose of this feature is to provide physical location data for MG 9000 gateways which host only ABI XPMs. This will aid in the determination and ultimately the resolution of ABI XPM and line troubles on the Core. Currently, these service impacting failures can occur in many different points in the Succession networks.This feature will aid in identifying the failure points detectable by the Core by providing necessary and accurate location data. **A00003489 -- ABI SMS support (UA-IP)**

Table 1
SN07 IP features (Sheet 15 of 25)

Feature descriptions
This activity adds support for the SMS and its subtending SLC-96s to the list of legacy PMs supported by the ABI program. The ABI program allows legacy host XPMs to be connected to the packet network without use of an ENET and an I/W Bridge. Instead the XPM is connected to an ABI card in the MG 9000 via its legacy DS-512 interface. The MG 9000 in turn provides connectivity to the packet network. This feature will support Mode 1 and Mode 2 SLC-96s. It will work with both the existing ATM MG 9000 and be integrated with the new IP version. The main customer viable changes for this activity will be the ability yo provision the EXTDS512 optional field as part of the tuple in table LTCINV for the SMS Peripheral Type. The optional field is used to identify the IP Address of the ABI Card and the Gateway Controller that the peripheral is ‘hosted’ off (the GWC must be datafilled in table SERVRINV prior to entering this information). **A00003490 -- Support for ABI XPM tuple change (UA-IP)** Currently, legacy XPMs are connected to either a ENET or JNET network. Rehome of the legacy XPMs to the ABI configuration is accomplished by connecting the XPM to the DS512 interface in a MG 9000 gateway. The DS512 serves as the interface between the TDM links to the XPM and the OC3 interface coming out of the MG 9000 and into the ATM network. This feature provides the ability: • to change the network fabric for a TDM based XPM from Enet/Jnet to DS512 interface • restrict the use of this change only during the XPM rehome procedures **A00003604 -- OC-3 Channelized Support (UA-IP)** This feature allows a user of the MG 9000 LCI to provision a carrier in "Channelized" mode in addition to the previously existing functionality. This provisioning capability is only for SONET carrier and is not applicable for SDH. **A00003693 -- MG 9000 ESA for SMS subtending ABI (UA-IP)** This feature adds Subscriber Carrier Module SLC-96 (SMS) to the supported XPM peripheral types for ESA service for lines off the ABI cards of an MG 9000. **A00003729 -- IP ABI Dedicated PVC & Inservice PVC Parameter Adjustment (UA-IP)**

Table 1
SN07 IP features (Sheet 16 of 25)

Feature descriptions
This feature implements the software needed to support the Access Bridge Interface (ABI) card on the Universal Access-Internet Protocol (UA-IP) Media Gateway. This includes some new provisioning to supply the data needed for the ABI card to function. This data is a set of parameters associated with a new Permanent Virtual Circuit (PVC). This new PVC will carry the messaging traffic associated specifically with the ABI cards. The bearer traffic will utilize the existing Call Control PVC which the bearer and messaging of the Internet Telephony Processor (ITP) card currently use. The functionality of the existing Call Control PVC does not change for the ITP card. The new ABI messaging PVC will carry H.248, Nortel PPVM, CSM, and Link Maintenance messaging traffic specific to the ABI card only.
A00003737 -- LCI Remote access (UA-IP)
This feature implements security for the DCC ethernet interfaces into the MG 9000 and supplies the MG 9000 customer a means for querying the ESA state and the SNMP alarm log history for a node that has lost MG 9000 Manager connectivity.
A00003774 -- Support for new ITP and ABI cards (UA-IP)
This feature will introduce the new ITP (PEC code NTNY30CA) and the new ABI (PEC code NTNY43BA) cards starting with SN07 loads. Previously, there were two separate ITP cards - NTNY30AB for AAL1 and NTNY30BA for IP application, and ABI cards supported only AAL1 application. The main enhancement of the new cards over the previous ITP / ABI is the ability to support AAL1 or IP products without any hardware changes. Based on the MG 9000 configuration (through MG 9000 Manager), ITP and ABI can now support AAL1 or IP application.
A00003775 -- MG 9000 Electrically Programmable Logical Device Loader (EPLD) (UA-IP)
This feature implements the electrically programmable logic devices (EPLD) on the MG 9000 via the Joint Test Action Group (JTAG) interface. Previously, re-programming these parts on the MG 9000 meant that affected cards had to be removed from the shelf and sent in for the new firmware to be loaded. This feature allows new firmware to be applied along with a new MG 9000 load. The new application, the MG 9000 EPLD Loader (MEL), will load newer firmware versions on the targeted devices as a result of a power-up or card reset.
A00004960 -- DS1 IMA IP (UA-IP)

Table 1
SN07 IP features (Sheet 17 of 25)

Feature descriptions
This feature provides a DS1-IMA network interface for the UA-IP MG 9000 solution. Prior to the SN07 release, a UA-IP MG 9000 was available only with an OC-3 network interface. **A00005282 -- MG 9000 Board Diagnostics Framework (UA-IP)** This feature introduces the MG 9000 Board Diagnostics Framework. The Diagnostics Subsystem, when requested through node maintenance, will test various board functionalities and report hardware failures to the least testable component. The Diagnostic Framework is the generic portion of the Diagnostics Subsystem, which can be refined on each card to provide the actual tests. **A00005538 -- Preset Conference in Succession (UA-IP)** This feature addresses the functionality of Preset Conference in Succession. It provides support for the following types of lines on both North American and International markets. • CICM lines - i2002, i2004 and m6350 softclients • MG 9000 Pphones and IBN lines **A00006639 -- MG 9000 Overload OM pegs (UA-IP)** When a Media Gateway 9000 (MG 9000) begins to reach an overload threshold call connections request are denied. This condition can occur on an ITP, ABI or at the nodal level (DCC). A log is currently generated corresponding to the line or trunk which requested the connection. Overload condition occurs when the MG 9000 has reached a threshold where subsequent calls with the exception of calls marked ‘essential or emergency’ must be denied to prevent further catastrophic degradation of the MG 9000 node. With this feature, an Operational Measurement (OM) register will be incremented for every connection which is denied. A new OM group GWOVLOM will be defined and the register OVERLOAD will be incremented upon connection denial. **MG 9000 Manager features** **A00003074 -- MG 9000 Manager Capacity Increase (UA-IP)**

Table 1
SN07 IP features (Sheet 18 of 25)

Feature descriptions
In the SN07 release the MG 9000 Manager will be required to support a maximum capacity of 110,000 H.248 native lines and 75 MG 9000 network elements. The pre-SN07 maximum capacity for the MG 9000 Manager is 55,000 lines and 60 MG 9000 network elements. The recovery time for the 55,000 line configuration is 90 minutes per SN06 Engineering Guidelines. This feature by requirement will meet or exceed the current documented SN06 recovery time, under the new extended capacity requirements. The reason for the long recovery times is that per the current software architecture, managed objects have to be instantiated within the Manager to allow OAM&P. To achieve the SN07 requirements specific managed objects in the MG 9000 Manager design will be collapsed. These objects will have their data persisted to the Oracle database and their business logic collapsed into a container class. This design simplifies the recovery of the ìleaf nodes in the system, which require the most memory footprint and instantiation resources during application startup. **A00003531 -- MG 9000 Manager Frame Location Enhancements (UA-IP)**

Table 1
SN07 IP features (Sheet 19 of 25)

Feature descriptions
This feature includes following deliverables: • Office Frame number is displayed in MG 9000 Manager Alarm browser, Integrated EMS alarm browser and any other alarm browser/s provided by OSS. • Internal frame number is hard-coded to zero in VMG name, while provisioning VMG. • In MG 9000 Manager Frameview, frames are displayed without gap. However, any gap present between shelves will continue to be displayed. • Office Frame number is used in place of Internal frame number in OMC CSV OM file (a stretch deliverable) • A complete flow through provisioning is supported for ITP VMGs. With this, Frame location information, which is specified in MG 9000 Manager while provisioning ITP VMGs, is sent to SESM. SESM in turn, updates XA-CORE table LGRPINV. • With these changes, Craft-person need not manually fill Frame location information in the table LGRPINV. Craft-person just need to provision Frame location information at MG 9000 Manager. • A partial flow through provisioning is supported for ABI VMGs. With this, Frame location information, which is specified in MG 9000 Manager while provisioning ABI VMGs, is sent to SESM. However, SESM does not in turn updates XA-CORE table GWINV. • There is no impact on the way Craft-person handles ABI VMGs, because of these changes. i.e., he/she still needs to manually fill Frame location information in the table GWINV, apart from provisioning Frame location information at MG 9000 Manager. **A00003567 -- MG 9000 Manager support for ABI ESA (UA-IP)** In SN07, ESA capability will be introduced for ABI lines. ABI ESA provides the ability to support basic XPM calls within the MG 9000. The MG 9000 ABI cards will terminate CSide links of the extending XPMs and give them ESA capability if the MG 9000 is out of communication with its assigned Gateway Controller (GWC). The element manager will build on existing ITP ESA functionality for retrieving the ESA translation data from the core and pushing it to the MG 9000. Data common to ITP and ABI VMGs will be handled as in SN06.2. Additionally , new data specific to ABI cards will be retrieved from the core and sent to the MG 9000. This data will include, node, BNV and term type entries. This new data will allow the MG 9000 to support the associated call processing features for ABI while in ESA mode.

Table 1
SN07 IP features (Sheet 20 of 25)

Feature descriptions
A00003571 - MG 9000 Cards Support (UA-IP) This activity supports the release of the following PECCODEs for ITP, ITX, ABI and SCO cards in the MG 9000 Manager: • Internet Telephony Processor (ITP): NTNY30CA (IP and AAL1 modes) • Internet Telephony Extender (ITX): NTNY41BA • Super Core OC3 (SCO): NTNY45CA • Access Bridging Interface (ABI): NTNY43BA (IP and AAL1 modes) The user interface for the ITP, ITX, SCO and ABI are not impacted by this feature. The new VMG of type ABI-IP is added to the VMG provisioning creation. The areas for ‘Silence Suppression (VoIP)’ and ‘QoS Threshold (VoIP Only)’ will be un-gray for this new VMG type (same configuration rules as the current ITP-IP VMG type). A new field ‘Bearer Address’ will be added in the GW Config panel. This field will be editable for ABI-IP Vmg type and it will be gray out for all other VMG types but it will display the same IP address use in the CIPOA Address field. The ‘CIPOA Address’ label will be renamed ‘Signalling Address’. The OVLD alarm and logs format are used to report the failures of the ‘Stream Control Transmission Protocol’ (SCTP) reported by the ABI. The MG 9000 is reporting SCTP Operational measurements via a OM collector interface (please refer to A00003767 ‘IP ABI PPVM ROBUSTNESS and MSG LOSS’ for more information on OM fields an data collected). **A00003591 -- MG 9000 OC3 channelization support from the MG 9000 Manager (UA-IP)** This feature enables the user to view and modify the channelized carrier (OC3) configuration from the MG 9000 Manager. Only the administrative and configuration status can be modified. **A00005016 -- VMG Out-of-service Alarms (UA-IP)**

Table 1
SN07 IP features (Sheet 21 of 25)

Feature descriptions
In SN06.2, there is only one alarm that is raised if a VMG has been provisioned that is in an Out of Service state. Unfortunately, the state of VMG Out of Service is symptomatic of many problems that could be occurring. This feature addresses the problem that resolution of a single VMG OOSV alarm is too complex, especially at VMG provisioning time. Instead of the single fault raised in SN06.2 - VMG300 - VMG OOS, there will instead be a number of faults, each describing a different root cause for why the MG 9000 is not in service. Raising different alarms, helps the user to narrow their resolution /debugging efforts to what is specifically broken. In addition, because these different alarm reasons are logged, there will now be extra information in the logs when the VMG goes out of service as to why it did so (manually set to out of service vs. GWC unreachable vs. GWC not responding). As a result of this feature, when a VMG goes out of service, the Alarm Browser will show the VMG300 alarm only in very unusual circumstances - instead, one or more faults will be raised. **CS 2000 Management Tools features** **A00002585 -- TMM support for PTS trunks (PT-IP)** This feature adds the following components to the TMM application: • post by carrier - allows TMM to post and perform maintenance actions on trunks based on specific carriers • show trunk type - enhances the "PostByGatewayName" operation to add the trunk type to the results • online help - provides online help for TMM **A00003371 -- Common inventory and data consolidation (IAC, PT-IP, UA-IP)** This activity introduces customer logs that indicate failure to obtain a database connection, which can be generated when a resource limit has been exceeded, a database password is changed, or when the database server has stopped or restarted. **A00003454 -- Secure and firewall compatible CS 2000 Management Tools and MG 9000 Manager client GUI communication (IAC, PT-IP, UA-IP)**

Table 1
SN07 IP features (Sheet 22 of 25)

Feature descriptions
The primary purpose for this feature is to facilitate firewall protection for traffic for the Succession OAM&P GUI Client/Server communication, the Succession GUI's will work even with the addition of a firewall in the customer network. Along with sending the date through a firewall, the data will also be encrypted. **A00003560 -- NPM patching for Integrated EMS, CBM, and SSPFS (IAC, PT-IP, UA-IP)** This activity adds the Succession Server Platform Foundation Software (SSPFS), Core and Billing Manager (CBM), and Integrated Element Manager Server (Integrated EMS) as components that can be patched using the Network Patch Manager (NPM) GUI or CLUI. This feature also adds the capability to patch the active and inactive nodes in a two-server configuration. **A00003600 -- CS 2000 SAM21 Manager support for new GWC hardware (IAC, UA-IP)** This feature introduces support for provisioning the GWC application on the Force 695 card. **A00003613 - Core Billing Manager configuration parameters (PT-IP)** This activity introduces the following configuration options in the Succession Server Platform Foundation Software (SSPFS) command line interface (CLI): • CM Internet Protocol (IP) address • Login greeting • System location **A00003615 -- SSPFS packaging and patch enhancements (PT-IP)** This activity implements patching SSPFS using the Network Patch Manager (NPM), or provides MNCLs through electronic software delivery (ESD). This feature also reduces SSPFS downtime during an upgrade, enhances debugging tool and adds Sun Explorer data collector **A00003617 -- SSPFS resource monitoring extensions (PT-IP)**

Table 1
SN07 IP features (Sheet 23 of 25)

Feature descriptions
This feature consists of the following activities: • introduces AlarmD, which is a utility that: — keeps track of alarms on a Succession Server Platform Foundation Software (SSPFS) platform — lights a light that corresponds to the raise or clear of an alarm — writes a customer log corresponding to the state of an alarm. • introduces three new system resource monitors: — memory usage — CPU usage — swap space usage • enhances the file system resource monitor to indicate when a file system is not mounted and when a file system write or read operation failed. • provides a command to query all faults on the SSPFS platform **A00003618 -- SSPFS High-availability enhancements (PT-IP)** This activity enhances the SSPFS high-availability (HA) framework. Most of the enhancements are transparent to the user. The enhancements visible to the user include: • introduction of Continuous Computing Corporation's UpLink product, which on simplex systems, removes the use of Solaris IP multipathing and therefore, reduces the number of IP addresses required by SSPFS • introduction of a new option in the SSPFS command line interface (CLI) to enable, disable, or invoke a cluster failover • introduction of a new option in the SSPFS command line interface (CLI) to configure public addresses on both simplex and HA systems **A00003630 -- TGCP for the cable market (IAC)** This activity introduces the trunking gateway control protocol (TGCP) for ISDN User Part (ISUP) and Per Trunk Signaling (PTS) trunk groups on the Communication Server 2000. The CS2000 GWC Manager GUI is modified to support TGCP and PTS functionality. **A00003667 -- SESM NB alarm interface changes required for OSS (UA-IP)**

Table 1
SN07 IP features (Sheet 24 of 25)

Feature descriptions
This activity modifies the Succession Element and Sub-element Manager (SESM) alarm system as follows: • It refines and updates the CORBA interface to include data that enhances the usability of the alarm notifications. This includes a resynchronization mechanism, improved performance, and a change to the data passed to include additional alarm information. • It changes the SESM default setup to not generate syslogs for alarms, and changes the SSPFS default setup to route customer logs to the Integrated Element Manager Server (Integrated EMS) instead of the CS 2000 Core Manager. • It eliminates the acknowledge and de-acknowledge interfaces. **A00003691 - Integrated EMS SNMP OM polling from GWC and SC (UA-IP)** This activity allows the SNMP poller application to read MIB data for the SAM21 Shelf Controller (SC) and the Gateway Controller (GWC) from a location other than the CS 2000 Management Tools server. A new subnet configuration capability is added to the CS 2000 SAM21 Manager client to provision or modify the IP address where the SNMP poller application resides **A00003948 -- Trimodal server support on SESM and GWC Manager (UA-IP)** This activity changes the CS2000 GWC Manager GUI and OSSgate interface to allow provisioning of multiple network codec profiles, specifying a bearer network fabric instance and a codec profile for each GWC. **A00003995 -- H.323 gateway change capability (UA-IP)** This activity modifies the CS 2000 GWC Manager GUI and OSSgate interface to accommodate H323 provisioning. **A00004860 -- N240 cluster upgrade procedure (PT-AAL1, UA-IP)** This activity implements the upgrade procedure for a Sun Netra 240 two-server (cluster) configuration.

Table 1
SN07 IP features (Sheet 25 of 25)

Feature descriptions
A00005485 -- SAM21 Platform Installation on SSPFS Version 2 (IAC, PT-IP, UA-IP) In SN06, a SAM21 Platform Installation tool was introduced, on SSPFS for the Hybrid Solution, to allow the user a mechanism to install the SAM21 Platform Package on the SSPFS box. This tool read the DAT tape on the SSPFS box and expanded the “TAR” file creating the correct directory structure on SSPFS. This tool was then expanded to install the Call Agent and Message Controller Linux loads. In SN07, the new SSPFS box does not contain a DAT Tape Drive but only a CD/DVD ROM drive. Therefore, this tool will be further enhanced to allow the user to extract the SAM21 Platform Package from CD where it is stored in a “RPM” format. What this means is that this tool will now be used in ALL Solutions to allow the user to install the SAM21 Platform Loads using a DAT tape, to be backward compatible, and CDROM moving forward. The CDROM will be of ISO format containing the following files: • SAM21 Platform Fileset (This is used for installation on the AIX SDM) • SAM21 Platform TAR file • SAM21 Platform RPM file

What's new for the CS 2000 Management Tools

What's new in (I)SN07

Following is a list of activities that are new for the CS 2000 Management Tools and the Succession Server Platform Foundation Software (SSPFS) in the (I)SN07 release:

A00001893/1894 - MG9K imaging

This activity introduces the capability to manually image one MG 9000 device at a time through the MG 9000 GUI and to automatically image MG 9000 devices through the Network Patch Manager (NPM) GUI or CLUI. This feature adds the following items:

- a Software Image command to the MG 9000 Manager GUI interface
- a SmartImage command to the NPM GUI and CLUI interfaces, and two predefined device sets; MG9KDEVICES and GWCDEVICES
- an information log that indicates success or failure of an image and an Audit log that indicates user access of the image command

A00001935 - Provisioning support for Centrex IP nodes and lines

This activity integrates Centrex IP client provisioning (nodes provisioning for Centrex IP Client Manager [CICM] gateways and lines provisioning for CICM terminations) using the OSSgate interface (SERVORD+ system) within the Succession Element and Sub-element Manager (SESM).

A00002512 - GWC Manager internet transparency VCAC provisioning

This activity supports Limited Bandwidth Link (LBL) provisioning from the CS 2000 GWC Manager GUI and the OSSgate interface. It supports the following operations:

- add, delete, modify Limited Bandwidth Link (LBL) middleboxes in addition to Network Address Translation (NAT) devices
- add, delete, modify resource user IDs
- assign an LBL Media Proxy (MP) to a gateway

A00002585 - TMM development for PTS trunk

This activity provides the Trunk Maintenance Manager (TMM) with the capability to post and perform maintenance actions on trunks based on specific carriers. It enhances the operation "PostByGatewayName" to add trunk type in result. This feature also adds online help for TMM.

A00002644 - Common topology identifier provisioning

This activity introduces the following operations through the CS 2000 GWC Manager GUI or OSSgate interface to allow the configuration and use of intra-domain SIP-T trunks in (I)SN07:

- provision the call agent ID
- display the call agent ID
- specify the NAT middlebox ID during NAT provisioning
- display/list the NAT middlebox ID for a selected NAT
- warning message upon deletion of a NAT middlebox

A00003371 - Common inventory and data consolidation

This activity introduces customer logs that indicate failure to obtain a database connection, which can be generated when a resource limit has been exceeded, a database password is changed, or when the database server has stopped or restarted.

A00003454 - Secure and firewall compatible CS 2000 Management Tools and MG 9000 Manager client GUI communication

This activity facilitates firewall protection for traffic for the Succession OAM&P GUI client/server communication. It restricts the number of ports the GUI clients use to communicate with the server. Data is sent through the firewall and encrypted. The ports are configurable.

A00003560 - Common patching user interface

This activity adds the Succession Server Platform Foundation Software (SSPFS), Integrated Element Management System (EMS), and Integrated EMS security as components that can be patched using the Network Patch Manager (NPM) GUI or CLUI. This feature also adds the capability to patch the active and inactive nodes in a two-server configuration.

A00003562 - New card support in SAM21 Manager

This activity provides the CS 2000 SAM21 Manager with the capability to support the Centrex IP Client Manager (CICM) and CICM service types in addition to the existing service types, on an MCPN5385 card. This feature also enables provisioning of GWC application on Force 695 card.

A00003561 - Upgrade Adventnet to 4.0

This activity upgrades the Adventnet software included with the Succession Server Platform Foundation Software (SSPFS), to version 4.0.2.

A00003568 - CICM ECS location identification support

This activity introduces the following operations through the CS 2000 GWC Manager GUI:

- configure, change, or remove the Location Recipient
- enable or disable Location Identification reporting

A00003576 - TGCP security

This activity enables IP security (IPSec) for some GWC trunking profiles. It modifies the IPSec provisioning panel on the CS 2000 GWC Manager GUI.

A00003613 - Core Billing Manager configuration parameters

This activity introduces the following configuration options in the Succession Server Platform Foundation Software (SSPFS) command line interface (CLI):

- CM Internet Protocol (IP) address
- Login greeting
- System location

A00003615 - SSPFS packaging and patch enhancements

This activity implements patching SSPFS using the Network Patch Manager (NPM), or provides MNCLs through electronic software delivery (ESD). This feature also reduces SSPFS downtime during an upgrade, enhances debugging tool and adds Sun Explorer data collector.

A00003617 - SSPFS resource monitoring extensions (alarmD integration)

This activity introduces AlarmD, which is a utility that keeps track of alarms on a Succession Server Platform Foundation Software (SSPFS) platform, lights a light that corresponds to the raise or clear of an alarm, and writes a customer log corresponding to the state of an alarm. This activity also introduces three new system resource monitors; memory, CPU, and swap space usage, and enhances the file system resource monitor to indicate when a file system is not mounted, and when a file system write or read operation failed. In addition, this activity provides a command to query all faults on the SSPFS platform.

A00003618 - SSPFS - High-availability enhancements

This activity enhances the SSPFS high-availability (HA) framework. Most of the enhancements are transparent to the user. The enhancements visible to the user include:

- introduction of Continuous Computing Corporation's UpLink product, which on simplex systems, removes the use of Solaris IP multipathing and therefore, reduces the number of IP addresses required by SSPFS
- introduction of a new option in the SSPFS command line interface (CLI) to enable, disable, or invoke a cluster failover
- introduction of a new option in the SSPFS command line interface (CLI) to configure public addresses on both simplex and HA systems

A00003630 - TGCP for the cable market

This activity introduces the trunking gateway control protocol (TGCP) for ISDN User Part (ISUP) and Per Trunk Signaling (PTS) trunk groups on the Communication Server 2000 (CS2K). The CS 2000 GWC Manager GUI is modified to support TGCP and PTS functionality.

A00003666 - Integrated EMS HA support and co-residency with CS2M

This activity enables the Integrated Element Management System (EMS) to co-reside with all applications in the CS2M load on Sun Netra 240 servers (one-server or two-server configuration), and on Sun Netra t1400 servers.

A00003667 - SESM NB alarm interface changes required for OSS

This activity modifies the Succession Element and Sub-element Manager (SESM) alarm system as follows:

- It refines and updates the CORBA interface to include data that enhances the usability of the alarm notifications. This includes a resynchronization mechanism, improved performance, and a change to the data passed to include additional alarm information.
- It changes the SESM default setup to not generate syslogs for alarms, and changes the SSPFS default setup to route customer logs to the Integrated Element Management System (EMS) instead of the core manager.
- It eliminates the acknowledge and de-acknowledge interfaces.

A00003691 - Integrated EMS SNMP OM polling from GWC and SC

This activity allows the SNMP poller application to read MIB data for the SAM21 Shelf Controller (SC) and the Gateway Controller (GWC) from a location other than the CS 2000 Management Tools server. A new subnet configuration capability is added to the CS 2000 SAM21 Manager client to provision or modify the IP address where the SNMP poller application resides.

A00003717 - CICM flowthrough provisioning

This activity provides support for the flow through of line and user provisioning data between the Succession Element Sub-element Manager (SESM) OSSGate provisioning interface and the Centrex IP Client Manager (CICM) platform.

A00003912 - Centralized OAM&P Security and Administration

This activity implements the central security server, which provides the following features:

- central administration of user accounts
- central authentication
- central authorization
- single sign-on (SSO) - enables users to access multiple network elements, applications, and features from a single login session.
- customer plugability - allows third-party plug-ins for authentication and authorization

A00003948 - Tri-modal server support on SESM and GWC Manager

This activity changes the CS 2000 GWC Manager GUI and OSSgate interface to allow provisioning of multiple network codec profiles, specifying a bearer network fabric instance and a codec profile for each GWC.

A00003995 - H323 gateway change capability

This activity modifies the CS 2000 GWC Manager GUI and OSSgate interface to accommodate H323 provisioning.

A00004860 - Netra 240 cluster upgrade procedure

This activity implements the upgrade procedure for a Sun Netra 240 two-server (cluster) configuration.

A00004981 - GWC Manager Internet Transparency-VCAC provisioning support for CICM gateways

This activity supports virtual connections admission control (VCAC) for CICM gateways and provides the following capabilities using the CS 2000 GWC Manager or OSSgate interface:

- provision a set of root middleboxes (maximum 5) for each CICM gateway
- change the provisioning of root middleboxes against provisioned CICM gateways
- display or query the root middleboxes that are provisioned against a CICM gateway

A00005123 - CS2M configuration install script enhancements

This activity modifies how the Succession Element and Sub-element Manager (SESM) software handles database upgrades, which reduces the time to upgrade the SESM software.

A00006340 - GWC Manager support for MTX_TRUNKNA and MTX_TRUNKINTL GWC profiles

This activity introduces two MTX-specific profiles, NA (North America) and INTL (international), that can be provisioning from the CS 2000 GWC Manager GUI.

Overview

This document describes the following North American Succession Internet Protocol (IP) solutions:

- Integrated Access - Cable (IAC)
- Packet Trunking - IP (PT-IP)
- Universal Access - IP (UA-IP)
- Trimodal network configuration

IAC solution

The Integrated Access-Cable (IAC) solution delivers full featured IP telephony to residences over the Hybrid Fiber Coax Cable System (HFC) infrastructure (see the figure IAC compact architecture). Cable multiple system operators (MSOs) may choose to offer any combination of

- regulatory compliant primary voice services
- alternative secondary voice services
- long distance services

Inter operability with a selection of third party access solutions, such as Cable Modem Termination System (CMTS), Multimedia Terminal Adapter (MTA), and PSTN Trunk Media Gateway (MG) is enabled by the solution's adherence to the PacketCable™ architecture defined by CableLabs® and in particular the PacketCable® protocol specifications such as Network-based Call Signaling (NCS), Dynamic Quality of Service (DQoS), Security, and PSTN Gateway Call Signaling Protocol (TGCP).

In the IAC solution, the CS 2000 is PacketCable 1.0 qualified as a PacketCable Call Management Server (CMS) and Media Gateway Controller (MGC).

The following PacketCable capabilities are supported:

- Network Call Signalling (NCS) Protocol
- Dynamic Quality Of Service (DQoS)
- Trunk Gateway Control Protocol (TGCP)
- PacketCable Signaling Security using IP Security (IPSec) to MTAs, CMTSs, and Trunk Media Gateways

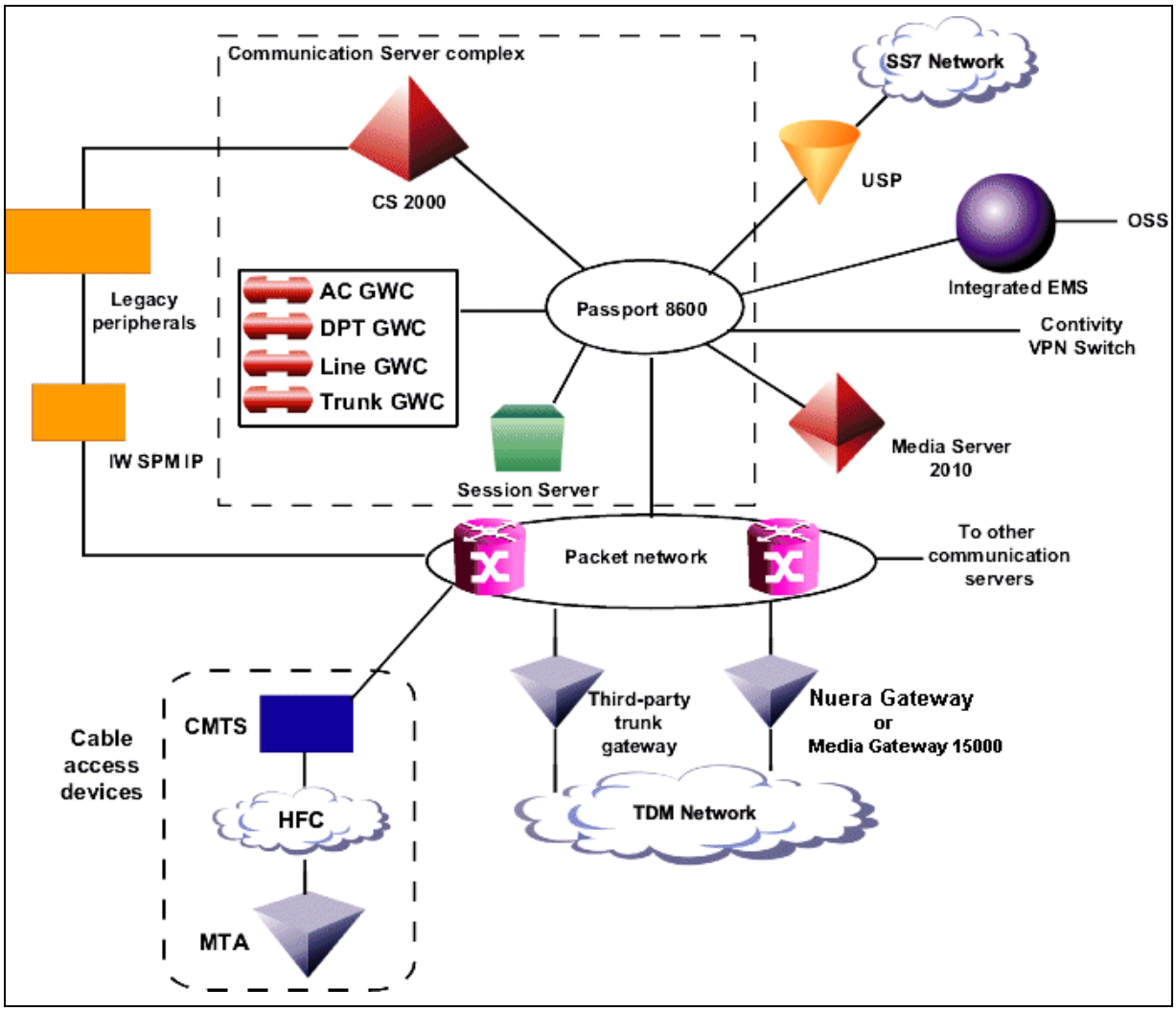
Call processing and control, signaling and trunking to the TDM network, announcements, conferencing, and lawful intercept all interwork by means of standard interfaces over the IP backbone. At the same time, the IAC solution offers the flexibility to support market-driven end-user services utilizing PacketCable™ endorsed specifications. This solution takes advantage of the cost efficiency, open standards, and reduced time-to-market for new services by IP packet networks.

The IAC solution addresses the following market requirements:

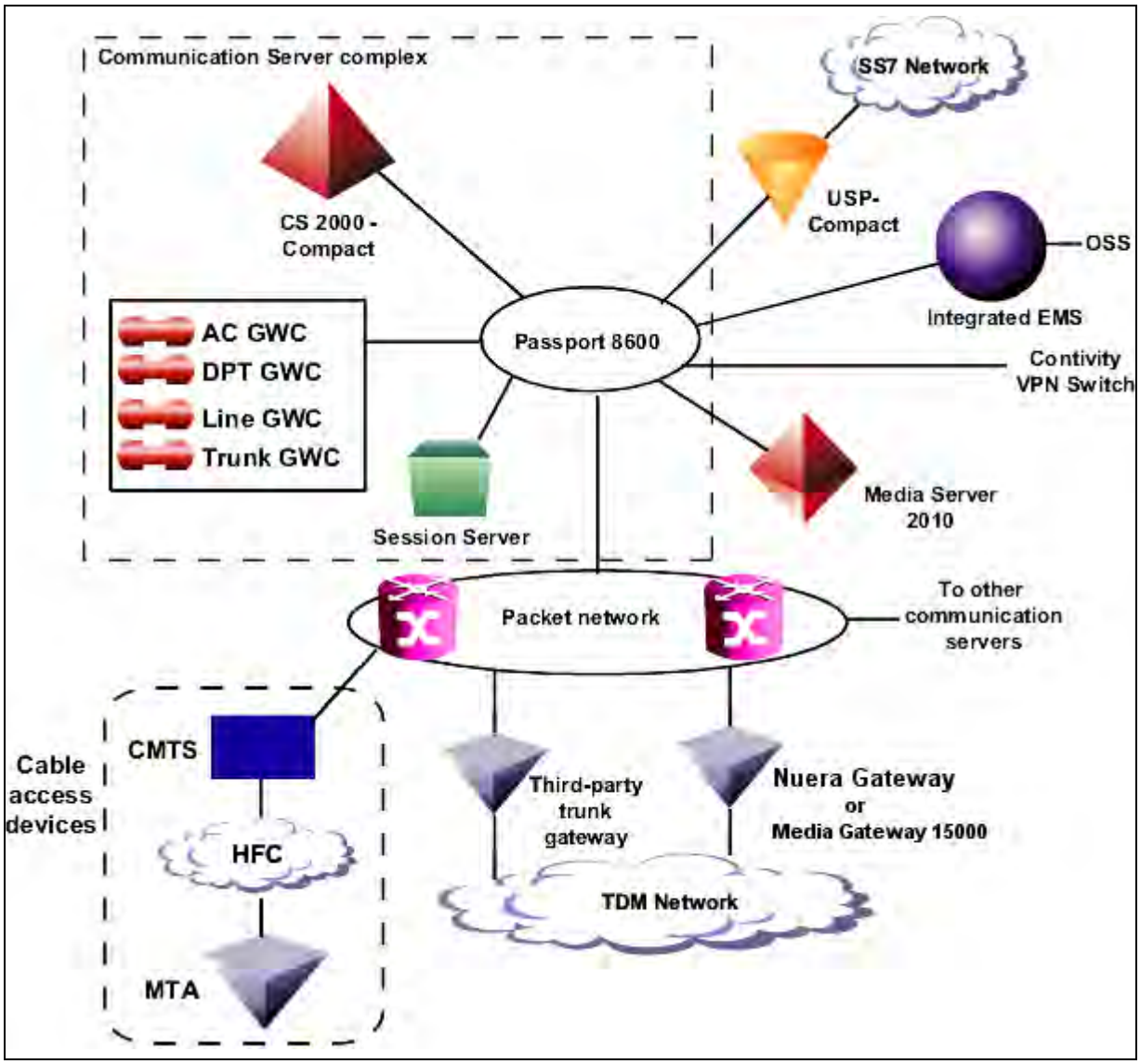
- targets the unique needs of cable operators serving the residential market segment
- increases access and transport efficiency by means of unified packet telephony access in a multi-service packet network space
- enables cable MSOs or overbuilders to provide telephony without deploying legacy switching equipment
- provides Greenfield solutions to MSOs and overbuilder carriers that capitalize on the DMS service set
- for customers with existing DMS equipment, provides an easy transition to a IP architecture by means of:
  - — support of Hybrid configurations with both legacy peripherals and IP
  - — reusing the existing XA-Core architecture
  - — supporting existing OSS interfaces
- provides support for DMS feature sets on a unified software load

The figures below shows the IAC and IAC compact network architectures.

IAC architecture



IAC compact architecture



Packet Trunking - IP, or - AAL2 solutions

Nortel Networks supports two variations of this Packet Trunking (PT) solution:

- Packet Trunking - IP (PT-IP) supports AAL5 and uses an IP network as the backbone network for bearer traffic.
- Packet Trunking - AAL2 (PT-AAL2) is based on PT-IP. PT-AAL2 supports AAL2 and uses an ATM network as the backbone network for bearer traffic. PT-AAL2 also supports compression Codecs such as G.726.

PT-IP and PT-AAL2 are standards-based switching architectures that integrate voice and data networks through a high capacity packet switching technology. Narrowband TDM switch architecture is evolving to take advantage of the broadband capabilities of packet switching. This solution addresses the following Inter-exchange Carrier (IXC) networking needs:

- reduces support costs for existing narrowband switch installations
- enhances trunking capacity to meet increasing demand for wider bandwidth
- provides existing narrowband switches access to the high-bandwidth capacity of packet networks

PT-IP and PT-AAL2 provide increased efficiencies in the trunking network through the introduction of packet multiplexing and switching technology.

PT- AAL2 utilizes ATM adaptation layer 2. AAL2 provides a means to multiplex up to 255 user data within a single VCC for transferring short and variable length packets in delay sensitive applications under a way of saving bandwidth. AAL2 is best known for multiple, short packet based user channels over the same ATM connection. The following are the characteristics of AAL2:

- AAL2 is a multiplexed ATM adaptation layer for voice, data, video, and signalling
- more than one type 2 information stream can be supported on a single ATM connection (multiplexed in a single cell)
- provides for bandwidth efficient transmission of low-rate, short, and variable length packets in delay sensitive applications
- best for voice over ATM and for compressed speech

PT-IP utilizes ATM adaptation layer 5 (AAL5). AAL5 transports connectionless, non-real-time variable bit rate (nrt-VBR) traffic where a timing relationship between the traffic source and destination is not required. AAL functions in support of variable bit rate, delay-tolerant connection-oriented data traffic requiring minimal sequencing or error detection support. AAL5 provides the means to detect the error on the user data in the transferring and the capability to forward corrupted data to user if user accepts. IP traffic typically uses AAL5. AAL5 is the dominant data service.

PT-IP and PT-AAL2 allow service providers to deploy trunking over a backbone IP or ATM packet network. PT-IP, and PT-AAL2 address the following Long Distance (LD) and tandem market requirements:

- voice-over-packet network services (voice application over a packet network)
- scalability (incremental port and Busy Hour Call Attempts (BHCA) capacity)
- reliability (99.999% service availability and in-service software upgrades during which no calls are lost)
- minimal footprint (high port density in a small amount of space)
- interoperability (system is standards-based so it is interoperable with other emerging solutions)
- reduced cost of ownership (lower cost of network infrastructure and operations)
- Greenfield and Evergreen solutions for smooth transition and upgrade plan to voice-over-packet unified network infrastructures (reuse of existing XA-Core architecture, support for existing OSS interfaces, preservation of DMS features, and integration of TDM and IP)
- support for DMS 100, 200, 250, and 500 feature sets on a unified software load

Benefits of PT-IP (and PT-AAL2) include the following:

- serves as enabler for the transformation of a TDM-based network to a packet-based network
- allows service validation including billing certification
- provides packet network validation
- provides Media Gateway 15000 or Media Gateway 7400 functionality
- PT-IP supports hybrid networks using the IW-SPM-IP, which permits Succession and legacy network interworking (PT-AAL2 does not support hybrid networks)
- supports multiple point codes (MPC)
- provides solution and management familiarity to customers

The PT-IP solution is deployed as either a Greenfield or a Hybrid network. In a Greenfield network, Nortel Networks installs a new switch for the customer. The CS 2000 uses SIP-T communication, allowing ANSI ISUP payload to be transported over a packet network. Hybrid means that the CS 2000 functionality can be extended into the existing

legacy DMS equipment of the customer. The hybrid capability allows the CS 2000 to simultaneously manage TDM components and packet components interconnected by an IW SPM-IP.

The PT-AAL2 solution is deployed as a Greenfield or Hybrid network. However, PT-AAL2 does not support the IW SPM-IP, so any hybrid configuration for the PT-AAL2 must use physical loop-around trunks to provide connections between the time division multiplex (TDM) and packet networks. The loop-around trunk is terminated on a Digital Trunk Controller (DTC) or Spectrum Peripheral Module (SPM) on the TDM side. The other end of the loop around trunk is terminated on the TDM side of a Media Gateway 15000 or Media Gateway 7400. The XA-Core call processing software handles the call set up at either end of the loop around trunk just as if a call were to and from a remote node. Each end of a loop-around trunk is separately defined by datafill in the XA-Core and has different SS7 point codes.

TDM peripherals modules (PMs) are those PMs that currently reside in a legacy, circuit-switched network. PT-IP and PT-AAL2 support the co-existence of the following TDM peripherals modules:

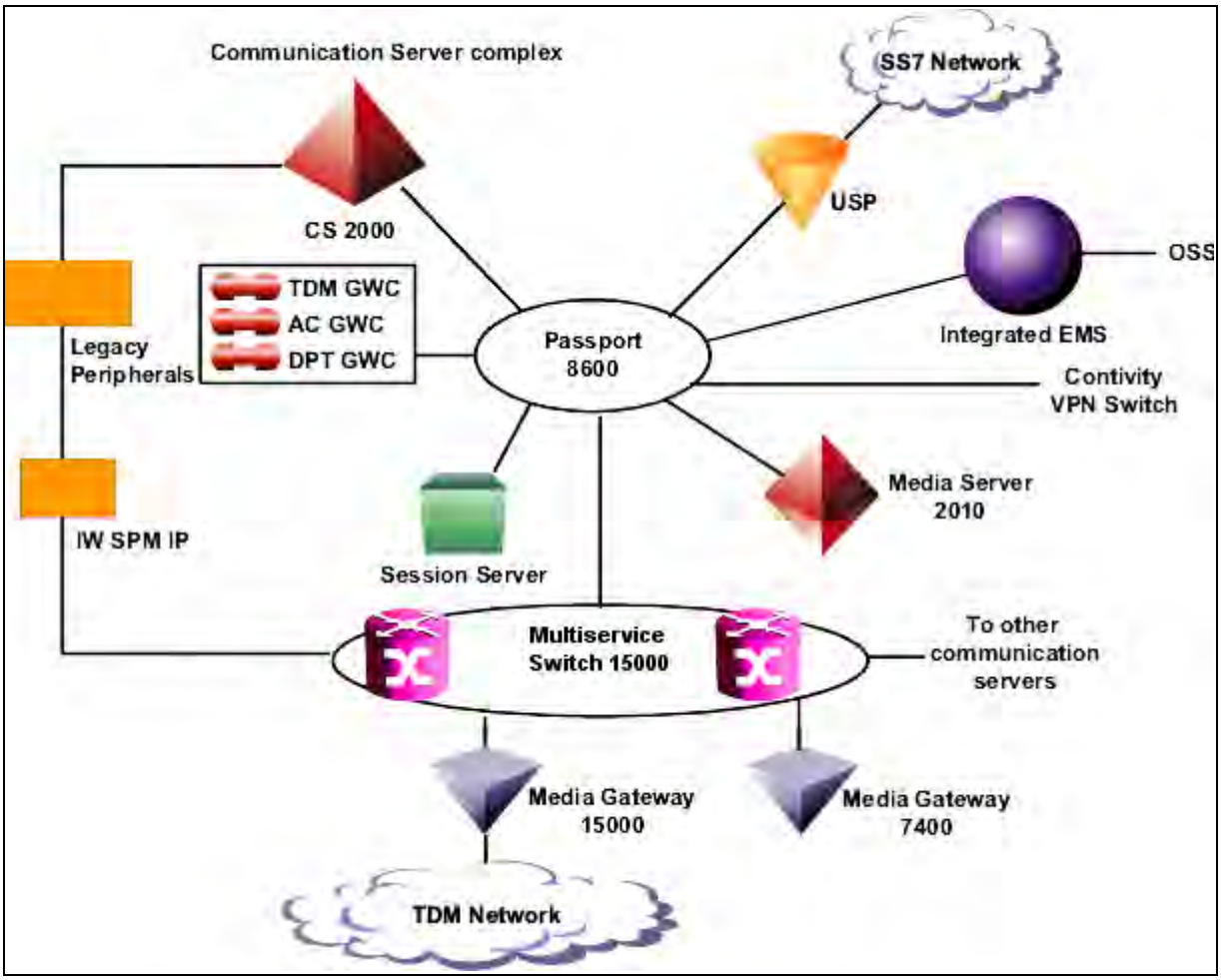
- Digital Trunk Controller (DTC)
- Digital Trunk Controller with ISDN (DTCI)
- Spectrum Peripheral Module (SPM)
- Maintenance Trunk Module (MTM)
- Trunk Module 8-wire (TM8)
- Digital Trunk Module (DTM)
- Line Trunk Controller (LTC)
- Line Trunk Controller with ISDN (LTCI)

PT-IP and PT-AAL2 support interworking with the following TDM peripherals:

- DTC
- DTCI
- SPM
- LTC
- LTCI

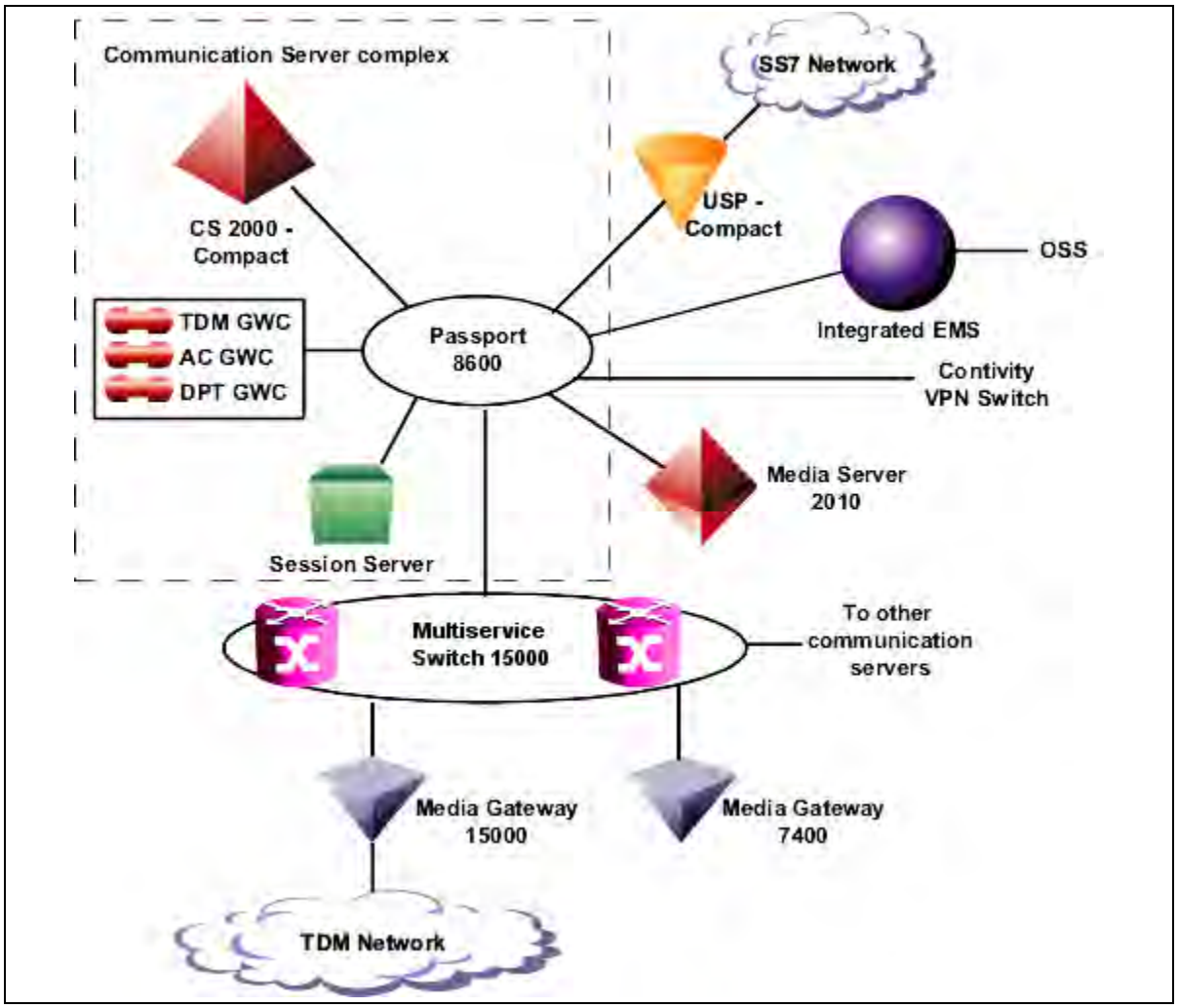
The figure PT-IP AAL5 hybrid architecture with CS 2000 shows the PT-IP AAL5 hybrid architecture with CS 2000.

PT-IP AAL5 hybrid architecture with CS 2000



The figure PT-IP AAL5 architecture using CS 2000 - Compact shows the PT-IP AAL5 architecture with CS 2000 - Compact.

PT-IP AAL5 architecture using CS 2000 - Compact



Universal Access - IP solution

UA-IP delivers end-office line and trunk services over an IP packet network. UA-IP supports the following time division multiplex (TDM) services:

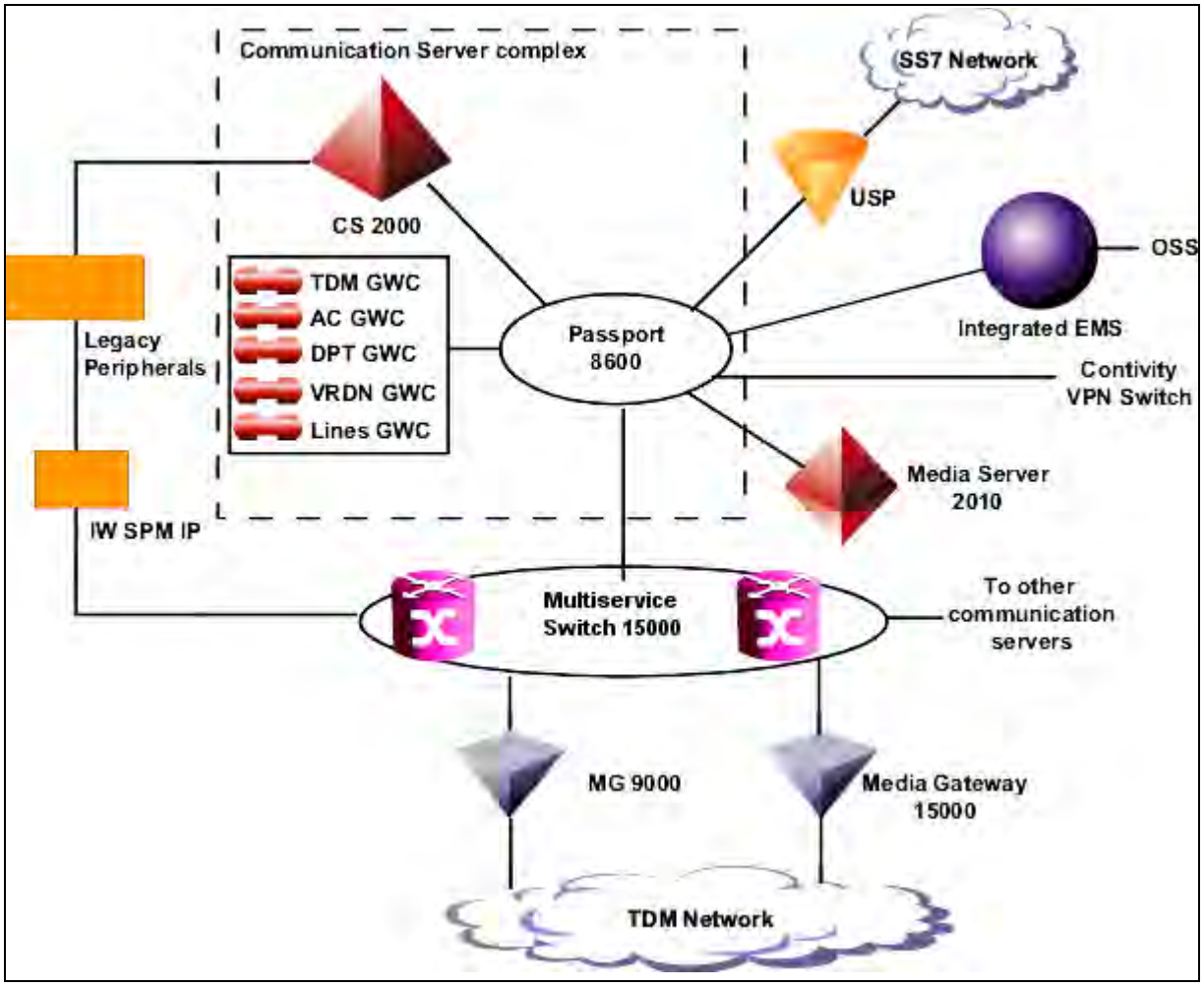
- Line services
  - — Plain old telephone services (POTS)
  - — Digital Subscriber Line (DSL)
- trunk services
  - — ISUP (integrated services digital network user part)
  - — PRI (primary rate interface)

In addition UA-IP uses the Session Initiation Protocol for Telephony (SIP-T) to set up bearer path Dynamic Packet Trunking (DPT) trunks across the packet network. Dynamic Packet Trunking allows traffic to be routed between Succession Network nodes over an IP packet network.

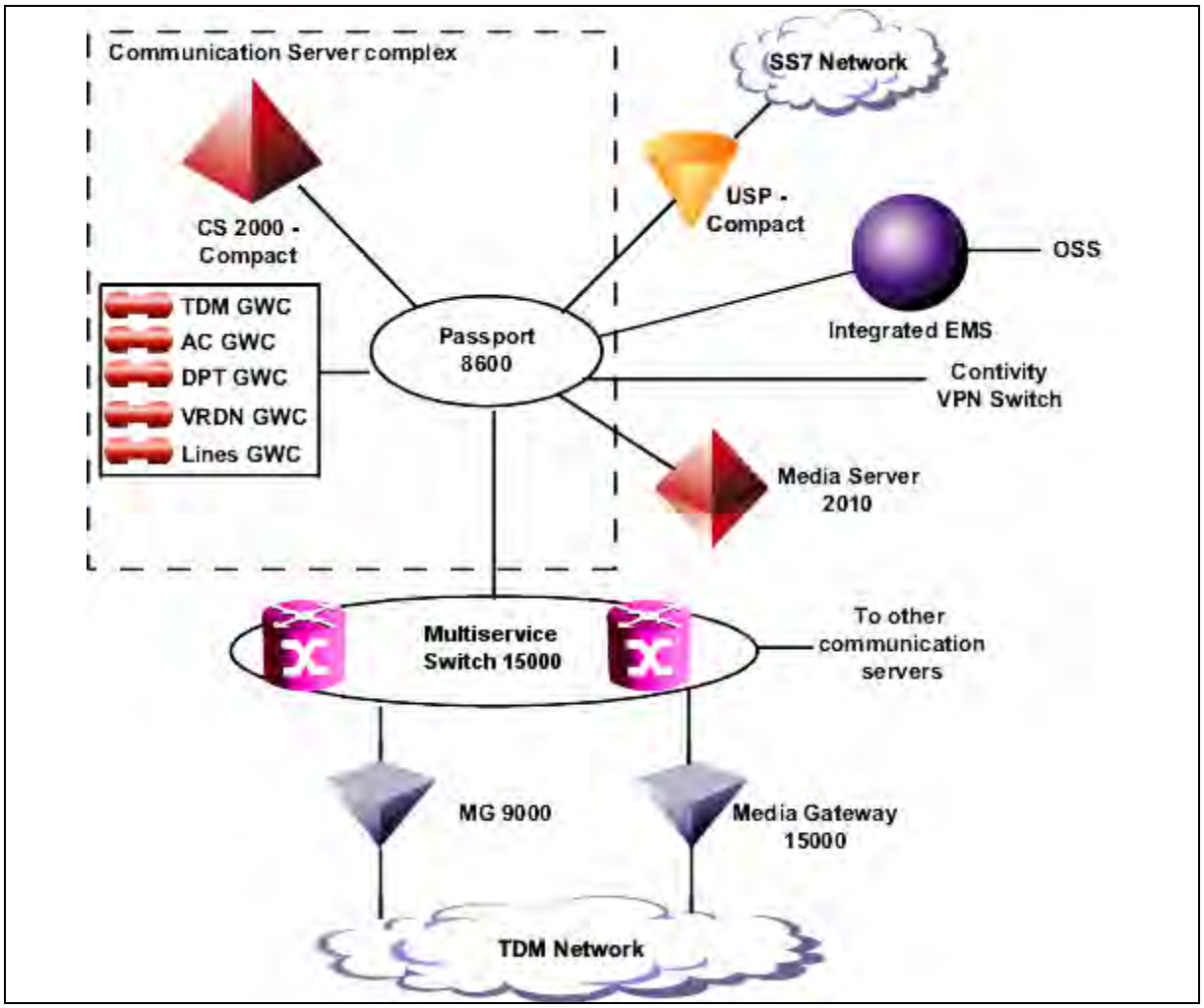
In the SN06 release, Nortel Networks offers UA-IP as a new installation (greenfield).

The figure UA-IP Architecture shows the UA-IP architecture.

UA-IP Architecture



UA-IP Compact Architecture



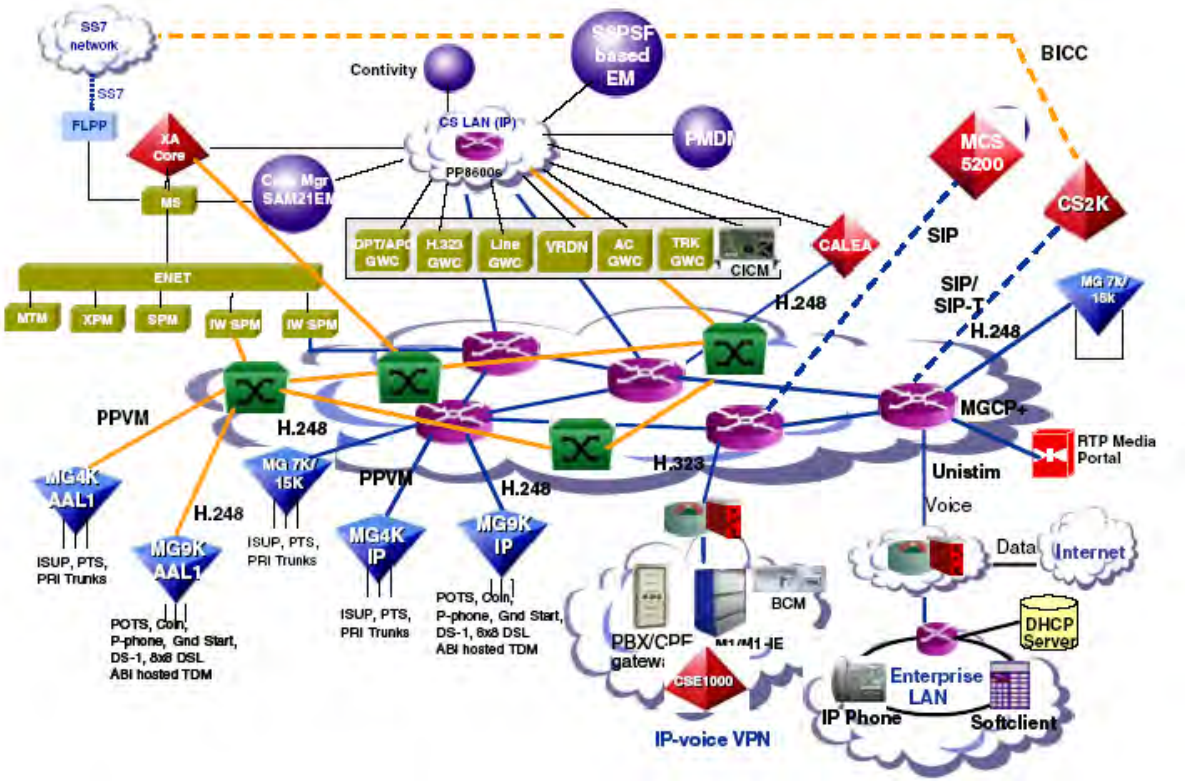
Trimodal network configuration

In the SN07 release, support is introduced on the CS 2000 to support the following bearer networks:

- ENET
- AAL1 packet network
- IP packet network

The following figure illustrates a network with a trimodal CS 2000.

Trimodal network configuration



The trimodal CS 2000 allows interworking between the UA-AAL1 and UA-IP configurations in a multi-bearer network configuration. In SN07, interworking between the H.323 gateway and the IW-SPM IP is not supported. Due to this constraint, a looparound trunk hosted by either a Media Gateway in the UA-IP network or an MG 4000 in the UA-AAL1 network is used to provide connectivity between the H.323 gateway and all other agents in the CS 2000.

The following gateways and packet agents are supported in this multi-bearer network configuration.

Supported gateways and packet agents

Bearer network type	Gateway	Agents
UA-AAL1	MG4000	ISUP trunks PTS trunks PRI trunks BICC DPT trunks
	GWC	BICC DPT trunks
	MG9000	POTS lines Pphone lines Coin lines Ground Start lines
	MG9000 with ABI	supported SN07 ABI peripherals which includes both lines and trunk
	DPT SPM	BICC DPT trunks
UA-IP	Media Gateway (for loop-around trunk access only for support of H.323)	ISUP trunks PRI trunks
	MG9000	POTS lines Pphone lines Coin lines Group Start lines
	MG9000 with ABI	supported SN07 ABI peripherals which includes both lines and trunk

Note: The GWC is not a true bearer gateway. This is included to illustrate the support for BICC DPT trunk support.

Connectivity between the supported bearer networks is accomplished by using IW SPM bridges. The trimodal CS 2000 allows support of both the ATM AAL1 based IW SPM and the IP based IW SPM at the same time. Prior to SN07, the CS 2000 could only support one type of IW SPM. A single IW bridge pool was supported. In SN07, support for multiple bridge pools is introduced.

Control is given to the Succession customer to configure how the supported bearer networks in the CS2000 Call Server connect to each other. This is controlled by provisioning the types of interworking bridges needed to connect one bearer network to another. The interworking bridges available in SN07 are the following:

- IW SPM AAL1 - connects an AAL1 bearer network to the ENET
- IW SPM IP - connects an IP bearer network to the ENET

Prior to SN07, Succession configurations used the IW SPM AAL1 to connect an AAL1 bearer network to the ENET and used the IW SPM IP to connect an IP bearer network to the ENET. This is still supported in SN07 with multi-bearer network support. In this multi-bearer network configuration, a connection between an AAL1 bearer network and an IP bearer network will use two IW bridges (i.e., 1 IW SPM AAL1 and 1 IW SPM IP using the ENET to connect the two packet bearer networks).

The role of each component in the IAC, PT-IP, PT-AAL2, and UA-IP solutions

The following table lists the components that make up the IAC, PT-IP, PT-AAL2, and UA-IP solutions and provides a brief description of their function.

Note: The CS 2000 - Compact is a small-footprint alternative to the CS 2000. The CS 2000 - Compact is designed for new installations, and provides the same functionality as the CS 2000.

Components and their function (Sheet 1 of 22)

Components	Sub-component	Function
Network intelligence		
Communication Server 2000 (CS 2000) 		The CS 2000 solution has evolved from the DMS family of TDM central office switches. CS 2000 reuses much of the existing DMS TDM service software, as well as the carrier grade DMS hardware. CS 2000 provides the following primary functions • call processing (including translations and routing) • SS7 signaling • call feature processing (including features inherited from the DMS) • billing
CS 2000	Extended Architecture Core (XA-Core)	The XA-Core is the computing engine of CS 2000. The XA-Core provides maintenance, call processing, and billing functionality. The CS 2000 also sends control messages (for connection set-up) to media gateways (such as the Media Gateway 15000), Multimedia Terminal Adapter, and MG 9000. The Ethernet or high speed Input/Output Processor (EIOP/HIOP), which resides on the XA-Core, enables the XA-Core to connect to the packet network.

Components and their function (Sheet 2 of 22)

Components	Sub-component	Function
CS 2000	Message Switch (MS)	The message switch routes messages from the XA-Core to the ENET, IOM, FLPP, and CS 2000 Core Manager. The MS supports control messaging between the XA-Core and FLPP and between the XA-Core and CS 2000 Core Manager.
CS 2000	Enhanced network (ENET)	The ENET is an optional component (not supported by the IAC solution except in a Hybrid CS 2000 configuration). The ENET is the enhanced network for the XA-Core. It is a fully duplicated switching fabric that performs call switching. The ENET provides the messaging path from CS 2000 to any legacy peripherals and is required for access to test trunk facilities.
CS 2000	Input/ Output Module (IOM)	The IOM provides input/output (I/O) interface to the CS 2000.
CS 2000	Cabinetized Integrated Service Module (CISM)/ Integrated Service Module Enhanced (ISME) and the Office Alarm Unit (OAU)	The CISM/ISME and the OAU provide test and service circuit functions required by the CS 2000 feature set.
CS 2000	Services Application Module 21 (SAM21)	The SAM21shelf houses the CS 2000 GWC cards (see the next row in this table). All tools and utilities for the SAM21 are provided by CS 2000 SAM21 Manager.

Components and their function (Sheet 3 of 22)

Components	Sub-component	Function
CS 2000	CS 2000 Gateway Controller (GWC) CS 2000 Gateway Controller (GWC) 	The CS 2000 GWCs provide protocol mediation between the XA-Core and media gateways such as the Media Gateway 15000, and MG 9000. In other words, the CS 2000 GWCs convert proprietary supervision messages from the XA-Core to protocols recognized by the media gateways. The CS 2000 GWCs support these protocols: H.248, ASPEN, SIP-T, IUA, SNMP, M3UA, packetable NCS, and packetable DQoS COPS. IP solutions use different types of CS 2000 GWCs, based on the media gateway or service that requires management. Every CS 2000 GWC uses the same hardware and software. Profiles applied at the CS 2000 GWC Manager define the type of GWC. The IP solutions use the following types of GWC: • Audio Control (AC): is required for all IP solutions • Dynamic Packet Trunking (DPT): is required for all IP solutions • Time division multiplex (TDM) trunks: is required for UA-IP, PT-IP and PT-AAL2 • Lines: is required for UA-IP, and IAC

Components and their function (Sheet 4 of 22)

Components	Sub-component	Function
CS 2000	Session Server 	The Session Server replaces the Virtual Routing Destination Node (VRDN) Gateway Controller as a SIP interface. The Session Server is a software application that provides interoperability with third-party application servers and softswitches. The Session Server consists of a Network Equipment-Building System (NEBS) Level 3 compliant hardware platform plus a software framework and architecture for developing Carrier Grade applications and services. ***Note:*** For a series of calls servers that is serviced by one Session Server, the minimum release for all the supported call servers needs to be SN06. The Session Server is not backwards compatible to SN05 CS 2000s.
	Fiberized Link Peripheral Processor (FLPP)/Link Peripheral Processor (LPP)	The FLPP/LPP functions as the default SS7 signaling server for evergreen hybrid applications, when an existing DMS switch (supporting legacy peripherals) is converted to a CS 2000. FLPP uses SR 128 sub-rate fiber links to connect the CS 2000 to the SS7 network. LPP is a modular equipment package that consists of small, peripheral modules. Each LPP supports up to thirty-six 56 kbps SS7 links. The FLPP/LPP provides link interface unit 7 (LIU7) support. FLPP/LPP also provides EIU support for collecting faults and alarms, modifying switch table databases for Product and Services Provisioning (PSP), delivering loads electronically, and monitoring switch performance through telnet.

Components and their function (Sheet 5 of 22)

Components	Sub-component	Function
CS 2000	Universal Audio Server (UAS) 	The UAS is capable of providing media services such as the delivery of voice announcements, the collection of dual-tone multi-frequency (DTMF) digits, speech recognition, text-to-speech synthesis, speaker verification, audio conferences, and facsimile. For the IAC, PT-IP, PT-AAL2, and UA-IP solutions, the UAS provides voice announcements and facilitates the lawful electronic surveillance of voice and voice-band data traffic in the network (Lawful Intercept). The UAS resides on the SAM16 hardware platform. The UAS has an OC-3c connection to the packet network for bearer path connections. In addition the UAS has a 100Base-T Ethernet connection to the CS LAN, that is used for H.248 call control messaging between the UAS and CS 2000. In addition, the CS LAN provides operations, administration, and maintenance (OAM&P) messaging to the UAS.

Components and their function (Sheet 6 of 22)

Components	Sub-component	Function
CS 2000	Media Server 2010 	The MS 2010 is a replacement for the UAS. As an application server supporting audio services, the MS 2010 provides an interface for caller interactive features that require the collection of user input and prompt playback. In this capacity, the MS 2010 supports the following functions: • plays announcements stored as G.711 encoded mulaw and alaw • plays a set of announcements to the caller which can be interruptible by Dual Tone MultiFrequency (DTMF) digit entry • plays an announcement and collects DTMF digits • plays a particular announcement and collects DTMF digits, potentially looking for a specific DTMF digit response using a specified DTMF digit pattern (specific digits, maximum number of digits, or specific digits that can interrupt the announcement) • plays an announcement that is stored in the runtime database
CS 2000	Audio Provisioning Server (APS).	APS is a subcomponent of UAS and MS 2010. APS contains the APS application. APS provides a central database for network-wide provisioning and maintenance of announcements. APS assures that all UASs or MS 2010 in the network use the same announcements. APS is required whenever the UAS/MS 2010 is used as the announcement server. APS is a non-call processing component. It uses a user-friendly web interface to provision audio services and to set up distribution of announcements to UASs\MS 2010 in the network.

Components and their function (Sheet 7 of 22)

Components	Sub-component	Function
CS 2000	Universal Signaling Point (USP) and USP Compact 	The USP is the default SS7 signaling server for new installations (greenfield). The USP supports a redundant 10/100BaseT IP interface. This release provides the following capabilities: • high speed link interface support to signaling transfer point (STP): DS-1 ATM SAAL SS7 links (8 DS-0 equivalent) • high speed link interface support to simple control transmission protocol (SCTP): IETF SIGTRAN SCTP/M2PA IP high speed link (8-20 DS-0 equivalent) • DS0A, V.35, and channelized T1/E1 low speed link support • direct messaging to the GWC by means of M3UA/UDP for TDM ISUP trunking • load sharing between SS7 links • supports co-resident STP capability • support for ANSI ISUP trunks • high service availability of 99.999% and in-service software upgrades during which no calls are lost • in-service LIU7 application upgrade from FLPP to USP • access to HMI through the ethernet • support for 4 multi-point code for direct messaging but up to 16 may be supported with message bounce off the XA-Core (if configured) • support for up to 440 low speed SS7 links The USP - Compact provides the same basic functionality as the USP, but is used for networks with smaller call capacities. The USP - Compact resides on two identical blades in a CS 2000 - Compact or SAM21 shelf and supports up to 16 channelized T1/E1 links and up to 8 multi-point codes.

Components and their function (Sheet 8 of 22)

Components	Sub-component	Function
CS 2000	Communication Server local area network (CS LAN)	The CS LAN provides secure, carrier-grade, fully-redundant routing of call processing, signaling, and management messages between the CS 2000 and the other components in the solution (for example, the Media Gateway 15000, the MG 9000, GWCs. (Optionally, the CS LAN can provide a bearer path between components). The CS LAN is fully integrated with the CS 2000, and consists of a dual Passport 8600 router configuration with 10/100 Base-T Ethernet links to components.
CS 2000 - Compact 		The CS 2000 - Compact is a full-featured, small-footprint alternative to the CS 2000, that is designed for new installations. The CS 2000 - Compact performs call processing, messaging, routing, translations, centralized systems delivery, and storage of office images and system data.
CS 2000 - Compact	Call Agent	The Call Agent is the computing engine of CS 2000 - Compact. The Call Agent provides maintenance, call processing, and billing functionality. The Call Agent also sends control messages (for connection set-up) to media gateways (such as the Media Gateway 15000, the Multimedia Terminal Adapter, and MG 9000)
CS 2000 - Compact	STOrage Management (STORM)	STORM provides network file system (NFS) services to applications running in the CS 2000 - Compact. An NFS is a distributed file system that allows applications to access files and directories on remote computers. STORM acts as an NFS server for the clients running on the Call Agent, and the USP - Compact. Each STORM card is attached to a persistent data storage (PDS) device.

Components and their function (Sheet 9 of 22)

Components	Sub-component	Function
Gateways		
Interworking Spectrum Peripheral Module IP (IW SPM-IP) 		The IW SPM-IP is used with the PT-IP solution in the hybrid configuration. The IW SPM-IP provides interworking capability between the IP packet network and TDM access domains. The IW SPM-IP also serves as a bridge for bearer traffic between lines and trunks served by packet gateways, and ENET-based TDM lines and trunks hosted by the same CS 2000. One side of the IW SPM-IP connects to the ENET using DS-512 TDM connections, and the other side connects to the IP packet core network using GigE links. It allows the legacy TDM equipment to access dynamic packet trunks (DPT) and make connections to far-end nodes. In addition, the IW SPM-IP provides MG 9000 lines, and Media Gateway trunks with access to CS 2000 services such as digital recorded announcement module (DRAM)-based announcements, test trunks, and conference circuits that are provided by ISM - or MTM-based peripherals. IW SPM-IP Maintenance functions, such as alarms and logs, are performed through MAPCI on the XA-Core. High density is available with a maximum of 2016 DS0 per shelf/4032 DS0 per frame. This release supports Diffuser QoS and RMON statistics.

Components and their function (Sheet 10 of 22)

Components	Sub-component	Function
Nuera Gateway 		The Nuera ORCA BTX Media Gateway is used in the IAC solution for PacketCable™ compliance. The Nuera Gateway provides interworking between the Packet network and the TDM network. The Nuera Gateway provides the following features: • TGCP call control • SS7 trunk groups for bearer traffic • MF trunk groups for emergency and operator services For additional information about the Nuera Gateway, refer to the following documents. • BTX System Overview • ORCA BTX-Series Software Manual • ORCA Gateway Hardware Manual • *GWC Basics,* NN10189-111 • *GWC Configuration Management,* NN10205-511

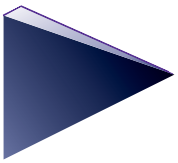
Components and their function (Sheet 11 of 22)

Components	Sub-component	Function
Media Gateway 15000 		Media Gateway 15000 serves as a media gateway in the Succession Network. It supports the ASPEN2.1 and H.248 protocols for communication between the GWCs and Media Gateways. The Media Gateway 15000 supports the following functions: • tone generation on the TDM side of the gateway, such as basic service tones, basic call progress tones, and expanded call progress tones • in-band DTMF digit collection for ISUP and PRI trunk agencies • clear channel data functionality for test trunk capability • modem and fax services over G.721 CODEC • software maintenance and release upgrade • carrier grades attributes, such as NEBS level 3 compliancy, hot swap capability of CP cards, and hot swap capability of VSP cards • T108 test trunk termination • interworking with TDM trunks through IW-SPM-IP • four-port Gigabit Ethernet card • VSP3-0 card • Hitless Software Migration (HSM) • two-port Gigabit Ethernet on the VSP3 card

Components and their function (Sheet 12 of 22)

Components	Sub-component	Function
Media Gateway 7400 		The Media Gateway 7400 is a small scale Media Gateway (compared to the Media Gateway 15000) that can co-exist in a network that contains a Media Gateway 15000. The Media Gateway 7400 does not support Hitless migration, Hot Equipment protection, and VSP3 FP It does support the following functions: • silence suppression • tone generation on the TDM side of the gateway, such as basic service tones, basic and expanded call progress tones • DTMF digit collection for ISUP and PRI trunk agencies • modem and fax services over G.711 CODEC • clear channel data support for test trunk capability • software maintenance and release upgrade support • interworking with TDM trunks through IW-SPM-IP
Succession Media Gateway 9000 (MG 9000) 		MG 9000 is a lines gateway used in the UA-IP solution. MG 9000 terminates subscriber voice and data lines, and switches this traffic internally (if necessary) or transmits the traffic over the packet network. MG 9000 supports several line card types, such as analog subscriber lines for plain old telephone service (POTS), P-Phone, Coin line services, trunking services, and digital subsurface lines (DSL). It also supports up to four XPMs (ESMA/LGCI) through four pairs of Access Bridging Interface (ABI) over DS-512 cards.

Components and their function (Sheet 13 of 22)

Components	Sub-component	Function
Cable Modem Termination System (CMTS)		CMTS is a third-party component used in the IAC solution. CMTS is located at the cable television system head-end, or distribution hub. CMTS provides connectivity to cable modems over the Hybrid Fiber Coax (HFC) access network.
Multimedia Terminal Adapter (MTA) Media Terminal Adapter 		MTA is a third-party component used in the IAC solution. MTA is located at the subscriber's site and is connected to CMTS by means of the HFC access network. MTA is client device that contains a subscriber-side interface that connects to the subscriber's customer premises equipment (CPE). In addition, MTA has a network-side signaling interface connected to call control elements in the network. MTA provides Codecs and all signaling encapsulation functions required for media transport and call signaling.

Components and their function (Sheet 14 of 22)

Components	Sub-component	Function
Network management		
Succession Integrated Element Management System (Integrated EMS)		Integrated EMS is a next-generation element management system (EMS) that provides a single point of data integration and network management for the Carrier VoIP network. At the central office level, Integrated EMS provides the following functions: • Provides graphical topology and inventory relationships between network elements and element management systems • Aggregates all fault and performance data from network elements and element management systems • Provides integrated fault and performance streams to the Network Management Layer • Provides customer choice of operations support system (OSS) interfaces • Provides extensible markup language (XML) aggregation of comma-separated value (CSV) files for performance • Provides centralized fault and performance viewer with filtering capabilities • Provides context-sensitive launching of network management interfaces: • Provides enhanced security features by improving the centralization of authentication, authorization, and administration, while also providing interfaces to external security databases • Supports localization in many languages

Components and their function (Sheet 15 of 22)

Components	Sub-component	Function
Integrated EMS	CS 2000 Core Manager	The CS 2000 Core Manager provides OAM&P functionality for the XA-Core and the subtending TDM components of the CS 2000. It resides on the SuperNode Data Manager (SDM) platform and includes much of the SDM's existing OAM&P functionality. CS 2000 Core Manager also provides access to logs for the MG 9000, GWC, UAS\MS 2010, Media Gateway 15000, SAM21 and XA-Core. In addition, CS 2000 Core Manager provides performance metrics for XA-Core, Preside MDM, and Media Gateway 15000. Lastly, the CS 2000 Core Manager provides access to logs, alarms, and performance monitoring data relating to call processing on the CS 2000 - Compact.
Integrated EMS	Core and Billing Manager	The Core and Billing Manager (CBM) is provides the OAM&P functionality of the CS 2000 Core Manager. It resides two Sun Netra 240 servers housed in the Cabinetized Operations Administration and Maintenance (COAM) cabinet. The CBM supports the following applications: • SuperNode Billing Application (SBA) • Operational Measurement (OM) delivery • Passport log streamer • Operations Systems Support (OSS) applications and communication services

Components and their function (Sheet 16 of 22)

Components	Sub-component	Function
Integrated EMS	CS 2000 Management Tools	CS 2000 Management Tools is a suite of network management tools used in Succession solutions. The CS 2000 Management Tools suite consists of the following network management tools: • GWC Manager • UAS Manager • Audio Provisioning Server (APS) • Audio Provisioning Server (APS) manager • SAM21 Manager • Network Patch Manager (NPM) • Nodes Configuration • Trunks Configuration • Carrier Endpoint Provisioning • Lines Configuration • Trunk Maintenance Manager (TMM) • Line Test Manager (LTM) • Lines Maintenance Manager (LMM) • V5.2 Configuration • V5.2 Maintenance • PM Poller • QoS Collector Application
Integrated EMS	Call Agent Manager	The CS 2000 - Compact Call Agent Manager is a menu driven console application that provides access to SAM21 platform alarms, platform performance monitoring, platform logs, platform connectivity, and platform patching. In addition, Call Agent Manager is the primary interface for platform functions such as a cold switch of activity, routine exercise text, jamming and synchronization of the call processing application.

Components and their function (Sheet 17 of 22)

Components	Sub-component	Function
Integrated EMS	STORage Management Manager (STORM Manager)	STORM Manager is used with CS 2000 - Compact. STORM Manager is a Web-server application that runs on the STORM card. STORM Manager allows you to: • Provision application-level STORM functions • Control application-level STORM functions • Modify STORM file systems • View STORM logs
Integrated EMS	CS 2000 SAM21 Manager	CS 2000 SAM21 Manager is a graphical user interface that provides access to platform OAM&P functions such as platform software load, platform diagnostics, platform upgrade, and Network File System (NFS) mount provisioning. In addition, you would use the CS 2000 SAM21 Manager for provisioning the hardware of a CS 2000 GWC, for fault management of a CS 2000 GWC card, and to upgrade the firmware of a CS 2000 GWC. CS 2000 SAM21 Manager has two components: the element manager server and the element manager client. The CS 2000 SAM21 element manager server resides on the same server that hosts the Succession Server Platform Foundation Software (SSPFS) NCL software package (part of the CS 2000 Management Tools software). Currently, the SSPFS package runs on a Sun Netra t1400 or Netra 240. Note that CS 2000 SAM21 element manager server does not have a graphical user interface (GUI). The CS 2000 SAM21 element manager client runs on either a PC or Sun Solaris machine and provides a GUI of the physical layout of the SAM 21 shelf for fault management and configuration management of the SAM21 shelf.

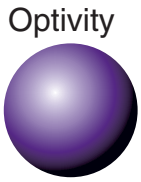
Components and their function (Sheet 18 of 22)

Components	Sub-component	Function
Integrated EMS	CS 2000 GWC Manager	The primary function of the CS 2000 GWC Manager is to coordinate the configuration of the CS 2000 GWCs. In addition, you would use the CS 2000 GWC Manager for fault management of a CS 2000 GWC node.
Integrated EMS	Session Server Manager	The Session Server Manager is a web-based interface residing on the Session Server to perform the provisioning and maintenance activities. This interface consists of a web system running on the Session Server Manager that provides provisioning web pages as well as maintenance related web pages. ***Note:*** The Session Server can be configured to use Integrated EMS between the customer operation LAN and the CS 2000 LAN or it can be configured without Integrated EMS.
Integrated EMS	Trunk Maintenance Manager (TMM)	TMM provides an XML interface that allows you to use client applications (GUIs) to perform basic maintenance operations on GWC-managed trunks, such as posting, busying, and returning to service.
Integrated EMS	Line Maintenance Manager (LMM)	LMM provides an XML interface that allows you to use client applications (GUIs) to perform basic maintenance operations on GWC-managed lines, such as posting, busying, and returning to service. LMM is only available for the IAC solution.

Components and their function (Sheet 19 of 22)

Components	Sub-component	Function
Integrated EMS	Preside Multiservice Data Manager (Preside MDM)	Preside MDM allows you to manage Media Gateway 15000/7400. Preside MDM allows you to perform fault management, configuration management, data collection, performance management, and security management. In addition, Preside MDM forwards Media Gateway 15000/7400 performance management, and fault management information to the CS 2000 Core Manager. Preside MDM resides on a Sun-based workstation.
Integrated EMS	MG 9000 Manager	The Succession Media Gateway 9000 Manager (MG 9000 Mgr) allows technicians to remotely manage all MG 9000 components in a Succession network. The MG 9000 is a client-server application that consists of the following components: • Server software that resides on a central server • Mid-tier database between the client and server for data storage The MG 9000 Mgr supports most common management operations, including the following: • Network element discovery • Equipment provisioning • Carrier provisioning • Service provisioning • Fault handling and reporting • Operational measurements
Integrated EMS	Universal Audio Server Manager (UAS Manager)	UAS Manager allows you to configure the UAS, as well as to monitor fault and performance data for the UAS. You use UAS Manager in conjunction with APS Manager to completely manage the UAS.
Integrated EMS	Audio Provisioning Server Manager	The APS Manager provides a web-based GUI that allows you to manage announcements from any workstation. The APS Manager client runs on a PC.

Components and their function (Sheet 20 of 22)

Components	Sub-component	Function
Integrated EMS	Universal Signaling Point (USP) Manager	USP Manager is a Windows 2000 workstation that provides a GUI for provisioning and monitoring SS7 interfaces. USP Manager also provides backup and software upgrade facilities for the USP.
Integrated EMS	Device Manager (for Passport 8600)	The Device Manager (for Passport 8600) is a suite of GUI applications that allows you to manage and configure a Passport 8600 chassis. It can be launched independently or as part of Optivity.
Optivity 		Optivity is a network management application capable of managing multiple Passport 8600s from a single location.
Centrex IP		
Centrex IP Client Manager		The Centrex IP Client Manager (CICM) product delivers Centrex capabilities to users connected to an IP network using VoIP technology. The CICM performs the following functions: • provides the interface between the Centrex feature set and an IP network • transcodes voice between IP data from the client network and PCM data from the Succession XPM The CICM client allows a user to initiate and receive VoIP calls and to receive Centrex features from the CS 2000. • the m6360 SoftClient application • the Nortel Networks i200x Etherset telephones For more information on CICM, refer to *CICM Basics,* NN10044-111.

Components and their function (Sheet 21 of 22)

Components	Sub-component	Function
Remote access support		
Contivity 600 Contivity 600 		The Contivity 600 VPN Switch enables secure IP connections from a location outside the customers network to provide solution support remotely. The Contivity Extranet Switch provides authentication, authorization, encryption, and routing for connecting to components from outside the customers network. It can provide up to 30 simultaneous, authorized connections.

Components and their function (Sheet 22 of 22)

Components	Sub-component	Function
Integrated Services Module (ISM)		
Integrated Services Module (ISM)		In new installations (greenfield), you have the option of using the ISM. ISM is a specialized module designed to accommodate test and service circuit packs that are used in switch and facility maintenance. In a CS 2000 configuration, ISM houses Input/Output Modules (IOMs). IOMs provide ports for serial input and output, enabling local and remote devices to communicated with the rest of CS 2000 IOMs through the CS 2000 message switch. IOMs support data links that you can use to bring the CS 2000 Core Manager or the CS 2000 into services. Each card supports up to 16 ports for 64 Kb/s synchronous V.35 links or 28.8 Kb/s asynchronous RS232 links.
Office alarm unit (OAU)		In new installations (greenfield), you have the option of using the OAU. OAU is used to connect a CS 2000 with the office alarm system to provide notification of physical or electrical problems. OAU comprises two main types of functional elements: • Scan points and monitoring devices for collecting environmental input (for example, temperature levels) and detecting state changes in peripheral equipment. • Output devices such as signal distribution points (SDPs) that provide collected information for inclusion in logs and displays, and to activate audible alarms when required. OAU is a single-shelf peripheral that is housed in an integrated services module (ISM) cabinet. OAU is directly connected to the Enhanced Network (ENET). ENET is in turn connected to the message switch, which facilitates communication between the OAU and the XA-Core

Call processing for IP

This section discusses the call processing operations that are common to all IP solutions. The topics covered in this section are

- the SIP-T protocol for set up and take down of dynamic packet trunks between Succession switches
- the ASPEN and H.248 protocols for messaging between GWCs and gateways
- the H.248 protocol between GWCs and the UAS for announcement control

IP call processing with SIP-T

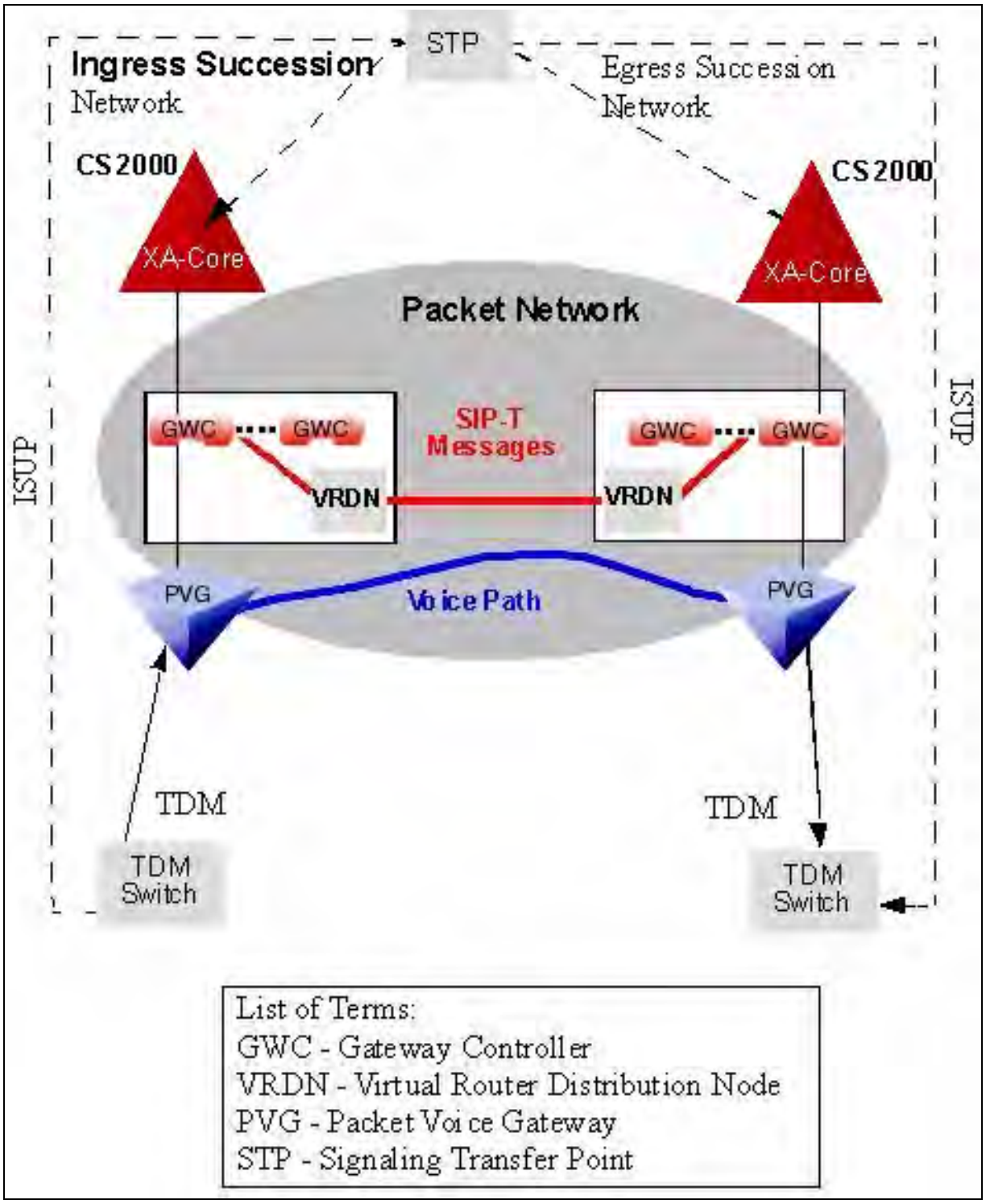
SIP-T introduces the following concepts to Succession Call Processing:

- Dynamic Packet Trunks (DPTs). Represent a bearer path connection across a packet network. DPTs allow connections to other Succession Network nodes over a packet network.
- SIP-T signaling. SIP-T supports PSTN signaling transparency by encapsulating ISUP messages within SIP methods.

SIP-T supports PSTN signaling transparency by encapsulating ISUP messages within SIP methods. During call setup, the Ingress GWC sends bearer path information in a SIP-T message to the Egress GWC. Once the Egress Succession Network receives the appropriate SIP-T message, the Egress Succession Network can use the information in the SIP-T message to establish a bearer path across the packet network.

For the Succession Network, SIP-T works between GWCs in order to bridge the PSTN networks with the packets networks as shown in the figure SIP-T message path and voice path.

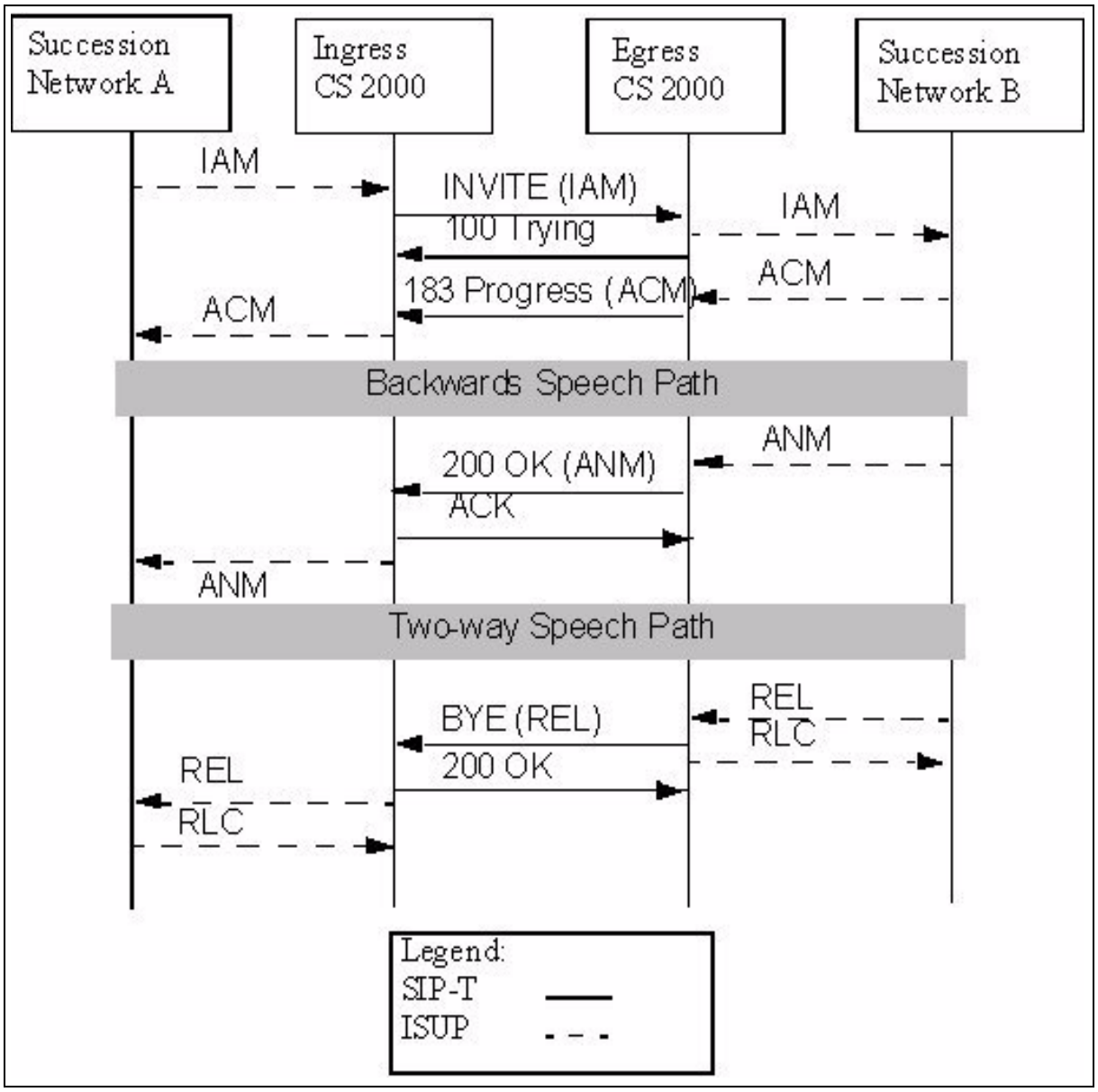
SIP-T message path and voice path



Note: The Virtual Router Distribution Node (VRDN) provides a single IP Address for remote Media Gateway Controllers (MGCs) to communicate with the host MGC. The VRDN distributes the calls over the available SIP-T GWCs. It also distributes the SIP-T messages from the GWC to the appropriate MGCs.

SIP-T has been extended with application/ISUP version for several variants of ISUP as illustrated in Figure ISUP and SIP-T messaging. The use of ISUP encapsulation allows ISUP signalling messages to be tunneled between GWCs. Version control is used in the SIP-T to allow for differentiation between different ISUP variants. This enables the terminating GWC to recognize and parse the messages correctly, or reject the message if the ISUP variant is not supported.

ISUP and SIP-T messaging



IXC services with SIP-T

The following inter-exchange carrier (IXC) services can be used with SIP-T trunks in both a DMS-100/200 to DMS-250 CS 2000 configuration and a DMS-500 CS 2000 configuration:

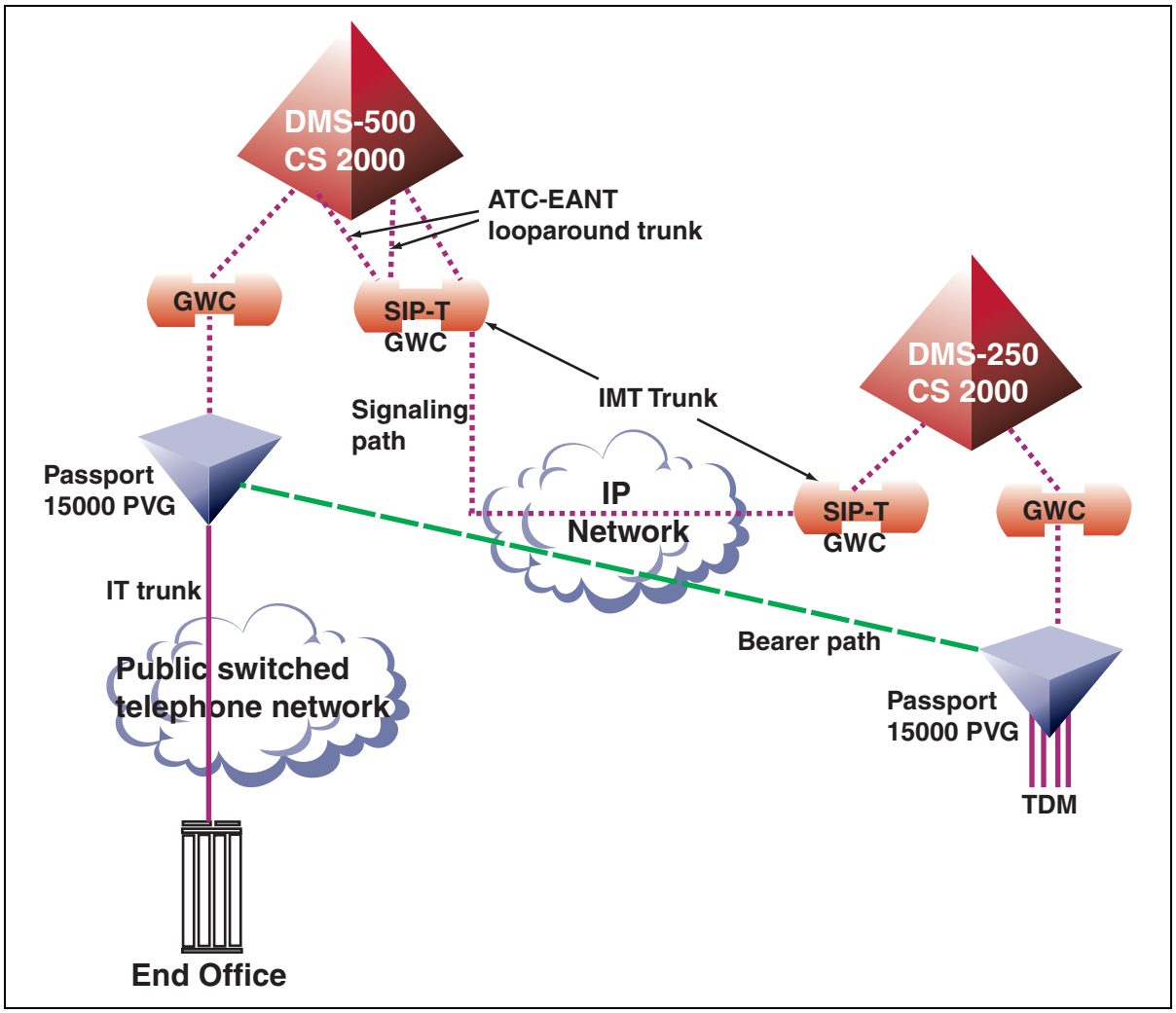
- Mechanized Calling Card Services (MCCS)
- Reorigination
- Auth Codes/PIN Codes/Account Codes

- Network Route Advance
- FGD (Feature Group D) Cut-through, Transitional, and Universal Access Dialing

Internal SIP-T looparound trunks can be used in a DMS-500 CS 2000 configuration. A Virtual Router Distribution Node (VRDN) GWC is also required for SIP-T loopparounds. Internal SIP-T looparound trunks provide the same capabilities as traditional DMS-500 looparound trunks without requiring physical trunks. The only hardware needed for internal SIP-T looparound trunks is a SIP-T Gateway Controller (GWC).

Figure DMS-500 CS 2000 SIP-T with looparound trunks shows one example of the signaling and bearer paths for a call that routes through a DMS-500 CS 2000 to a DMS-250 CS 2000 by means of a SIP-T GWC.

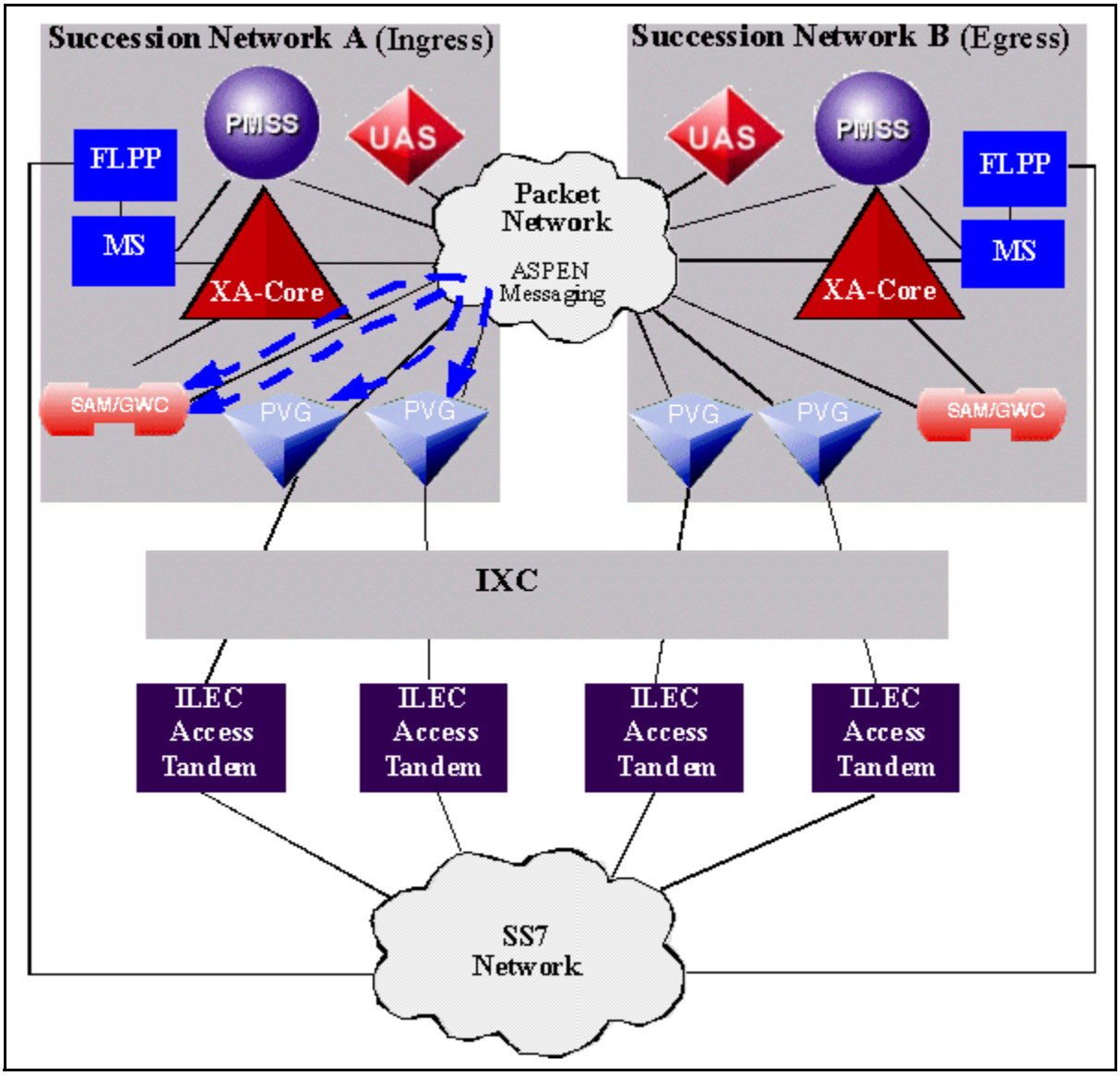
DMS-500 CS 2000 SIP-T with looparound trunks



IP call processing with ASPEN

ASPEN is the interface protocol that is used between GWCs and the Media Gateway 15000 or Media Gateway 7400. This protocol is based on the IETF MGCP protocol and architecture with extensions made to suit needs discovered by Nortel Networks. The figure ASPEN message flow shows the ASPEN message flow.

ASPEN message flow



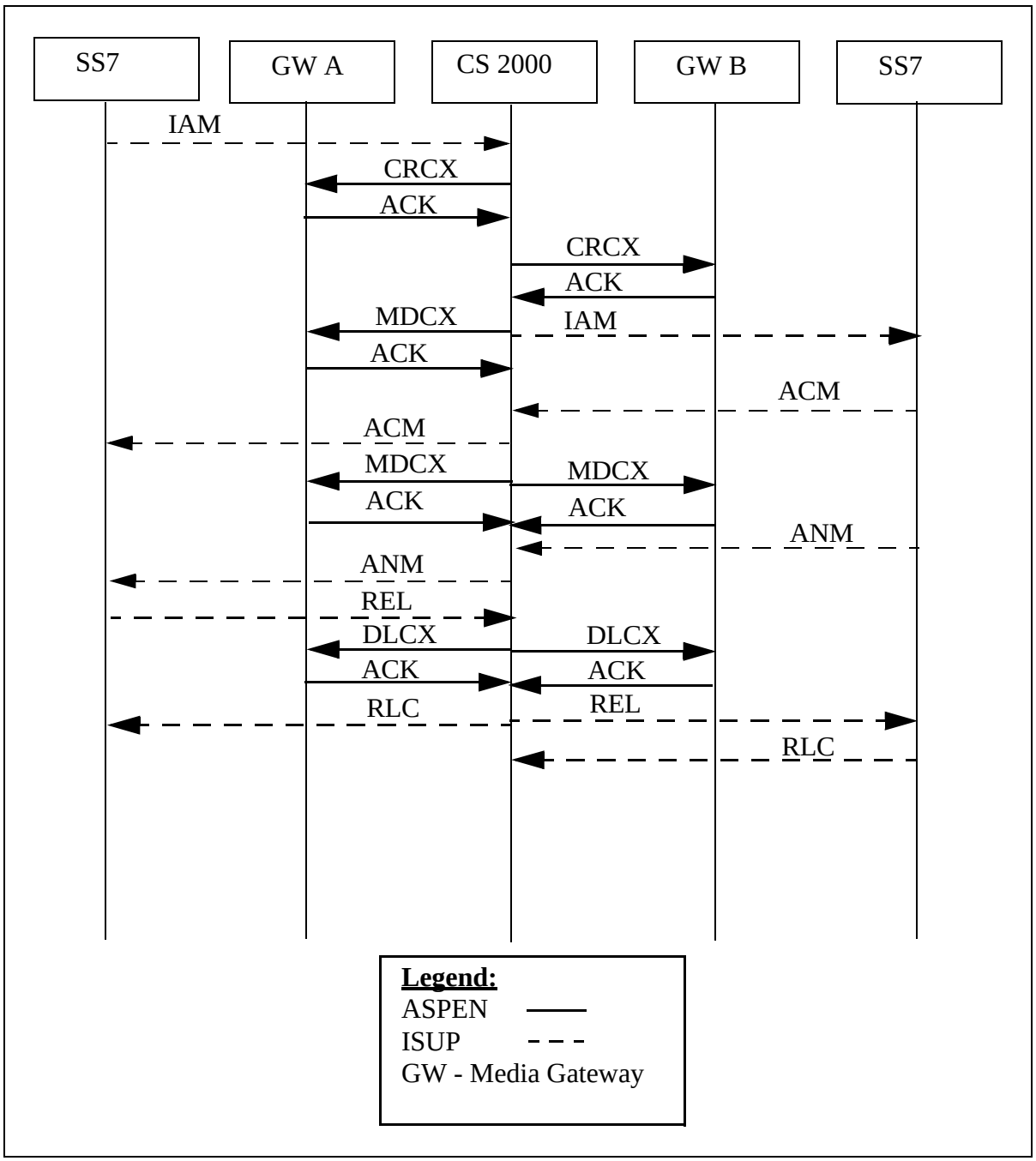
ASPEN messages are transmitted over User Datagram Protocol (UDP) across the packet network. The port number for the GWC and the controlled Media Gateway 15000/7400s should be set up by means of provisioning on both components. Since UDP is subject to losses, all commands are assigned timers and will be repeated if the timers expire. Also, all connection commands are sent sequentially for a given endpoint by the GWC to guarantee that order is preserved and to minimize race conditions. To further minimize delay and loss, all commands are limited in length to the current IPv4 Ethernet byte limit of 1440 bytes.

For control of basic connections, ASPEN provides the following commands:

- CreateConnection (CRCX) - requests the establishment of a connection.
- ModifyConnection (MDCX) - requests modification of a previously established connection.
- DeleteConnection (DLCX) - requests deletion of one or more connections (from GWC).

The response to these commands is always an Ack message that provides the result of processing the command. The figure ASPEN Messaging (the CRCX is being sent to the incoming GWC first) shows an example of ASPEN messaging during a call where the CRCX is being sent to the incoming GWC first.

ASPEN Messaging (the CRCX is being sent to the incoming GWC first)

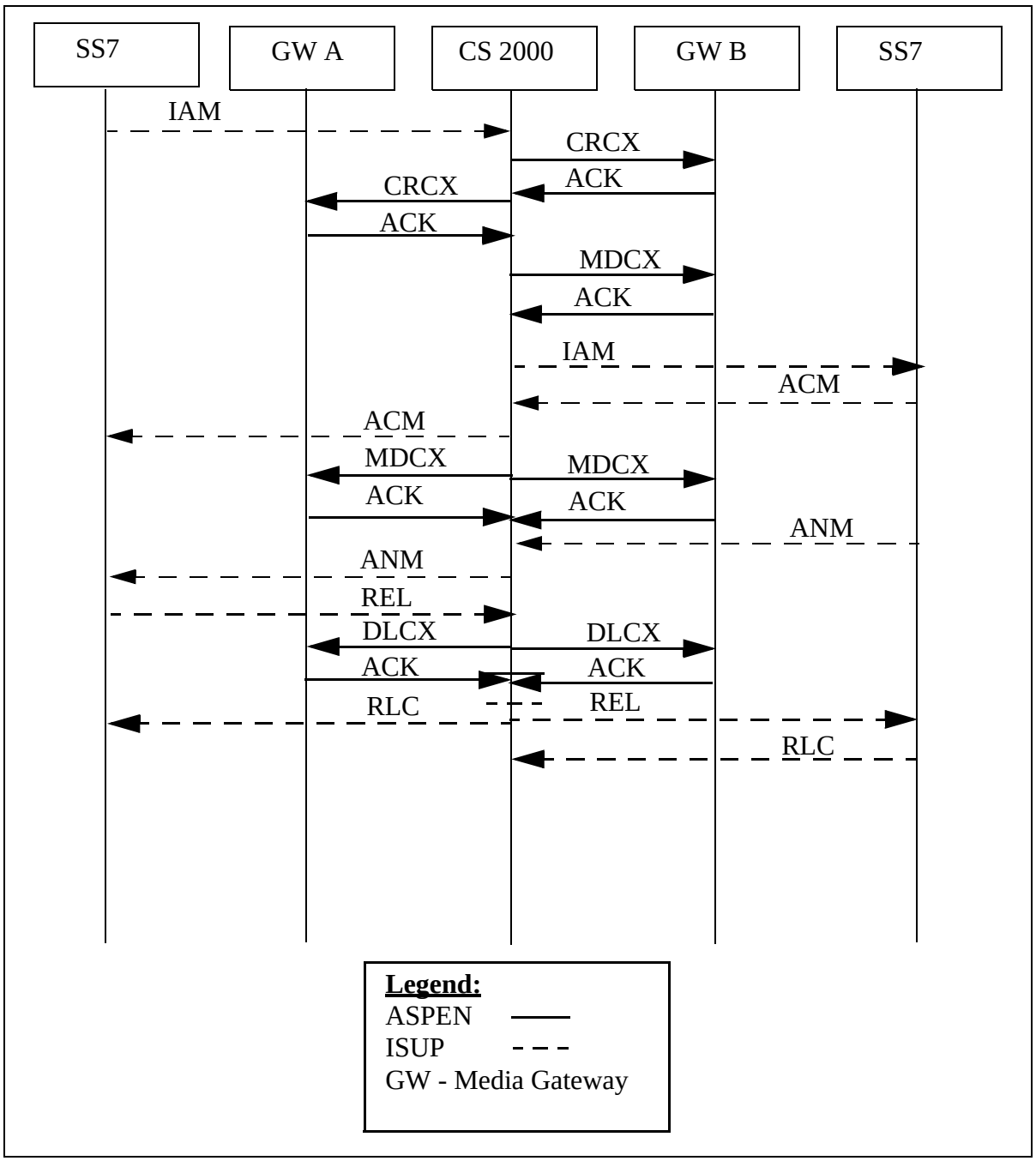


The above call flow is an example of an ASPEN flow with the CRCX being sent to the incoming media gateway first. The determination of which end of the connection gets the first CRCX is based on the media gateway node pair and the endpoint type. Most endpoints (including the trunk ASPEN endpoints) do not have a preference and the

determination is based on a fixed relationship between the two media gateways involved in the call. One media gateway in each media gateway pair will always get the first CRCX for every connection between those two media gateways. The media gateway node pair relationships are setup such that a specific media gateway will always get the first CRCX when connecting to half the other media gateways in the office and the second CRCX when connecting to the other half of the media gateways in the office. This relationship between the media gateways is setup to improve the caching efficiency of connection oriented bearer paths and balance the messaging and work load across each media gateway in the office.

The CS 2000, therefore, does not always send the first CRCX to the originator. For a basic call between two media gateways it is equally likely that it will send the first CRCX to the terminator. The figure ASPEN Messaging (the terminator gets the first CRCX) shows an example of ASPEN messaging during a call where the terminator gets the first CRCX.

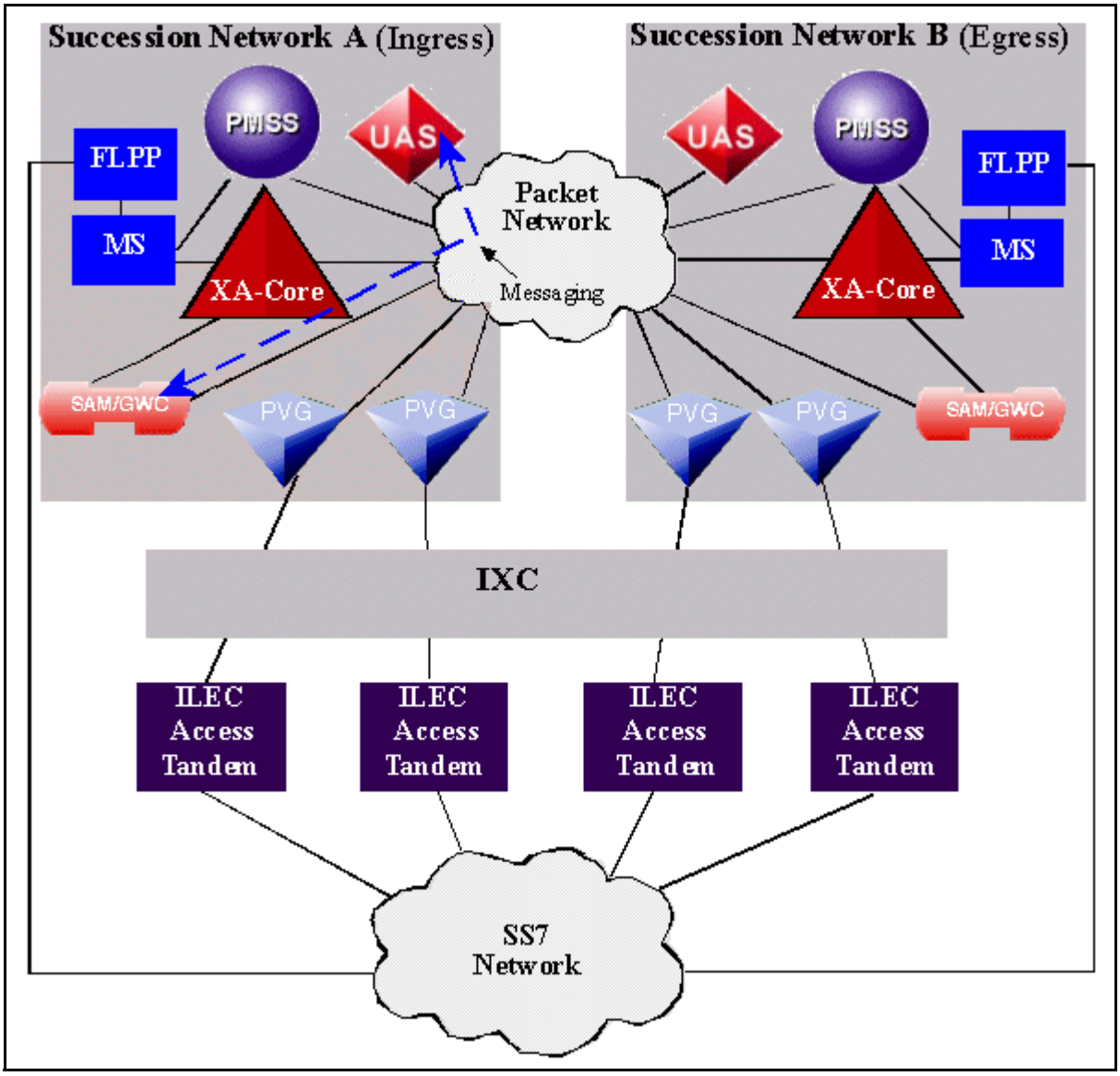
ASPEN Messaging (the terminator gets the first CRCX)



IP call processing with H.248

The interface protocol used between GWCs and UAS for announcements is H.248. The figure H.248 message flow shows the H.248 message flow.

H.248 message flow

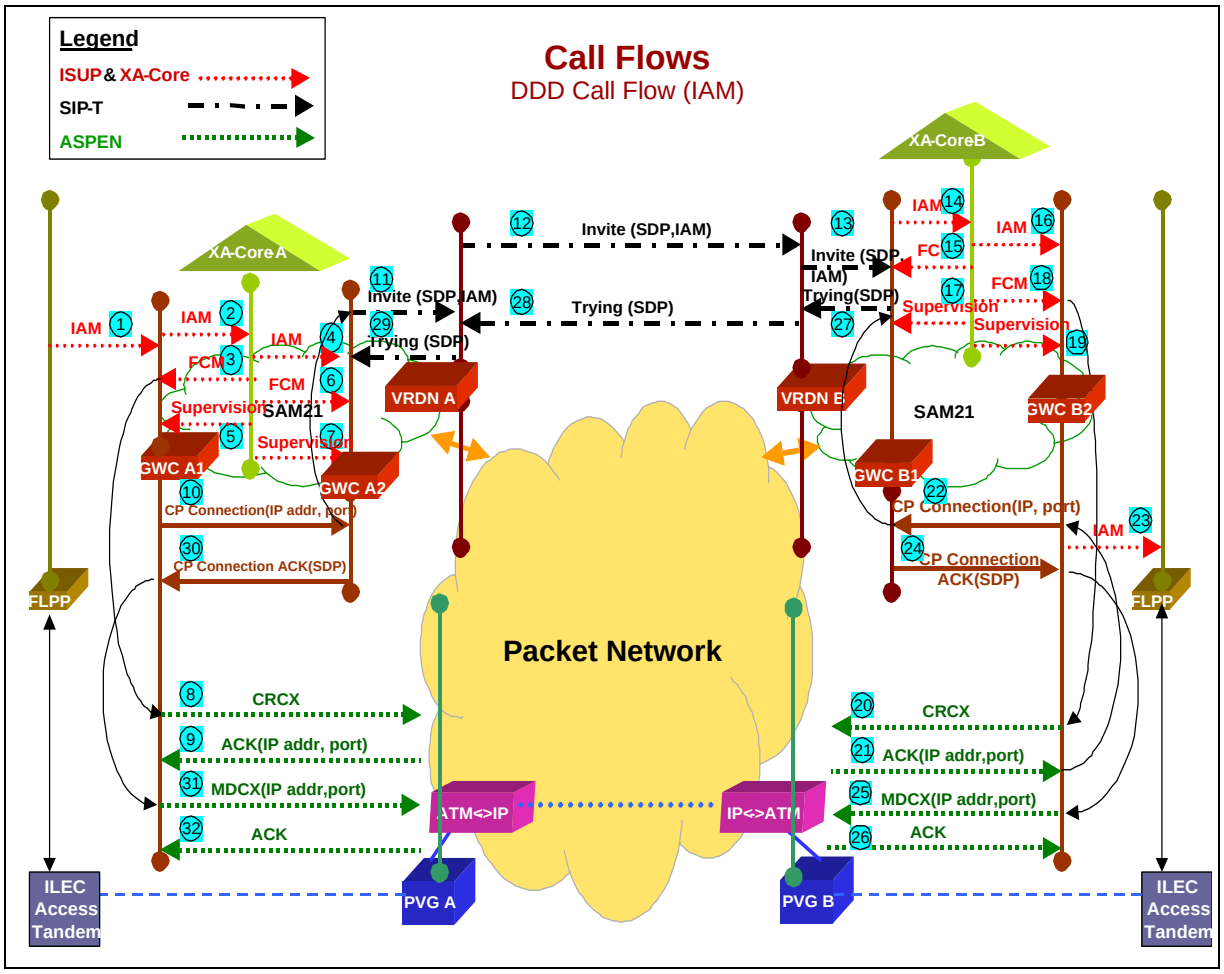


The UAS sends a response to each message it receives from the GWC. The response may indicate the result of processing the command.

IP call setup of basic direct distance dialing

The figure Basic DDD call flow (IAM) shows the call setup of a basic direct distance dialing (DDD) call flow. DDD calls consist of calls between two Succession switches. Following the illustration is a detailed, step-by-step description of the call flow.

Basic DDD call flow (IAM)



1. The originating end office sends an IAM message over the SS7 network to an FLPP at the ingress Succession Network. Based upon data from table C7TRKMEM, the FLPP maps the CIC of the IAM to the corresponding DS0 circuit on PVG-A and forwards the IAM message to the GWC controlling PVG-A, which is GWC-A1.

   Note 1: If the call terminates to an SS7 FGD trunk that is datafilled with the IMTFGD option, the CS 2000 creates a Generic Digits (GD) parameter and attaches it to the outgoing SS7 IAM message. The access information consists of the switch ID of the CS 2000 (obtained from the ORIG_SWITCH_ID parameter in Table OFCVAR) and the originating trunk group number (obtained from the ADNUM field in Table CLLI).

   Note 2: In a Centralized Translations Control (CTC) environment, all call originations that do not contain routing information are sent from the CS 2000 to CTC to request

translations of the dialed digits. The CS 2000 uses the routing label returned by CTC to identify the route for completing the call. Translation information is sent to the next Call Server through the GD parameter in the IAM message.

2. GWC A1 passes the IAM to XA-Core-A. The XA-Core-A translates and routes the call using routing tables. As a result of translations, a route list is identified that contains a single DPT trunk group. (Note: DPTs are provision in the translation tables in the same manner as existing TDM trunks).
3. A Fabric Control Message (FCM) is sent to GWC-A1 to create the originating half call to the TDM trunk.
4. Since DPTs have trunk members like TDM trunks, XA-Core-A checks to see if an idle DPT trunk member is available. If so, XA-Core-A constructs the outgoing IAM message and sends it to GWC-A2.

   Note: Until an Answer Message (ANM or ANSWER) is received, the voice path between GWC-A1 and GWC-A2 is active in the receive direction and inactive in the transmit direction.

5. An ISUP supervision message is sent to the GWC-A1 to instruct it on how the originating half call should behave.
6. An FCM is sent to GWC-A2 to create the terminating half call to the DPT.
7. An ISUP supervision message is sent to GWC-A2 to instruct it on how the terminating half call should behave.
8. Once GWC-A1 receives FCM from XA-Core-A, GWC-A1 sends an ASPEN create connection (CRCX) request to PVG-A to establish a bearer connection across the packet network.
9. PVG-A sends an ASPEN acknowledgement (ACK) message back to the GWC-A1 to acknowledge receipt of the CRCX message.
10. When GWC-A1 receives the ACK message, GWC-A1 sends a CP Connection message to GWC-A2 to inform GWC-A2 to initiate a connection from one Succession Network to another Succession Network.
11. GWC-A2 populates the SIP-T Invite message with the Session Descriptor Protocol (SDP) and envelopes the ISUP IAM inside the Invite message and forwards it to the Virtual Router Distribution Node (VRDN) A. The SDP contains information, such as the requested CODEC standard, for this call.

12. VRDN-A translates the routing information of the egress Succession Network, within the SIP-T Invite message, to an IP address, so that the SIP-T Invite message is routed to the correct egress Succession Network. VRDN-B receives the SIP-T Invite message.
13. VRDN-B identifies the SIP-T Invite message being routed, then selects a SIP-T GWC (GWC-B1) to handle the incoming SIP-T call.
14. GWC-B1 extracts the IAM from the SIP-T Invite message and forwards it to XA-Core-B on an idle DPT associated with GWC-B1. XA-Core-B receives the IAM and initiates the call. The information in the IAM is used to translate and route the call.

    Note: Until an Answer Message (ANM or ANSWER) is received, the voice path between GWC-A2 and GWC-B1 is active in the receive direction and inactive in the transmit direction.

15. XA-Core-B sends a FCM to GWC-B1 to establish originating half call to the DPT.
16. As a result of translations on XA-Core-B, a route list is identified which contains a single TDM trunk group. The TDM voice circuit is seized and the IAM is routed out the FLPP through GWC-B2.
17. An ISUP supervision message is sent to GWC-B1 to instruct it on how the originating half call should behave.
18. XA-Core-B sends an FCM to GWC-B2 to establish the terminating half call to the TDM trunk.

    Note: Until an Answer Message (ANM or ANSWER) is received, the voice path between GWC-B1 and GWC-B2 is active in the receive direction and inactive in the transmit direction.

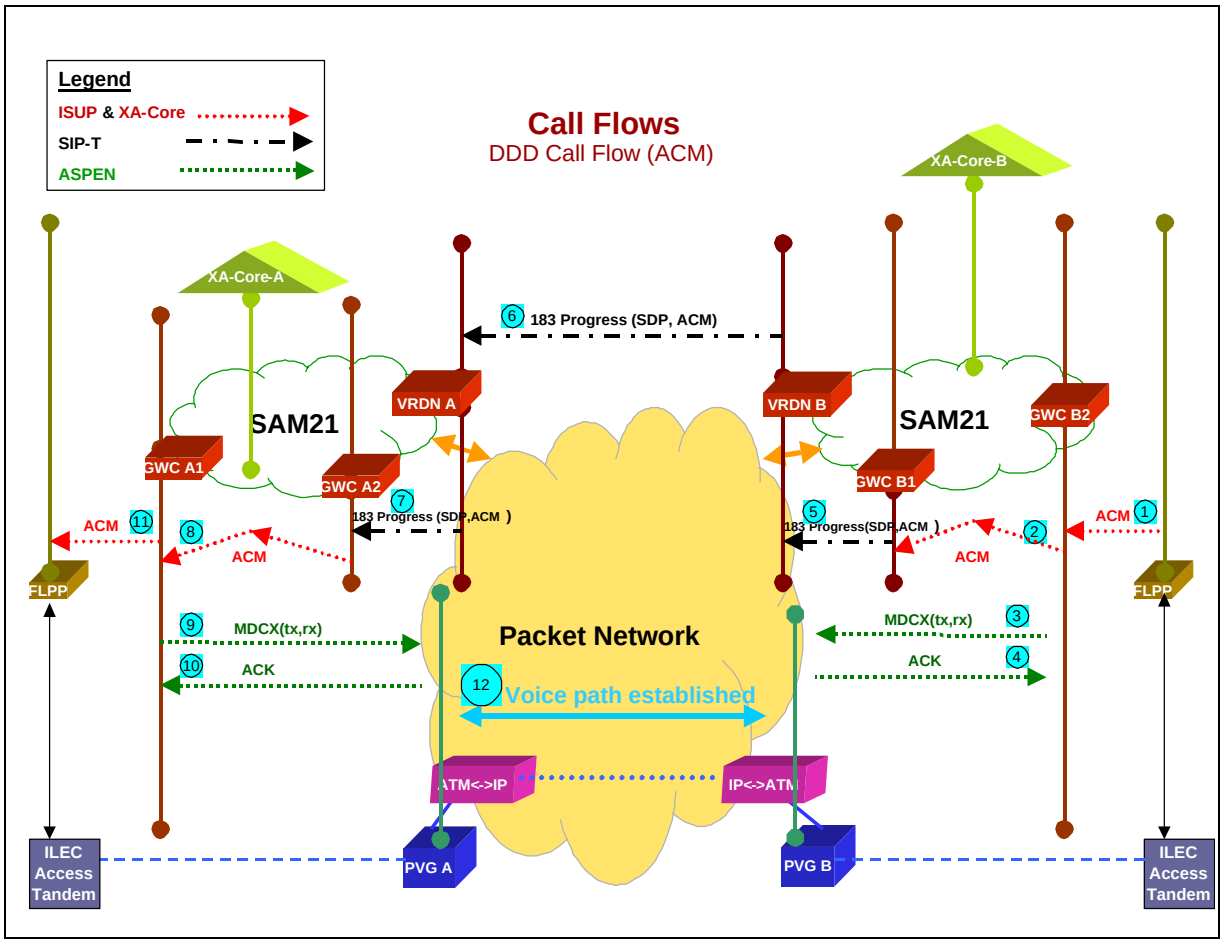
19. An ISUP supervision message is sent to the GWC-B2 to instruct it on how the terminating half call should behave.
20. Once GWC-B2 receives the FCM from XA-Core-B, GWC-B2 will send a create connection (CRCX) request to PVG-B to establish a bearer connection across the packet network.
21. PVG-B sends an acknowledgement (ACK) message back to GWC-B2 to acknowledge receipt of the CRCX message.
22. When GWC-B2 receives the ACK message, GWC-B2 sends a CP Connection message to GWC-B1 to inform GWC-B1 to initiate a connection from one Succession Network to another Succession Network.

23. GWC- B2 forwards the ISUP IAM to the FLPP to be transported to the PSTN.
24. When the GWC-B1 receives the CP Connection message from GWC-B2, GWC-B1 responds with a CP Connection Acknowledge (ACK) message containing the SDP.
25. When the GWC-B2 receives the CP Connection ACK message, GWC-B2 sends a ASPEN modify connection (MDCX) message to modify the packet connection.
26. When PVG-B receives the ASPEN MDCX message, PVG-B responds with an ASPEN ACK message.
27. After GWC-B1 receives the CP Connection message, GWC-B1 sends a SIP-T Trying message containing the SDP to VRDN-B. The SDP contains the code information.
28. VRDN-B translates the routing information of the ingress Succession Network, within the SIP-T Trying message, to an IP address, so the SIP-T Trying message is routed to the correct ingress Succession Network. VRDN-A receives the SIP-T Trying message.
29. VRDN-A identifies the SIP-T Trying message to route to GWC-A2 and routes the SIP-T Trying message to GWC-A2.
30. When GWC-A2 receives the SIP-T Trying message, GWC-A2 sends a CP Connection ACK message to GWC-A1, informing GWC-A1 that a voice path connection is established across the packet network. The CP Connection ACK message contains the SDP from the egress Succession Network.
31. GWC-A1 sends an ASPEN modify connection (MDCX) message to PVG-A.
32. PVG-A responds to the MDCX to GWC-A1 with an ASPEN ACK message.

IP Address Complete Message (Ringing) stage of a DDD call flow

The figure Basic DDD call flow (ACM) shows the address complete (ringing) stage of a basic DDD call flow. Following the illustration is a detailed, step-by-step description of the call flow.

Basic DDD call flow (ACM)



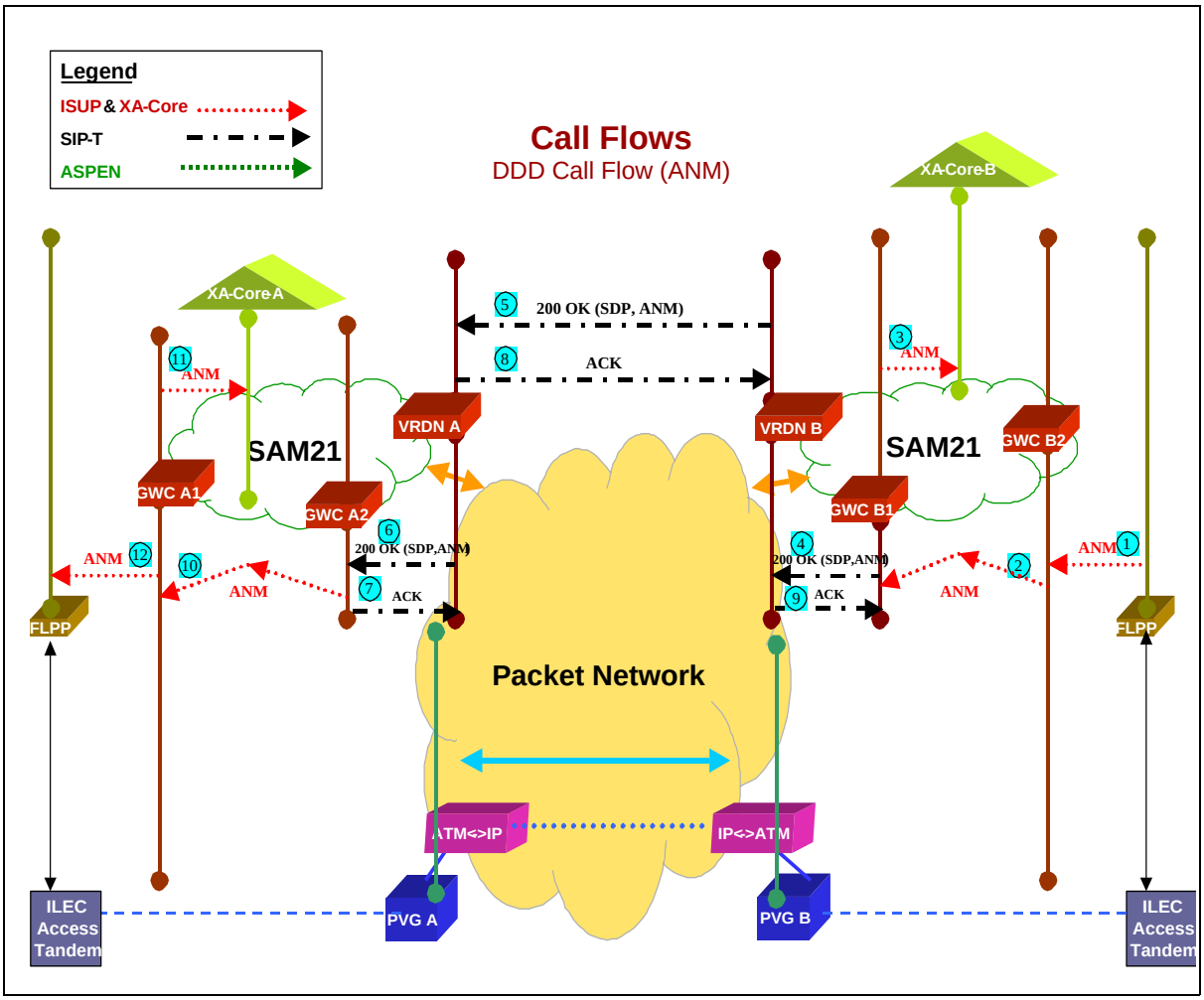
1. The terminating PSTN located on the egress Succession Network sends an ISUP ACM through the SS7 network. The FLPP located in the egress Succession Network forwards the ACM message to GWC-B2.
2. GWC-B2 forwards the ACM through the XA-Core to GWC-B1.
3. GWC-B2 sends an ASPEN modify connection (MDCX) message to PVG-B.
4. PVG-B responds to the ASPEN MDCX with an ASPEN ACK message to GWC-B2.
5. When GWC-B1 receives the ACM message, GWC-B1 populates the SIP-T 183 Progress message with the SDP and envelops the ISUP ACM inside the 183 Progress message and forwards it to VRDN-B. The SDP contains information, such as the CODEC standard for this call.

6. VRDN-B translates the routing information of the ingress Succession Network, within the SIP-T 183 Progress message, to an IP address, so the SIP-T Invite message is routed to the correct ingress Succession Network. VRDN-A receives the SIP-T 183 Progress message.
7. VRDN-A identifies the SIP-T 183 Progress message to route to GWC-A2.
8. GWC-A2 extracts the ACM from the SIP-T 183 Progress message and forwards it through XA-Core-A to GWC-A1.
9. When GWC-A1 receives the ISUP ACM, GWC-A1 sends an ASPEN modify connection (MDCX) to PVG-A.
10. PVG-A acknowledges the MGCX message by sending an acknowledge (ACK) message to GWC-A1.
11. GWC-A1 forwards the ISUP ACM to the FLPP to be sent on the SS7 network to the originating PSTN.

IP answer message stage of a DDD call flow

The figure Basic DDD call flow (ANM) shows the answer of a basic DDD call flow. Following the illustration is a detailed, step-by-step description of the call flow.

Basic DDD call flow (ANM)



1. The terminating PSTN located on the egress Succession Network sends an ISUP ANM through the SS7 network. The FLPP located in the egress Succession Network forwards the ANM message to GWC-B2.
2. GWC-B2 forwards the ANM through the XA-Core to GWC-B1.
3. GWC-B1 reports the ANM to XA-Core-B so that billing information can begin recording.
4. When GWC-B1 receives the ANM. GWC-B1 populates the SIP-T 200 OK message with the SDP and envelopes the ISUP ANM inside the 200 OK message, then forwards it to VRDN-B. The SDP contains information, such as the CODEC standard for this call.
5. VRDN-B translates the routing information of the ingress Succession Network, within the SIP-T 200 OK message, to an IP address, so the SIP-T 200 OK message is routed to the correct

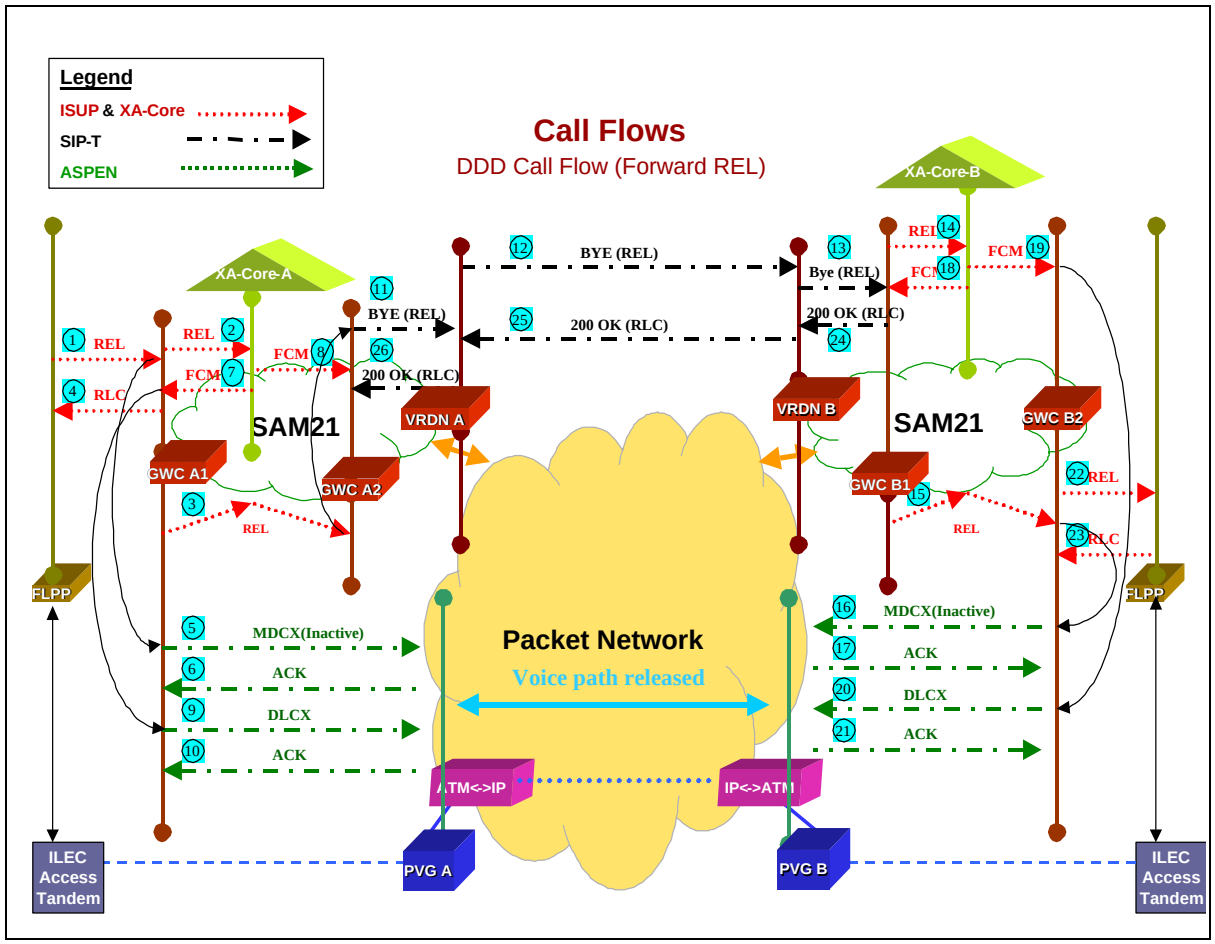
ingress Succession Network. VRDN-A receives the SIP-T 200 OK message.

6. VRDN-A identifies the SIP-T 200 OK message to route to GWC-A2.
7. GWC-A2 responds to the SIP-T 200 OK message by sending a SIP-T acknowledge to VRDN-A to be sent to the egress Succession Network.
8. VRDN-A translates the routing information of the egress Succession Network, within the SIP-T ACK message, to an IP address so the SIP-T ACK message is routed to the correct egress Succession Network. VRDN-B receives the SIP-T ACK message.
9. VRDN-B identifies the SIP-T ACK message to route to GWC-B1.
10. When GWC-A2 receives the ANM message, GWC-A2 extracts the ANM from the SIP-T 200 OK message and forwards it through XA-Core-A to GWC-A1.
11. GWC-A1 reports the ANM to XA-Core-A so billing information can be recorded.
12. GWC-A1 forwards the ISUP ANM to the FLPP to be sent on the SS7 network to the originating PSTN.

IP forward release message stage of a DDD call flow

The figure Basic DDD call flow (REL) shows the answer of a basic DDD call flow. Following the illustration is a detailed, step-by-step description of the call flow.

Basic DDD call flow (REL)



1. The originating end office sends a REL message over the SS7 network to an FLPP at ingress Succession Network. Based upon data from table C7TRKMEM, the FLPP maps the CIC of the REL to the corresponding DS0 circuit on PVG-A and forwards the REL message to the GWC controlling PVG-A, which is GWC-A1.
2. GWC-A1 passes the REL to XA-Core-A. XA-Core-A records billing information in the billing records.
3. GWC-A1 forwards the REL to GWC-A2 through XA-Core-A.
4. GWC-A1 sends an ISUP RLC message to the FLPP to be sent to the originating PSTN through the SS7 network.
5. GWC-A1 sends an ASPEN modify connection (MDCX) message to PVG-A.
6. PVG-A responds to the MDCX through GWC-A1 with an ASPEN ACK message.

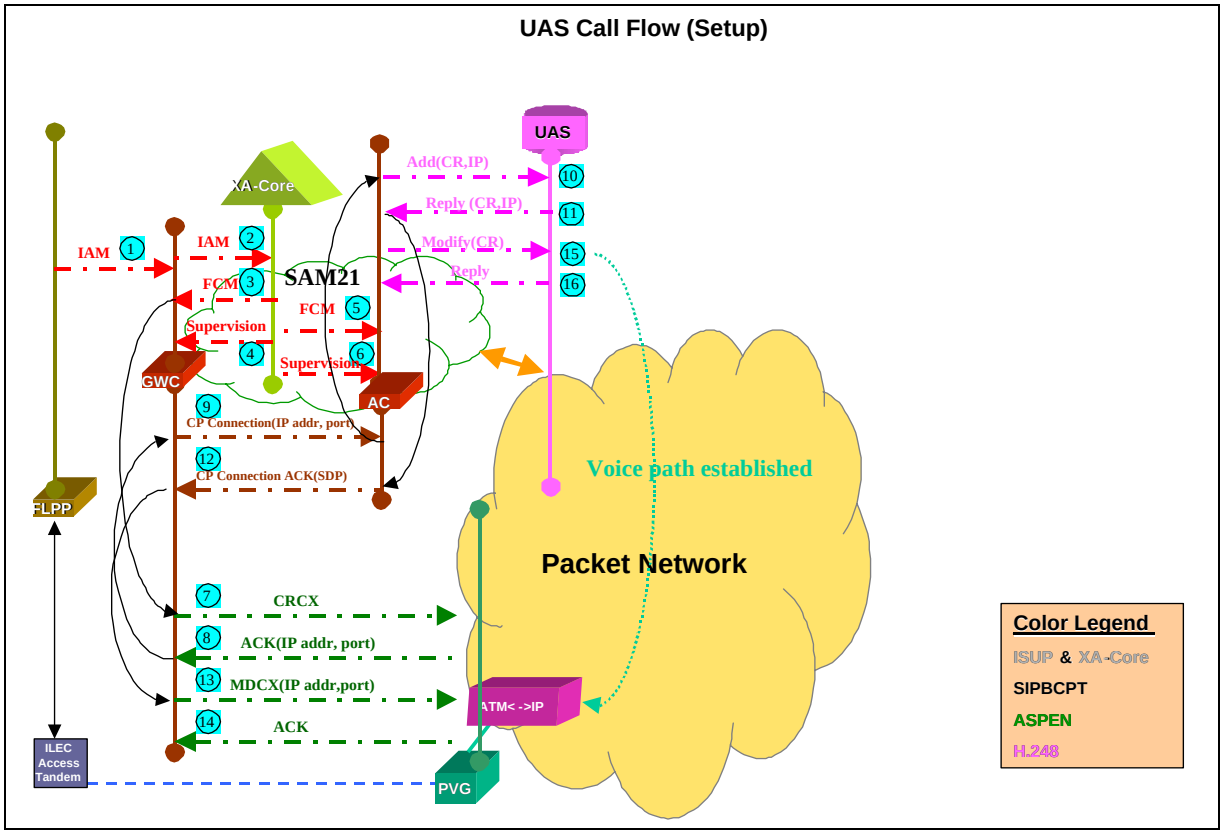
7. A Fabric Control Message (FCM) is sent to GWC-A1 to release the originating half call to the TDM trunk.
8. An FCM is sent to GWC-A2 to release the terminating half call to the DPT.
9. When GWC-A1 receives the FCM message, GWC-A1 sends an ASPEN delete connection (DLCX) message to PVG-A.
10. PVG-A responds to the DLCX through GWC-A1 with an ASPEN ACK message.
11. GWC-A2 populates the SIP-T BYE message and envelopes the ISUP REL inside the BYE message, then forwards it to VRDN-A.
12. VRDN-A translates the routing information of the egress Succession Network, within the SIP-T BYE message, to an IP address, so the SIP-T BYE message is routed to the correct egress Succession Network. VRDN-B receives the SIP-T BYE message.
13. VRDN-B identifies the SIP-T BYE message to route to GWC-B1.
14. GWC-B1 extracts the REL from the SIP-T BYE message and forwards it to XA-Core-B for the DPT associated with GWC-B1. XA-Core-B receives the REL to release the call.
15. GWC-B1 forwards the REL to GWC-B2 through XA-Core-B.
16. GWC-B2 sends an ASPEN modify connection (MDCX) message to PVG-B.
17. PVG-B responds to the MDCX through GWC-B2 with an ASPEN ACK message.
18. XA-Core-B sends an FCM to GWC-A1 to release the originating half call to the DPT.
19. XA-Core-B sends an FCM to GWC-B2 to release the terminating half call to the TDM trunk.
20. When GWC-B2 receives the FCM message, GWC-B2 sends an ASPEN delete connection (DLCX) message to PVG-B.
21. PVG-B responds to the DLCX through GWC-B2 with an ASPEN ACK message.
22. When GWC-B2 receives the ISUP REL message from GWC-B1, GWC-B2 forwards the ISUP REL to the FLPP to be transported to the PSTN.
23. When the PSTN receives the ISUP REL message, the PSTN acknowledges the REL message by sending an ISUP RLC.
24. After GWC-B1 receives the FCM message from XA-Core-B, GWC-B1 sends a SIP-T 200 OK message, containing the ISUP RLC, to VRDN-B.

25. VRDN-B translates the routing information of the ingress Succession Network, within the SIP-T 200 OK message, to an IP address, so the SIP-T 200 OK message is routed to the correct ingress Succession Network. VRDN-A receives the SIP-T 200 OK message.
26. VRDN-A identifies the SIP-T 200 OK message to route to GWC-A2 and routes the SIP-T 200 OK message to GWC-A2.

IP Universal Audio Server call flow (Setup)

The figure Universal Audio Server (UAS) call flow (Setup) shows the setup of a UAS call flow.

Universal Audio Server (UAS) call flow (Setup)



1. The originating end office sends an IAM message over the SS7 network to an FLPP at the ingress Succession Network. Based upon data from table C7TRKMEM, the FLPP maps the CIC of the IAM to the corresponding DS0 circuit on the PVG and forwards the IAM message to the controlling GWC.
2. The GWC passes the IAM to XA-Core which translates and routes the call using routing tables. As a result of translations, a route list is identified that contains an Announcement member. (Note:

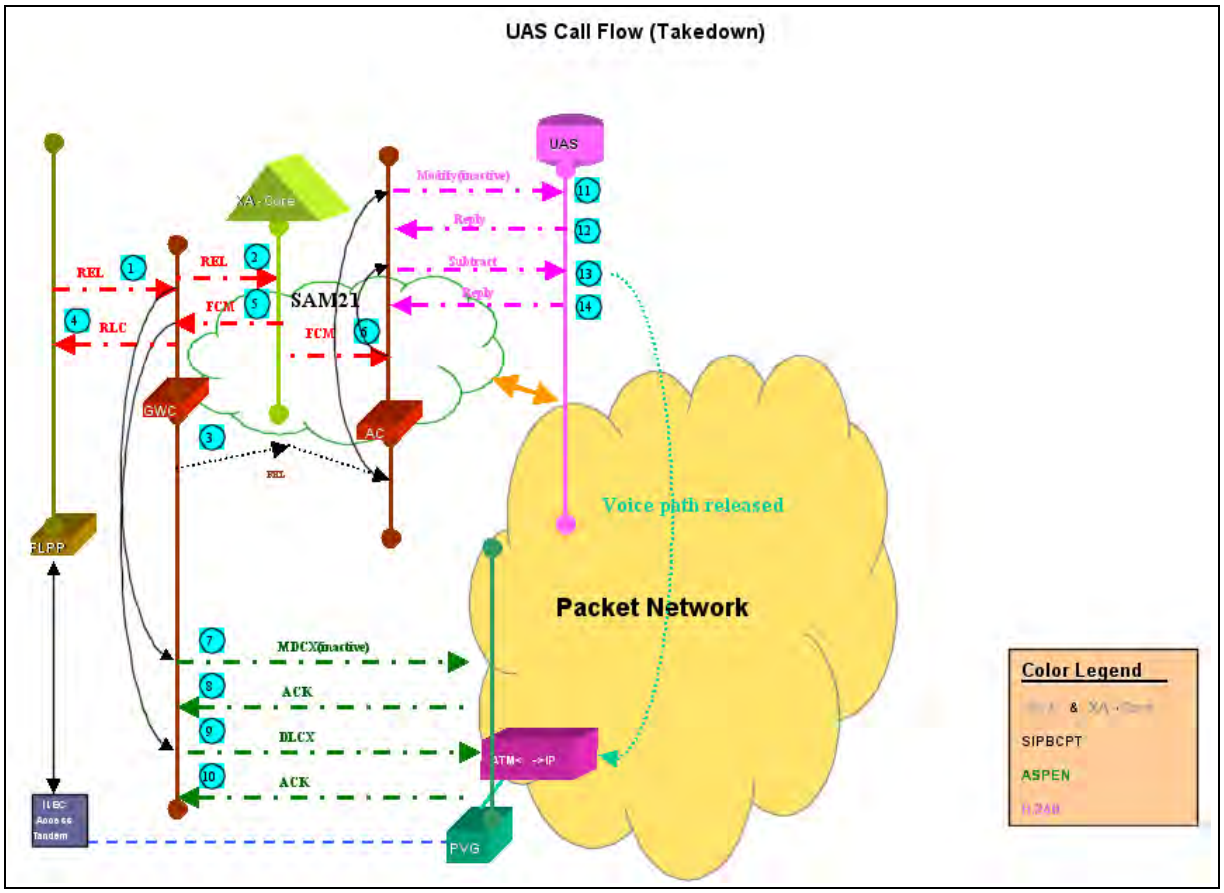
Announcements are provision in the translation tables in the same manner as existing TDM Announcements).

3. A Fabric Control Message (FCM) is sent to the GWC to create the originating half call to the TDM trunk.
4. An ISUP supervision message is sent to the GWC to instruct it on how the originating half call should behave.
5. An FCM is sent to AudioController (AC) to create the terminating half call to the Announcement.
6. A supervision message is sent to the AC to instruct it on how the terminating half call should behave.
7. Once the GWC receives FCM from XA-Core, it sends an ASPEN create connection (CRCX) request to the PVG to establish a bearer connection across the packet network.
8. The PVG sends an ASPEN acknowledgement (ACK) message back to the GWC to acknowledge receipt of the CRCX message.
9. When the GWC receives the ACK message, it sends a CP Connection message to AC to inform it to initiate a connection to the specified Announcement.
10. Once the AC receives the CP connection message, it sends an H.248 Add request to the Universal Audio Server (UAS) to establish a bearer connection between the Announcement and the incoming port on the PVG.
11. The UAS sends an H.248 Reply message back to the AC to acknowledge receipt of the Add message.
12. Once the AC receives the Reply message from the Add, it sends an ASPEN Connection message ACK with SDP to continue establishing the connection.
13. Upon receiving the CP Connection message ACK, the GWC sends an ASPEN modify connection (MDCX) message to the PVG.
14. The PVG sends an ASPEN acknowledgement (ACK) message back to the GWC to acknowledge receipt of the MDCX message.
15. The AC sends an H.248 Modify message to the UAS.
16. The UAS sends an H.248 Reply message back to the AC to acknowledge receipt of the Modify message.

IP Universal Audio Server call flow (Take down)

The figure Universal Audio Server (UAS) call flow (Take down) shows the take down of a UAS call flow.

Universal Audio Server (UAS) call flow (Take down)



1. The originating end office sends a REL message over the SS7 network to an FLPP at ingress Succession Network. Based upon data from table C7TRKMEM, the FLPP maps the CIC of the REL to the corresponding DS0 circuit on the PVG and forwards the REL message to the controlling GWC.
2. The GWC passes the REL to the XA-Core which records billing information in the billing records.
3. The GWC forwards the REL to AC through XA-Core.
4. The GWC sends an ISUP RLC message to the FLPP to be sent to the originating PSTN through the SS7 network.
5. A Fabric Control Message (FCM) is sent to GWC to release the originating half call to the TDM trunk.
6. An FCM is sent to AC to release the terminating half call to the Announcement.
7. The GWC sends an ASPEN modify connection (MDCX) message to the PVG.

8. The PVG responds to the MDCX through GWC with an ASPEN ACK message.
9. When GWC receives the FCM message, it sends an ASPEN delete connection (DLCX) message to PVG.
10. The PVG responds to the DLCX through the GWC with an ASPEN ACK message.
11. The AC sends an H.248 Modify message to the UAS.
12. The UAS responds to the Modify through the AC with an H.248 Reply message.
13. When the AC receives the FCM message, it sends an H.248 Subtract message to the UAS.
14. The UAS responds to the Subtract through the AC with an H.248 Reply message.

Call processing for IAC

This section discusses call processing functions that are unique to the IAC solution. The IAC described in this section (see the table Call flows) are intended to provide a high level understanding of the interactions of the solution components.

Call flows

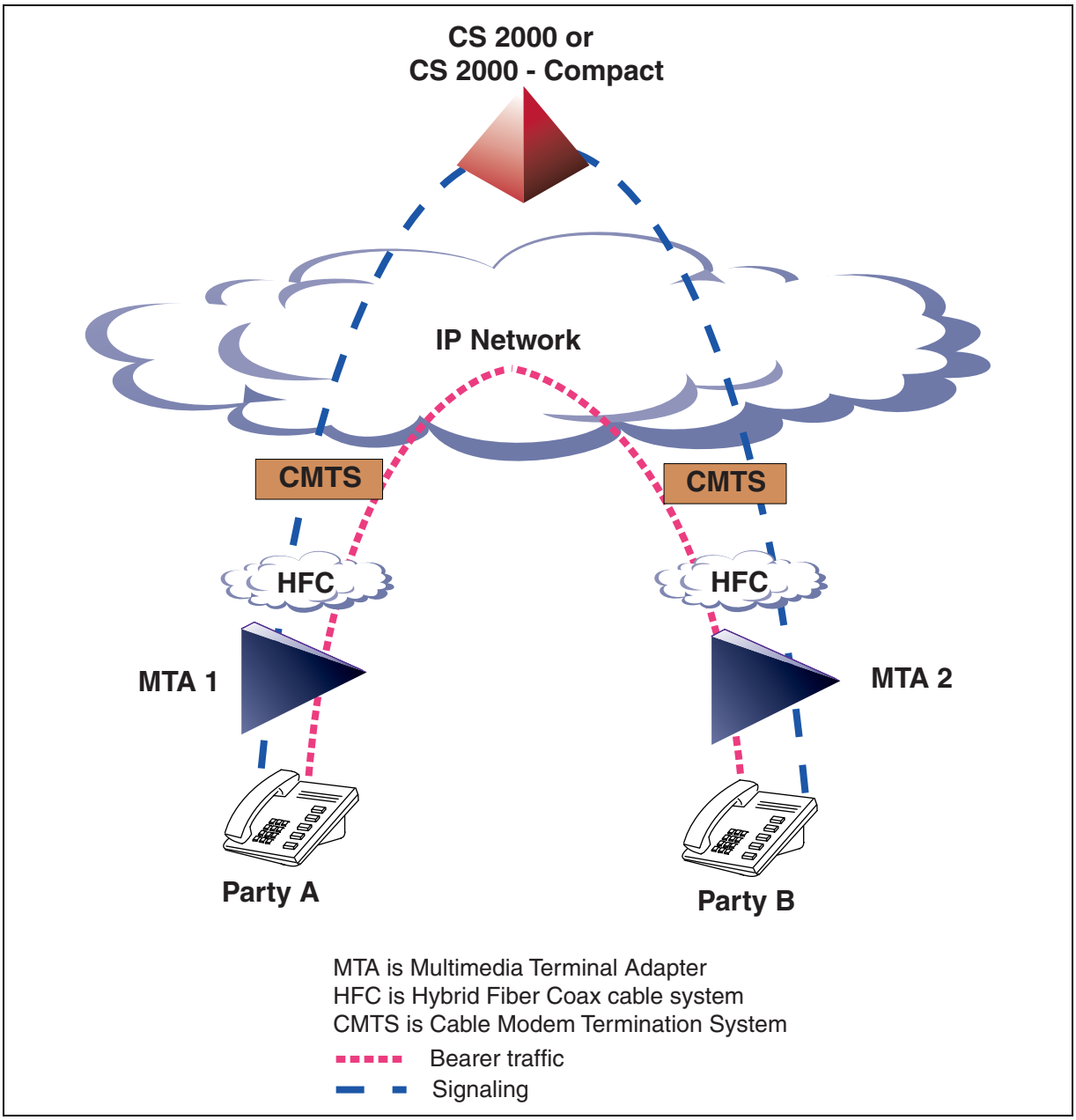
Call flow
On-net to On-net Dynamic Quality of Service (QoS) call flows

On-net to On-net

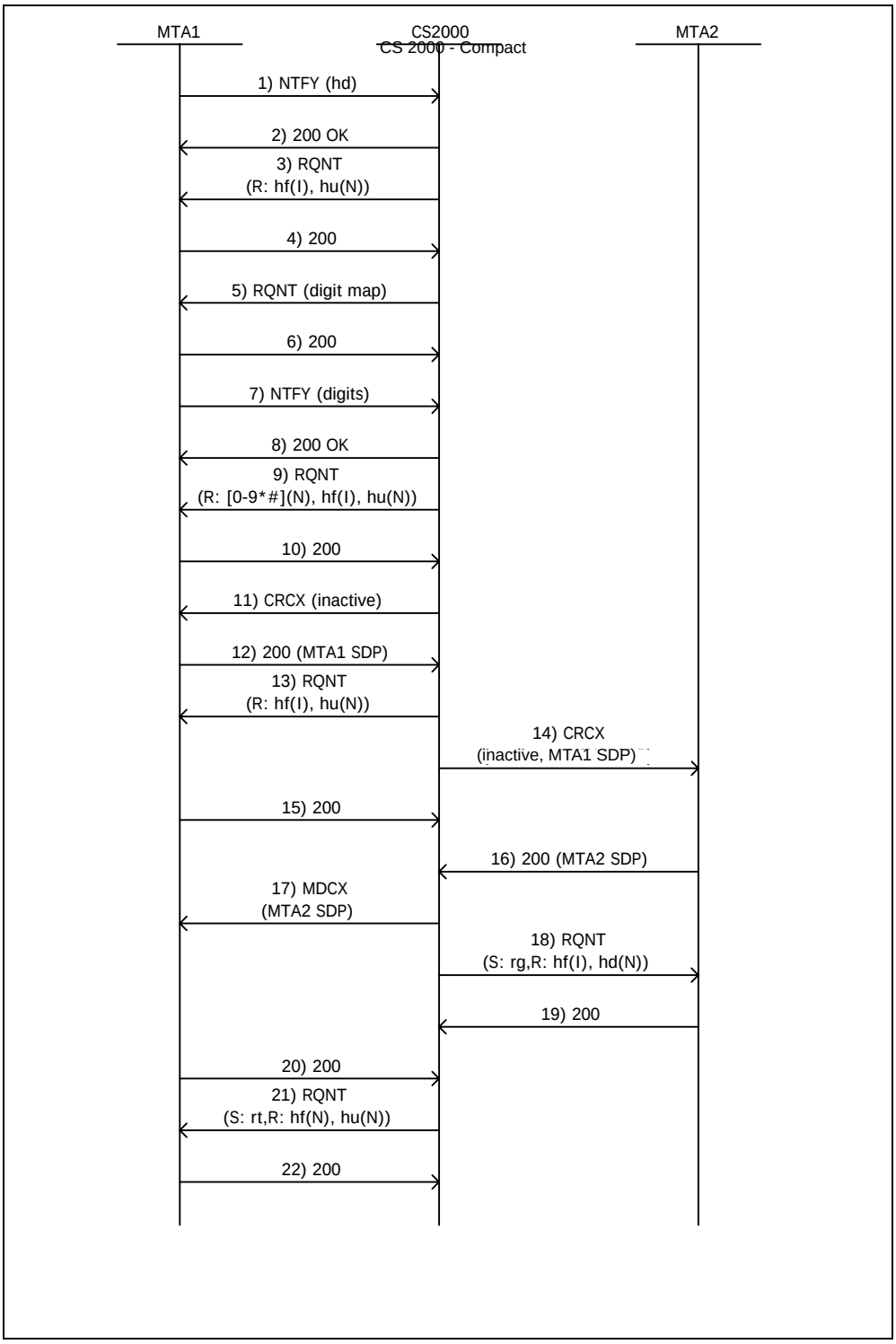
Figures On-net to On-net call,On-net to On-net,On-net to On-net (continued), and On-net to On-net (continued) display the On-net to On-net call flow overview:

- Basic line to line call
- Party A calls Party B
- Party A releases first

On-net to On-net call



On-net to On-net



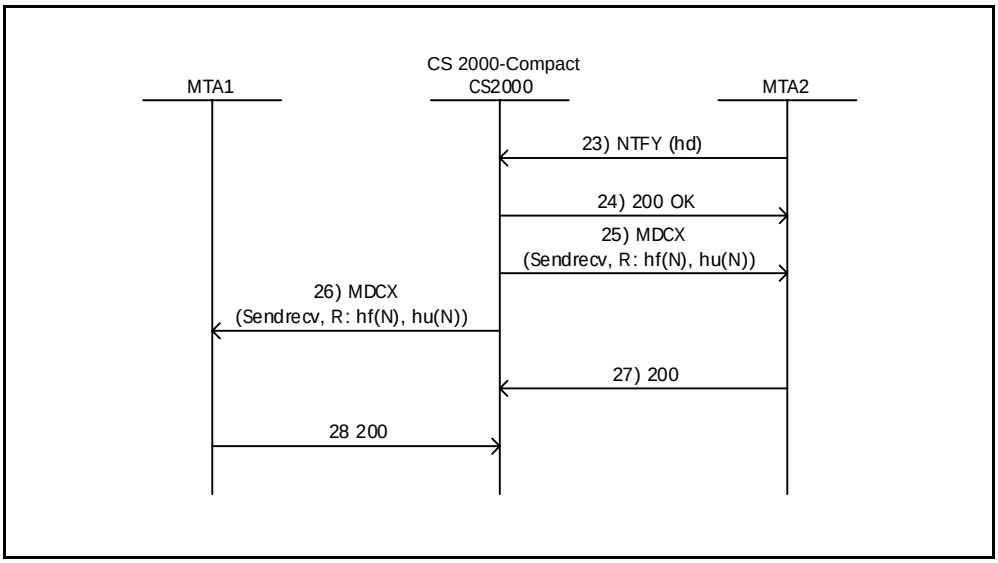
1	MTA detects off hook event and reports to CS 2000 or CS 2000 - Compact platforms.
2	Acknowledgement.
3	Either platform instructs MTA to ignore hook-flash but to report hang-up.
4	Acknowledgement.
5	Either platform provides digit map to MTA and requests digit collection.
6	Acknowledgement.
7	MTA reports digits to either platform.
8	Acknowledgement.
9	Either platform requests notification of further digits or hang-up but not of hook flash.
10	Acknowledgement.
11	Either platform performs translations and routing on the called DN received in step 7 and determines that the called DN is served by the CS 2000 or CS 2000 - Compact. Either platform creates an inactive connection on MTA1 (Party A).
12	MTA1 acknowledges and includes its SDP information.
13	Either platform instructs MTA to ignore hook-flash but to report hang-up.
14	Either platform creates a connection on MTA2 (Party B) passing SDP information about MTA1.
15	Acknowledgement.
16	MTA2 acknowledges and include its SDP information.
17	Either platform modifies connection on MTA1 to include SDP information about MTA2.
18	Either platform instructs MTA2 to apply power ringing to the telephone and to ignore hook-flash but to report hang-up.
19	Acknowledgement.
20	Acknowledgement.

21 Either platform instructs MTA1 to play audible ringing tone to Party A and to report hook-flash or hang-up.

22 Acknowledgement.

At this point Party B's phone is ringing and Party A is hearing audible ringing tone.

On-net to On-net (continued)



23 MTA2 notifies either platform that the Party B has answered.

24 Acknowledgement.

25 Either platform modifies connection on MTA2 for two way communication and requests notification of hook-flash or hang-up.

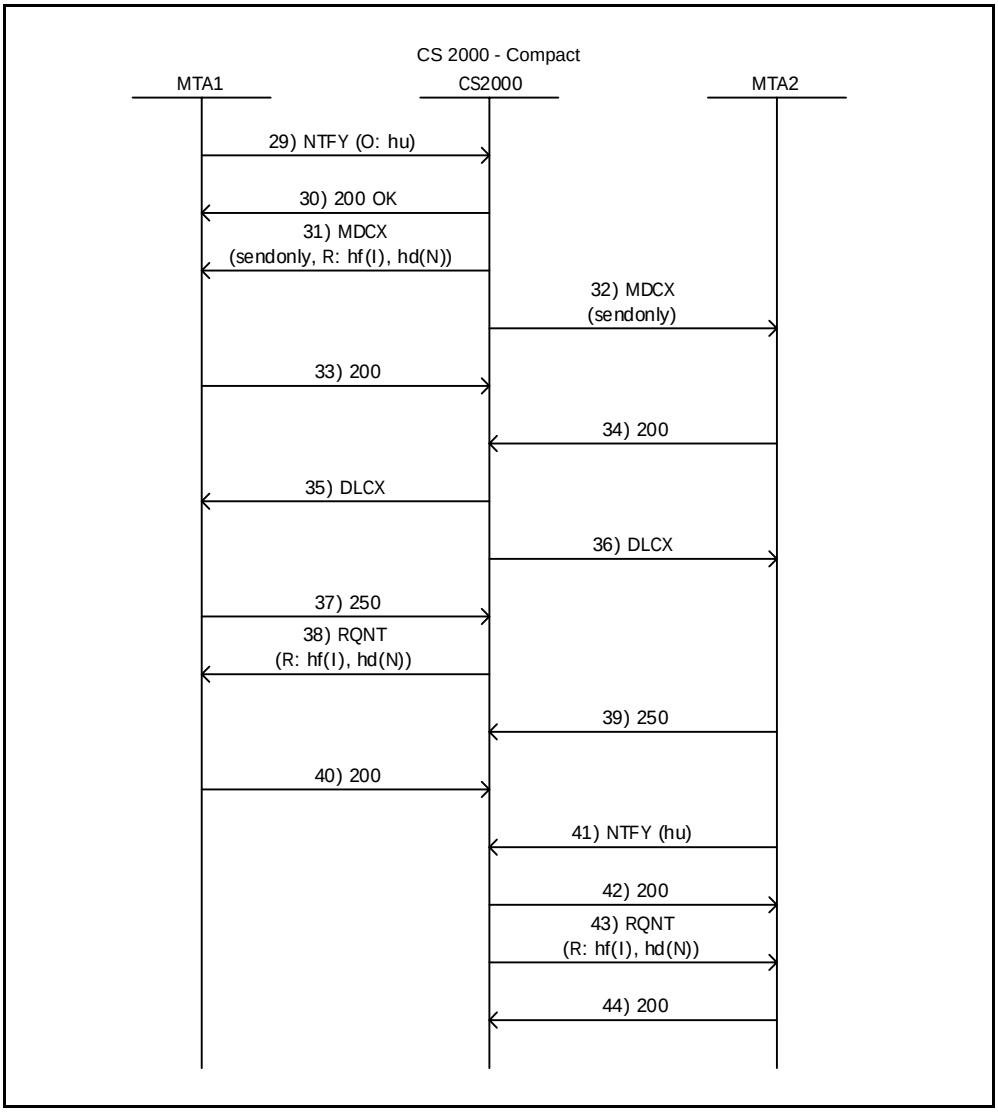
26 Either platform modifies connection on MTA1 for two way communication and requests notification of hook-flash or hang-up.

27 Acknowledgement.

28 Acknowledgement.

At this point the call has been answered, a two-way speech path has been established, and the two parties are in conversation.

On-net to On-net (continued)



29	MTA1 reports that the party A has hung up.
30	Acknowledgement.
31	Either platform modifies the connection on MTA 1 to send only and request notification if the phone goes off hook.
32	Either platform modifies the connection on MTA2 to send only.
33	Acknowledgement.
34	Acknowledgement.

35	Either platform deletes connection on MTA1.
36	Either platform deletes connection on MTA2.
37	Acknowledgement.
38	Either platform instructs MTA to ignore hook-flash but to report hang-up.
39	Acknowledgement.
40	Acknowledgement.
41	MTA 2 reports that Party 2 has hung up.
42	Acknowledgement.
43	Either platform instructs MTA to ignore hook-flash but to report hang-up.
44	Acknowledgement.

At this point the call has ended, both parties have hung up and both MTAs have been instructed to watch for the phones being picked up to originate new calls.

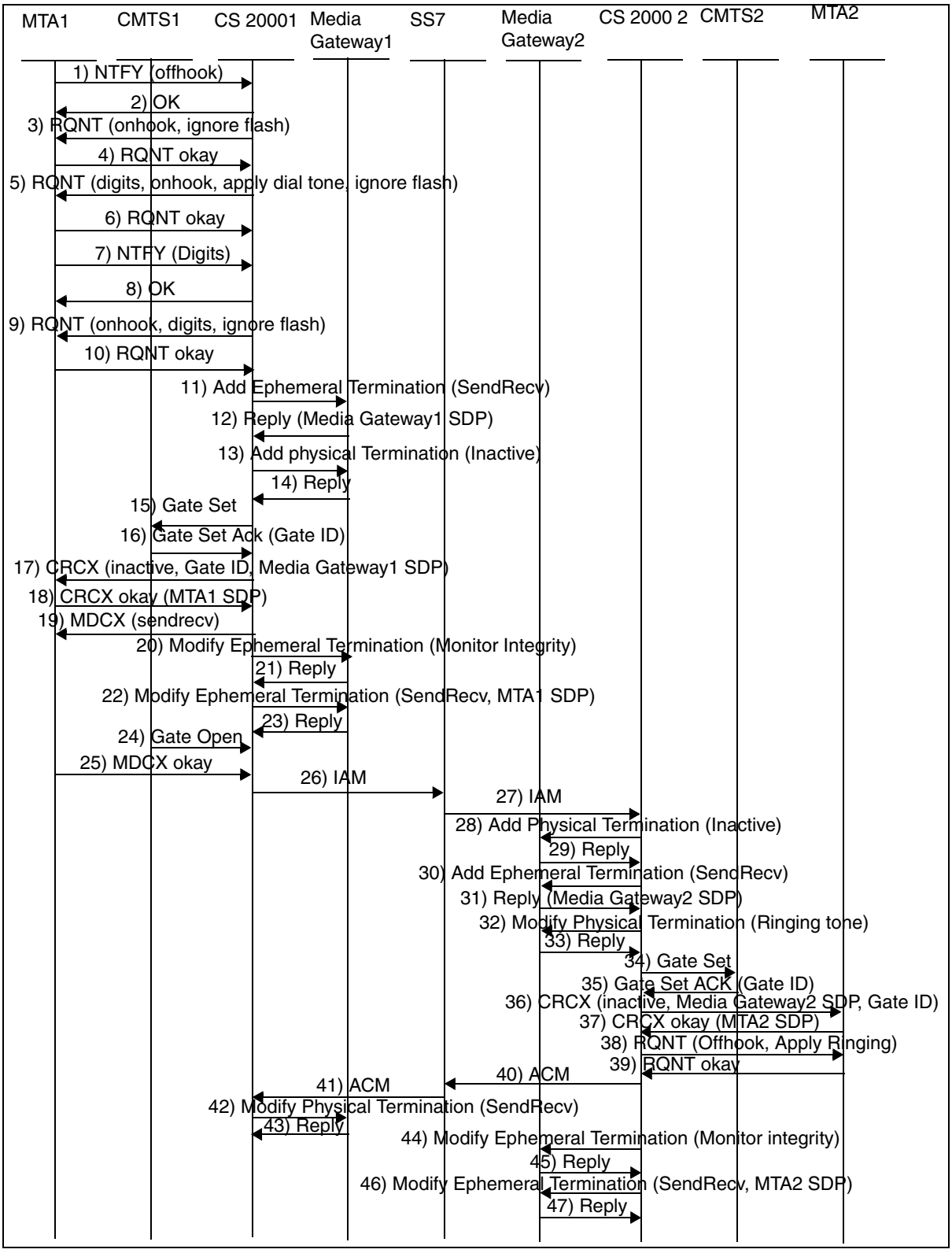
Dynamic Quality of Service (QoS) call flows

The Dynamic QoS call flow is broken down into three sections:

- Originator goes offhook (Dynamic QoS)
- Terminating party answers (Dynamic QoS)
- Originating and terminating parties go onhook (Dynamic QoS)

The figure Originator goes offhook (Dynamic QoS) shows the call flow sequence when the originating party goes offhook.

Originator goes offhook (Dynamic QoS)



The following steps provide an explanation of the events that occur when the originating party goes offhook and dials the digits of the terminating party.

1. NTFY (offhook) (message~mta1~cs2k1).
   MTA 1 notifies CS 2000 1 that the subscriber has gone offhook.
2. Ok (message~cs2k1~mta1~).
   CS 2000 1 acknowledges.
3. RQNT (onhook, ignore flash) (message~cs2k1~mta1~).
   CS 2000 1 requests notification of onhook, and requests that MTA 1 ignore hookflash.
4. RQNT okay (message~mta1~cs2k1~).
   MTA1 acknowledges.
5. RQNT (digits, onhook, apply dial tone, ignore flash) (message~cs2k1~mta1~).
   CS 2000 1 requests that MTA1 apply dial tone, and requests notification of digits based on a digit map.
6. RQNT okay (message~mta1~cs2k1~).
   MTA1 acknowledges.
7. NTFY (Digits) (message~mta1~cs2k1~).
   MTA1 notifies CS 2000 1 of digits dialed by the subscriber.
8. OK (message~cs2k1~mta1~).
   CS 2000 1 acknowledges.
9. RQNT (onhook, digits, ignore flash) (message~cs2k1~mta1~).
   CS 2000 1 requests notification of onhook, requests digits, and requests that MTA1ignore hookflash.
10. RQNT okay (message~mta1~cs2k1~).
    MTA1 acknowledges.
11. Add Ephemeral Termination (SendRecv) (message~cs2k1~mta1~).
    CS 2000 1 analyzes the digits dialed by the subscriber, and determines that the call is destined for the public switched telephone network. CS 2000 1 selects the trunk group and member to route the call. The trunk group/member corresponds to an endpoint on the Media Gateway. As a first step in establishing the connection, CS 2000 1 instructs the Media Gateway to add an ephemeral termination in a new context, and supplies Local Connection Options for the connection. The connection is specified to be in send/receive mode but the physical termination (added in a subsequent step) must also be set to send/receive mode for bearer traffic to be transmitted or received on the time division multiplex side of the connection message.

12. Reply (mg1 SDP) (mg1~cs2k1~).
    Media gateway1 replies with an identifier for the context and the termination, and replies with session Description Protocol (SDP) information.
13. Add Physical Termination (Inactive) (message~cs2k1~mg1~).
    CS 2000 1 instructs media gateway 1 to add the physical termination for the endpoint to the context.
14. Reply (message~mg1~cs2k1~).
    Media gateway 1 replies.
15. Gate Set (message~cs2k1~cmts1~).
    CS 2000 1 instructs CMTS1 to set up a gate authorizing the MTA connection.
16. Gate Set Ack (Gate ID) (message~cmts1~cs2k1~).
    CMTS1 acknowledges, supplying a Gate ID.
17. CRCX (inactive, Gate ID, mg1 SDP) (message~cs2k1~mta1~).
    CS 2000 1 instructs MTA 1 to create an inactive connection, supplying local connection options, the Gate ID from the CMTS, and the SDP from media gateway 1.
18. CRCX okay (mta1 SDP) (message~mta1~cs2k1~).
    MTA1 acknowledges, returning its SDP.
19. MDCX (sendrecv) (message~cs2k1~mta1~).
    CS 2000 1 instructs MTA 1 to modify the connection to be in send/receive mode. MTA1 then sends a DSA request to the CMTS for bandwidth allocation (not shown in the diagram).
20. Modify Termination (Monitor Integrity) (message~cs2k1~mg1~).
    CS 2000 1 requests media gateway 1 to monitor for integrity.
21. Reply (message~mg1~cs2k1~).
    Media gateway 1 replies.
22. Modify Ephemeral Termination (sendRecv, mta1 SDP) (message~cs2k1~mg1~).
    CS 2000 1 instructs the media gateway to modify the ephemeral termination, supplying SDP from MTA1.
23. Reply (message~mg1~cs2k~).
    Media Gateway 1 replies.
24. Gate open (message~cmts1~cs2k1~).
    CMTS 1 reports that the gate is open, after allocation of bandwidth.
25. MDCX okay (message~mta1~cs2k1~).
    MTA 1 acknowledges.
26. IAM (message~cs2k1~ss7~).
    With the connection resources allocated CS 2000 1 sends an IAM

to the SS7 network by means of the signaling gateway (for simplicity the signaling gateway is not shown in the figure).

27. IAM (message~ss7~cs2k2~).
CS 2000 2 receives an IAM.

28. Add Physical Termination (Inactive) (message~cs2k2~mg2~).
CS 2000 2 instructs media gateway 2 to add the physical termination for the end point to a new context.

29. Reply (message~mg2~cs2k2~).
Media gateway 2 replies with an identifier for the new context.

30. Add Ephemeral Termination (SendRecv) (message~cs2k2~mg2~).
CS 2000 2 instructs media gateway 2 to add an ephemeral termination in the context, and supplies local connection options for the connection. The connection is specified to be in send/receive mode.

31. Reply (mg2 SDP) (message~mg2~cs2k2~).
Media gateway 2 replies with an identifier for the termination, plus Session Description Protocol (SDP) information.

32. Modify Physical Termination (Ringing Tone) (message~cs2k2~mg2~).
CS 2000 2 instructs media gateway 2 to modify the physical termination to provide audible ringing tone towards the public switched network.

33. Reply (message~mg2~cs2k2~).
Media gateway 2 replies.

34. Gate Set (message~cs2k2~mg2~).
CS 2000 2 instructs CMTS 2 to set up a gate authorizing the MTA connection.

35. Gate Set Ack (Gate ID) (message~cmts2~cs2k2~).
CMTS2 acknowledges, supplying a Gate ID.

36. CRCX (inactive, mg2 SDP, Gate ID) (message~cs2k2~mta2~).
CS 2000 2 instructs MTA 2 to create an inactive connection, supplying local connection options, the Gate ID from the CMTS, and the SDP from the media gateway.

37. CRCX okay (mta2 SDP) (message~mta2~cs2k2~).
MTA2 acknowledges, returning its SDP.

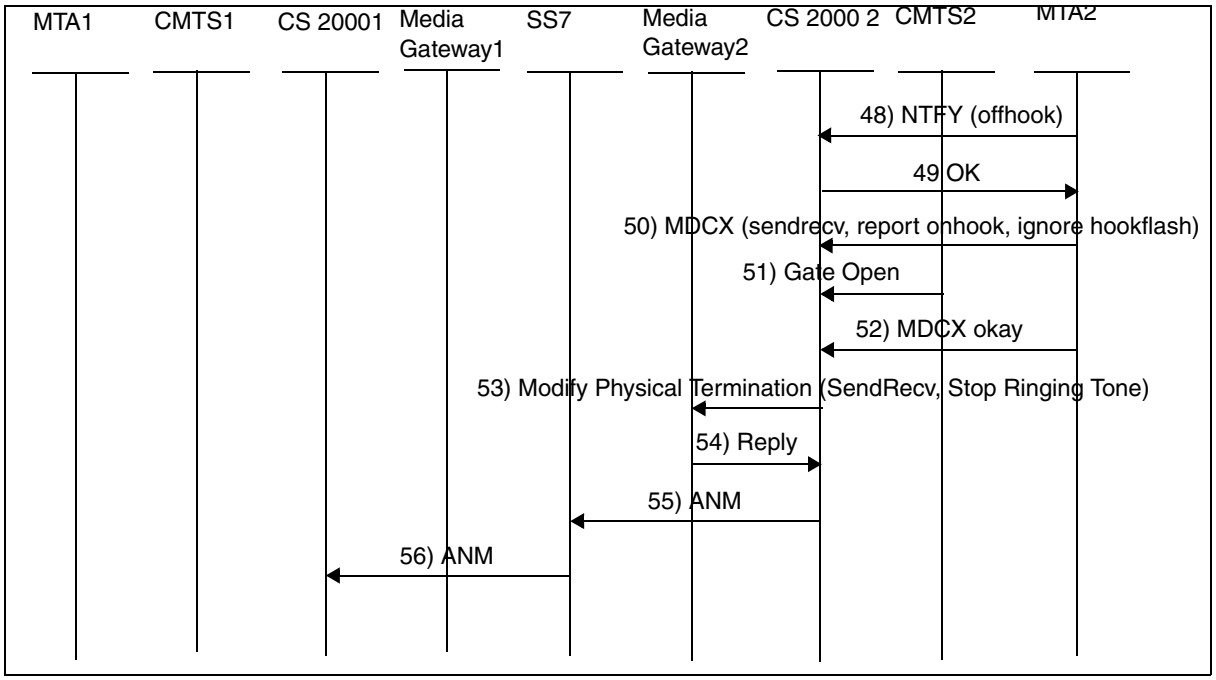
38. RQNT (Offhook, Apply Ringing) (message~cs2k2~mta2~).
CS 2000 2 requests notification of the subscriber going offhook, and instructs MTA2 to apply physical ringing.

39. RQNT okay (message~mta2~cs2k2~).
MTA 2 acknowledges.

40. ACM (message~cs2k2~ss7~).
    CS 2000 2 sends an ACM indicating that the terminator is ringing.
41. ACM (message~ss7~cs2k1~).
    CS 2000 1 receives an ACM indicating that the terminator is ringing.
42. Modify Physical Termination (SendRecv) (message~cs2k1~mg1~).
    CS 2000 1 instructs media gateway 1 to modify the physical termination, setting the connection to send/receive mode.
43. Reply (message~mg1~cs2k1~).
    Media gateway 1 replies.
44. Modify Ephemeral Termination (Monitor Integrity) (message~cs2k2~mg2~).
    CS 2000 2 instructs media gateway 2 to monitor for integrity.
45. Reply (message~mg2~cs2k2~).
    Media gateway 2 replies.
46. Modify Ephemeral Termination (SendRecv, mta2 SDP)(message~cs2k2~mg2~).
    CS 2000 2 instructs media gateway 2 to modify the ephemeral termination, supplying SDP from the MTA.
47. Reply (message~mg2~cs2k2~).
    Media gateway 2 replies.

The figure Terminating party answers (Dynamic QoS) shows the call flow sequence when the terminating party goes answers (Dynamic QoS).

Terminating party answers (Dynamic QoS)



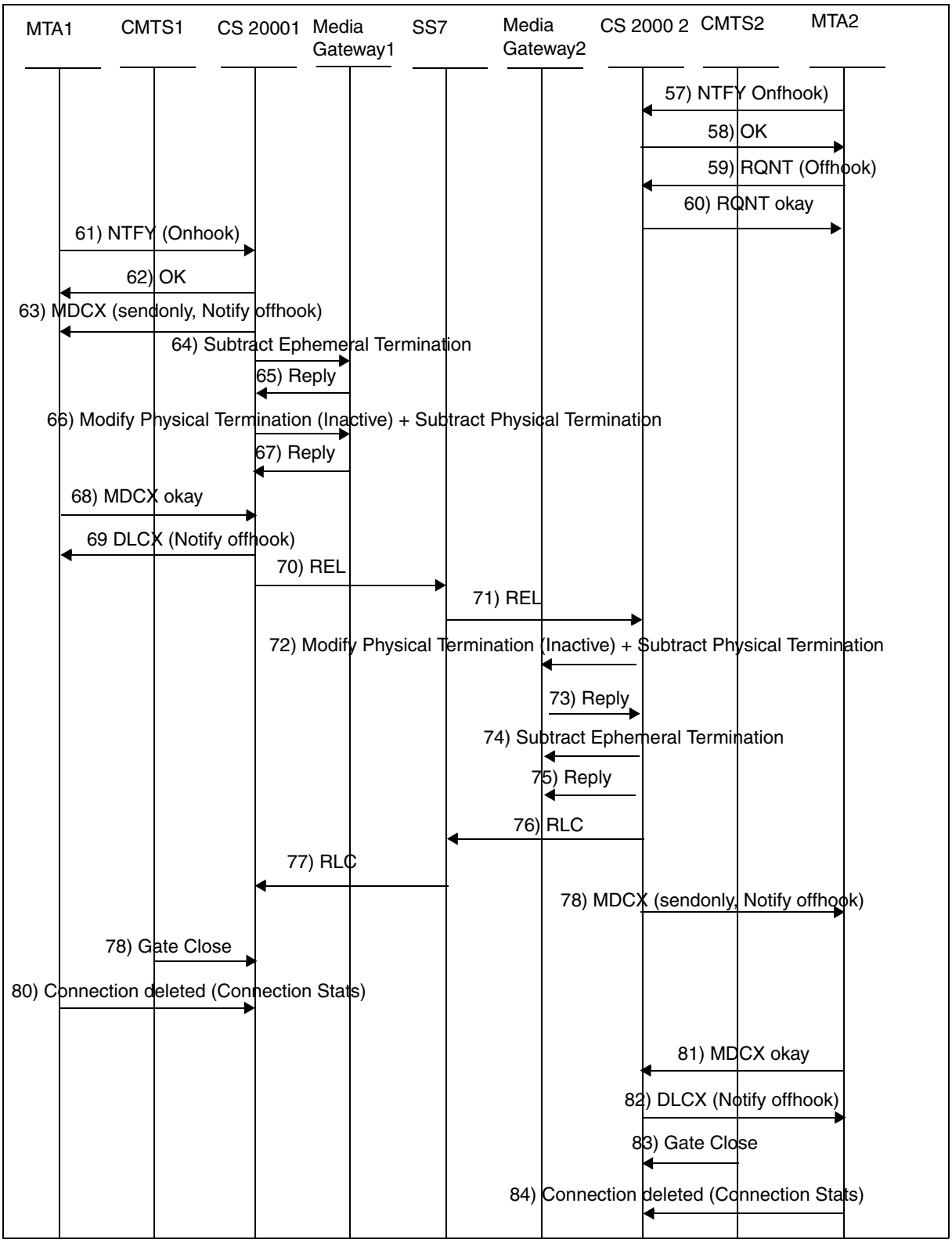
The following steps provide an explanation of the events that occur when the terminating party answers (Dynamic QoS).

48. NTFY (Offhook) (message~mta2~cs2k2~).
    MTA 2 notifies CS 2000 2 that the terminating party is gone offhook.
49. OK (message~cs2k2~mta2~).
    CS 2000 2 acknowledges.
50. MDCX (sendrecv, report onhook, ignore hook flash) (message~mta2~cs2k2~).
    CS 2000 2 instructs MTA2 to modify the connection to send/receive, plus report onhooks and ignore hook flashes. MTA2 then sends a DSA request to the CMTS for bandwidth allocation (not shown in diagram).
51. Gate Open (message~cmts2~cs2k2~).
    CMTS2 reports that the gate is open, after allocation of bandwidth.
52. MDCX okay (message~mta2~cs2k2~).
    MTA 2 acknowledges.
53. Modify Physical Termination (SendRecv, Stop Ringing Tone) (message~cs2k2~mg2~).
    CS 2000 2 instructs media gateway 2 to modify the physical termination, setting the connection to send/receive, and stopping the ringing tone.

54. Reply (message~mg2~cs2k2~).
    Media gateway2 replies.
55. ANM (message~cs2k2~ss7~).
    CS 2000 2 sends an ANM indicating the terminator has answered.
56. ANM (message~ss7~cs2k1~).
    CS 2000 1 receives an ANM indicating the terminator has answered.

The figure Originating and terminating parties go onhook (Dynamic QoS) shows the call flow sequence when the terminating party hangs up.

Originating and terminating parties go onhook (Dynamic QoS)



The following steps provide an explanation of the events that occur when the originating and terminating parties go onhook (Dynamic QoS).

57. NTFY (Onhook) (message~mta2~cs2k2~).
    MTA 2 notifies CS 2000 2 that the terminating party has gone onhook.
58. OK (message~cs2k2~mta2~).
    CS 2000 2 acknowledges.
59. RQNT (offhook) (message~mta2~cs2k2~).
    CS 2000 2 requests notification of a subscriber going offhook.
60. RQNT okay (message~cs2k2~mta2~).
    MTA 2 acknowledges.
61. NTFY (onhook) (message~mta1~cs2k21~).
    MTA1 notifies CS 2000 1 that the terminating party has gone onhook.
62. OK (message~cs2k1~mta1~).
    CS 2000 1 acknowledges.
63. MDCX (sendonly, Notify offhook) (message~cs2k1~mta1~).
    CS 2000 1 instructs MTA 1 to modify the connection to be sendonly, and requests notification of the subscriber going onhook.
64. Subtract Ephemeral Termination (message~cs2k1~mg1~).
    CS 2000 1 instructs media gateway 1 to subtract the ephemeral termination.
65. Reply (message~mg1~cs2k1~).
    Media gateway 1 replies.
66. Modify Physical Termination (Inactive) + Subtract Physical Termination (message~cs2k1~mta1~).
    CS 2000 1 instructs media gateway 1 to modify the physical termination, setting the connection inactive, and then to subtract the physical termination from the context.
67. Reply (message~mg1~cs2k1~).
    Media gateway 1 replies.
68. MDCX okay (message~mg1~cs2k1~).
    MTA 1 acknowledges.
69. DLCX (Notify offhook) (message~cs2k1~mta1~).
    CS 2000 1 instructs MTA 1 to delete the connection, and requests notification of the subscriber going offhook. MTA 1 instructs the CMTS to release bandwidth (not shown in the figure).
70. REL (message~cs2k2~ss7~).
    CS 2000 1 sends an ISUP REL message.

71. REL (message~ss7~cs2k2~).
CS 2000 2 receives an ISUP REL message.

72. Modify Physical Termination (Inactive) + Subtract Physical Termination (message~cs2k2~mg2~).
CS 2000 2 instructs media gateway 2 to modify the physical termination, to set the connection inactive, and then to subtract the physical termination from the context.

73. Reply (message~mg2~cs2k2~).
Media gateway 2 replies.

74. Subtract Ephemeral Termination (message~cs2k2~mg2~).
CS 2000 2 instructs media gateway 2 to subtract the ephemeral termination.

75. Reply (message~cs2k2~mg2~).
Media gateway 2 replies.

76. RLC (message~cs2k2~ss7~).
CS 2000 2 sends an ISUP RLC message.

77. RLC (message~ss7~cs2k1~).
CS 2000 1 sends an ISUP RLC message.

78. MDCX (sendonly, Notify offhook) (message~cs2k2~mta2~).
CS 2000 2 instructs media gateway 2 to modify the connection to be sendonly, and requests notification of a subscriber going offhook.

79. Gate Close (message~cmts1~cs2k1~).
CMTS1 notifies CS 2000 1 that the gate has closed.

80. Connection deleted (Connection Stats) (message~mta1~cs2k1~).
MTA 1 acknowledges, and supplies connection statistics.

81. MDCX okay (message~mta2~cs2k2~).
MTA 2 acknowledges.

82. DLCX (Notify offhook) (message~cs2k2~mta2~).
CS 2000 2 instructs media gateway 2 to delete the connection, and requests notification of the subscriber going offhook. MTA 2 instructs the CMTS to release bandwidth (not shown in the diagram).

83. Gate Close (message~cmts2~cs2k2~).
CMTS2 notifies CS 2000 2 that the gate has been closed.

84. Connection deleted (Connection State) (message~mta2~cs2k2~).
MTA 2 acknowledges, and supplies connection statistics.

Call processing for PT-IP and PT-AAL2

This section describes call processing that is unique to the PT-IP, and PT-AAL2 solutions. For general call processing information that is common to all the IP solutions, see Call processing for IP.

PT-IP call processing with IW SPM-IP in a hybrid network

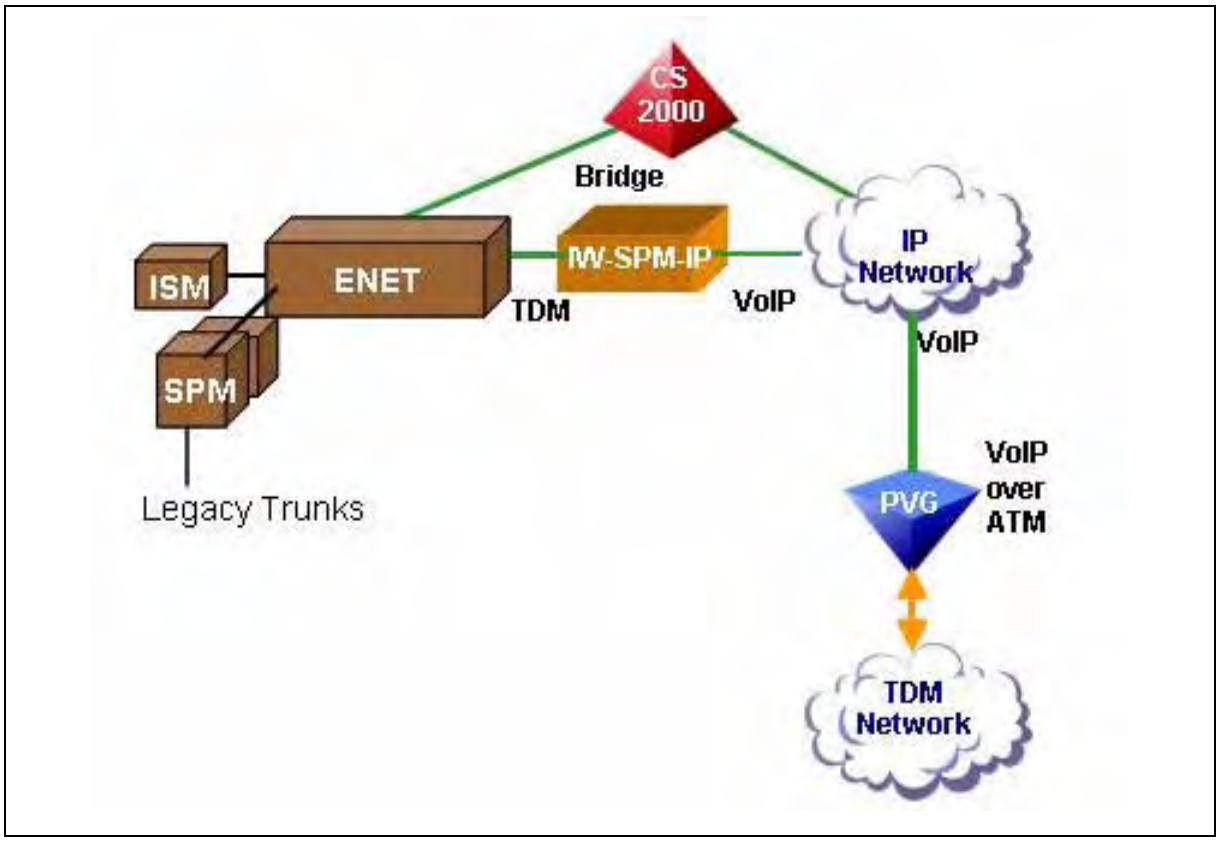
The Interworking SPM-IP (IW SPM-IP) is a component that builds upon the technology of the Spectrum Peripheral Module (SPM). The SPM is a multi-application peripheral program with a common platform that represents the application of Spectrum technology to a DMS switch. The IW-SPM-IP connects the existing DMS infrastructure to an IP based network, providing a mechanism for bridging calls between an IP network and an existing TDM network by transcoding voice data between RTP/UDP/IP and TDM voice. The IW-SPM-IP is connected to the Enhanced Network (ENET) via DS512 links and to the IP network via a Gigabit Ethernet Interface.

Call processing control is managed by CS 2000 and is passed through the Message Switch (MS), Enhanced Network (ENET), and enters the IW-SPM-IP though fiber optic DS-512 links between the Common Equipment Modules (CEMs) on the IW-SPM-IP and port cards on the ENET. The CEMs route the data over S-links through the backplane to the IP RM cards. The IP RM cards manage any processing on the data and then transmit the signals out the IW-SPM-IP over the Gigabit Ethernet Interface. The figure IW-SPM-IP within PT-IP hybrid solution shows how IW-SPM-IP fits into the Succession Network.

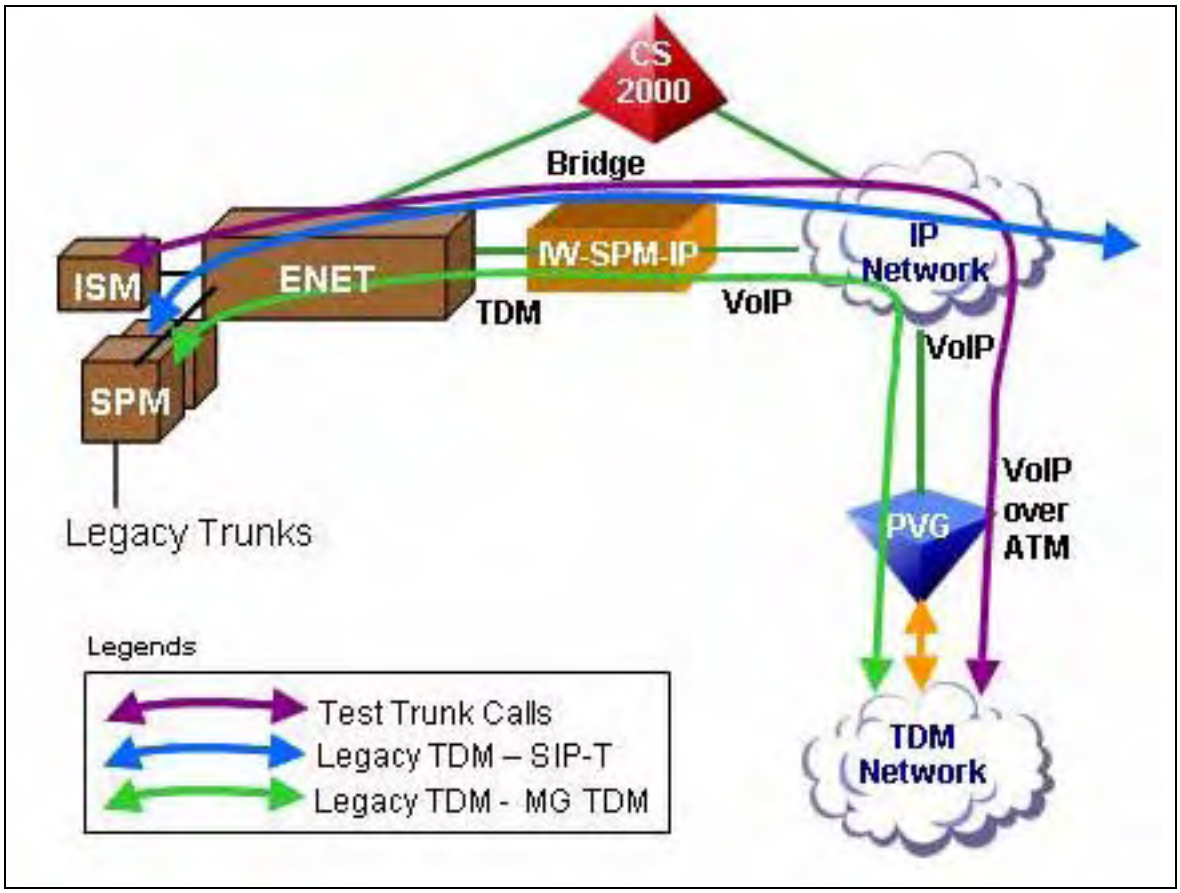
IW-SPM-IP supports three types of calls. The figure IW-SPM-IP call support for PT-IP hybrid solution illustrates these call types:

- trunk testing calls on the Gateway trunk using legacy MTM test circuit
- legacy TDM trunk and Gateway TDM trunk interworking calls
- legacy TDM trunk and SIP-T DPT trunk interworking calls

IW-SPM-IP within PT-IP hybrid solution

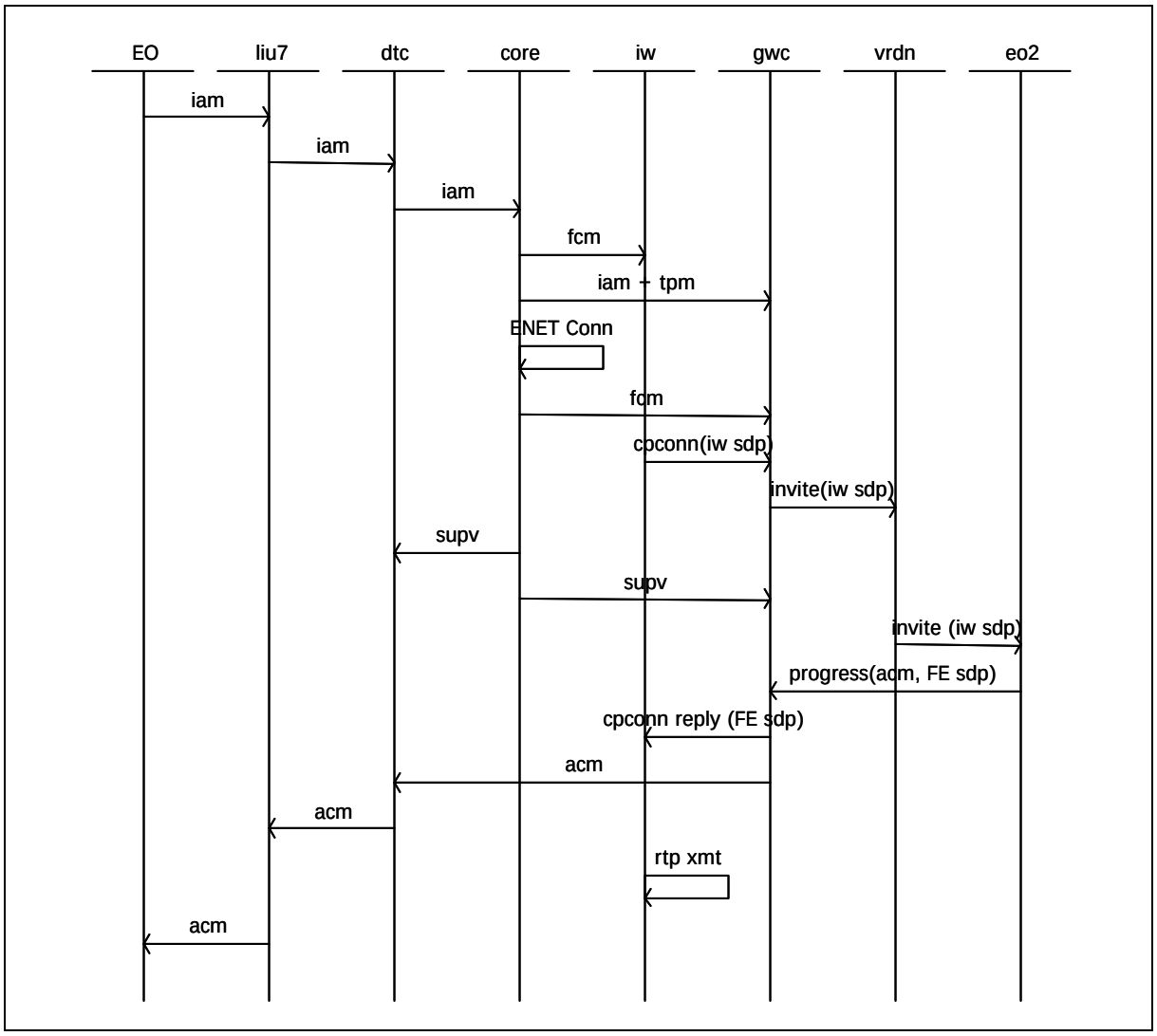


IW-SPM-IP call support for PT-IP hybrid solution



The figure IW-SPM-IP message flow for PT-IP hybrid solution illustrates how a call from an SPM destined for another IXC office is processed through an IW-SPM-IP.

IW-SPM-IP message flow for PT-IP hybrid solution



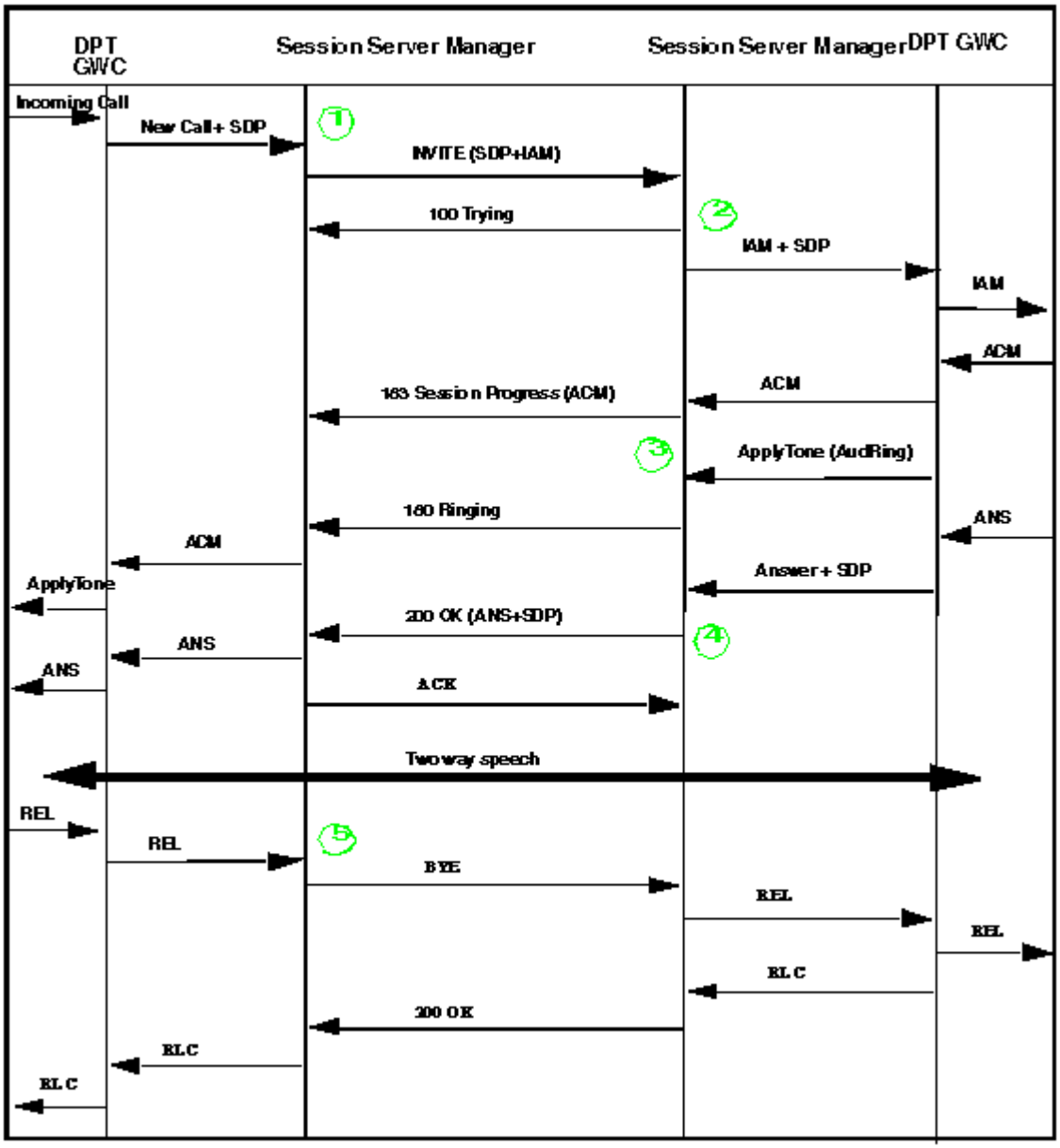
AAL2 call processing with loop-around trunks in a hybrid network

The AAL2 solution uses loop-around trunks (in a hybrid architecture) to provide connections between the legacy time-division multiplex (TDM) peripherals, and the packet network. For the legacy TDM peripherals on the AAL2 switch, the loop-around trunk is terminated on a Digital Trunk Controller (DTC) or Spectrum Peripheral Module (SPM). In the packet environment the loop-around trunk is terminated on the TDM side of a Media Gateway 15000. Both of these trunk terminations must be on components that are controlled by the same CS 2000 switch. XA-Core call processing software handles a call made to either end of the loop around trunk like a call to or from a remote node. Each end of a loop around trunk is separately defined by means of datafill in the XA-Core and have different CCS7 point codes.

Call flow for a SIP bridging scenario with Session Server Manager

The figure below illustrates a sample call flow for a SIP bridging scenario with a Session Server on both sides. Key points on the incoming and outgoing side of the call are discussed below.

Sample Session Server SIP call flow



Steps of call flow

1 The core selects one DPT GWC to process the outgoing call. If there is more than one DPT GWC, then the core employs a round-robin algorithm to determine the GWC to which to present the call.

On receipt of the IAM message, the DPT GWC on receipt of the IAM message does the following:

a Extracts the trunk information and determines if a SIP Access Link is associated with this trunk.

b If a SIP Access Link is not associated with this call, the call is setup as a pre-Session Server Manager SIP call.

c If a SIP Access Link is associated with this call, the IP address of the Session Server Manager is retrieved and the IAM is forwarded to the Session Server Manager. The IP address of the Session Server Manager is sent to the GWC as part of the GWC discovery process.

d The Session Server Manager then extracts the SIP Access information and retrieves information regarding the remote SIP server to which the call is intended.

e The SIP INVITE message is constructed with appropriate headers, session description, and payloads (if applicable) and is sent to the remote SIP server.

2 On receipt of an incoming SIP call, the Session Server Manager sends back a 100 Trying message to the sending entity while the INVITE is processed. A call processing application retrieves the host or IP address information from the header information to determine the characteristics of the sending entity.

Once the remote server profile is retrieved, the SIPLINK name associated with the remote SIP server is retrieved. The ISUP IAM payload, if any, is also retrieved and forwarded to the DPT GWC along with the SIPLINK information.

The DPT GWC gets the SIP LINK information from the Session Server Manager and determines the trunk, on which the incoming call is processed.

3 Once the incoming INVITE is processed, the remote SIP server can send any number of provisional responses (18X). ISUP payloads, such as ACM or CPG, are encapsulated in an appropriate provisional response if the remote server is capable of handling ISUP messages.

It is also possible that the provisional responses are used to apply local ringing and/or pass any media information to which the terminating side would like the originating side to hear.

4 When the terminating side answers the call, it forwards the ANS ISUP message (if applicable) along with its session description in a 200 OK message to the originating side.

The originating side extracts the relevant information and forwards the terminating SDP to the appropriate endpoint. It also returns a SIP ACK request to the terminating SIP server to complete the three-way hand-shake.

5 When either the originating or terminating sides ends the call, the ISUP REL message is forwarded to the Session Server Manager. The Session Server Manager then builds a SIP BYE message, encapsulates the ISUP message, if applicable, and sends it to the remote SIP server.

The remote SIP server on receipt of the BYE message, extracts the ISUP message, if applicable, and forwards to the DPT GWC on its way to the core. It also responds to the BYE with a 200 OK and encapsulates the ISUP RLC whenever applicable.

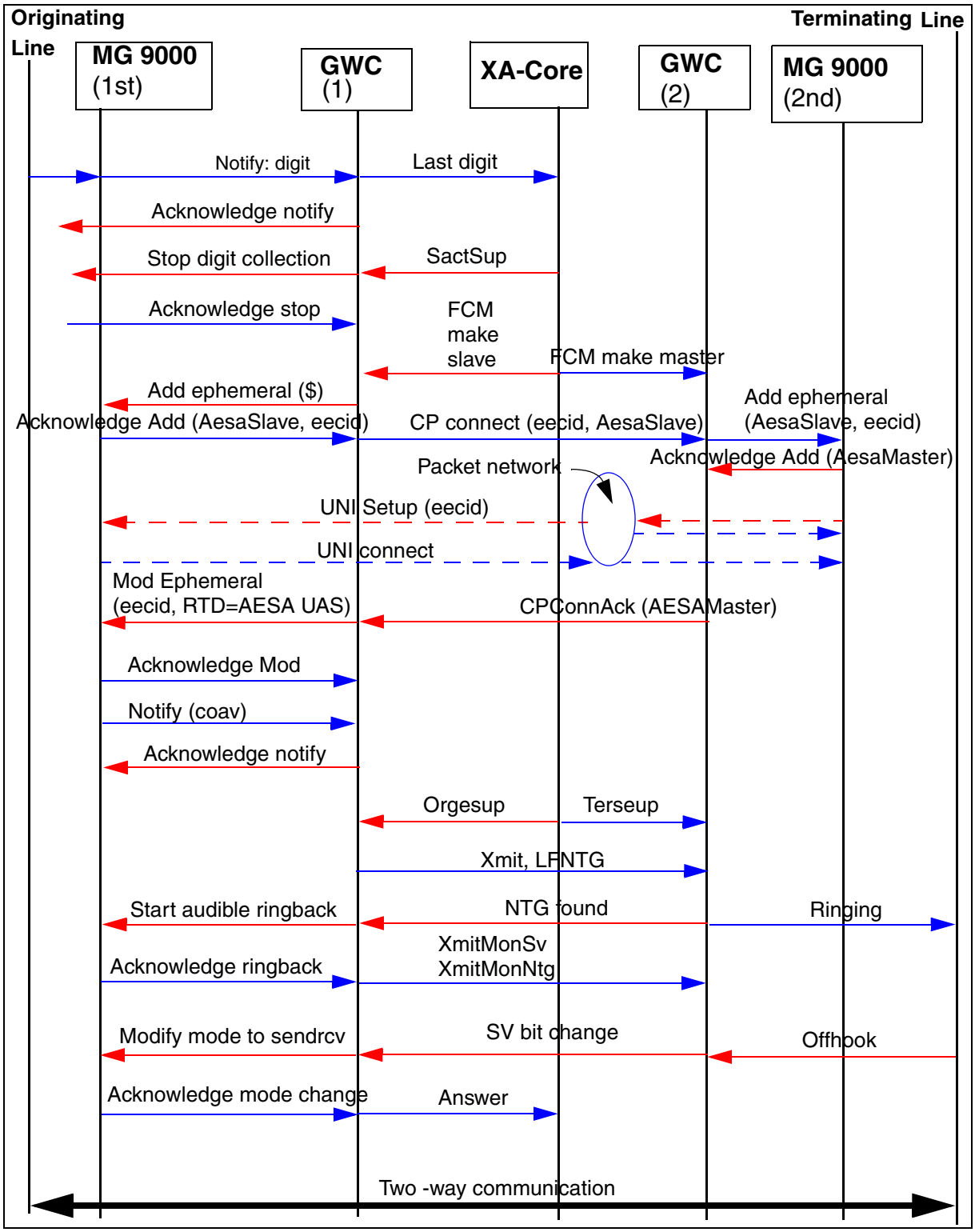
Call processing for UA-IP

This section discusses call processing that is unique to the UA-IP solution. For general call processing information that is common to all the IP solutions, see Call processing for IP

UA-IP MG 9000 to MG 9000 call setup

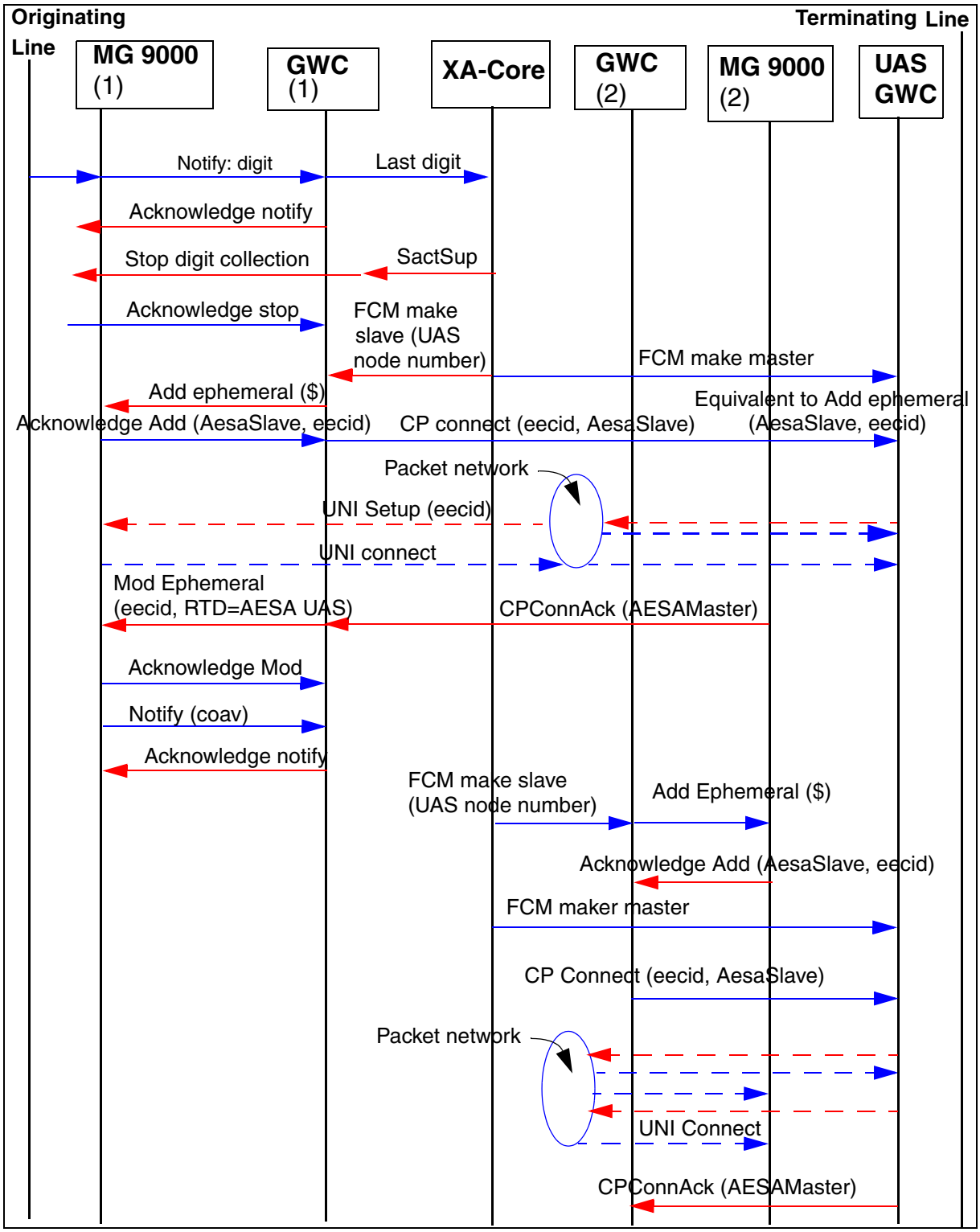
The figure MG 9000 to MG 9000 call setup shows a call walk through for a call that originates on one MG 9000 and terminates on another MG 9000.

MG 9000 to MG 9000 call setup

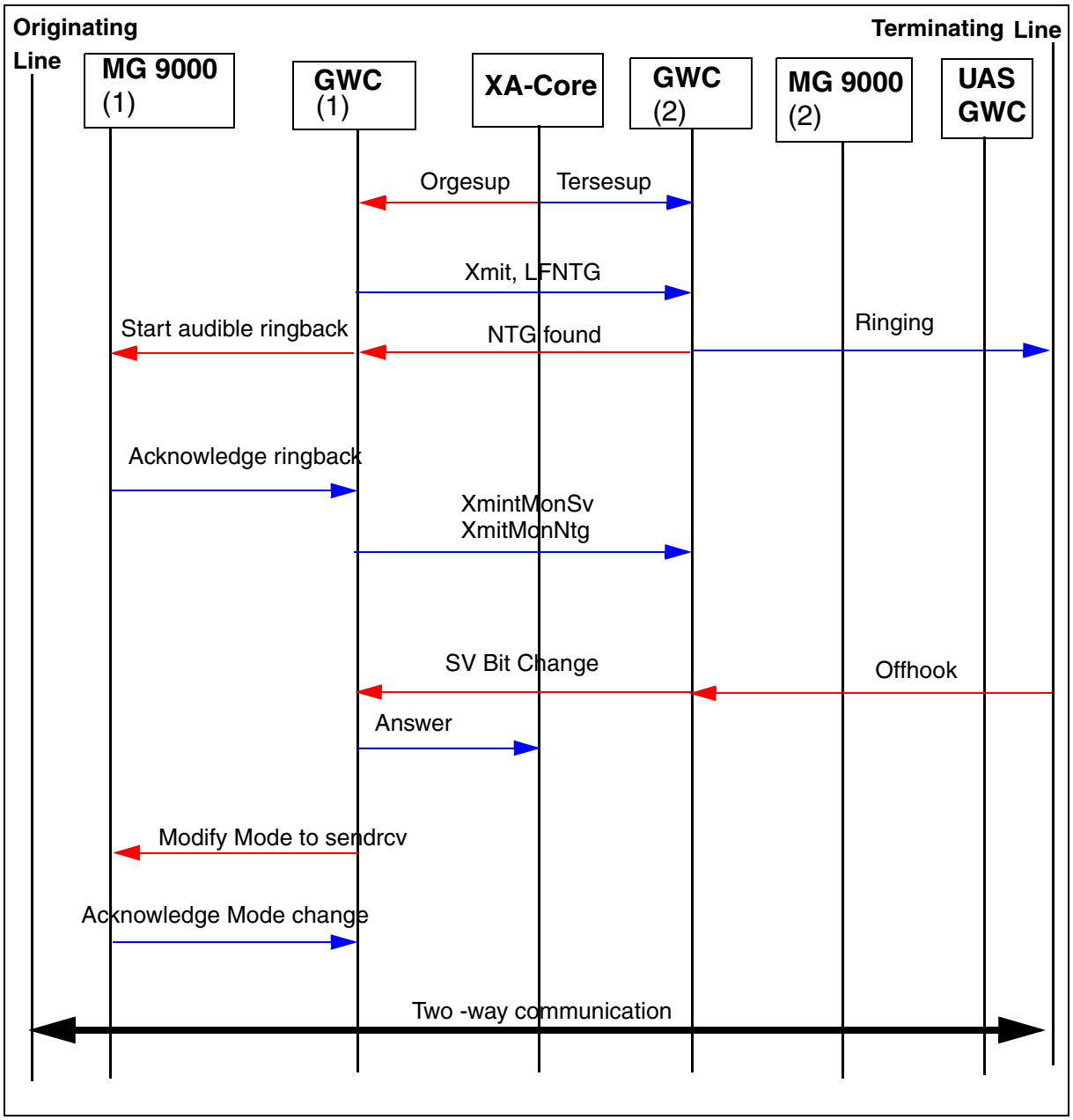


The figure MG 9000 to MG 9000 call setup with Lawful Intercept (part 1 of 2) shows a call walk through for an intercepted call (Lawful Intercept) that originates on one MG 9000 and terminates on another MG 9000.

MG 9000 to MG 9000 call setup with Lawful Intercept (part 1 of 2)



MG 9000 to MG 9000 call setup with Lawful Intercept (part 2of 2



UA-IP Intra-MG 9000 POTS call involving Caller Identification

The figure Intra-MG 9000 POTS call with Caller Identification (involving two lines) shows a plain old telephone service (POTS) call walk through for a call that originates and terminates on the same MG 9000 (two separate lines) and involves Caller Identification.

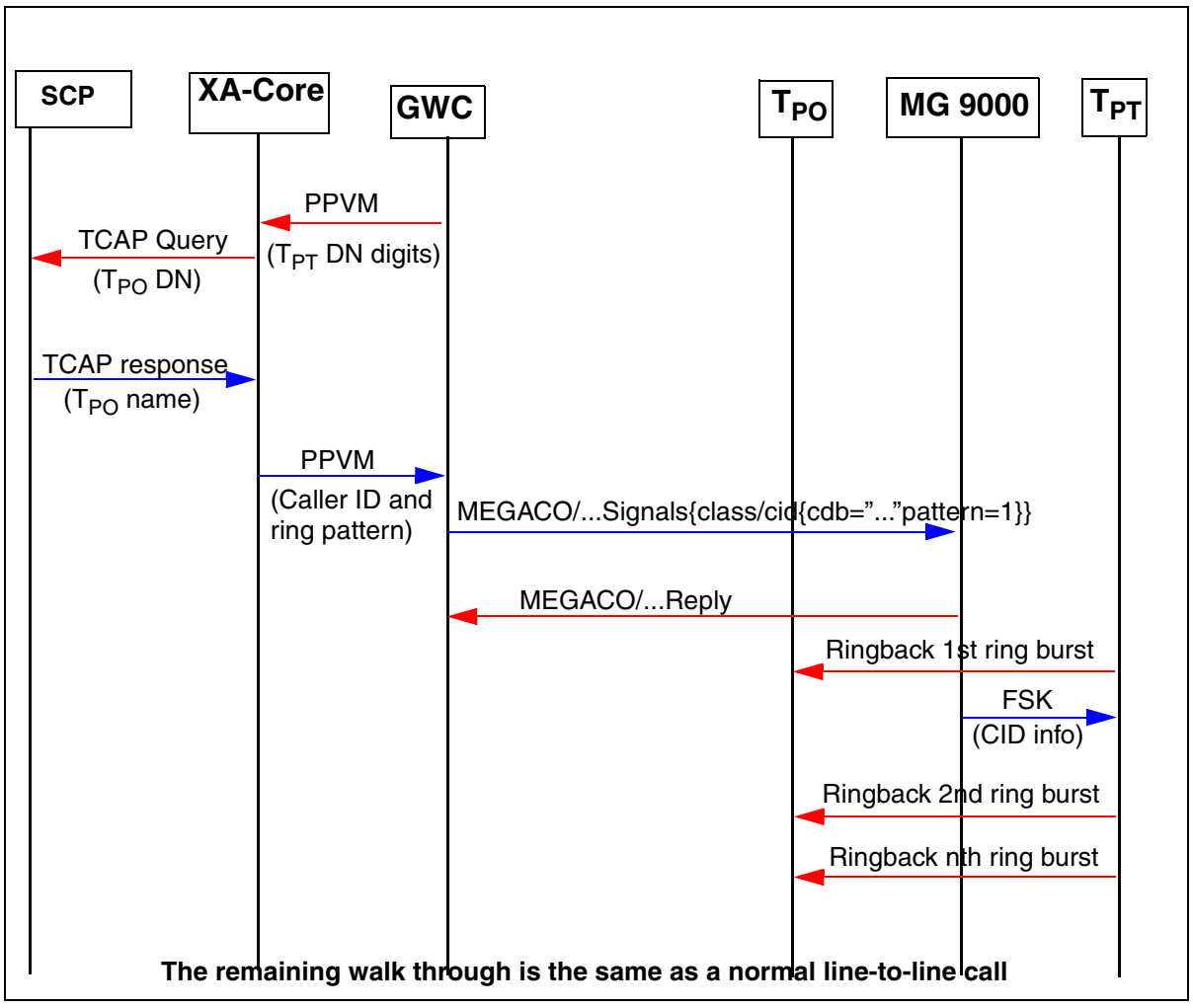
Note 1: The walk through for Calling Number Delivery (CND) or Calling Name Delivery (CNAMD), and Calling Number Delivery

Blocking (CNDB), or Calling Name Delivery Blocking (CNAMB) are identical except for the query of the name database. The only differences lie in the encoding of the data stream sent in the Megaco request message, which is invisible to the MG 9000.

Note 2: If the called party goes off hook during the first ringing interval, or during the FSK transmission, the CMR portion of the call is aborted and the caller ID information is discarded.

Note 3: Any CMR failure is contained or handled within the MG 9000. When this happens, the caller ID information is discarded; however, ringing continues normally.

Intra-MG 9000 POTS call with Caller Identification (involving two lines)



UA-IP Intra MG 9000 POTS call with Spontaneous Call Waiting Identification

The figure Intra MG 9000 POTS call involving SCWID shows a plain old telephone service (POTS) call walk through for a call involving Spontaneous Call Waiting Identification (SCWID). This call originates and terminates on the same MG 9000 and uses three separate lines.

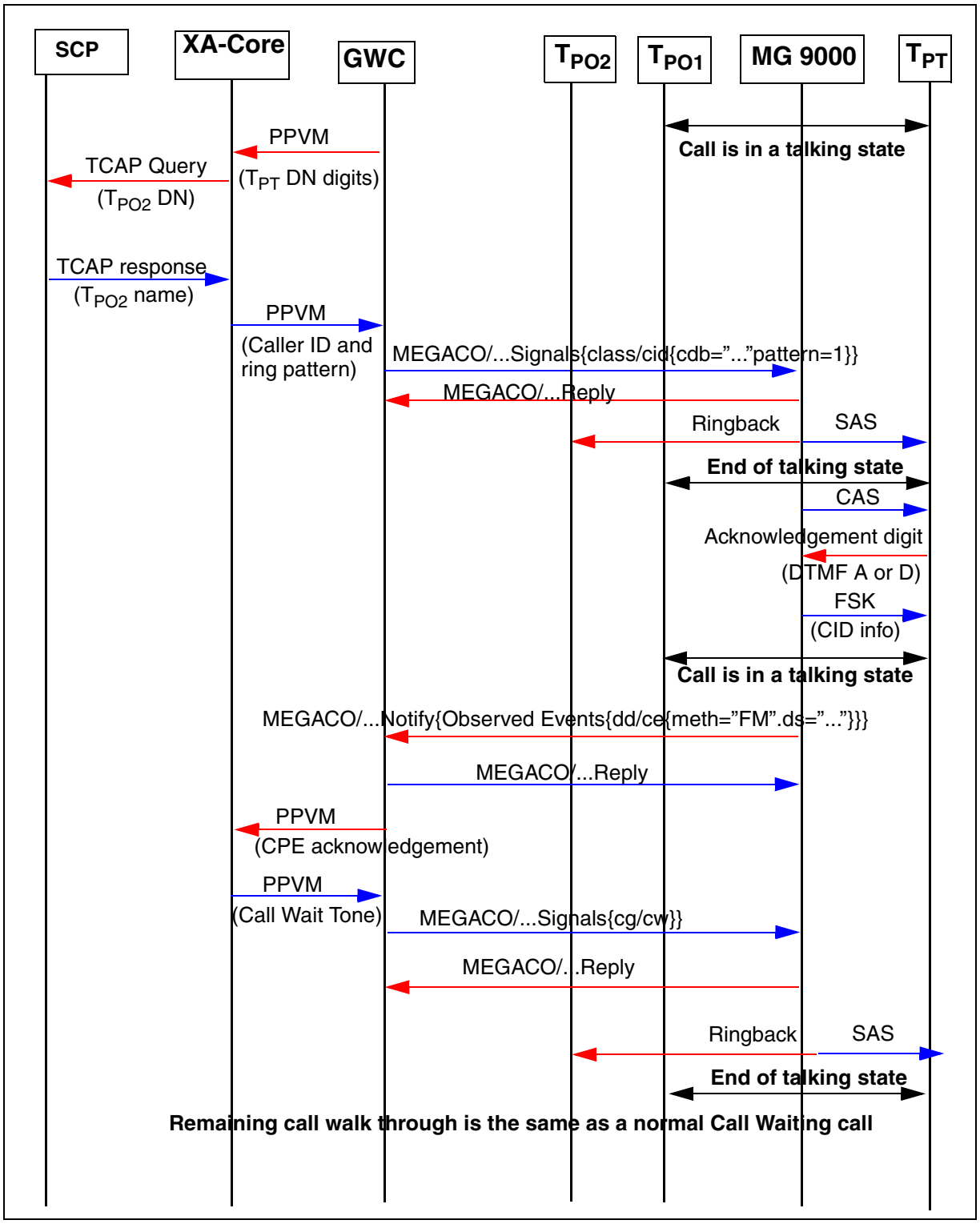
Note 1: The Megaco message for SCWID is identical to Caller ID. This Megaco message is distinguished by the MG 9000 by means of the switch hook status of the line.

Note 2: The encoding of the data stream content for Calling Number Delivery (CND) or Calling Name Delivery (CNAMD), and Calling Number Delivery Blocking (CNDB), or Calling Name Delivery Blocking (CNAMB), for SCWID, are identical to Caller ID. This encoding is invisible to the MG 9000.

Note 3: If the Called Party hook flashes during CAS, or during the FSK transmission, the CMR portion of the call is aborted and the Caller ID information is discarded.

Note 4: Any CMR failure is contained or handled within the MG 9000. In the case of CMR failure, the MG 9000 does not send the held acknowledgement digit which causes the GWC to resend the Call Waiting ID information with a second SAS request. If a CMR failure occurs after a second SAS request, the Call Waiting ID information and any collected acknowledgement digits are discarded.

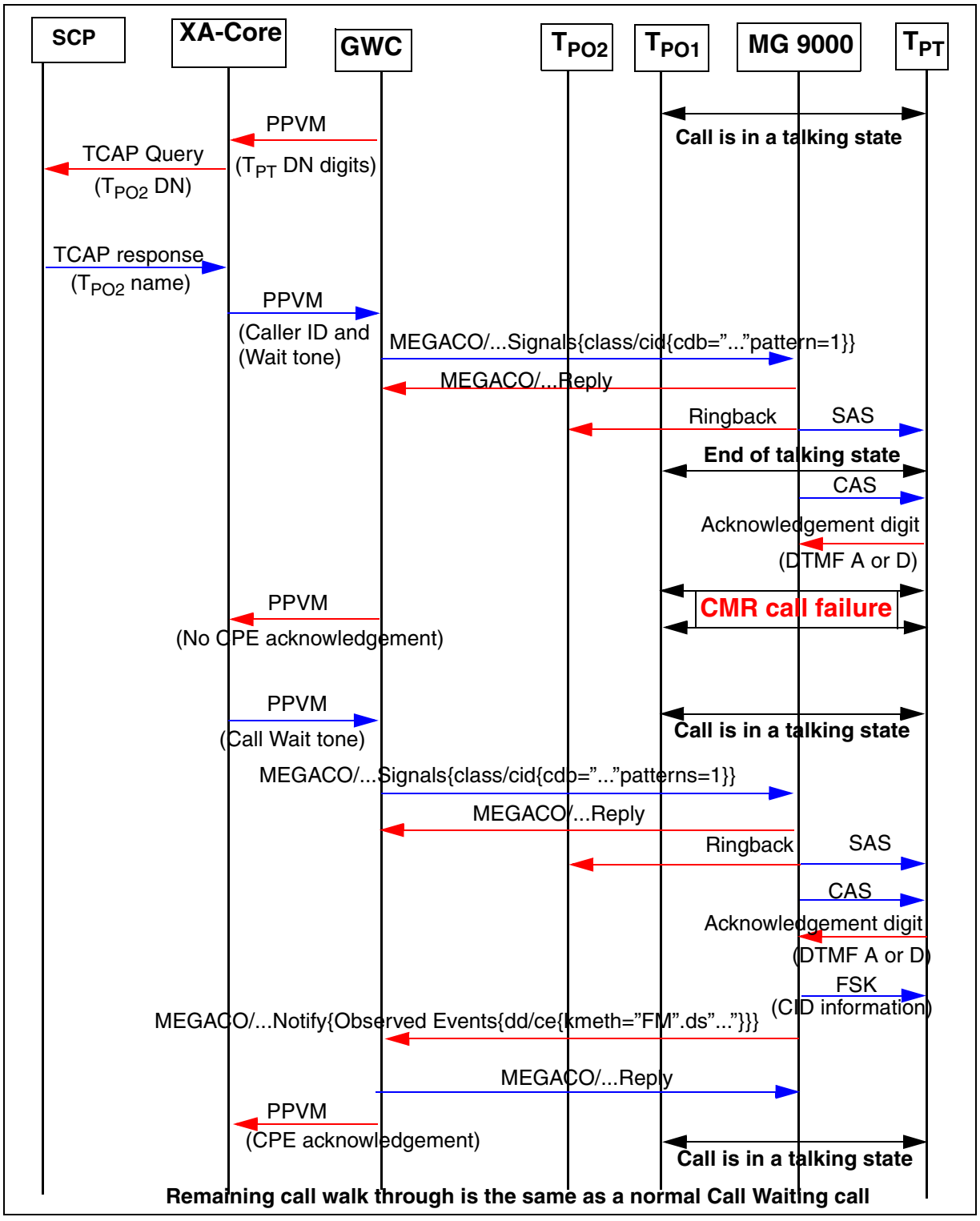
Intra MG 9000 POTS call involving SCWID



UA-IP Intra MG 9000 POTS call failure involving Spontaneous Call Waiting Identification

The figure Intra MG 9000 POTS call failure involving SCWID shows a plain old telephone service (POTS) call failure walk through for a call involving Spontaneous Call Waiting Identification (SCWID). This call originates and terminates on the same MG 9000 and uses three separate lines.

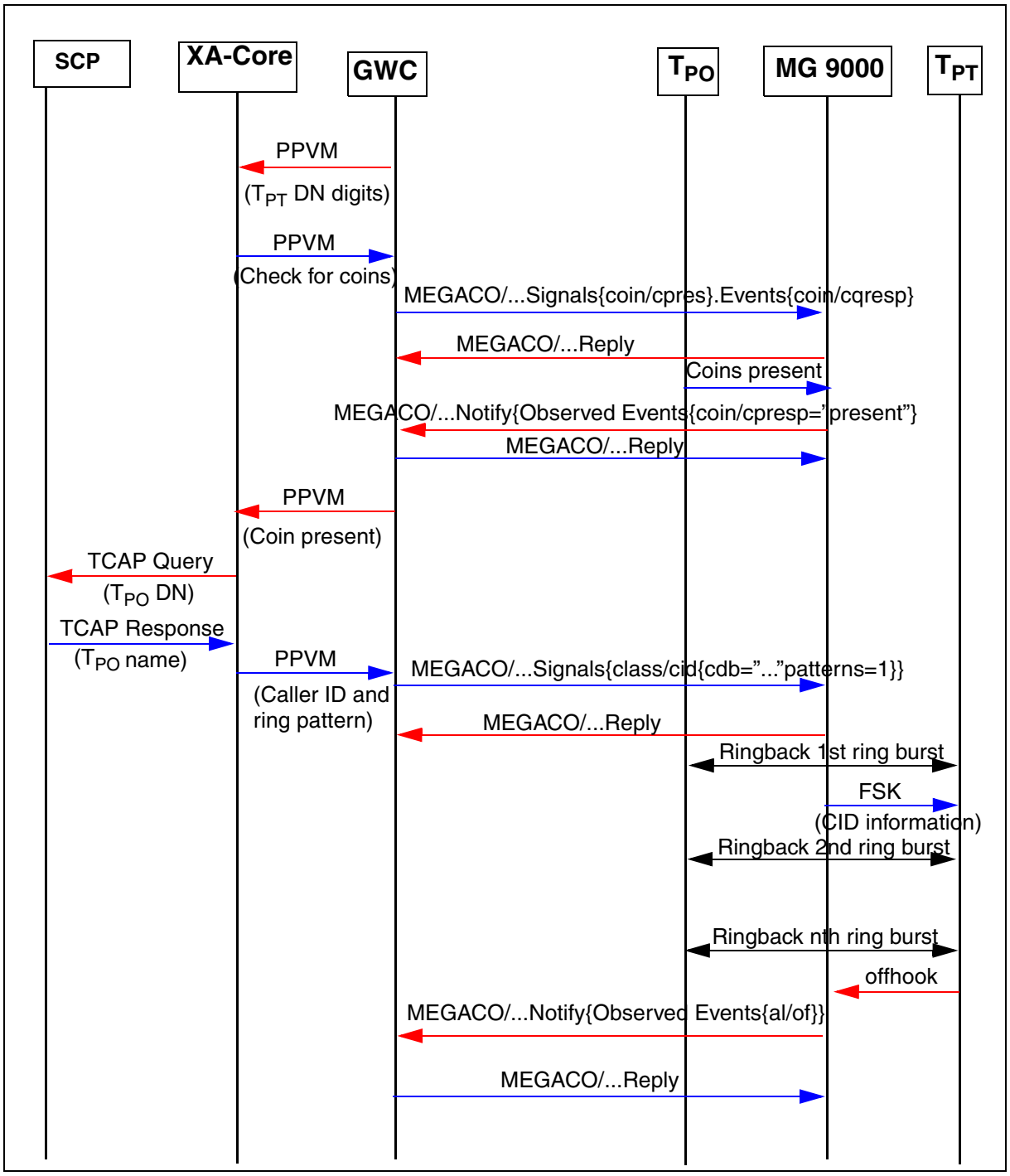
Intra MG 9000 POTS call failure involving SCWID



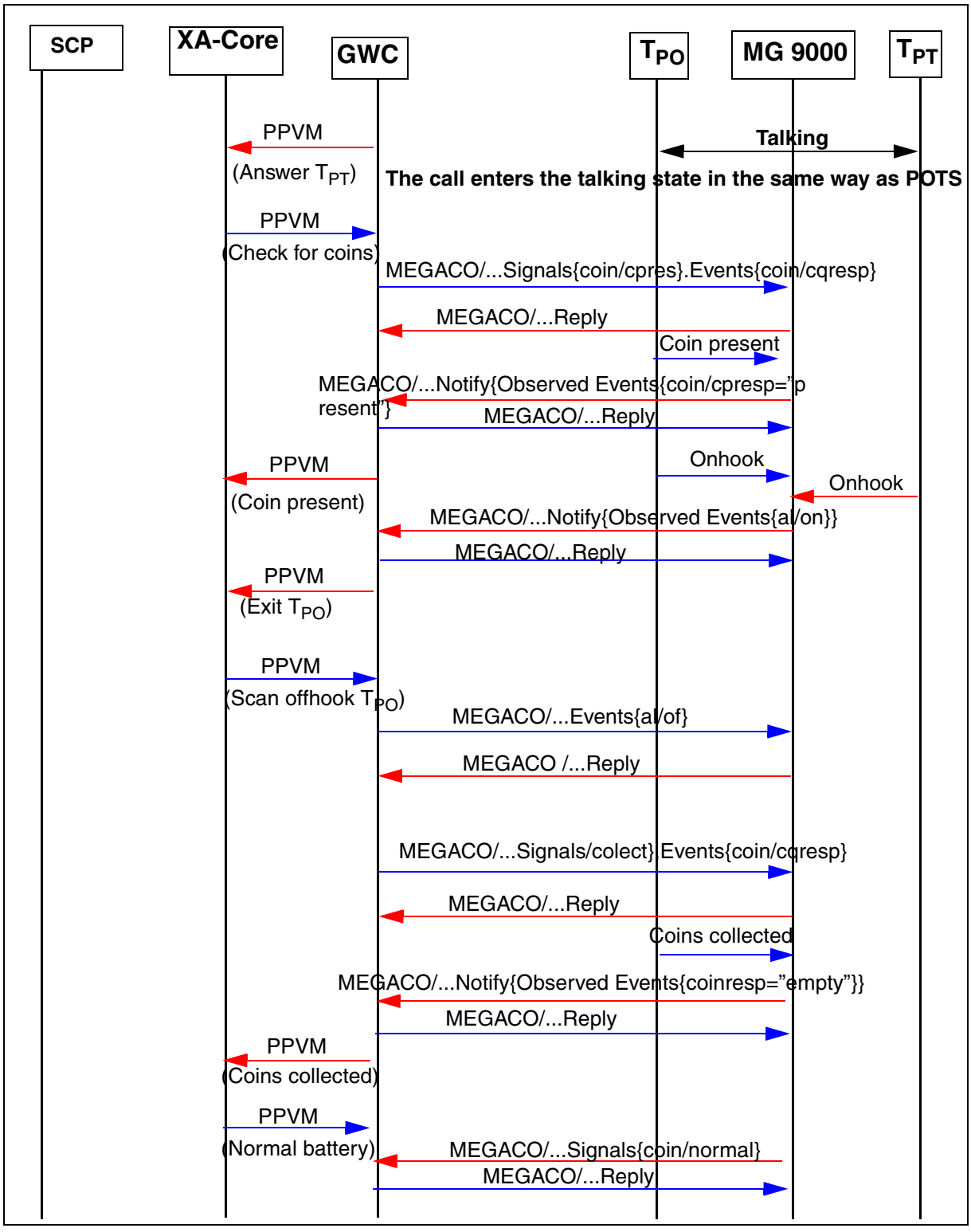
UA-IP Intra MG 9000 coin call

The figure Intra MG 9000 coin call (part 1 of 2) shows a walk through for a call that originates at a pay phone and terminates on another line on the same MG 9000.

Intra MG 9000 coin call (part 1 of 2)



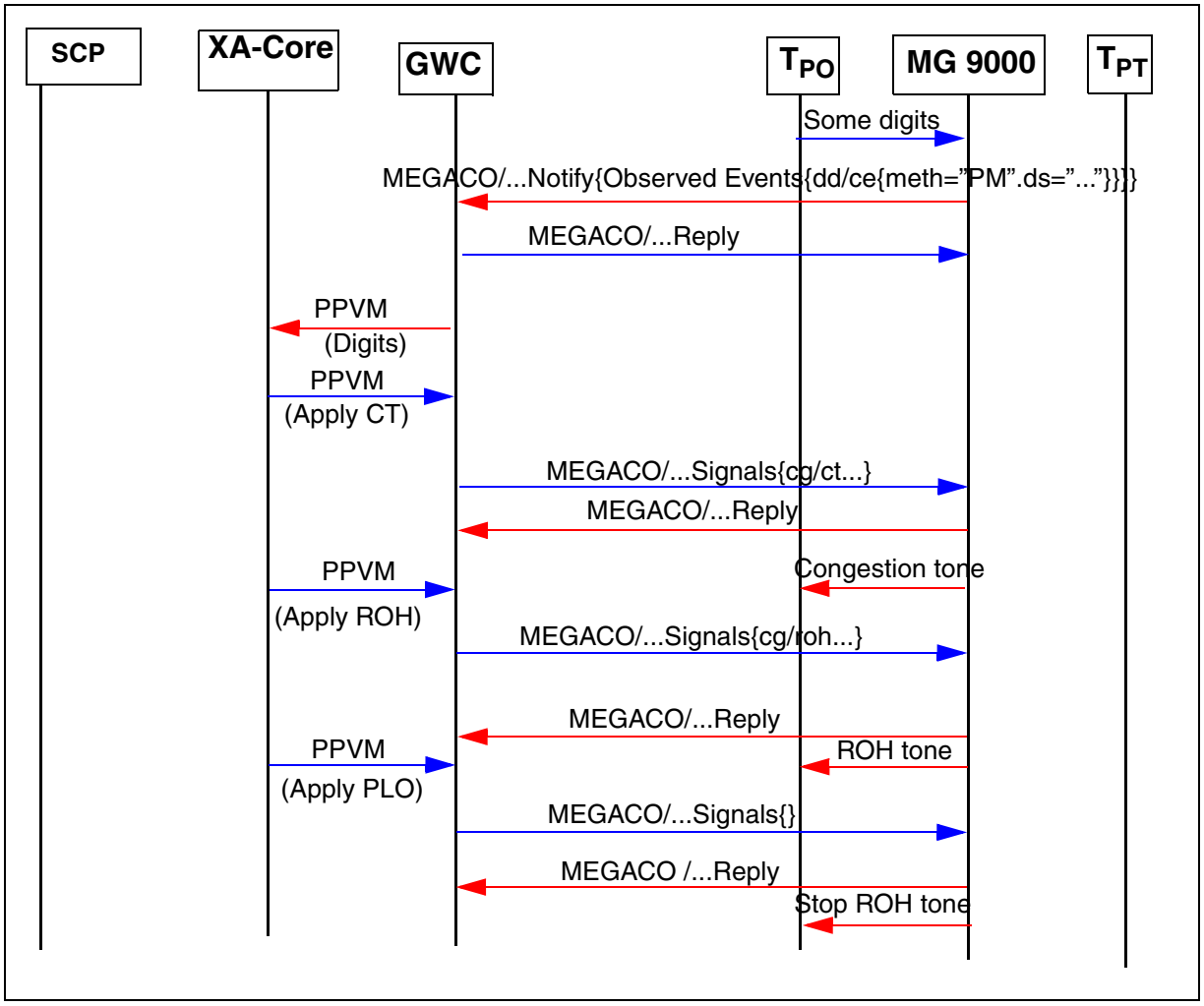
Intra MG 9000 coin call (part 2 of 2)



UA-IP Intra MG 9000 POTS call involving partial dial treatment

The figure Intra MG 9000 POTS call involving partial dial treatment shows a call walk through for a plain old telephone service (POTS) call involving a failure and partial dial treatment. This call originates and terminates on the same MG 9000 and uses two separate lines.

Intra MG 9000 POTS call involving partial dial treatment



UA-IP Intra MG 9000 call walk through involving routing to local treatment

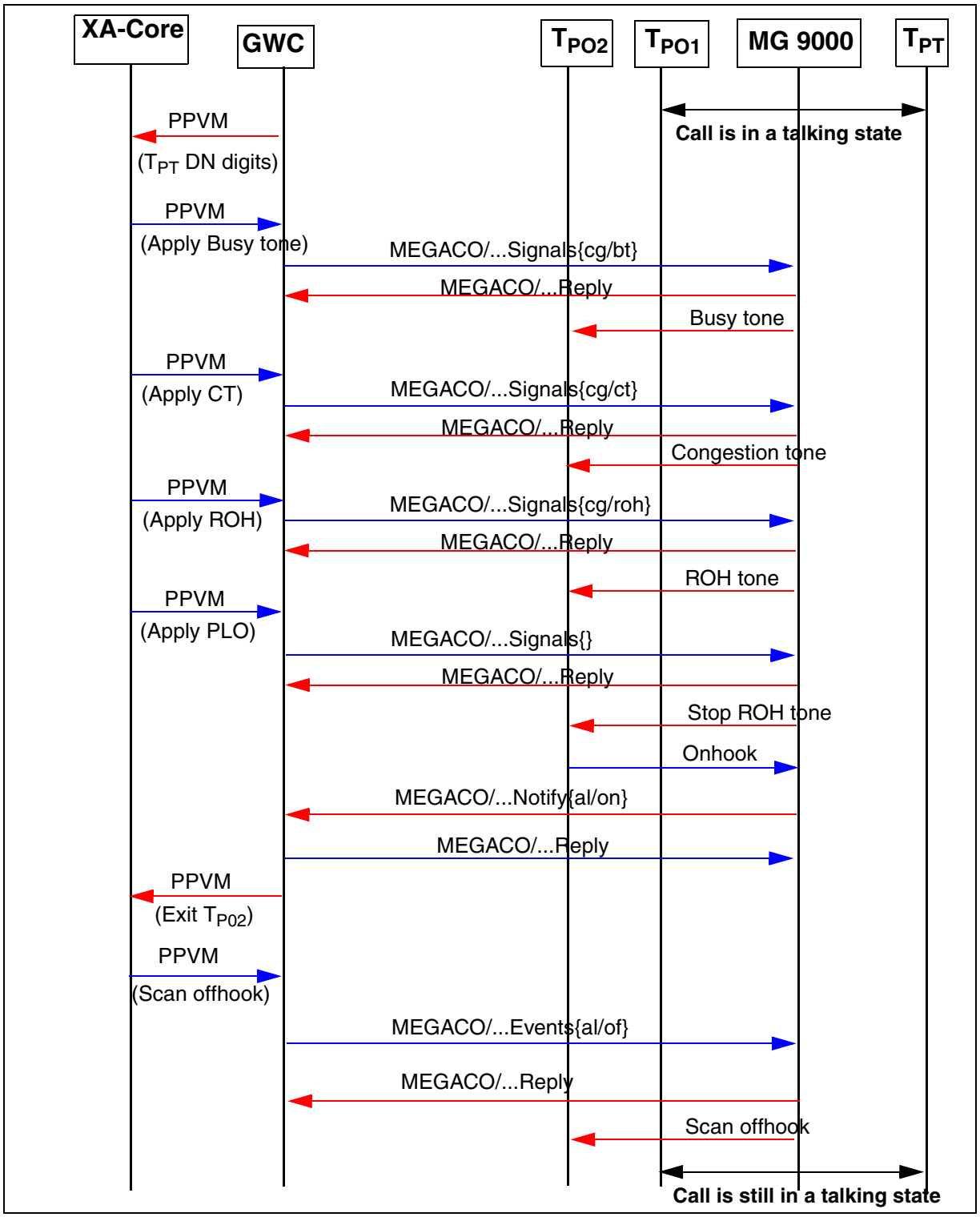
The figure Intra MG 9000 call involving routing to a local treatment shows a call walk through for a plain old telephone service (POTS) call

involving a failure and partial dial treatment. This call originates and terminates on the same MG 9000 and uses three separate lines.

Note 1: This is only one scenario for local treatment. The UA-IP system behavior of the depends on datafill. It is possible that the Congestion tone will not be requested. It is also possible, in the case of and architecture that includes the IW SPM, that ROH will not be requested.

Note 2: Timing for tones is handled in the XA-Core.

Intra MG 9000 call involving routing to a local treatment



Network interfaces and protocols for IP solutions

A Succession Network uses the following network interfaces and protocols:

Note: Proper configuration of OSS network equipment to support the management protocols is the responsibility of the customer. The OSS network requires two Ethernet connections to the CS LAN. Nortel Networks recommends that you install a fire wall on the OSS side of the Ethernet connections to the CS LAN.

ARP
ARP (address resolution protocol) is a low-level protocol within the transmission control protocol/Internet protocol (TCP/IP) suite that maps IP addresses to the corresponding Ethernet addresses.

ASPEN
ASPEN is a Nortel Networks proprietary connection control protocol used to support messaging between the GWC and the Media Gateway 15000. ASPEN is similar to media gateway control protocol (MGCP) but is more explicit and specific than MGCP.

COPS
COPS is a protocol used to support messaging between a GWC and the CMTS.

Ethernet
Ethernet is a physical link and data link protocol reflecting the two lowest layers of the DNA/OSI model.

FTP
The FTP (file transfer protocol), an IETF standard, is used to transfer software from an OSS to the CS 2000 Core Manager.

H.248
H.248 is an ITU-T standard that supports messaging between a GWC and the UAS. H.248 allows a GWC to manipulate terminations on the UAS, and Multiservice Switch 15000/7400.

ICMP
ICMP (Internet control message protocol) is a network-layer control protocol that provides message packets to report errors and other information relevant to IP packet processing.

IP
IP (Internet protocol) is a standard describing software that keeps track of the Internet's addresses for different nodes.

IPSec
IPSec (IP Security) is the security protocol used in the IAC solution to secure communication between the GWC, MTA, CMTS, and Trunk Media Gateway

ISUP
Integrated services digital network user part (ISUP) is a sub-protocol of SS7. ISUP provides for transfer of call setup signaling information between signaling points.

IUA
IUA is a protocol that supports messaging between a GWC and a Media Gateway 15000.

M3UA
M3UA is a protocol that support messaging between a GWC and the USP.

MTP
Message transfer part (MTP) is a sub-protocol of SS7. MTP provides functions for basic routing of signaling messages between signaling points.

NCS
NCS is a protocol that supports messaging between a GWC and an MTA.

NTP
NTP (network time protocol) maintains a common sense of time among Internet hosts around the world.

OSPFIGP
Open shortest path first Internet gateway protocol (OSPFIGP) is a replacement for routing information protocol (RIP).

PPVM
Peripheral processor virtual machine (PPVM) is a proprietary Nortel Protocol used for messaging between the XA-Core (or Call Agent) and components such as the IW SPM-IP, CS 2000 Core Manager.

RTCP
Real time control protocol (RTCP) is a protocol that supports messaging between a Media Gateway 15000 and UAS. In the PT-IP solution the IW SPM-IP also supports RTCP.

RTP
Real-time Transfer Protocol is an IETF standard for streaming real-time media over IP in packets. RTP supports transport of real-time data such as voice and video over packet switched networks. RTP supports messaging between a Media Gateway

15000 and UAS. In the PT-IP solution the IW SPM-IP also supports RTCP.

SCCP

Signaling connection control part (SCCP) is a sub-protocol of SS7. SCCP provides additional routing and management functions for transfer messages (other than call setup) between signaling points.

SCTP

SCTP is a protocol that supports messaging between a GWC and a Media Gateway 15000.

SIP

Session Initiation Protocol (SIP) is a signaling protocol for Internet conferencing, telephony, presence, events notification and instant messaging. The Session Server Manager is used to convert open interop SIP messaging into messages understandable by the CS 2000.

SIP-T

Session Initiation Protocol for Telephony (SIP-T) is an application layer control (signaling) protocol for creating, modifying, and terminating sessions with one or more participants. SIP-T supports communication between peer communication servers by encapsulating and transparently conveying SS7 signaling and complementary session description protocol (SDP) session descriptions using Multipurpose Internet Mail Extensions (MIME) mechanism. CS 2000 (or CS 2000 - Compact) uses SIP-T to negotiate connections between GWCs, between GWCs and a GWC Virtual Router Distribution Node (VRDN), between GWC VRDN and GWC VRDN, and between a GWC VRDN and other CS 2000.

SNMP

SNMP (simple network management protocol) is used by network management applications to query a management agent using a supported MIB (management information base).

SS7

Signaling System 7 (SS7) is a family of signaling protocols used to set up, manage and tear down connections, as well as to exchange non-connection associated information.

STP

Spanning tree protocol (STP) supports self-learning, filtering, security and automatic reconfiguring of routers and bridges.

TCAP

Transaction capabilities application part (TCAP) is a sub-protocol of SS7. TCAP provides the signaling function for network

databases. TCAP is an ISDN application protocol. TCAP supports non-circuit related transaction based information exchange between SS7 network entities. TCAP is used for the exchange of information outside the context of a call or connection.

TCP

TCP (transmission control protocol) is a transport-layer connection oriented, end-to-end protocol. It provides reliable sequenced and unduplicated bytes to a remote or local user.

Telnet

Telnet, an IETF standard, is used for remote access to the Preside CS 2000 Core Manager.

TFTP

The TFTP (trivial file transfer protocol), an IETF standard, is used to transfer the software loads.

TGCP

The Packetcable TGCP (trunk gateway control protocol) is used in the IAC solution for communication between the GWC and Trunk Media Gateway.

UDP

UDP (user datagram protocol) is a TCP/IP protocol describing how messages reach application programs within a destination computer.

VRRP

Virtual router redundancy protocol (VRRP) allows the two Passport 8600 chassis to share a single IP address.

Network physical interfaces and protocols for IP solutions

This section identifies the physical interfaces and protocols that are associated with each of the components that together make up the PT-IP solution.

CS 2000 physical interfaces

There are two 10/100 Base-T Ethernet links running from the High Performance I/O Processor (HIOP) cards (of the CS 2000) to the CS LAN. Each Ethernet link connects to a different Passport 8600. Ten IP addresses are required.

In addition to the Ethernet interfaces, the XA-Core is connected to both Message Switch (MS) by dual OC-3 connections. Each MS has several DS512 port interfaces. Two of these DS512 interfaces are used to interface to each FLPP unit. An additional DS512 pair is used to interface to the CS 2000 Core Manager on the SDM platform.

Protocols supported by the CS 2000

The CS 2000 uses the proprietary Peripheral Processing Virtual Machine (PPVM) protocol to communicate call control information to the GWCs.The GWCs convert these messages (from the CS 2000) to the open standard protocols that media gateways use.

CS 2000 - Compact physical interfaces

There are two 10/100 BaseT Ethernet links running from the Call Agent of the CS 2000 - Compact to the CS LAN. Each Ethernet link connects to a different Passport 8600.

Protocols used by the CS 2000 - Compact

The CS 2000 - Compact uses the proprietary Peripheral Processing Virtual Machine (PPVM) protocol to communicate call control information to the GWCs.The GWCs convert these messages (from the CS 2000 - Compact) to the open standard protocols that media gateways use. The CS 2000-Compact also supports SMDI over TCP/IP for Message Waiting Indication for Voice Mail.

GWC physical interfaces

There are two 10/100 BaseT Ethernet links running from each GWC pair to the CS LAN. Four IP addresses are required for each GWC pair. There is a maximum of eight GWC pairs for each SAM21. Each shelf controller unit (SCU) card has one 10/100 BaseT Ethernet link to the CS LAN. Four IP addresses are required for each SCU pair. You can equip a maximum of two SCUs for each SAM21 shelf.

Protocols supported by GWCs

H.248 and media gateway control protocol (MGCP) are used by the GWC for communication and control messages to and from the UAS. ASPEN, H.248, and IUA protocols support messaging between a GWC and Media Gateway 15000. SIP-T supports messaging between GWCs. SNMP is supported for OAM&P functions between GWCs and GWC Manager and PM Poller. SCTP supports messaging between two GWCs, and between GWC and Media Gateway 15000. M3UA supports messaging between a GWC and USP. NCS is a protocol that supports messaging between the GWC the MTA. COPS is a protocol that supports messaging between the GWC and the CMTS.

Session Server interfaces

The SAM-XTS is configured with 4 Gigabit Ethernet ports. Each Session Server is configured with two 1000Mbs/100Mbs/10Mbs (depending on the IP router configuration) interfaces directed to the LAN switch. In addition, two interfaces connect unit 0 to unit 1.

Protocols supported by the Session Server

The Session Server supports SNMP V3 with “No Privacy” and “No Authentication” options. Additionally , the following protocols are supported to provide access to the server:

- SFTP or SCP
- SSH, including
  - 3DES 168 bits
  - Blowfish 128 bits
  - Twofish 128 bits
  - AES 128 bits
- HTTP
- HTTPS

Universal Audio Server physical interfaces

The Universal Audio Server (UAS) has redundant 10/100 BaseT Ethernet interface links to the CS LAN from each NMS CG6000 card (on the UAS). In addition, there are redundant 10/100 BaseT Ethernet links (to the CS LAN) from the CPV5370 processor cards on the UAS. There are also redundant 10/100 BaseT Ethernet links from the Audio Provisioning Server (APS) to the CS LAN.

Protocols supported by the UAS and APS

The UAS supports the media gateway control protocol (MGCP) and H.248 protocol for call control messages sent between the UAS and the

GWC. The GWC acts a protocol converter for the call control messages that originate on the CS 2000 or CS 2000 - Compact. MGCP enables external control and management of media gateways by call agents running on GWCs. The MGCP messaging interface translates MGCP messages that are sent from the call agent to the UAS. In addition the MGCP messaging interface builds MGCP messages to be sent from the UAS to the call agent on the GWC.

Simple network management protocol (SNMP) is supported by both CS 2000 Management Tools and the UAS in order to implement fault management, configuration management, and performance management.

Real time protocol (RTP) or real time control protocol (RTCP) are supported by the UAS in order to transmit audio between the UAS and the bearer channel network.

Network file system (NFS) protocol is supported by both the UAS and APS and is used to transfer audio files (stored on the APS) to the UAS.

MS 2010 physical interfaces

The MS 2010 uses redundant 10/100 BaseT Ethernet to connect to the CS LAN. Each pair of interfaces uses one IP address and operates in active/standby mode. There are also redundant 10/100 BaseT Ethernet links from the Audio Provisioning Server (APS) to the CS LAN.

Protocols supported by the MS 2010

The MS 2010 uses H.248 to transmit call control signals over the packet network.

Real Time Protocol/Real Time Control Protocol (RTP/RTCP) is used by the MS 2010 to transmit audio on the bearer network.

Universal Signaling Point physical interfaces

The 10/100 BaseT Ethernet links from the USP to the CS LAN are provisioned based on the amount of traffic. Normally these links are engineered in mated pairs. USP SS7 links are also provisioned according to traffic, and engineered in mated pairs. USP supports DS0 or DS1 links to the SS7 network.

Protocols supported by USP

On the SS7 side of the USP, the supported protocols are SS7, MTP, SCCP, TCAP, ISUP. On the CS LAN-side of the USP, the supported protocol is M3UA for messaging between a GWC and the USP.

Media Gateway 15000 physical interfaces

There is a 10/100 BaseT Ethernet link to the CS LAN from each CP3 card on the Media Gateway 15000. OC-3c, or OC-12, and Gigabit Ethernet interfaces to the packet network are supported. DS3, or OC-3 interfaces are supported on the TDM-side.

The UA-IP solution now supports DS3 connectivity to the Nortel Networks Media Gateway 15000 Core using a channelized OC3 interface and a fiber network that multiplexes/demultiplexes DS3 traffic. Nodal Provisioning templates are available to provision the DS3 interface for connectivity between a Media Gateway 15000 and a Media Gateway 9000 over the fiber network.

Protocols supported by Media Gateway 15000

ASPEN, SCTP, IUA, and H.248 support messaging between GWCs and Media Gateway 15000s. RTP and RTCP support the transmission of audio (from the UAS) on the bearer traffic network.

Media Gateway 7400 physical interfaces

There are asynchronous transfer mode (ATM) interfaces from the VSP2 card of the Media Gateway 7400. In addition, there is a 10/100 BaseT Ethernet link to the CS LAN.

Protocols supported by Media Gateway 7400

ASPEN, SCTP, IUA, and H.248 support messaging between GWCs and Media Gateway 7400s. RTP and RTCP support the transmission of audio (from the UAS) on the bearer traffic network.

MG 9000 physical interfaces

The MG9000 is equipped with SuperCore data control cards that can be configured to support either an OC3c optical network interface with APS (Automatic Protection Switching) or a DS1 IMA copper network interface with the data stream split across 2 to 8 DS1 spans.

In SN07, Channelized OC-3 capability was added in addition to the OC-3c and DS-1 IMA. The Channelized OC-3 allows the MG 9000 to provide a single STS-1 (or DS-3) rate of traffic over the network.

Protocols supported by the MG 9000

The following protocols supported by the MG 9000: IMA1.0, ITU H.248, ATMF UNI 4.0, SNMP 2.0.

Passport 8600 physical interfaces

The Passport 8600 terminates all 10/100 BaseT Ethernet links, and all Gigabit Ethernet links from other components on the CS LAN. In

addition, Passport 8600 supports Gigabit Ethernet links to the backbone packet network.

Protocols supported by Passport 8600

Passport 8600 supports Ethernet, virtual router redundancy protocol (VRRP), and spanning tree protocol (STP).

IW SPM-IP physical interfaces

IW SPM-IP is an ENET-hosted SPM that has four C-side DS512 links connecting the common equipment module (CEM) of the IW SPM-IP to the enhanced network (ENET). On the P-side (facing the packet network) the IW SPM-IP has two Gigabit Ethernet links to Passport 8600s in the CS LAN.

Note: IW SPM-IP is only used in the PT-IP solution.

Protocols supported by IW SPM-IP

PPVM for communication with the XA-Core. RTP, and RTCP for bearer connections between IW SPM-IP and Media Gateway 15000 (or 7400), and between IW SPM-IP and the UAS.

CS 2000 Core Manager physical interfaces

The CS 2000 Core Manager (on the SDM platform) terminates four DS512 links to the message switch (on the CS 2000). In addition the CS 2000 Core Manager terminates two 10/100 BaseT Ethernet links to the CS LAN.

Protocols supported by CS 2000 Core Manager

The following protocols are used on the Ethernet path from the CS 2000 Core Manager to the OSS: IP, ICMP, SNMP, ARP, TCP, FTP. The following protocols are used on the Ethernet path from the CS 2000 Core Manager to the Preside MDM: IP, ICMP, TCP, ARP, CORBA, FTP.Peripheral processor virtual machine (PPVM) is a proprietary Nortel Protocol used for messaging between the XA-Core and the CS 2000 Core Manager.

Core and Billing Manager physical interfaces

The Core and Billing Manager (CBM) connects to the CS 2000 through Ethernet links on the XA-Core high-performance input-output processor (HIOP). The CBM connects to the CS 2000-Compact through the CS 2000-Compact's Ethernet interface.

Protocols supported by the Core and Billing Manager

The following protocols are used on the Ethernet path from the CBM to the CS 2000: IP, ICMP, SNMP, ARP, TCP, FTP. The following protocols

are used on the Ethernet path from the CBM to the CS 2000-Compact: IP, ICMP, TCP, ARP, CORBA, FTP.

Preside MDM physical interfaces

Normally a pair of Preside MDM are used for the purpose of redundancy. Each Preside MDM has the following interfaces:

- one 10/100 BaseT Ethernet link to the CS LAN
- one 10/100 BaseT Ethernet link to the mate Preside MDM

Protocols supported by Preside MDM

The following protocols are used on the Ethernet path from the Preside MDM to the OSS: IP, TCP, ICMP, FTP, ARP.

IP hardware

This section provides a brief description of the hardware of each of the major components in the IP solutions. The table IP components and sources for detailed hardware information lists the components described in this section and indicates the documents where you can find additional information.

IP components and sources for detailed hardware information (Sheet 1 of 3)

Network element		Where to find additional information
CS 2000		Communication Server 2000 Basics, NN10197-111
	XA-Core	Communication Server 2000 Basics, NN10197-111
	Message switch	Communication Server 2000 Basics, NN10197-111
	FLPP	Communication Server 2000 Basics, NN10197-111
	CS LAN	Installing Passport 8600 Switch Modules, 312749-F
	CS 2000 SAM21	SAM21 Shelf Controller Basics, NN10025-111
	CS 2000 GWC	GWC Basics, NN10189-111
	Session Server	Session Server Basics, NN10333-111
	UAS	UAS Basics, NN10010-111
	MS 2010	MS 2000 Series Basics, NN10323-111
	APS	UAS Basics, NN10010-111 and MS 2000 Series Basics, NN10323-111
	USP	USP Basics, NN10008-111
CS 2000 - Compact		CS 2000 - Compact Basics, NN10021-111
	Call Agent	Call Agent Basics, NN10023-111

IP components and sources for detailed hardware information (Sheet 2 of 3)

Network element		Where to find additional information
	STORM	STORage Management Basics, NN10024-111
	CS 2000 SAM21 (CS 2000-Compact)	Call Agent Basics, NN10023-111
	CS 2000 GWC (CS 2000-Compact)	GWC Basics, NN10189-111
	Session Server (CS 2000-Compact)	Session Server Basics, NN10333-111
	USP - Compact	USP Basics, NN10008-111
	UAS (CS 2000-Compact)	UAS Basics, NN10010-111
	MS 2010 (CS 2000-compact)	MS 2000 Series Basics, NN10323-111
	APS (CS 2000-Compact)	UAS Basics, NN10010-111 and MS 2000 Series Basics, NN10323-111
	CS LAN (CS 2000-Compact)	Passport 8600 Software Upgrade, NN10235-461
IW SPM-IP		IW SPM-IP Basics, NN10181-111
Media Gateway 7400/15000		Nortel Networks Media Gateway 7480/15000 Technology Fundamentals, NN10600-780
	Media Gateway 7400 frame and chassis	Nortel Networks Media Gateway 7480/15000 Technology Fundamentals, NN10600-780
	Media Gateway 15000 frame and chassis	Nortel Networks Media Gateway 7480/15000 Technology Fundamentals, NN10600-780
MG 9000		MG 9000 Basics, NN10011-111
CS 2000 Core Manager		CS 2000 Core Manager Basics, NN10018-111

IP components and sources for detailed hardware information (Sheet 3 of 3)

Network element	Where to find additional information
Core and Billing Manager	Core and Billing Manager Basics, NN10355-111
CS 2000 Management Tools	Solution Basics
CS 2000 SAM21 Manager	Solution Basics and SAM21 Shelf Controller Basics, NN10025-111
Session Server Manager	Session Server Basics, NN10333-111
USP and USP-Compact manager	USP Basics, NN10008-111(documentation on the USP (and USP Compact) includes information about the USP Manager)
MG 9000 Manager	MG 9000 Basics, NN10011-111 (documentation on the MG 9000 includes information about the MG 9000 Manager)
Preside MDM	Preside MDM Overview, 241-6001-801
Device Manager	Passport 8600 Software Upgrade, NN10235-461 (documentation on the Passport 8600 includes information on the Device Manager.)
CICM	CICM Basics, NN10044-111
Secondary Power Distribution Center	Nortel Networks Engineering Change (EC) 101-08295

CS 2000

The table Principal CS 2000 components that follows lists the principal components that make up the CS 2000 solution.

Principal CS 2000 components

Description	PEC
extended architecture core (XA-Core) including: • processor element (PE) circuit cards • shared memory (SM) circuit cards • input/output processor (IOP) circuit cards	NTLX01
message switch (MS)	NT9X63
fiberized link peripheral processor (FLPP)	NT9X70
Services Application Module (SAM21) with gateway controller (GWC)	NTRX51

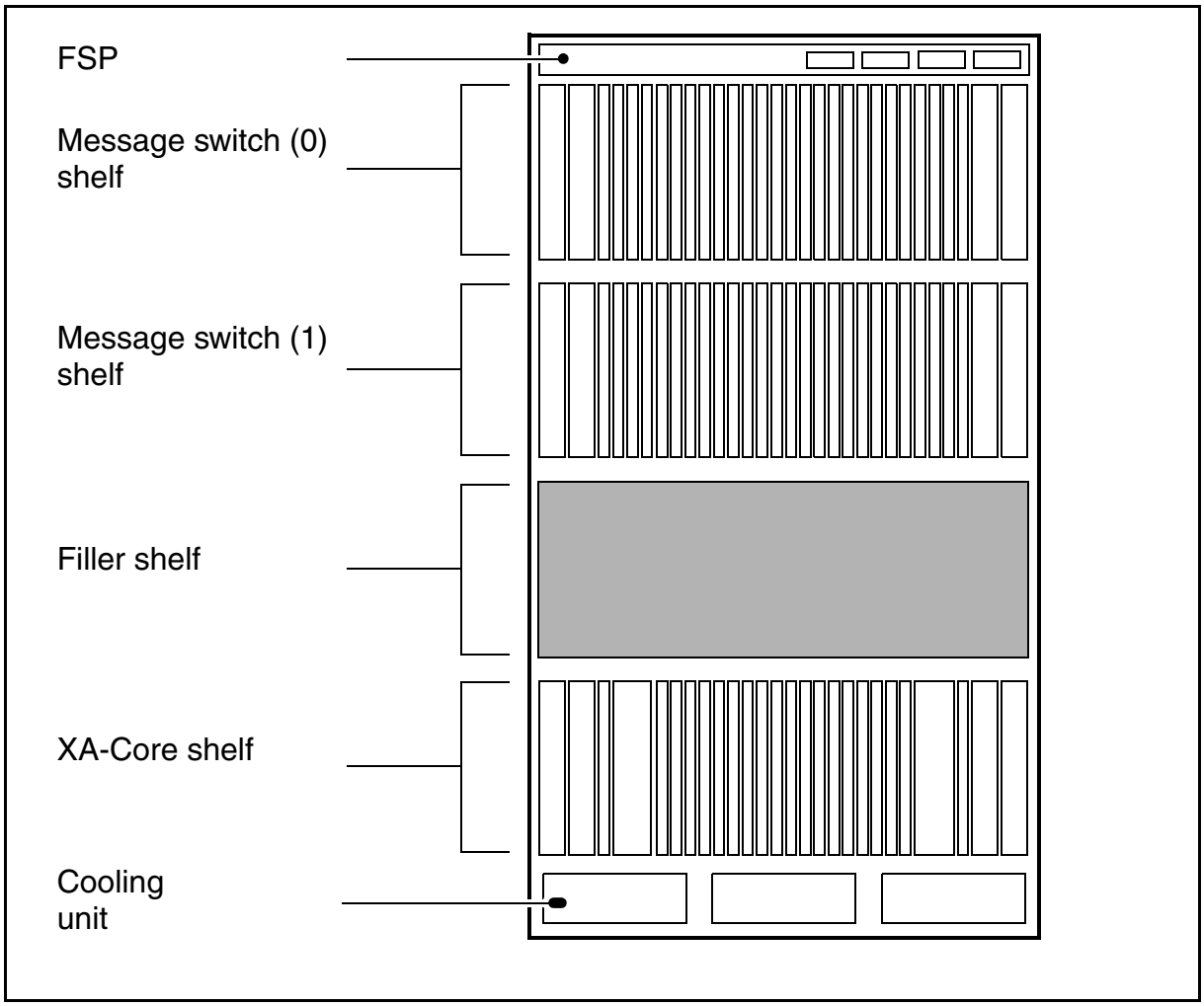
Note 1: The solution engineering code (PEC) identifies Nortel Networks solutions.

Note 2: CS 2000 principal components together with selected TDM-Core components, the SDM (which is part of Preside MSS), and the PP8600 together form the CS 2000 complex.

XA-Core

The extended architecture core (XA-Core) is the CS 2000 call processing component that controls signaling gateway and media gateway functionality. The XA-Core is a high-performance, multiprocessing, compute engine that is completely scalable in terms of processing, memory, and input/output capability. Adjusting the capacity of the system or adding another interface is as simple as plugging in a new circuit pack. The XA-Core shelf contains Processor Element circuit packs (PE), input Output Processor circuit packs (IOP), and Shared Memory circuit packs (SM). The XA-Core resides in an XA-Core SuperNode cabinet. The figure XA-Core frame shows the XA-Core cabinet for a greenfield application.

XA-Core frame



Message switch

The message switch (MS) is a communications bus that provides peer to peer messaging between the distributed CS 2000 components. The MS is made up of two identical load sharing planes (MS 0 and MS 1). Each MS plane provides a system clock and supports the full internal CS 2000 messaging load.

FLPP

The CS 2000 fiberized link peripheral processor (FLPP) includes the following components:

- up to three link interface shelves (LIS) that each support up to 12 slot-mounted CCS7 link interface units (LIU7)
- a link interface module (LIM) that includes two load-sharing local message switches (LMS).
- F-buses that support direct high-speed communication between CCS7 link interface units

The CCS7 link interface units (LIU7) within the FLPP use SR 128 sub-rate fiber links to connect the CS 2000 to the SS7 network. These links provide a V.35 interface to an CCS7 signaling multiplexer. Each interface can support three 64 kbps SS7 links.

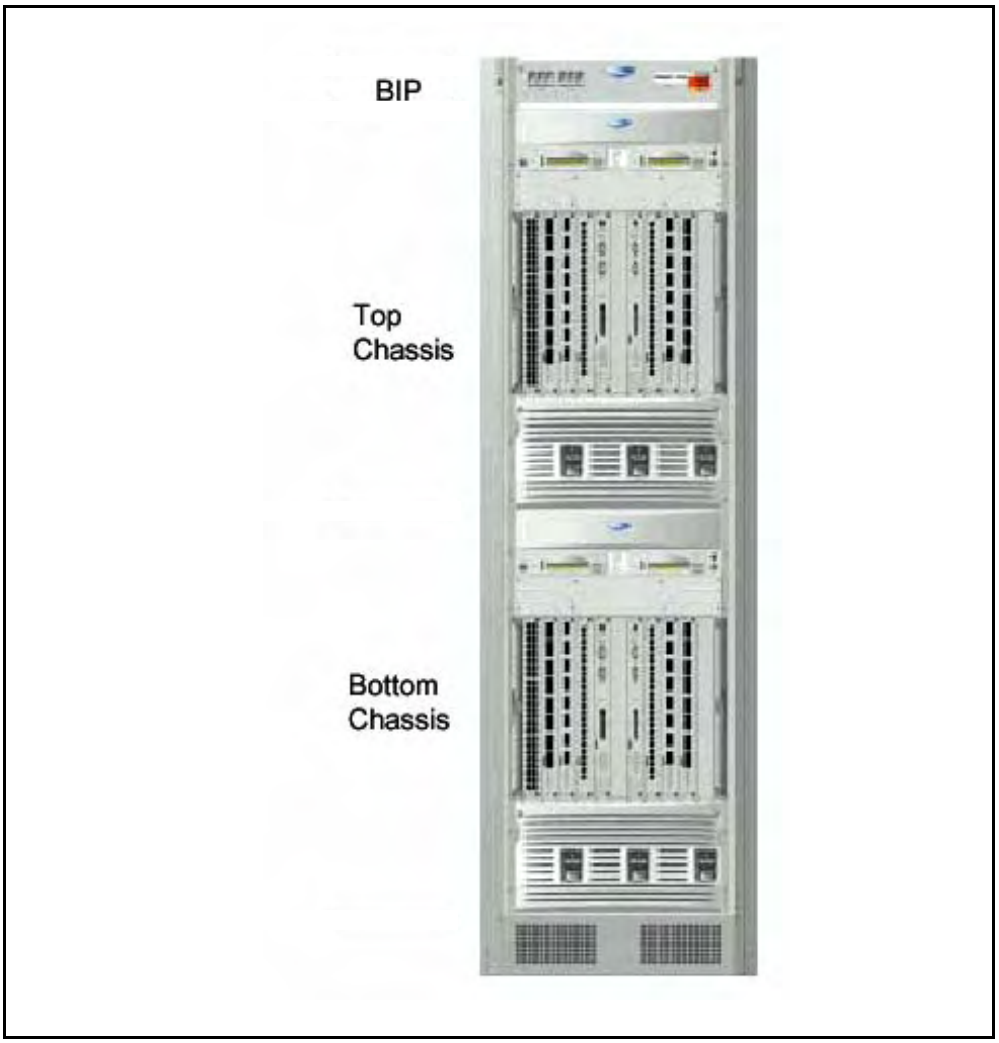
FLPPs also support TCP/IP over Ethernet links that comply with IEEE 802.3.

CS LAN

The Communication Server LAN (CS LAN) consists of duplicated Passport 8600s mounted in one or two NTJS20AA PTE2000 frames The Passport 8600s use the NEBS compliant 8010co chassis. A configuration with two Passport 8600s in a frame is shown in the figure PTE2000 frame with two Passport 8600s

The 8010co chassis is a 10 slot chassis with vertical slots for Passport 8600 modules. The modules of the Passport 8600 consist of the CPU/Switch Fabric (CPU/SF) module and various I/O modules. All packet switching occurs on the switch fabric, while the I/O modules perform buffering, address resolution, traffic classification, and provides the physical layer interface to the network. Eight slots (1 through 4 and 7 through 10) are available for interface modules and slots 5 and 6 are reserved for CPU/Switching Fabric modules.

PTE2000 frame with two Passport 8600s



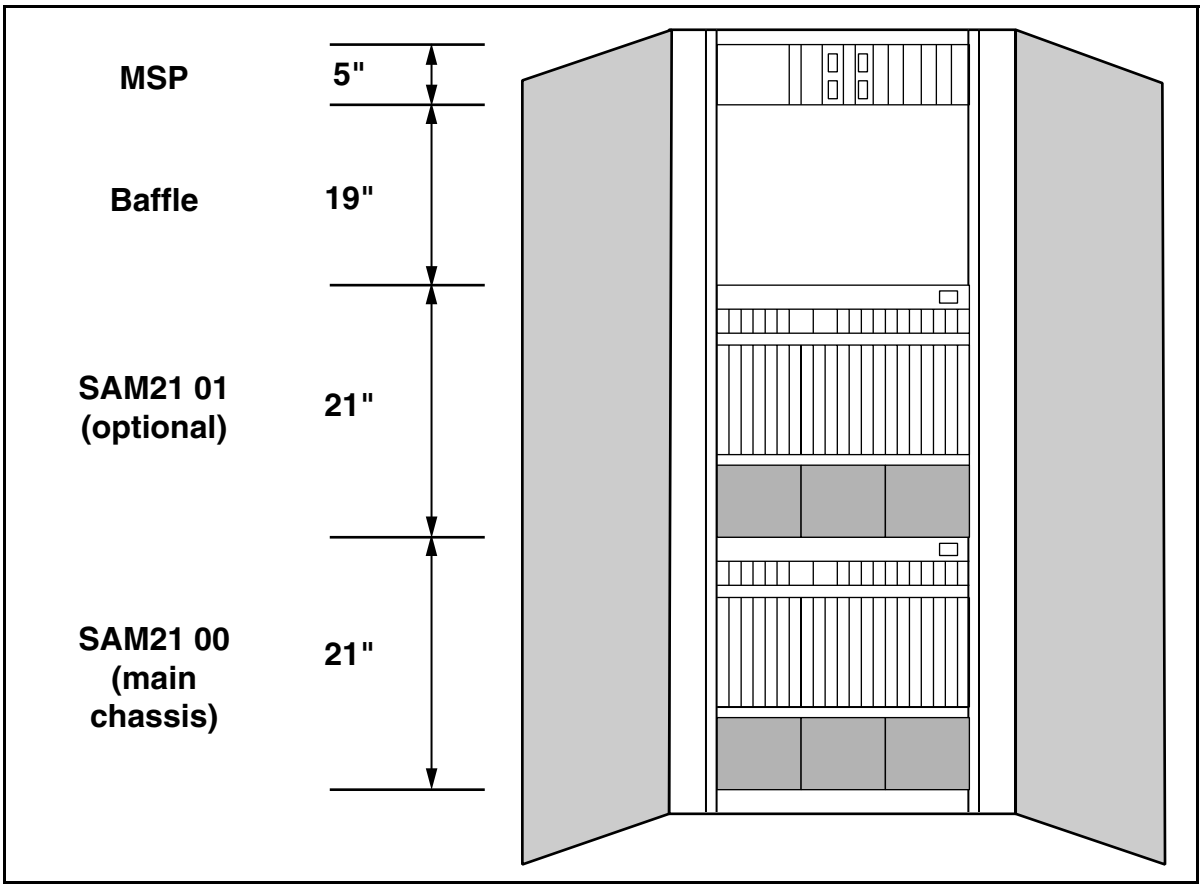
CS 2000 SAM21

The Cabinetized Services Application Module (CSAM) consists of one or two Services Application Module (SAM21) shelves mounted in a Nortel Networks C28 Model B (C28B) cabinet.

The SAM21 shelf has 21 chassis slots. The platform for the SAM21 shelf is the Motorola CPX8221 cPCI. Two slots are dedicated for MCP750HA PowerPC (PPC) Shelf Controller (SC) cards and two for hot swap controllers (HSC).

Figure Cabinetized Services Application Module shows a block diagram of a CSAM configured with an optional expansion shelf.

Cabinetized Services Application Module



If the SAM21 shelf is deployed in a CS 2000 - Compact configuration, the SAM21 shelf does not reside in a CSAM cabinet, it resides in the Call Control Frame. Refer to the *Call Agent Basics*, NN10023-111 for more information.

CS 2000 GWC

The Gateway Controller (GWC) acts as a protocol converter to create a bridge between media gateways and the call processing function provided by the CS 2000 XA-Core. To perform this function the GWC converts between proprietary Peripheral Processing Virtual Machine (PPVM) messages that the XA-Core uses and the open standard protocols that media gateways use. This conversion makes media gateways appear to the XA-Core like standard TDM call processing, messaging, and control peripherals.

Note: GWCs allow service providers to select the most appropriate media gateways for their specific business applications.

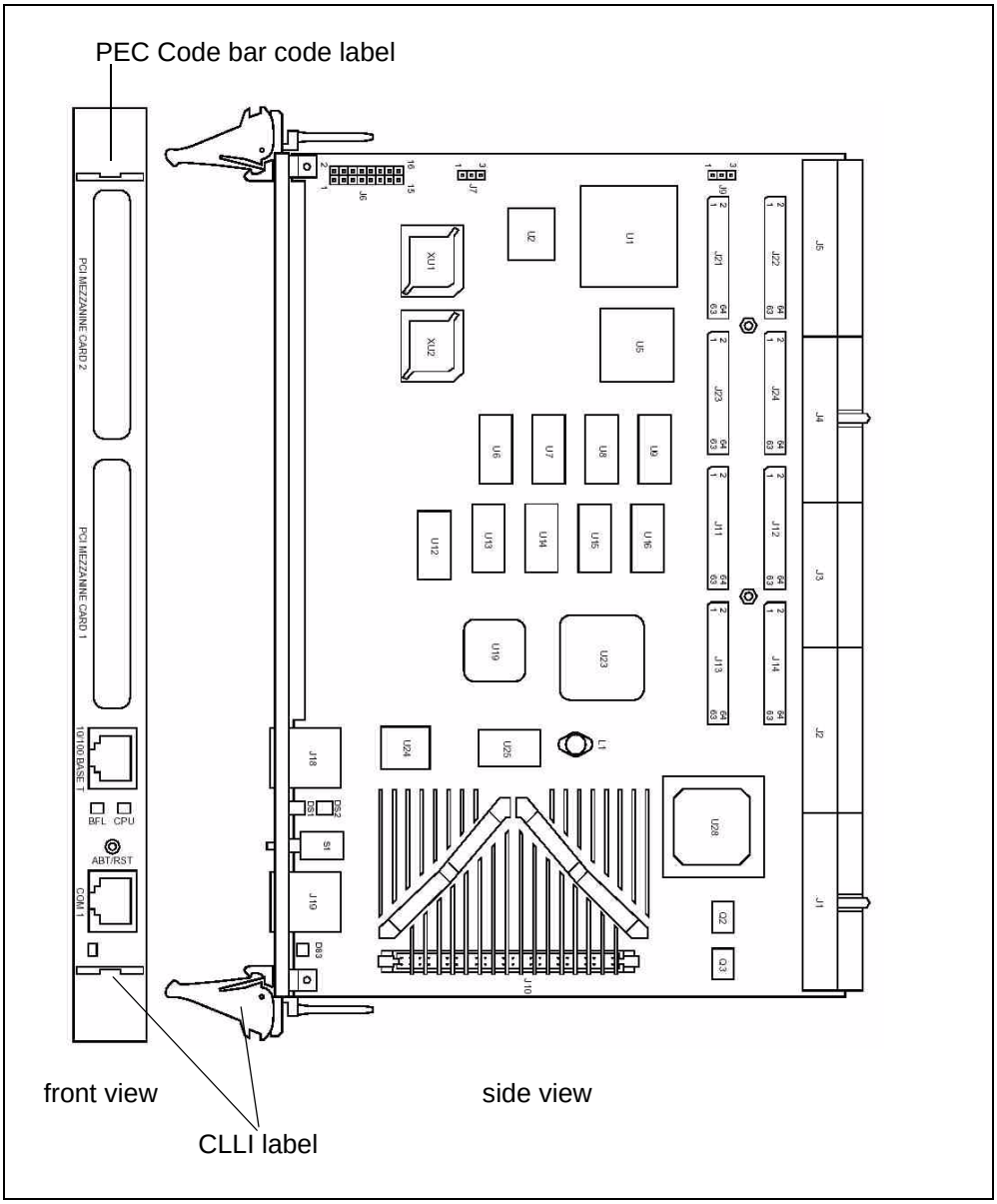
The GWC is based on the Motorola MCPN750 single board computer (SBC). Two redundant SBCs make up each GWC node. The SBCs are usually housed, side by side in the Services Application Module (SAM) CPX8221 compact personal computer interface (cPCI) chassis. This 21-slot chassis is referred to as the SAM21. One SBC card, unit 0 is active while the other card, unit 1, is in hot standby mode, ready to take over should the active card fail or when a manual action such as a SWACT is performed.

In addition to providing an XA-Core to media gateway interface, GWCs support communication between peer communication servers. This capability handles inter-MGC, networked calls using packet network protocols.

The GWC circuit cards host the gateway controller software that, together with the XA-Core, provide the CS 2000 with its media gateway controller (MGC) functionality. Processing capacity is scalable by adding GWC circuit card pairs.

The following figure provides some overall physical details about the GWC card.

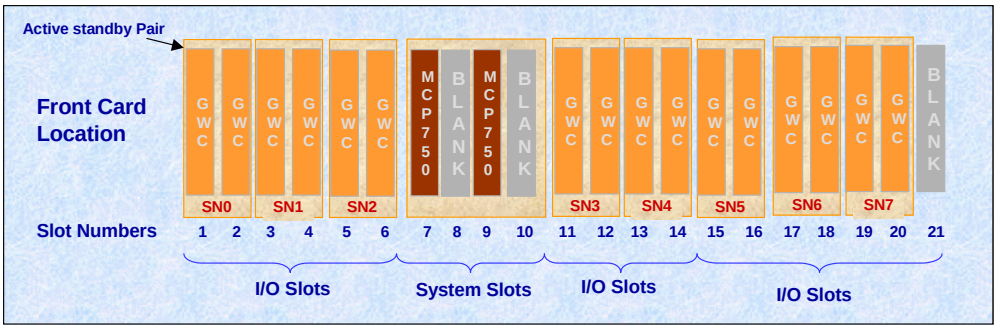
GWC card identification



There is a maximum of eight GWC card pairs for each SAM21 shelf for CS 2000. The 21st slot (front and rear) should always be empty. Other Succession solutions have different shelf capacity limits and configurations.

The SAM21 Shelf Controller provides physical management of the SAM21 shelf and supports resident GWC or other cards. All 16 I/O slots in the SAM21 shelf can be filled with GWC cards, as shown in the figure GWC Card positions in SAM21 shelf, depending on the customer's network requirements.

GWC Card positions in SAM21 shelf



Session Server

The Session Server technology is based on the SAM-XTS a second generation 2U NEBS compliant server from Intel. It is the same chassis as the SAM-XTS equipped for STORM, but adds additional CPUs and more RAM. Each server is equipped with:

- Dual Intel 2.4 GHz P4 Xeon Processors
- 4 GB RAM (Standard) to 12 GB RAM
- Memory Speed - 266 MHz DDR
- Local Disk - Dual hot swap 73GB
- Multiple GigE copper interfaces (2 on board + 2 Port NIC)
- NEBS Level 3 compliant
- 2U Form Factor

The field replaceable components on the Session Server are:

- Hard disk
- Power supply
- CD drive

UAS

The UAS runs Microsoft Windows 2K Server on a conventional Intel-based computing server platform. The UAS system architecture provides industry standard physical interfaces, standard internal buses, and standard protocols for communication with the network. Standard external physical interfaces supported by the UAS include 10/100 BaseT Ethernet (IP), and SONET OC-3c (ATM – AAL1 and ATM – AAL2).

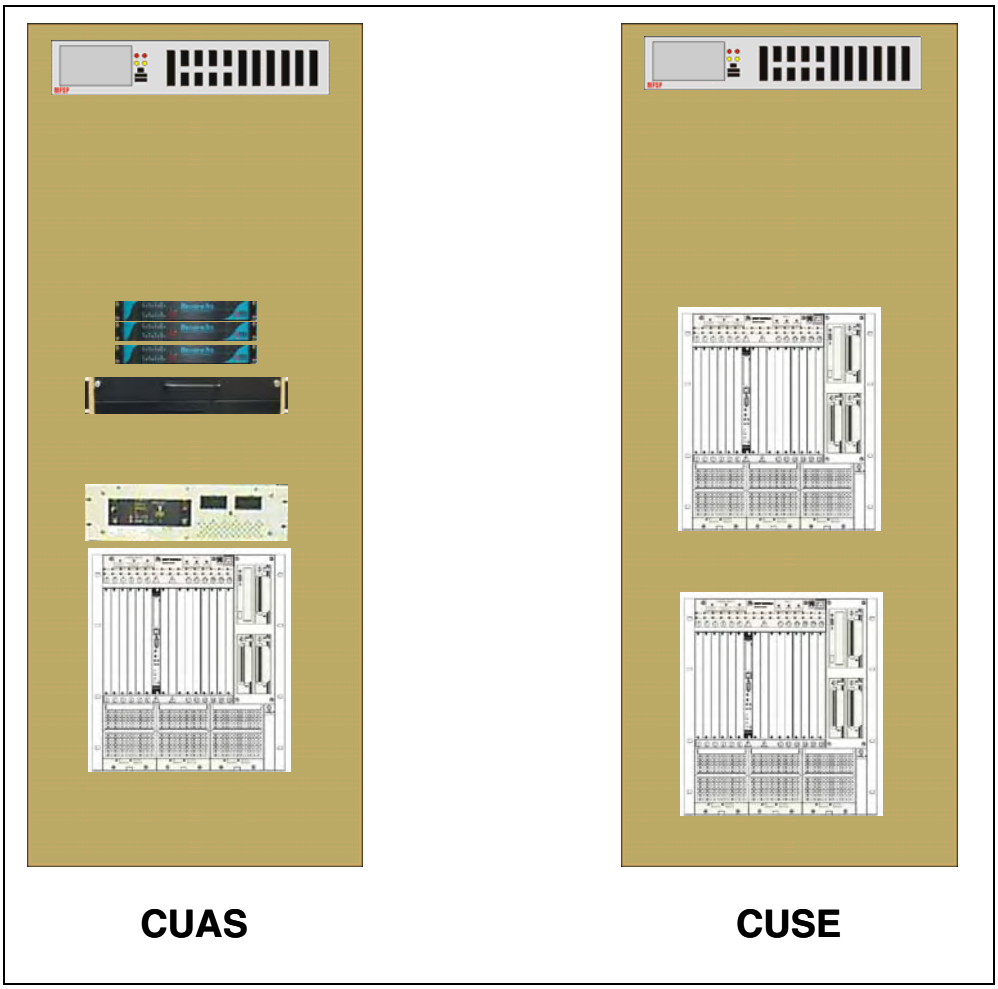
The UAS system architecture uses an industry-standard compact Peripheral Component Interconnect (cPCI) bus for data transfer and H.110 voice bus for time division multiplexed (TDM) voice transfer

between circuit packs. The PCI based cards provide voice capabilities, interfaces, and other special functions for the cPCI bus on each server.

The UAS is highly scalable. Each shelf (chassis) can contain up to two separate UAS nodes, and additional shelves can be added as capacity demands. Redundant hardware is provisioned on an N + 1 basis, thus ensuring that the engineered service capacity will not be degraded due to a single server outage. If the busy hour call volume does not exceed engineered capacity, the UAS blocks an average of one call per 10,000 due to server or service circuit outages.

Hardware redundancy is provided where it is required to ensure high reliability. For example, redundant power supplies and fans are provided since these hardware elements have a lower MTBF. Dual network interfaces prevent a failed router or bridge from taking a UAS out of service. The UAS resides in a SAM16 chassis in a Cabinetized Universal Audio Server (CUAS) cabinet. Additional UASs reside in a Cabinetized Universal Server Extension (CUSE) cabinet (see the figure UAS cabinets).

UAS cabinets



MS 2010

The Nortel MS 2010 is built on the AudioCodes IPmedia 2000 chassis. The IPmedia 2000 cPCI, rack mount chassis is 1U high and 19 inches wide. The chassis contains one board, the IPM-1610 and its rear transition module, which contains the Ethernet interface for the unit. Up to ten MS 2010 nodes can be configured in a SAMF frame.

Although the MS 2010 IPM-1610 board occupies only one slot in the IPmedia 2000 chassis, it consists of two separate, logical media gateway modules from an OAM&P management perspective. Each module has its own MAC address and IP address. Both modules share a redundant LAN connection through an internal Ethernet switch.

APS

The Audio Provisioning Server (APS) provides a central database for network-wide provisioning and maintenance of announcements. The

APS assures that all UASs in the network use the same announcements. The APS is required whenever the UAS is used as an announcement server.

The APS uses the following:

- commercially available hardware
- Sun Solaris operating system
- Oracle database software

The APS allows technician to perform the following functions:

- Create static audio database announcements
- Store announcements by service provider and service provider customer
- Use passwords to protect announcements
- Download announcements to all UASs in the network

The APS resides on a Sun Netra t 1400 server with the following hardware:

- 2 440-Mhz CPUs, expandable to 4 CPUs
- 2 GB RAM
- 4 internal 36-GB drives
- 10x DVD/CD-ROM drive
- Internal 4mm DDS-3 12 GB tape drive
- Redundant power supplies that consist of three units capable of hot swaps

USP

The USP includes the following components:

- Communications Applications Module (CAM)
- System nodes
- OAM&P workstation
- Remote access server (RAS)
- Ethernet hubs
- Cables for each card

A USP system consists of one or more CAM shelves: a single Control CAM shelf; or a control CAM shelf plus optional extension CAM shelves.

USP9 supports the datafill of up to five shelves: one control CAM shelf and four extension shelves. Shelves in a dual-shelf configuration can be inter-connected using OC3 cables or the InterCAM Communication Medium (ICCM). Shelves in a configuration of more than two shelves must be connected using the ICCM.

The modular design and ATM switching functionality of the CAM shelf can become a part of a multi-shelf USP configuration as the link system nodes (SS7 or IPS7) expand beyond 12.

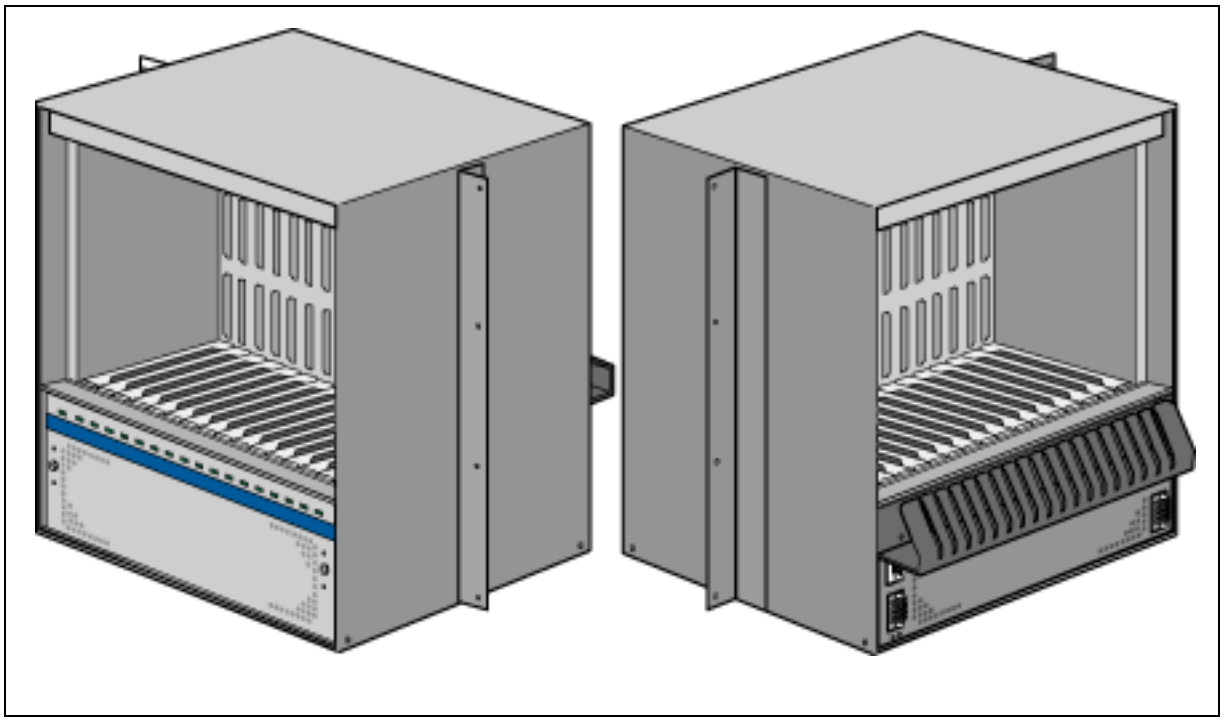
The introduction of ATM high-speed links (HSL) and SS7 IP High Speed links (M2PA over SCTP) reduces the number of links per link system node from four to one; however, it actually increases node capacity because each ATM HSL or IP HSL link provides the capacity equivalent to a minimum of eight low-speed links.

The following list details the configuration limits of the USP in the five shelf configuration:

- 16 IPS7 gateway nodes
- 40 SS7 IP HSL links
- 480 SS7 links (DS0, V.35 or E1 channelized)
- 40 ATM HSL link nodes

The USP CAM shelf includes 18 front and 18 rear slots. The cards in the front of the CAM shelf are called mission cards. The cards in the rear of the CAM shelf are called transition modules (TM). The figure USP CAM shelf shows the USP CAM shelf.

USP CAM shelf



CS 2000 - Compact

The CS 2000 - Compact consists of the following components:

- Call Agent
- STORM
- CS 2000 SAM21 (CS 2000-Compact)
- CS 2000 GWC (CS 2000-Compact)
- USP - Compact
- UAS (CS 2000-Compact)
- MS 2010 (CS 2000-compact)
- APS (CS 2000-Compact)
- CS LAN (CS 2000-Compact)

Note: The GWCs, USP, UAS\MS 2010, APS, and CS LAN hardware used with the CS 2000-Compact is identical to the hardware used with the CS 2000. However, in a few cases this hardware can be located in a different shelf or frame.

Call Agent

The Call Agent is the call processing engine of the CS 2000 - Compact. The Call Agent hardware is a Single Board Computer (SBC) that resides in a Services Application Module 21 (SAM21) shelf. Two Call Agent cards and two SAM21 shelves are required for redundancy. The two shelves are housed in a single Call Control Frame.The Call Agent provides the following functions:

- provides call processing services on line and trunk endpoints
- supports translations and routing for all endpoints served by the CS 2000 - Compact
- provides a provisioned view of profiles of
  - — subscriber services
  - — trunk group services
- collects and formats billing data before sending the data to the element management system (EMS)
- collects log, alarm, and operational measurement (OM) information for use by downstream network management systems

The Call Agent resides on the Call Agent card in the Compact CS-2000.

Note: The Call Agent card is also known as the 3rd Party Core (3PC) card.

STORM

STORM provides network file system (NFS) services to applications running in the CS 2000 - Compact. An NFS is a distributed file system that allows applications to access files and directories on remote computers. STORM acts as an NFS server for the following clients:

- Call Agent
- Universal Signaling Point- Compact (USP-Compact)

STORM resides on a card located in each CS 2000 - Compact domain. Each STORM is attached to a persistent data storage (PDS) device in the frame that contains a redundant array of inexpensive disks (RAID) disk array.

Note: In SN06, Nortel Networks is offering Hewlett Packard (HP) Servers that replace the STORM card and the RAID disk array. In SN06 you have the option of using either the STORM card and RAID disk array, or the replacement HP Servers.

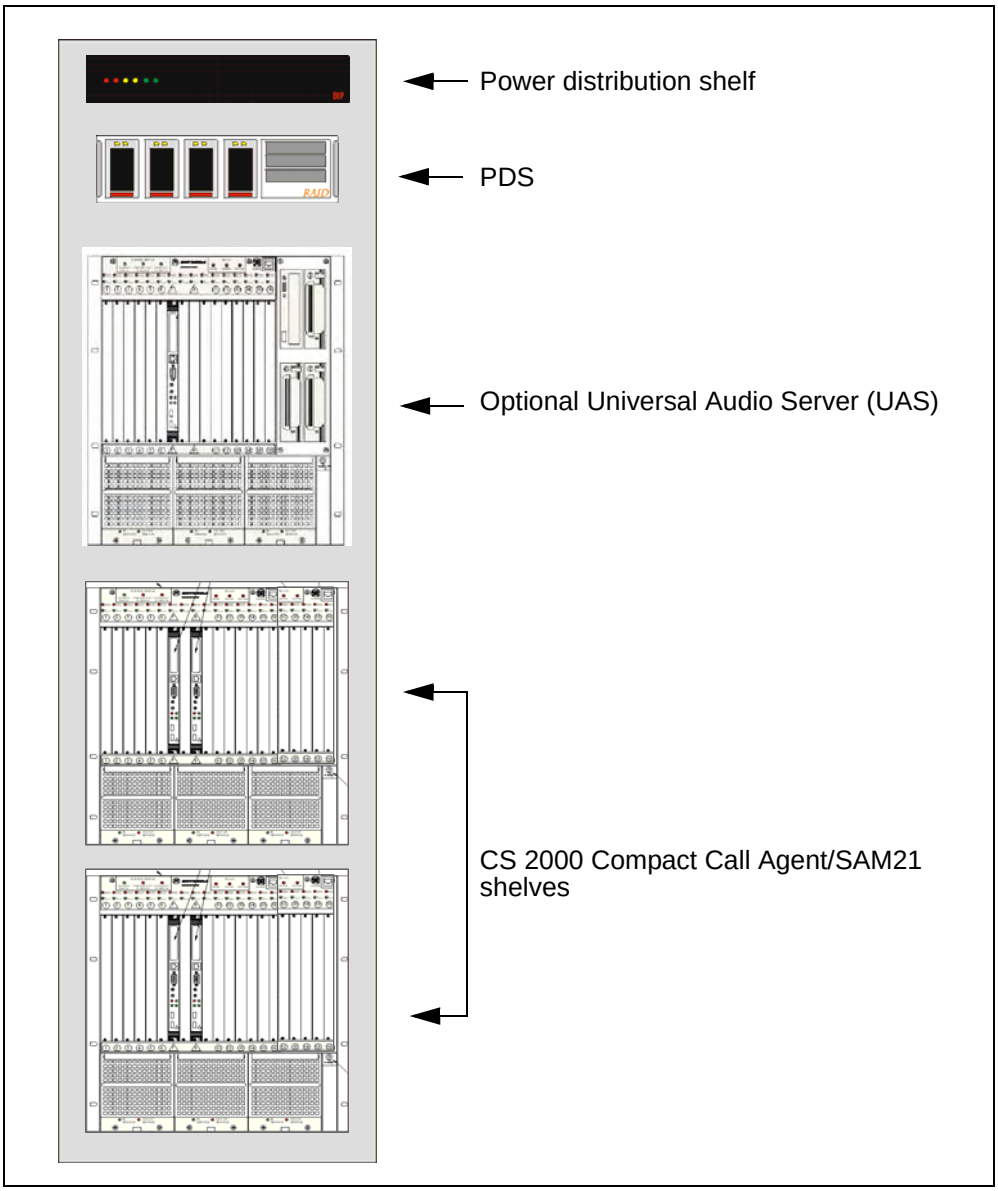
CS 2000 - Compact frame layout

The CS 2000 Compact resides in a Call Control Frame (CCF) in a PTE 2000 frame. Each CCF consists of the following components:

- two CS 2000 - Compact Call Agent/SAM21 shelves
- one optional SAM16 shelf for a Universal Audio Server (UAS)
- one PDC device that provides a RAID disk array and consists of
  - disk drives
  - power supply modules
  - cooling fan modules
  - event reporting modules
  - host input/output (I/O) modules
  - drive I/O modules
  - gigabit interface converter for the fiber channel to the STORM cards in the CS2000 - Compact Call Agent/SAM21 shelves.
- one Astec breaker interface panel (BIP) that serves as the power distribution shelf

The figure SAM21/Call Agent shelves in the CCF shows the Common Control Frame.

SAM21/Call Agent shelves in the CCF



CS 2000 SAM21 (CS 2000-Compact)

If the SAM21 shelf is deployed in a CS 2000 - Compact configuration, the SAM21 shelf does not reside in a CSAM cabinet, it resides in the Call Control Frame. Refer to the *Call Agent Basics*, NN10023-111 for more information.

CS 2000 GWC (CS 2000-Compact)

GWC hardware is the same for both the CS 2000 and CS 2000 - Compact. However, in the CS 2000 - Compact configuration, the GWC cards reside on the SAM21 shelf with the Call Agent, and STORM

cards. For more information, see CS 2000 GWC under the section on the CS 2000 hardware.

Session Server (CS 2000-Compact)

Session Server hardware is the same for both the CS 2000 and CS 2000 - Compact. For more information, see Session Server under the section on the CS 2000 hardware.

USP - Compact

The USP - Compact resides on two identical blades in a CS 2000 - Compact, or SAM21 shelf. The USP - Compact can reside on the same shelf as the CS 2000 - Compact or on different shelves within the same frame. For more information, see the description of USP. under the section on CS 2000 hardware.

UAS (CS 2000-Compact)

The UAS hardware used with the CS 2000 - Compact is identical to the hardware used with the CS 2000 (see UAS under the section on CS 2000 hardware). The only real difference is that with the CS 2000 - Compact, you have the option of locating the UAS on a shelf in the frame with the CS 2000- Compact (see the figure SAM21/Call Agent shelves in the CCF).

MS 2010 (CS 2000-compact)

The MS 2010 used with the CS 2000 - Compact is identical to the MS 2010 hardware used with the CS 2000 (see MS 2010 under the section on CS 2000 hardware).

APS (CS 2000-Compact)

The APS used with the CS 2000 - Compact is identical to the APS hardware used with the CS 2000 (see APS under the section on CS 2000 hardware).

CS LAN (CS 2000-Compact)

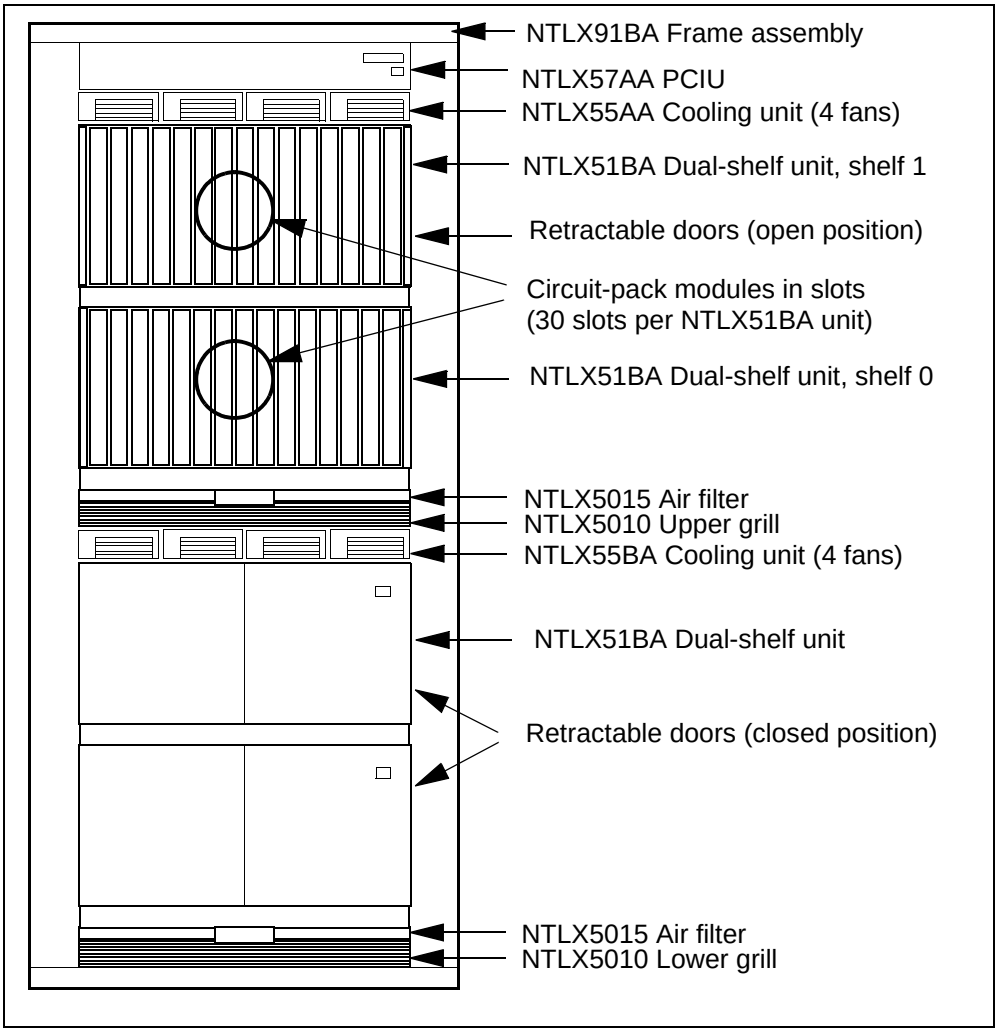
The CS LAN hardware is identical for both the CS 2000 and CS 2000 - Compact (see CS LAN under the section on CS 2000 hardware).

IW SPM-IP

The basic mechanical element of the IW SPM IP consists of a dual shelf assembly mounted to a common backplane. A shelf assembly contains two identical shelves. Each shelf contains modules which plug into the backplane. The modules contain circuit cards that perform a variety of functions such as call processing and high speed carrier capabilities. A standard equipment frame contains two dual shelf assemblies that provide two IW SPM-IP nodes.

As shown in the figure IW SPM-IP frame, the NTLX91BA frame assembly contains two NTLX51BA dual-shelf assemblies (two complete IW SPM IPs) and the necessary support equipment.

IW SPM-IP frame



Media Gateway 7400/15000

The Media Gateway 7400 is a medium-scale switch that supports up to 8,000 DS0s per frame. The Media Gateway 15000 is a large-scale switch that supports up to 38,000 DS0s per frame.

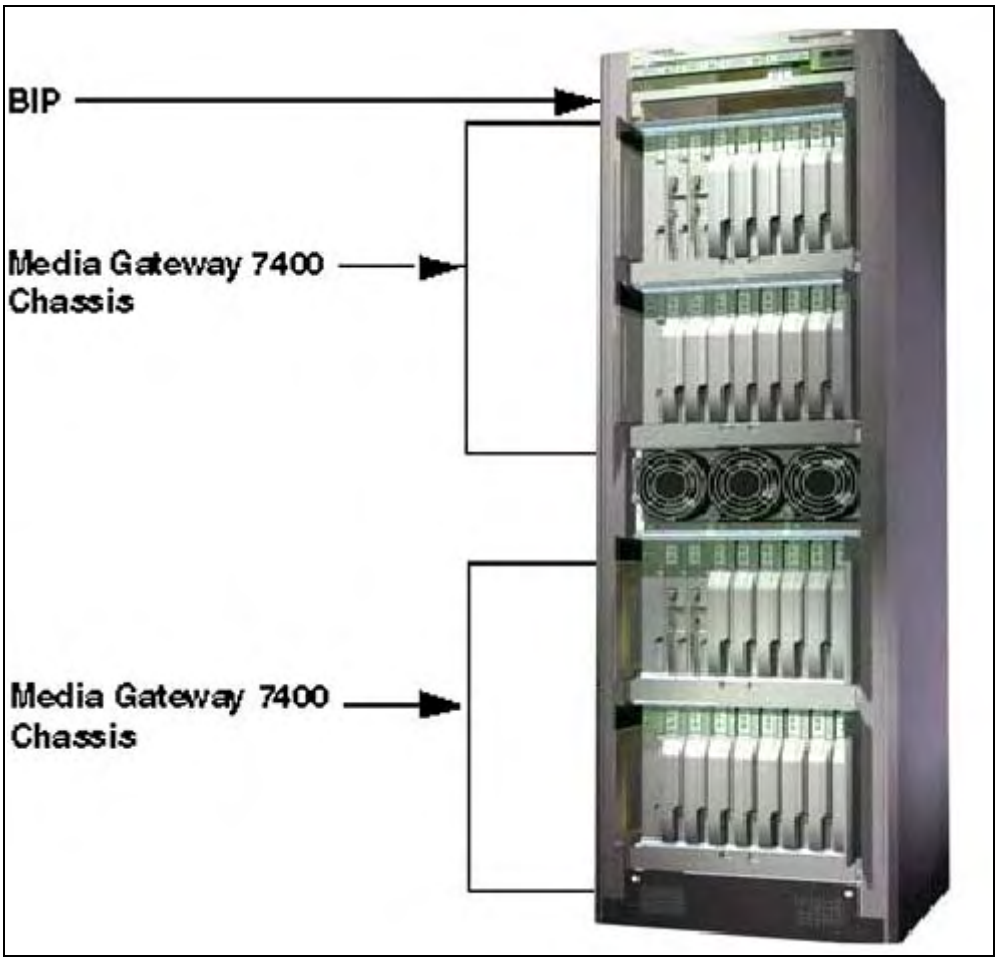
Media Gateway 7400 frame and chassis

The Media Gateway 7400 resides in a single frame assembly that includes the following:

- one breaker interface panel (BIP)
- up to two Media Gateway 7400 chassis, with each chassis containing a single row of 16 card slots

The figure Media Gateway 7400 frame shows the Media Gateway 7400 frame.

Media Gateway 7400 frame



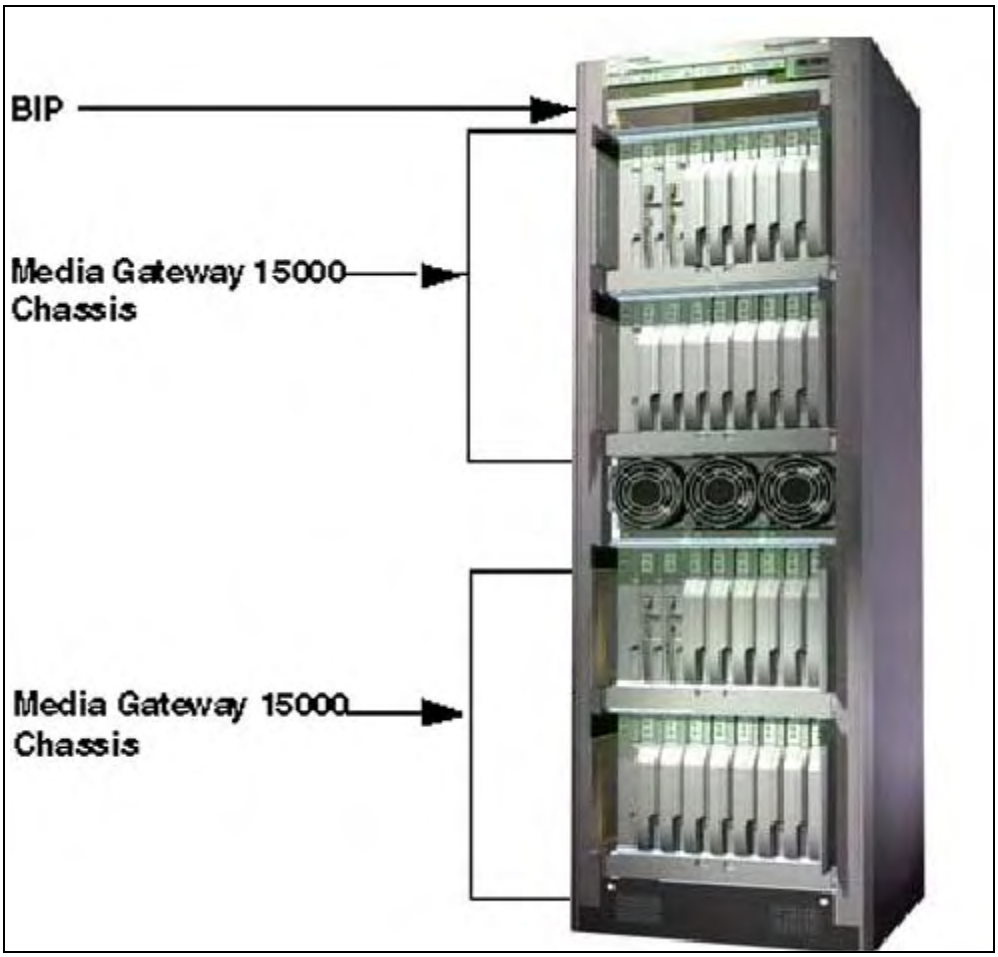
Media Gateway 15000 frame and chassis

The Media Gateway 15000 resides in a single frame assembly that includes the following:

- one breaker interface panel (BIP)
- up to two Media Gateway 15000 chassis, with each chassis containing two rows of 8 card slots

The figure Media Gateway 15000 frame shows the Media Gateway 15000 frame.

Media Gateway 15000 frame



MG 9000

The MG 9000 resides at the edge of the network, bridging the packet network with the time division multiplex (TDM) network. The MG 9000 supports the following interfaces:

- provides an optical carrier-level 3 concatenated (OC-3c) or synchronous transfer mode 1 (STM-1) Internet Protocol (IP) over asynchronous transfer mode (ATM) interface to the packet network.
- supports the following TDM access interfaces:
  - Plain old telephone service (POTS)
  - Coin
  - Ground start
  - P-phone
  - x-Digital Subscriber Line (xDSL)
- provides XPM (ESMA/LGCI) connectivity via Access Bridging Interface (ABI) over DS-512 cards

Nortel Networks offers a two MG 9000 frame configurations:

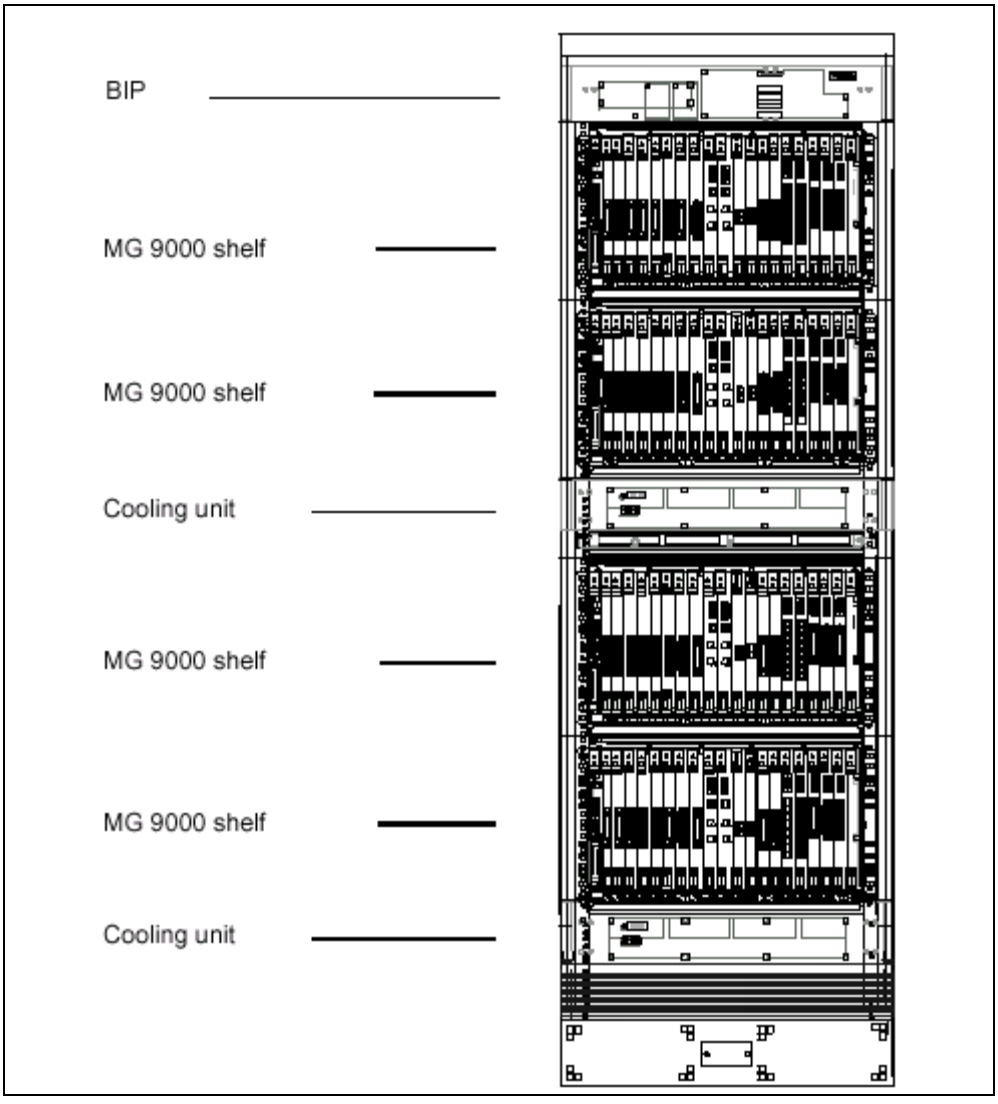
- The NTNY01BB frame configuration with four MG 9000 shelves

  The services available for the NTNY01BB frame include

  — up to 2016 lines in subtended frames

  — up to 1952 POTS lines in the first frame (or exchange for DSL, DS1, or ITX for future growth)

NTNY01BB frame frame



- the NTNY01CA MG 9000 data (MG9D) frame with additional DSL capability with three MG 9000 shelves

  The MG9D allows the MG 9000 to support additional digital subscriber line access module (DSLAM) lines. The MG9D frame

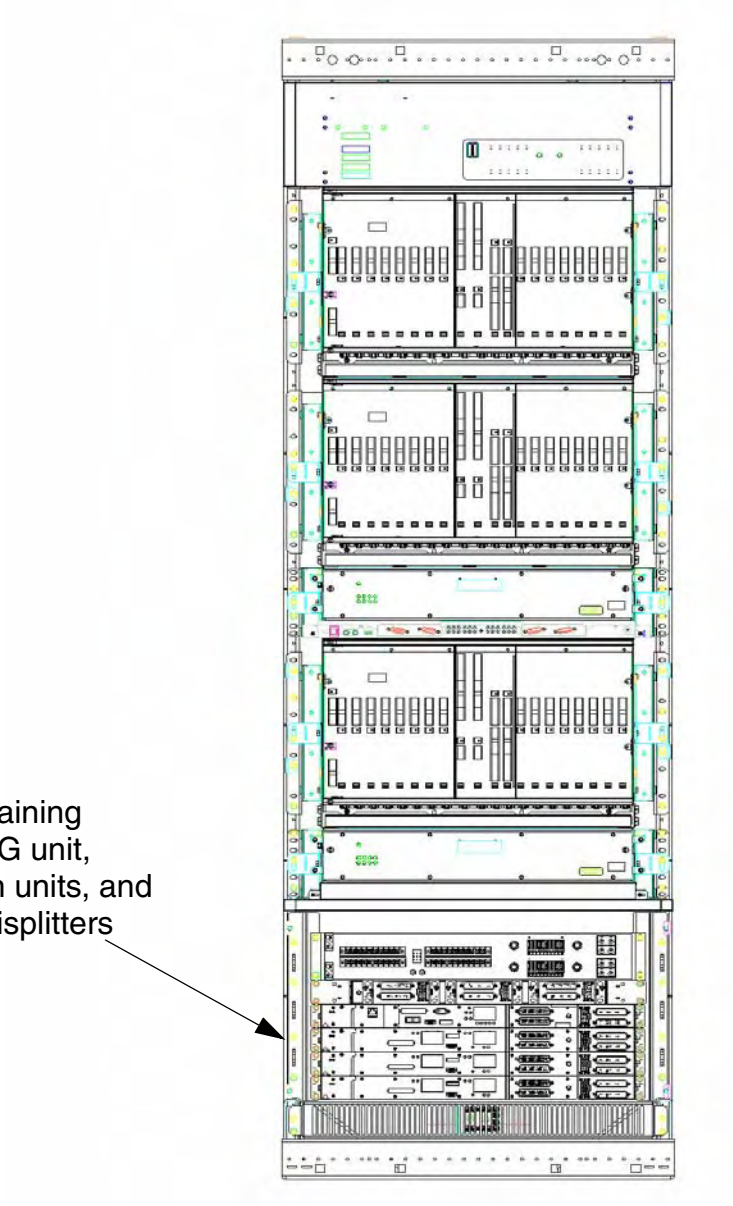
replaces the bottom MG 9000 shelf with space for the Broadband Access Services Gateway (BASG) 7500 (BASG 7600 for international applications).The BASG 7500 product consists of the following three components:

— Basic Unit - a one unit (1U) rack mount unit that supports the network interface and up to 32 DSL lines

— Extension - a one unit (1U) rack mount unit that supports an additional 64 DSL lines. One to three extension units can be provisioned with the basic unit.

— Minisplitters - a unit that supports 32 lines and mounts both next to the Basic and Extension units and in a special 1U Minisplitter tray

NTNY01CA (MG9D) frame with BASG DSLAM units



Each frame configuration provides the following components:

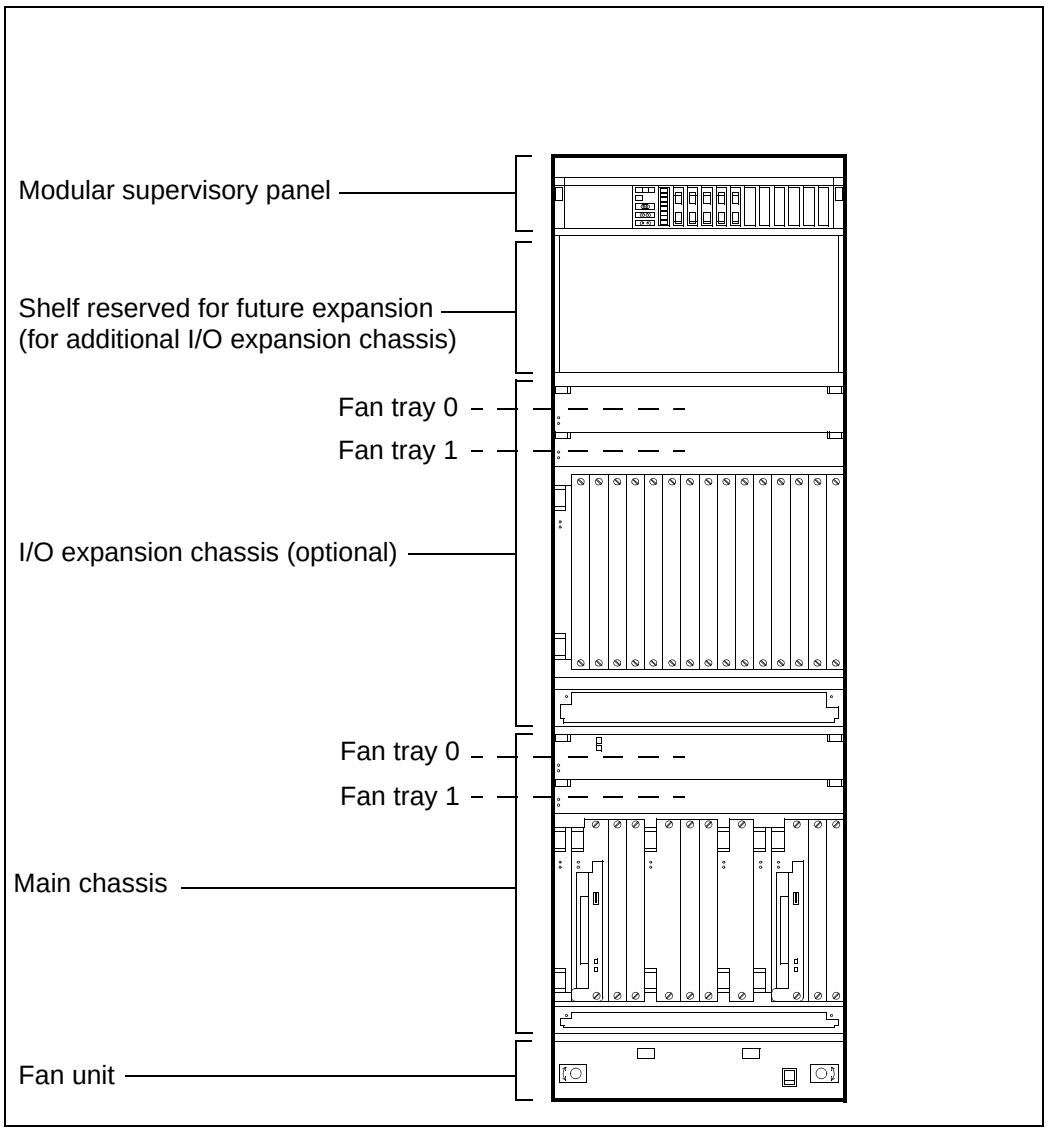
- a breaker interface panel (BIP)
- two cooling units
- front-only access

CS 2000 Core Manager

The CS 2000 Core Manager uses the Nortel C28 Model B (C28B) Streamlined cabinet. The cabinet contains a modular supervisory panel

(MSP), a shelf reserved for future expansion, an optional input/output (I/O) expansion chassis, a main chassis, and a fan unit. System modules are located at the front of the main chassis and the I/O expansion chassis. The figure Front view of the C28B cabinet shows a front view of the cabinet.

Front view of the C28B cabinet



Core and Billing Manager

The Core and Billing Manager resides on commercial off the shelf (COTS) hardware that uses the Solaris operating system. In SN07, the Core and Billing Manager resides on two Sun Netra 240 servers housed in the Cabinetized Operations Administration and Maintenance (COAM) cabinet.

CS 2000 Management Tools

The CS 2000 Management Tools software packages are installed on either a Sun Netra t1400 or Sun Netra 240 server from SUN Microsystems.

Hardware for client workstations is provided under Client workstation requirements.

CS 2000 SAM21 Manager

The CS 2000 SAM21 Manager server application is located on the server that hosts the CS 2000 Management Tools applications. The CS 2000 SAM21 Manager client application is started from a Web browser. For additional information, see CS 2000 Management Tools.

Session Server Manager

The hardware platform for the Session Server Manager is the Hewlett Packard HP-CC3310. Components include:

- Dual Intel 2.4 GHz P4 Xeon Processors
- Up to 12 GB RAM (Session Server is 4 GB)
- Memory Speed – 266 MHz DDR
- Local Disk – Dual 73GB or 146GB disk drives (Session Server is 73 GB)
- Multiple GigE copper interfaces (2 on-board plus 2 per NIC)
- 2U Form Factor

The HP-CC3310 provides processing, memory, and disk capacity for Storage Management (STORM), SIP, and planned SIP applications

USP and USP- Compact manager

The Universal Signaling Point (USP) Manager consists of a graphical user interface (GUI) that runs on a Window 2000 PC. The PC must have a file transfer protocol (FTP) client application to move installation files and image snapshots. The USP - Compact Manager also uses the Window 2000 PC as a hardware platform.

MG 9000 Manager

The MG 9000 Manager and MG 9000 Manager Mid-Tier GUI server reside on Sun Netra t1400 or Sun Netra 240 servers. The MG 9000 Manager client application runs on a UNIX workstation or a Windows 2000/NT PC.

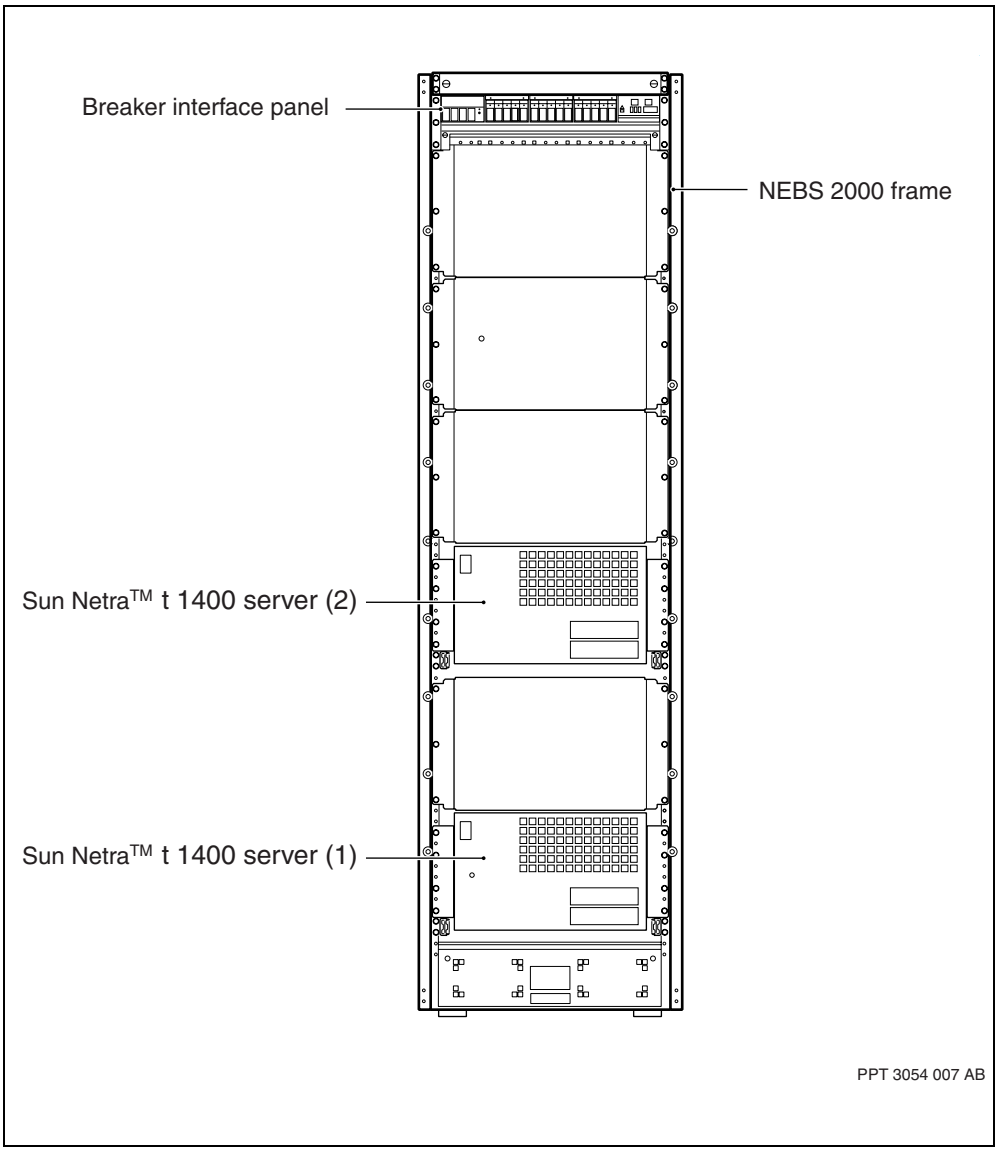
Preside MDM

Preside MDM software runs on dual Sun Netra™ t1400, NEBS-compliant, carrier-grade servers. These servers are connected through Ethernet links to each other and to the CS LAN. These servers have IP connectivity to the Multiservice Switch 15000, and the Media Gateway 7400s/15000s that they are managing. Because the servers are connected together, they operate in a redundant capacity where one server assumes the element manager activities in the event of a server or link failure. The two Sun Netra™ t1400 servers are NEBS-compliant, carrier-grade servers, both of which are installed in a 19-inch NEBS 2000 frame (see the figure Sun NetraTM t1400 servers mounted in NEBS 2000 frame). The servers are part of a network systems family of simplex multiprocessor (SMP) servers produced by Sun Microsystems Inc.

The t1400 servers are connected to each other over a 10Base-T Ethernet link. Each server checks the status of the other through this link. The Sun Netra™ t1400 servers running Preside MDM must be co-located with the Succession Core Manager in the central office.

You have the option of using an alternative server platform for running the Preside MDM software. This alternative platform is the Sun Fire™ V480. The Sun Fire™ V480 must be obtained directly from Sun Microsystems. The Sun Fire™ V480 is deployed in the network operations centers (NOCs) and provides the same management functionality as the Sun Netra™ t1400 but without the need of being co-located.

Sun Netra™ t1400 servers mounted in NEBS 2000 frame



Device Manager

The Device Manager manages the Passport 8600 that is used in the CS LAN. You have the option of using PC or UNIX platforms for the Device Manager software. The minimum system requirements for installing the Device Manager software on a PC workstation (running Microsoft Windows NT and Windows 95 or Windows 98) are as follows:

- 400 MHz or higher Pentium processor
- 128 Megabytes of DRAM
- 100 Megabytes of space on the hard drive

The minimum system requirements for installing the Device Manager software on a UNIX platform is any one of the three options that follow:

- SPARC workstation running the Sun operating system 5.6, or Solaris 2.6 (or higher) operating system with 128 Megabytes of DRAM (the preferred amount is 256 Megabytes of DRAM) and with 100 Megabytes available on the hard disk
- HP workstation running the HP/UP 11.0 (or higher) operating system with 256 Megabytes of DRAM and 100 Megabytes available on the hard disk
- AIX workstation running the AIX 4.3.3.10 (or higher) operating system with 256 Megabytes of DRAM and 100 Megabytes available on the hard disk.

CICM

The CICM is shipped as a series of components fitted into a standard NEBS3 compliant frame (also called a cabinet). CICM 7.11 uses the SAMF and CCF frames.

SAMF Frame

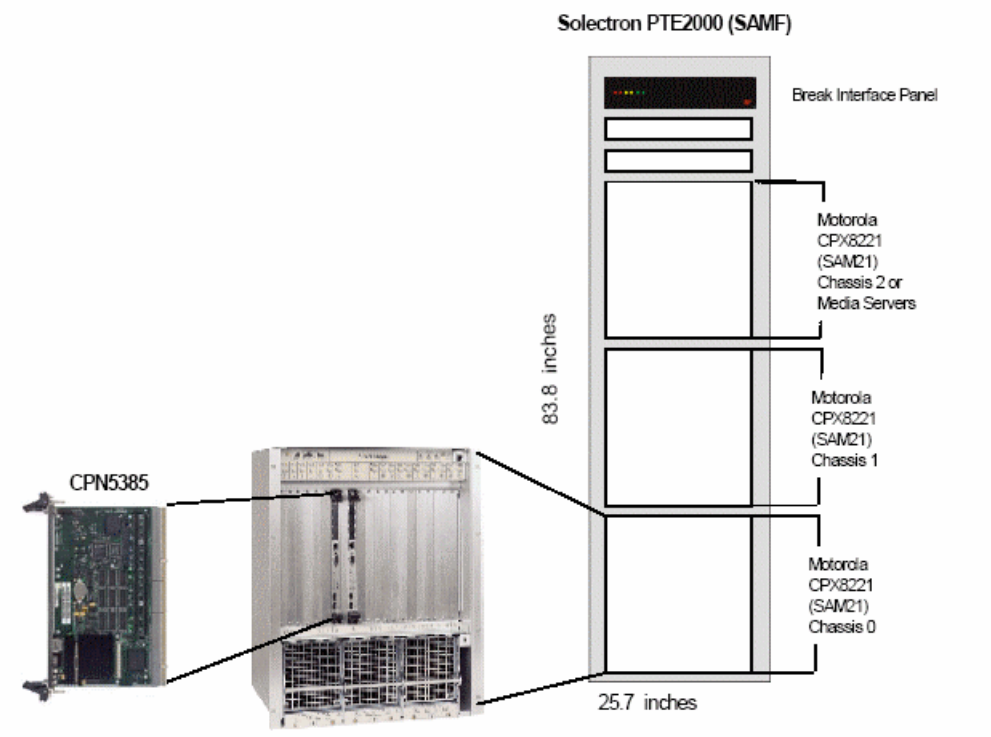
The SAMF frame is illustrated in the figure below, *SAMF frame*. The characteristics of the SAMF frame are:

- NEBS3 compliant
- Configurations supported:
  - — Up to 3 SAM21 Chassis, or
  - — Up to 2 SAM21 Chassis + Media Server Applications (up to 6 MS2010 IP Chassis if Media Servers are included in the Solution)
- 4 System slots already occupied (2 HSC and 2 shelf controllers)
- 17 application slots:
  - — 1 CICM-EM card (Motorola CPN 5385 processor board, NTRX51HJ, along with its transition module on the rear shelf, NTRX51HK). Its mate will be on another chassis for redundancy.
  - — Up to 10 CICM cards (Motorola CPN5385 processor board, NTRX51HJ, along with its transition module on the rear shelf, NTRX51HK). Their mates are on another chassis.
  - — Up to 6 GWC cards (Motorola N750, no rear transition module needed): 5 for CICM control and 1 for RTP Media Portal control (if Portals are used). Their mates are on another chassis. ONe

GWC pair supports 6400 CICM lines, or roughly 2 CICM card pairs.

— Application slots 15 and 16 do not support rear I/O because their rear slots are already occupied by the Extension Bridge circuit packs. These cards are required in the chassis and can not be removed.

SAMF Frame



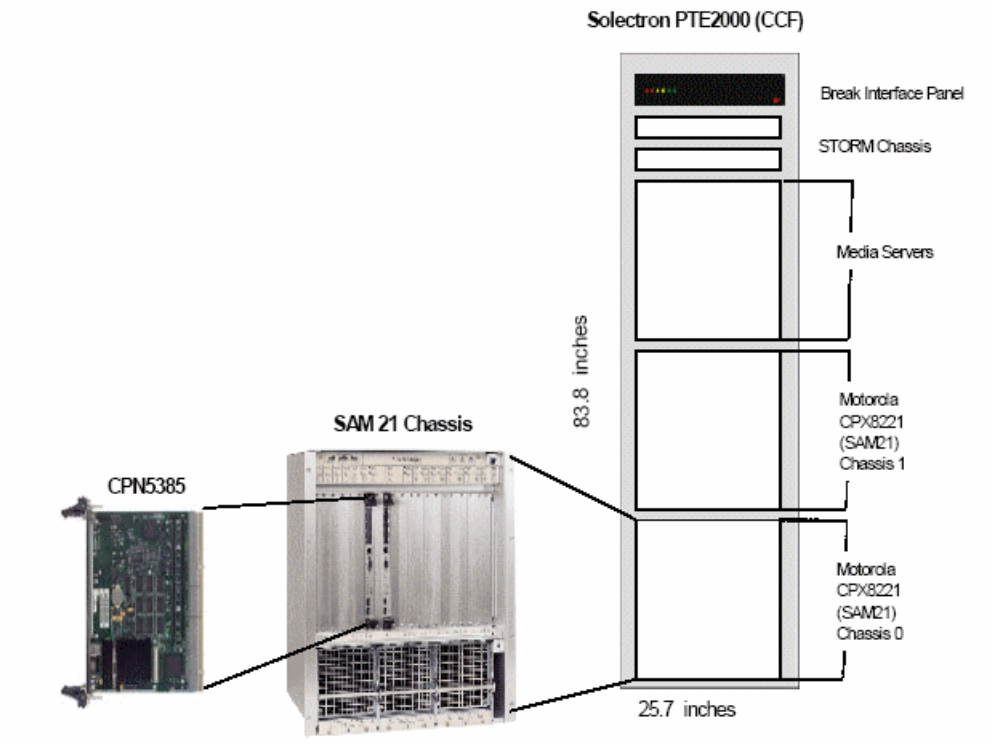
CCF Frame

The CCF frame is illustrated in Figure 29 below. The characteristics of the CCF frame are:

- NEBS3 compliant
- Configurations supported:
  - — Up to 2 SAM21 Chassis, or
  - — Up to 2 SAM21 Chassis + Media Server Applications (up to 6 MS2010 IP Chassis)
  - — STORM storage systems
- 4 System slots already occupied (2 HSC and 2 shelf controllers)

- 2 Slots are reserved, leaving a maximum of 13 slots available. The two reserved slots are:
  - — One slot for the Call Agent Card
  - — One slot for the USPc card
- There are 15 usable application slots: up to 13 of these slots are usable for CICM and the rest usable for GWC cards.
  - — 1 CICM-EM card (Motorola CPN 5385 processor board, NTRX51HJ, along with its transition module on the rear shelf, NTRX51HK). It is an active card, and its mate will be on another chassis for redundancy.
  - — Up to 8 CICM cards (Motorola CPN5385 processor board, NTRX51HJ, along with its transition module on the rear shelf, NTRX51HK). These are active GWC cards and their hot stand-by mates are on another chassis.
  - — Up to 6 GWC cards (Motorola N750): 4 for CICM control, and 2 for RTP Media Portal control (if portals are used). These GWC cards are active cards. Their hot standby mates are on another chassis.

CFF Frame



Element Manager

In the SAM21-based CICM 7.11, the CICM-EM is a pair of Motorola CPN5385 resource cards; one active and the other hot standby for redundancy. Although a CICM requires only one Element Manager, Nortel Networks recommends configuring EMs in redundant pairs to provide redundancy and to avoid a single point of failure.

Only one pair of the CICM-EM resource cards is required per CS2K, which is capable of supporting up to 100 pairs of CICM resource cards. The hot standby CICM-EM resource card is equivalent to the Secondary Element Manager (SEM) chassis in the SAM16-based CICM releases.

Secondary Power Distribution Center

You have the option of using a Secondary Power Distribution Center (SPDC) to power your IP solutions. SPDC is a high-capacity direct-current (DC) power distribution cabinet intended for deployment in a central office. SPDC can have from two-to-six input feeds from the main power plant, where each feed to the SPDC is protected for up to 600 Amperes. From input battery “A” the SPDC offers plug-in circuit breaker distribution to a maximum of 54 circuits rated from one-to-100 Amperes. From input “B” the SPDC offers plug-in circuit breaker distribution to a maximum of 54 circuits that are rated from one-to-100 Amperes. For additional information, see Nortel Networks Engineering Change (EC) 101-08295.

Sun Netra t1400

The t1400 server is a NEBS level 3 compliant computing platform that offers several configurations and performance points that can be expanded upon. It is based on the Ultra Sparc II processor clocked at 440 MHz. Up to 4 processors can be configured in a single server. It can also support up to 4 Gbytes of RAM and up to 4 disk drives on a SCSI internal bus that can be hot swapped.

The t1400 mounts in an OAME frame and has the following key features:

- 4 disks of 36 Gbytes each that are hot swappable. The disk drives are accessible from the front panel and are in-service Field Replaceable Units (FRUs).
- 2 Ultra SparcII processors at 440 MHz each with 4 Mbytes cache
- 2 Gbyte RAM
- 1 DVD ROM drive 10X
- 1 DDS-3 DAT drive
- 1 Quad Fast Ethernet card

Sun Netra 240

The Netra 240 server, also referred to as the Cabinetized Operations, Administration, and Maintenance (COAM) server, is a NEBS level 3 compliant computing platform that offers several configurations and performance points that can be expanded upon.

The COAM server, mounts in a COAM equipment cabinet, and has the following key features:

- 2 disks of 72 Gbytes each that are hot swappable. The disk drives are accessible from the front panel and are in-service Field Replaceable Units (FRUs).
- 2 Ultra Sparc IIIi processors at 440 MHz each with 4 Mbytes cache
- 2 Gbytes of RAM (basic model) or 4 Gbytes RAM
- 1 DVD/RW drive
- 3 PCI I/O slots
- 4 Ethernet ports 10/100/1000
- 1 SCSI port

The COAM servers can be provisioned as simplex units or as high availability (HA) pairs. The maximum number of COAM servers in a COAM equipment cabinet is six.

COAM servers provisioned in an HA pair, are referred to as a cluster. A cluster uses a minimum of three IP addresses; one for each COAM server and one for the cluster. While one of the cluster nodes is actively providing OAM&P services, the other remains on standby. An automatic failover takes place, when one of the following conditions occurs on the active node:

- power failure
- CPU failure
- double disk failure
- network inteface failure (all four network interfaces)
- system overheating
- memory failure

For maintenance or software upgrades, the user can also initiate a manual failover. Refer to procedure “Initiating a manual failover” in the ATM/IP Solution-level Fault Management document, NN10408-900.

ATTENTION

During an automatic or manual failover, the HA cluster takes approximately 5 minutes to failover and bring up the standby node to Active state.

Software baseline for IAC, PT-IP, PT-AAL2, and UA-IP

The table IAC, PT-IP, PT-AAL2, and UA-IP software baseline for SN07 lists the software baseline required to support the SN07 release of the IAC, PT-IP, PT-AAL2, and UA-IP solutions. Please note that not all entries in the table apply to every IP solution. The second column titled "Solution" contains a value that indicates the solution applicability. For example, if an item in the table applies to all four IP solutions, then "all" appears in the second column. If an item applies only to the IAC solution, then "IAC" appears in the second column.

IAC, PT-IP, PT-AAL2, and UA-IP software baseline for SN07 (Sheet 1 of 4)

Name	Solution	Order code	Notes
CS 2000 software			
Base PCL	all	SN000007	Communication Server 2000 and TDM core software (PCL). Includes the following DRUs: TOPS20, UCS20, CNA19, CCM20, PNM07, SHR20, MSH20, XPM20, SP/SPSH/MG4K20, TDMSP/TDMSPSH/SPD20 ,BASE21/TL20 (CSP20)
PPL Peripheral Load	all	PLLT0020	Comes with Base PCL load
NRL Commissioning Tools	all	INST0020	Comes with Base PCL load
MUL (MS Load)	all	MUC00020	Comes with Base PCL load
SAM21 Platform	all	SAM20070	Comes with Base PCL load
GWC09.2 (PGC load)	all	GWCC0070	Comes with Base PCL load
GWC09 Firmware	all	SAM20070	Comes with Base PCL load
Session Server	PT-IP	NGSS0070	
3PC SOS load (PCL)	all	SNC00007	
3PC Peel/Linux Load	all	3PC00070	

IAC, PT-IP, PT-AAL2, and UA-IP software baseline for SN07 (Sheet 2 of 4)

Name	Solution	Order code	Notes
STORM (DotHill)	all	STRM0004	Beginning with SN06 Nortel Networks offered HP servers that replace the STORM card and the RAID (see STORM-IA below). The new HP Server does not need the firmware load. Both platforms are available in SN06 and following releases. STORM (DotHill) consists of STRM0004 and SAM20006. STORM-IA (HP server) consists of only STRM0006.
STORM-IA (HP server)	all	STRM0006	(see STORM (DotHill))
3PC firmware	all	SAM20070	
STORM DotHill firmware	all	SAM20070	
IW SPM-IP	IAC PT IP	SIWI0070	IW SPM software (NCL)
UAS	all	UASA0008	
Media Server 2010	all	MS200070	
Audio Provisioning Server	all	APS00090	
USP	all	USP00090	
USP-Compact	all	USPL0090	
USP-Compact Firmware	all	SAM20070	
Media Gateway 7400 and Preside MDM comprehensive package	all	Not Available	Includes PCR6.1 software load and MDP software CD and patch
Media Gateway 15000 and Preside MDM comprehensive package	all	Not available	Includes PCR6.1 software load and MDP software CD and patch

IAC, PT-IP, PT-AAL2, and UA-IP software baseline for SN07 (Sheet 3 of 4)

Name	Solution	Order code	Notes
Multiservice Switch 15000 and Preside MDM comprehensive package	PT-IP PT-AAL2 UA-IP	Not available	Based on PCR6.1
Passport 8600	all	P86S0070	CS LAN only (Release 3.7)
MG 9000	UA-IP	MG9K0070	
Media Gateway 15000 or 7400 Anchor Packet Gateway	all	Not available	Identical hardware as Media Gateways.
Contivity 600 VPN Switch	all	Not available	
CS 2000 Core Manager	all	CS2E0070	AIX-based software
Core and Billing Manager	all	CBM0070	Solaris-based software
Integrated EMS	all	IEMS0070	
CS 2000 Management Tools	all	CS2M0070	
Succession Server Platform Foundation Software	all	SPFS0070	
CPS2000	IAC		Manager for PacketPorts. Uses CPS2000 V2.1 and includes Element Pro 1.0 software.
Preside MDM (supporting Multiservice Switch 15000)	PT-IP PT-AAL2 UA-IP		Preside MDM 15.1. Order the comprehensive package including MDP.
Preside MDM (supporting Media Gateway 15000 and 7400)	IAC PT-IP PT-AAL2 UA-IP		Preside MDM 15.1. Order the comprehensive package including MDP.
MG 9000 EMS	UA-IP	9KEM0070	

IAC, PT-IP, PT-AAL2, and UA-IP software baseline for SN07 (Sheet 4 of 4)

Name	Solution	Order code	Notes
Java Device Manager (EM for Passport 8600)	all	Not applicable	The software is automatically shipped when you order the Passport 8600 (DVM 5.5.6)
SAM16 Global Server Platform (for UAS only)	all	GSS00033	
DCE security	all	not available	Supported and verified DCE server with IBM DCE V3.1 for Solaris (on Solaris 2.7)
CICM			
Centrex IP Gateway	CHS	CICM0070	CICM7.11.184 load name
Centrex IP Client Manager EM	CHS	CICE0070	CICM7.11.184 load name
Centrex IP SoftClient	CHS	see comments	The CICM SoftClient is accessed from Nortel Network's e-delivery service. The customer accesses this site to download the client software. Therefore, an ordering code is not required.

Client workstation software baseline

This section defines the platform requirements, operating system requirements, and Web browser requirements for IP client workstations.

Platform requirements for client workstations

The table Platform requirements for IP client workstation lists the platform requirements and method of invocation for each client application used in IP solutions

Platform requirements for IP client workstation (Sheet 1 of 2)

Client Name	Invocation	Platform
SDM Clients (ETA, ATA, SFT)	Desktop	Sun
SAM21 Manager	Desktop	PC or Sun
CS 2000 Management Tools Selector	Browser (HTML)	PC or Sun
GWC Manager	Browser (JWS)	PC or Sun
UAS Manager	Browser (JWS)	PC or Sun
LMM	Browser (JWS)	PC or Sun
Nodes Provisioning	Browser (JWS)	PC or Sun
NPM	Browser (JWS)	PC
MG9000 Manager	Desktop	PC or Sun
MG9000 Local Craft Interface	Browser	PC
Trunk Provisioning	Telnet/STELNET	PC or Sun
Line Provisioning	Telnet/STELNET	PC or Sun
Nodes Provisioning	Telnet/STELNET	PC or Sun
USP Manager	Desktop (Citrix Metaframe 1.8)	PC or Sun
APS Manager	Browser	PC
Storm Manager	Browser (Proxy)	PC or Sun
3PC Manager	Telnet (Proxy)	PC or Sun
MDM/MDP (supported)	Desktop (X.11)	Sun
MDM/MDP (unsupported)	Desktop (Exceed)	PC

Platform requirements for IP client workstation (Sheet 2 of 2)

Client Name	Invocation	Platform
Device Manager	Desktop (Java)	PC or Sun
SDM Clients (ETA, ATA, SFT)	Desktop	PC or Sun

Operating system requirements for client workstations

The table Operating system requirements for IP client workstations lists the required operating system for each IP client workstation.

Operating system requirements for IP client workstations (Sheet 1 of 2)

Client name	Windows operating system	Solaris operating system
SDM Clients (ETA, ATA, SFT)	N/A	2.7, 2.8, 2.9 to Current
SAM21 Manager	98*, 98SE*, ME*, NT, 2000, XP to Current	2.7, 2.8, 2.9 to Current
CS2K Management Tools Selector	98*, 98SE*, ME*, NT, 2000, XP to Current	2.7, 2.8, 2.9 to Current
GWC Manager	98*, 98SE*, ME*, NT, 2000, XP to Current	2.7, 2.8, 2.9 to Current
UAS Manager	98*, 98SE*, ME*, NT, 2000, XP to Current	2.7, 2.8, 2.9 to Current
LMM	98*, 98SE*, ME*, NT, 2000, XP to Current	2.7, 2.8, 2.9 to Current
Nodes Provisioning	98*, 98SE*, ME*, NT, 2000, XP to Current	2.7, 2.8, 2.9 to Current
NPM	98*, 98SE*, ME*, NT, 2000, XP to Current	2.7, 2.8, 2.9 to Current
MG9000 Manager	98*, 98SE*, ME*, NT, 2000, XP to Current	2.7, 2.8, 2.9 to Current
MG9000 Local Craft Interface	98*, 98SE*, ME*, NT, 2000, XP to Current	Not supported
Trunk Provisioning	98*, 98SE*, ME*, NT, 2000, XP to Current	2.7, 2.8, 2.9 to Current

Operating system requirements for IP client workstations (Sheet 2 of 2)

Client name	Windows operating system	Solaris operating system
Line Provisioning	98*, 98SE*, ME*, NT, 2000, XP to Current	2.7, 2.8, 2.9 to Current
Nodes Provisioning	98*, 98SE*, ME*, NT, 2000, XP to Current	2.7, 2.8, 2.9 to Current
USP Manager	98*, 98SE*, ME*, NT, 2000, XP to Current	2.7, 2.8, 2.9 to Current
APS Manager	98*, 98SE*, ME*, NT, 2000, XP to Current	Not supported
Storm Manager	98*, 98SE*, ME*, NT, 2000, XP to Current	2.7, 2.8, 2.9 to Current
3PC Manager	98*, 98SE*, ME*, NT, 2000, XP to Current	2.7, 2.8, 2.9 to Current
MDM/MDP (supported)	N/A	N/A
MDM/MDP (unsupported	98*, 98SE*, ME*, NT, 2000, XP to Current	Not applicable
Device Manager	98*, 98SE*, ME*, NT, 2000, XP to Current	2.7, 2.8, 2.9 to Current

Note: An asterisk (*) indicates the release is desirable for remote access and work-at-home uses.

Web browser requirements for IP client workstations

The table Web browser requirements lists the Web browser requirements for each IP client workstation that uses a browser.

Web browser requirements (Sheet 1 of 2)

Client name	Invocation	Internet Explorer	Netscape
CS 2000 Management Tools Selector	Browser (HTML)	5.5 to current	6.1 to current
GWC Manager	Browser (JWS)	5.5 to current	6.1 to current

Web browser requirements (Sheet 2 of 2)

Client name	Invocation	Internet Explorer	Netscape
UAS Manager	Browser (JWS)	5.5 to current	6.1 to current
LMM	Browser (JWS)	5.5 to current	6.1 to current
Nodes Provisioning	Browser (JWS)	5.5 to current	6.1 to current
NPM	Browser (JWS)	5.5 to current	6.1 to current
MG9000 Local Craft Interface	Browser	Not supported	4.7 only
APS Manager	Browser	5.5 to current	6.1 to current
Storm Manager	Browser (Proxy)	5.5 to current	6.1 to current
Device Manager	Desktop (Java)	5.5 to current	6.1 to current

Software delivery and ordering processes

This section discusses the following topics about software delivery:

- Software delivery methods
- Electronic connectivity between Nortel Networks and its customers
- Customer regulatory, tax, and contractual considerations

Electronic connectivity between Nortel Networks and its customers

Nortel Networks Global Solutions (NGS) manages electronic connectivity to customer and facilities. NGS operates multiple worldwide extranets which are collectively known as the Customer Access Network (CAN). External partners connect to the CAN using dialup or leased circuits. The CAN has analog and ISDN dialup service and shared Frame Relay (V.35), X25 or T1 service. A Succession Network requirement for the delivery of PCL and NCL load files is a throughput of T1 or better service (> 1.544 Mbits/s) from the Nortel Networks CAN.

The external drop box can exist on the CAN or on a wide area network extranet maintained by the customer. A minimum of 5 Gbyte of disk space is required on the drop box, and the server must comply with Nortel Networks and customer network security requirements.

A customer e-mail address is required to deliver software loads. Nortel Networks will notify this contact when loads have been delivered

electronically. It is the responsibility of the customer to monitor notifications from Nortel Networks that a load is available for retrieval.

Release notes and other documentation are delivered with software as required. These documents are in PDF format for electronic delivery.

Customer regulatory tax and contractual considerations

Customers must be prepared for the regulatory tax and contractual considerations associated with receiving software solutions electronically. In some locations, electronically delivered software is exempt from sales tax.

OAM&P strategy

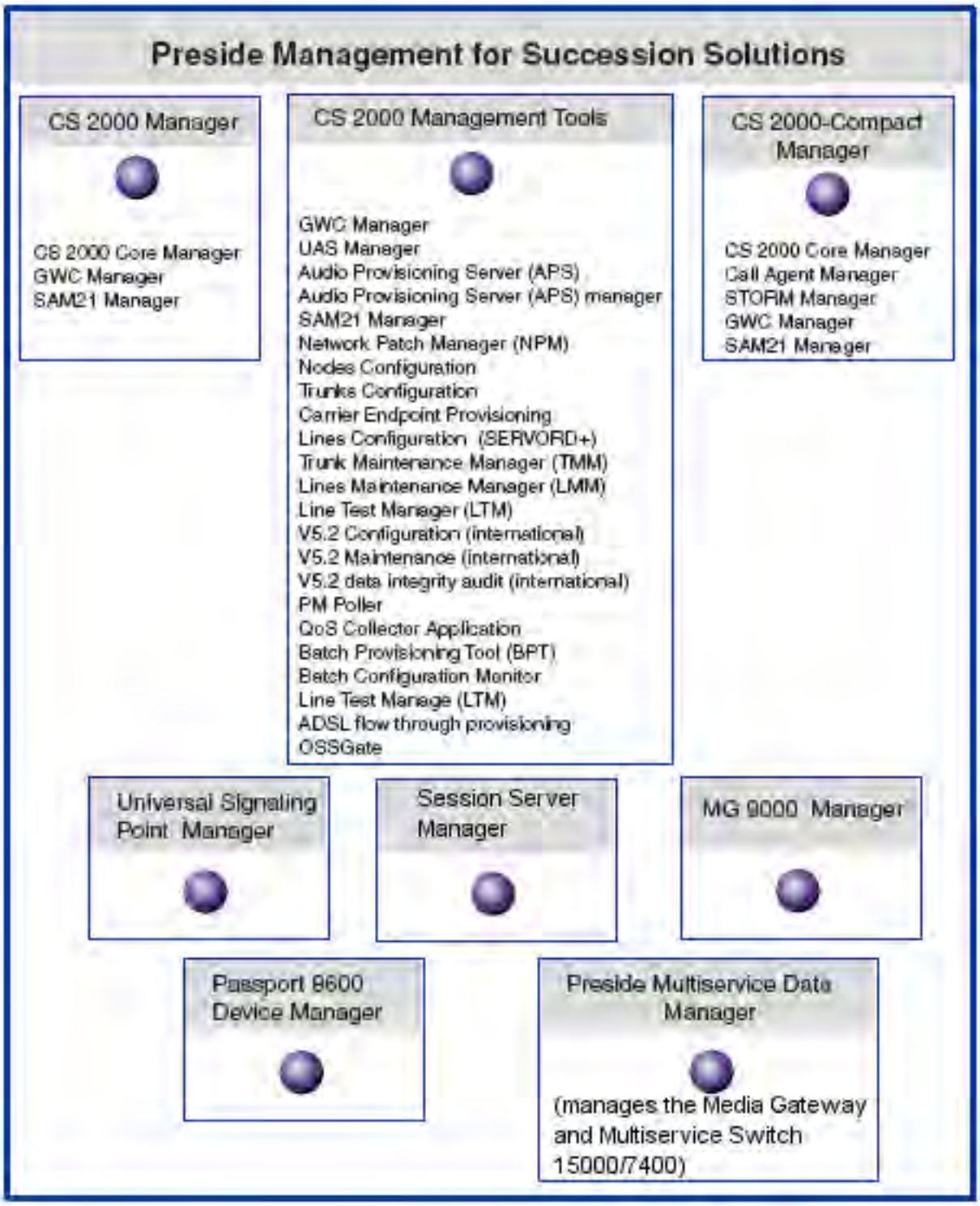
The distributed nature of the IP solutions have resulted in the development of a unique solution for managing the operations, administration, maintenance, and provisioning (OAM&P) functions. The applications used to manage the components of the <solution name> solution are collectively referred to as Preside Management for Succession Solution (Preside MSS).

With Preside MSS, the distributed elements of the network are brought together by enhancing the SuperNode Data Manager (SDM) platform and interworking new Succession applications on commercially available hardware platforms. The various applications support a variety of interfaces to network management applications or element managers.

A dedicated OAM&P network (called the Communication Server LAN) is used for transmitting software loads and Succession Network OAM&P data among the various elements.

The figure Preside MSS software suite shows the device managers and applications that make up the Preside MSS software suite. Notice that although the GWC Manager and SAM21 Manager are part of the CS 2000 Management tools they are also grouped under the CS 2000 Manager, and the CS 2000-Compact Manager. The various applications and devices managers that are collectively known as Preside MSS are discussed in greater detail under OAM&P strategy in this document.

Preside MSS software suite



OAM&P and the OSI Model

The traditional term for network management in the circuit switched TDM network is OAM&P (Operations, Administration, Maintenance and Provisioning). Network management systems in next generation data networks are based on the Telecommunications Management Network (TMN) framework which is more flexible and designed for managing distributed networks.

Preside MSS functional capabilities are described as ‘FCAPS’ (from the OSI model) based on the TMN architecture. The TMN model is used as the basis for Succession Networks OAM&P/FCAPS evolution in terms of functionality and capability.

FCAPS stands for:

- Fault - surveillance, maintenance, fault isolation and diagnostics, and reporting of results
- Configuration - equipment and service provisioning, software delivery, software inventory and configuration, and software queries of provisioned data
- Accounting - capturing of billing or call information
- Performance - recording and delivery of performance measurements (PMs) and operational measurements (OMs), as well as a control scheme to optimize network performance
- Security - authentication and authorization, and audit trails

Element managers used in Succession Network solutions

Element management takes place with the help of the following components:

- CS 2000 Manager consists of three element managers responsible for managing the CS 2000. CS 2000 Manager has the following sub-components:
  - CS2000 Core Manager manages the XA-Core and the subtending TDM components of CS2000. CS 2000 Core

Manager comprises functionality from the existing OAM&P SDM solution. These include:

- SDM Maintenance and Administrative Position (MAP) Passthrough
- SDM billing application (SBA)
- Secure file transfer (SFT)
- SDM Software inventory manager (SWIM)
- SDM Log delivery
- Operational Measurements (OM) Delivery (OMD)
- EADAS OM delivery using the GR740 Pass Through application

— CS2000 GWC Manager is a GUI software application that manages the gateway controllers. It enables users to remotely configure, monitor, and maintain the GWCs.

— CS 2000 SAM21 Manager is a GUI application that manages the SAM21. Its primary function is to represent the configuration and status of card slots on the SAM21 shelf. It also monitors hardware faults associated with the SAM21 shelf controller circuit packs.

• CS 2000 - Compact Manager consists of five element managers responsible for managing the CS 2000 - Compact.

CS 2000 - Compact Manager has the following sub-components:

— CS2000 Core Manager manages the XA-Core and the subtending TDM components of CS2000. CS 2000 Core

Manager comprises functionality from the existing OAM&P SDM solution. These include:

- SDM Maintenance and Administrative Position (MAP) Passthrough
- SDM billing application (SBA)
- Secure file transfer (SFT)
- SDM Software inventory manager (SWIM)
- SDM Log delivery
- Operational Measurements (OM) Delivery (OMD)
- EADAS OM delivery using the GR740 Pass Through application

— CS2000 GWC Manager is a GUI software application that manages the gateway controllers. It enables users to remotely configure, monitor, and maintain the GWCs.

— CS 2000 SAM21 Manager is a GUI application that manages the SAM21. Its primary function is to represent the configuration and status of card slots on the SAM21 shelf. It also monitors hardware faults associated with the SAM21 shelf controller circuit packs.

— Call Agent Manager

— Storage Management Manager (STORM Manager)

- UAS Manager is a software application that manages the following aspects of the UAS:

— manages the configuration of each UAS unit

— enables each UAS unit to receive and display alarms, logs, and OMs

— receives alarms and logs from the Audio Provisioning Server (APS)

— allows retrieval and viewing of performance measurements from the UAS

— allows maintenance action from the element manager like restarting and rebooting the UAS

— allows new UASs to be added to the network topology for management from the element manager

— allows the addition of APSs for centralizing monitoring of logs and alarms

- Preside MDM is the element manager for Media Server 15000/7400s and Multiservice Switch 15000s. Preside MDM coordinates group operations of these Passport components. Preside MDM manages the following aspects of these components:
  - physical platform components
  - software loads
  - TDM and IP physical interfaces and IP carriers
  - IP configuration parameters
  - Fault Management

  Note: Fault information from the Media Server 15000/7400s and Multiservice Switch 15000s is collected by Preside MDM, where this fault data is converted to SCC2 format. The SCC2 fault information is sent from the Preside MDM to the CS 2000 Core Manager, and then on to the operations support system (OSS).

- USP Manager is a Windows 2000 workstation which provides a graphical user interface for provisioning and monitoring of the SS7 interfaces. The workstation also provides backup and software upgrade facilities for the USP.

Tools, utilities, and user interfaces

The Succession Network comes with a number of tools, utilities, and user interfaces that enable the user to perform fault, configuration, accounting, performance management, security, and administrative tasks. Each task-based procedure identifies how to use the appropriate tool, utility, or user interface to perform the procedure.

CS 2000 Management Tools

The CS 2000 Management Tools is a collection of solutions used in the IP solutions. CS 2000 Management Tools consists of the GWC Manager, SAM21 Manager, UAS Manager, APS Manager, NPM, Nodes Configuration, Trunks Configuration, Carrier Endpoint Provisioning, Lines Configuration (SERVORD+), Line Test Manager (LTM),TMM, V5.2 Configuration, V5.2 Maintenance, APS, EMS Proxy Services, and PM Poller, QoS Collector Application, OSSGate.

Audio Provisioning Server

The Audio Provisioning Server (APS) is co-deployed with the CS 2000 GWC Manager and UAS Manager. It is a web-based tool which uses a database that manages all audio on all UASs in the network. It also consists of a user interface and a distribution service using NFS (network file system) for the distribution of announcements. It is required whenever the UAS is used as an announcement server. The

UAS uses the stored audio uploaded from the APS during call processing to play audio packages. The APS hardware platform is based on SUN Netra t1400 or Netra 240 series and uses Solaris 2.8 as its operating system.

CS 2000 Management Tools

CS 2000 Management Tools refers to a collection of software packages that contain a set of tools used to manage elements and sub-elements in a Succession network. This set of tools can run on a single server, multiple servers, or be split to run on different servers. Deployment depends on the size of the network being managed, and the customer's operational needs and preferences.

Note: The server on which the CS 2000 Management Tools software packages reside is referred to as the CS 2000 Management Tools server in the remainder of the documentation.

For a list of activities that are new for CS 2000 Management Tools in the (I)SN07 release, see What's new for the CS 2000 Management Tools on page 27.

Software

The CS 2000 Management Tools are delivered in three software packages:

- CS2M on page 206 (Call Server 2000 Management)
- APS on page 207 (Audio Provisioning Server)
- SSPFS on page 207 (Succession Server Platform Foundation)

CS2M

The CS2M (CS 2000 Management Components) software package consists of the following packages:

- the SESM (Succession Element and Sub-Element Manager) software package, which consists of the following applications:
  - CS2000 Management Tools application on page 223, which includes the following components:
    - CS 2000 GWC Manager on page 231
    - Universal Audio Server Manager on page 239
    - Audio Provisioning Server Manager application on page 229
    - V5.2 Configuration and Maintenance applications on page 55 (international version only)
    - V5.2 data integrity audit (international version only)
    - Line data integrity audit
    - Trunk data integrity audit
    - CS2K data integrity audit
    - Nodes Configuration
    - Trunks Configuration
    - Carrier Endpoint Configuration
  - Trunk Maintenance Manager on page 255 (TMM)
  - Line Maintenance Manager on page 249 (LMM)
  - Batch provisioning tool on page 259 (BPT)
  - Batch Configuration Monitor on page 265 (BCM)
  - Lines Configuration (Servord+)
  - Line Test Manager (LTM)
  - ADSL flowthrough provisioning
  - OSSGate on page 287
- the SAM21 EM (CS 2000 SAM21 Manager on page 277) software package, which consists of the CS 2000 SAM21 Manager application for the SAM21 shelf controller.
- the QCA (QoS Collector application on page 283) software package, which consists of the QoS collector application for QoS records sent from the GWC.

APS

The APS (Audio Provisioning Server) software package consists of the APS application, which enables the carrier to provision announcements on the Universal Audio Server (UAS). Refer to the UAS documentation suite for more information.

SSPFS

The Succession Server Platform Foundation Software (SSPFS).package consists of the base operating system and third-party application tools. Service applications provided in the main package are Resource monitor on page 295, Service application monitor (servman), and EMS proxy services. The Service application monitor (servman) is used to register, deregister and query the state of applications on the server where the SSPFS resides. Applications register with servman during package install, and deregister during package removal.

Sub-packages such as the PM poller on page 289, the OMPUSH application on page 291, and the Network Patch Manager on page 267, which contains the patch management application, are included as separate packages.

Oracle is the common database for the applications on the CS 2000 Management Tools server.

Hardware

The CS 2000 Management Tools software packages are installed on a Sun Netra t1400 on page 183or Sun Netra 240 on page 185server from SUN Microsystems.

Hardware for client workstations is provided under Client workstation requirements on page 211.

User interfaces

Following is a list of the applications available on the CS 2000 Management Tools server and their user interface:

- Batch provisioning tool on page 259 (BPT) - command line user interface (CLUI)
- Batch Configuration Monitor on page 265 (BCM) - web browser interface
- Line Maintenance Manager on page 249 (LMM) - graphical user interface (GUI)
- Trunk Maintenance Manager on page 255 (TMM) - web browser interface
- Network Patch Manager on page 267 (NPM) - GUI and CLUI (when installed and enabled on the same server as the CS 2000 Management Tools)
- CS2000 Management Tools application on page 223 (includes CS 2000
  GWC Manager, UAS Manager, APS Manager, V5.2 Configuration and Maintenance, Alarm Manager, and Audit System components) - GUI
- CS 2000 SAM21 Manager on page 277 - GUI
- PM poller on page 289 - CLUI
- OMPUSH application on page 291 - CLUI

For more information, refer to the description of the corresponding application in this document.

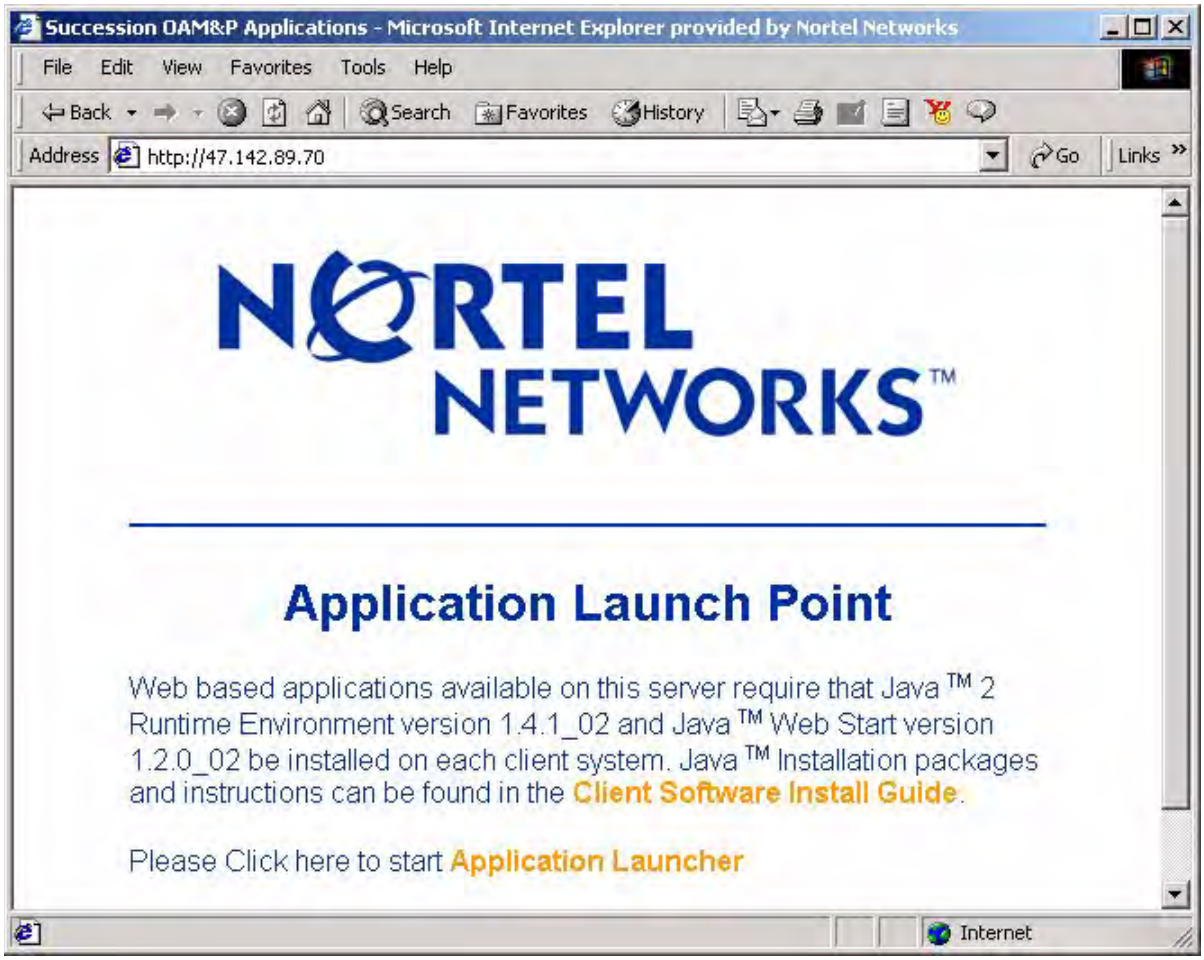
Accessing the user interfaces

Applications with a CLUI are accessed through a telnet session to the server where the applications reside.

Applications with a GUI or web browser interface are accessed through the Common launch page on page 209.

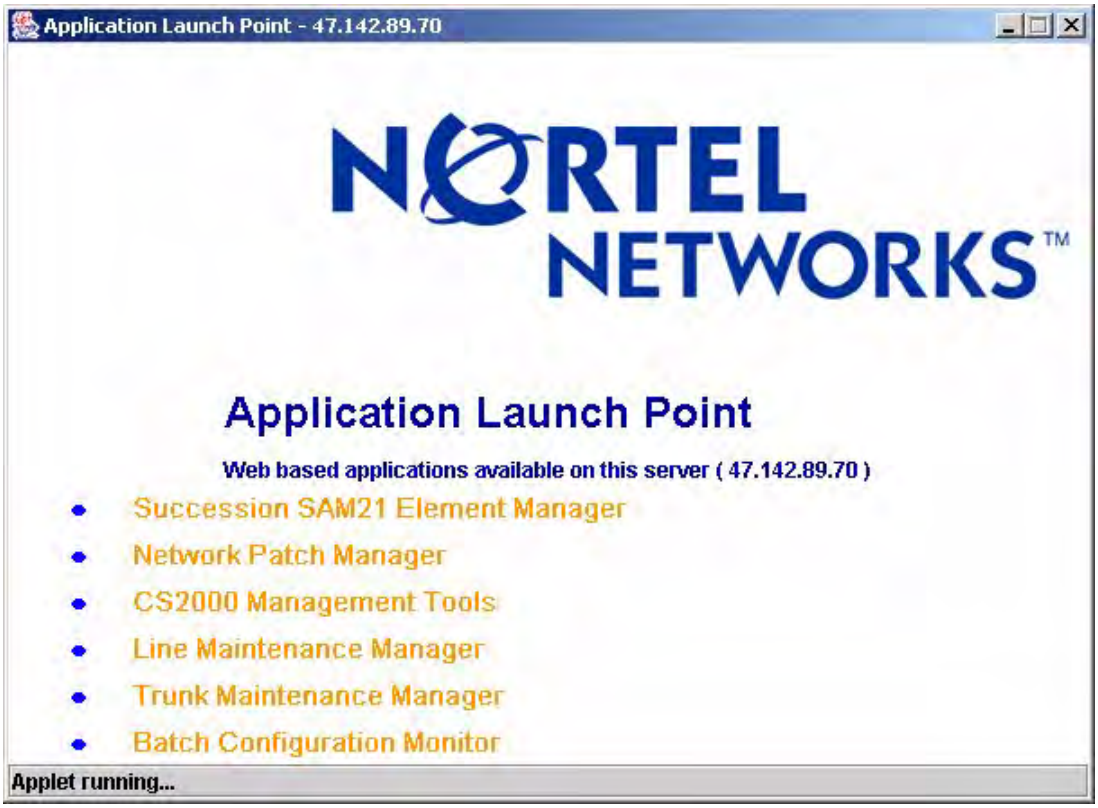
Common launch page

The launch page is accessible from a Windows or a Sun client workstation using the Internet Explorer or Netscape browser. Entering the IP address or hostname of the CS 2000 Management Tools server in the address field of the browser, launches the Application Launch Point page shown in the illustration that follows.



As indicated on the Application Launch Point page, Java ™ 2 Runtime Environment (JRE) version 1.4.1_02 and Java ™ Web Start (JWS) version 1.2.0_02 must be installed. If an older version of JWS and JRE is installed, an error message will be displayed when you click on the Application Launcher page. The “Client Software Install Guide” link on the Application Launch Point page, provides instructions on how to verify the version, and provides the installation packages and instructions, if required.

Clicking the “Application Launcher” link displays the applications that are installed and configured on the CS 2000 Management Tools server. For example, installing the CS2M software package and the NPM software package, provides links to all the applications shown in the illustration that follows.



Note 1: The “Network Patch Manager” link is only present if the NPM is installed and enabled on the same server as the CS 2000 Management Tools.

Note 2: You need to configure the Patching Server Element (PSE) to launch the NPM. Refer to procedures “Configuring the Patching Server Element” in the ATM/IP Solution-level Configuration Management document, NN10409-500. No manual configuration is necessary to launch the other applications.

To launch client applications, refer to procedure “Launching the CS 2000 Management Tools client applications” in the ATM/IP Security and Administration document, NN10402-600-600.

Note: You can also launch applications from the Integrated Element Management System (EMS) when the Integrated EMS is present in the office. Refer to the Integrated EMS User Guide, NN10321-111.

The table titled Application to solution mapping on page 211, lists the applications that can be launched from the Application Launch Point, and indicates for each application, whether it is supported for a specific Succession Solution.

Application to solution mapping

Application	PT-AAL1 NA	PT-AAL2 Int'l	PT-IP NA	PT-IP Int'l	UA-AAL1 NA	UA-IP NA	UA-IP Int'l	IAC	IA-IP	IAW
Trunk Maintenance Manager	n	n	y	y	n	y	y	y	y	y
CS2000 Management Tools	n	y	y	y	y	y	y	y	y	y
Line Maintenance Manager	n	n	n	n	n	n	n	y	y	y
Batch Configuration Monitor	n	n	n	n	y	y	y	n	n	n
Succession SAM21 Element Manager	n	y	y	y	y	y	y	y	y	y
Audio Provisioning Server Manager	n	y	y	y	n	y	y	y	y	y
n = not supported y = supported										

Client workstation requirements

The operating systems (O/S) supported to run the CS 2000 Management Tools client applications are as follows:

- Windows 2000, Windows XP, and Windows 2003 to current
- Solaris 2.8 and 2.9 to current

Note: The functionality of the client applications is the same on a Windows and Solaris O/S, but the appearance of the screens is different.

The supported browsers are as follows:

- Mozilla 1.4 to current (Solaris)
- Netscape 6.2 to current and Internet Explorer 6 SP1 to current (Windows)

Note: Ensure you keep your browser patch-current.

ATTENTION
It is important that your memory cache be large enough to keep large search result pages in memory. Therefore, ensure that your cache is set to a minimum of 1024 KB. For Netscape users, you can set your cache under Edit->Preferences->Advanced->Cache. For IE users, you can set your cache under Tools->Internet Options->General->Temporary Internet files->Settings.

Nortel Networks has explicitly tested the following versions:

- Windows: Netscape 6.2.3 and 7.0, Internet Explorer 6.1 SP1
- Solaris: Mozilla 1.4

Note 1: Nortel Networks recommends the use of Nortel-verified browser and operating system combinations. Use of other versions are supported. Any compatibility issues will be resolved using standard Nortel support processes.

Note 2: Ensure Solaris clients, using Java™ Web Start (JWS), have font package SUNWi1of installed. This font package ensures correct GUI (graphical user interface) display on Solaris clients. You can view font package requirements for Solaris as follows: http://<host>/client/solaris/font-requirements.html.

Note 3: The only user locale setting supported for proper functioning of the CS 2000 Management Tools applications on a Solaris or Windows operating system, is English. The user locale setting is used to display numbers, currencies, dates, and times.

Access to some functions of the CS 2000 Management Tools requires the use of SSH-compatible client software for access to secure telnet and ftp services through the SSH standards. SSH clients are supplied bundled with some operating systems, but may need to be obtained separately. Following are some sources for SSH clients:

- PUTTY - freeware
- OpenSSH - freeware
- SSH Inc.- commercial
- Secure CRT- commercial
- WinSCP - freeware

Note: Nortel Networks does not supply or recommend a particular supplier.

Minimum hardware

The minimum hardware for Windows clients is as follows:

- Monitor size: 19 in.
- Resolution: 1280x1024 with 256 colors
- Hard disk space: 10GB (500MB free space for all clients per switch)
- Processor: Pentium III 1.4GHz or higher
- RAM requirements: 1GB
- Network: 10/100Base-T Ethernet network connection

The minimum hardware for Solaris clients is as follows:

- Resolution: 1280x1024 with 256 colors
- Hard disk space: 200MB
- Processor: Ultra 10 400MHz or higher
- RAM requirements: 256MB
- Network: 10B/100Base-T Ethernet network connection

Succession Server Platform Foundation Software (SSPFS)

Overview

The Succession Server Platform foundation software (SSPFS) is a high-performance, UNIX-based processing platform based on Sun Microsystem's Netra line of NEBS compliant servers.

The SSPFS platform is intended to be used as the platform for OAM&P services in the Succession Network. These services include, but are not limited to the various Element Management systems for the Network Elements.

The Succession Server Platform foundation software (SSPFS) package consists of the base operating system and Third party common software on page 217. Service applications provided in the main package are, Resource monitor, on page 295, Service application monitor (servman), and EMS proxy services.

The Service application monitor (servman) is used to register, deregister and query the state of applications on the server where the SSPFS resides. Applications register with servman during package install, and deregister during package removal.

Service applications such as Sun Explorer, the , the , OMPUSH application, on page 291, and the , Network Patch Manager, on page 267, which contains the patch management application, are included as separate packages.

Only one instance of the NPM can be installed and enabled in an office. Depending on your office configuration, your choices are as follows:

- Integrated Element Management Server (EMS), which is the most preferred location
- CS 2000 Management (CS2M)Tools server when the Integrated EMS is not present in the network

Process Management

SSPFS platform process management performs the following functions:

- starts applications at boot up
- closes all applications at shutdown
- monitors applications to determine their condition
- restarts applications that fail

Data reliability software

The following features ensure reliable and continuous data storage:

- a journalled file system - confirms the accuracy of the resident file system after accidental shut down and power failure.
- logical volume partitioning - the SSPFS platform supports partitioning of disks into different logical volumes. Each logical volume can be considered an enforced partition of disk resources. Logical volume partitioning protects data and programs from exhaustion of their space by one or more processes.
- disk mirroring - the SSPFS platform stores a copy of all data that is written to logical volume. In the event of a disk failure, the system can read from and write to the remaining disk without interruption.

Third party common software

The SSPFS third party software is contained in SSPFS through the use of Sun packages. This provides a consistent way of delivering all of the Solaris software, third party software and Nortel applications. By using the same software packaging scheme, installing applications is consistent for all OAM&P products that make use of the SSPFS platform.

The following table lists the third party software that is included with the SSPFS:

Note: This product includes code licensed from RSA Security, Inc. Some portions licensed from IBM are available at http://OSS.software.ibm.com/icu4j/.

Software included with SSPFS

Vendor	Software
Sun Microsystems	• Solaris 8 Software OS • JDK/JRE • JAXP • Java JSSE • Java Web Start Client
AdventNet	• SNMP API • Adventnet
Apache	• Apache Web Server • Xerces Java Parser • Xalan
AppGate	• Mindterm
IBM	• DCE Client
Exolab group	• OpenORB notification • OpenORB Naming Service
Jakarta	• Tomcat • ORO • Log4J

Software included with SSPFS

Vendor	Software
Open Source	• OpenSSH • OpenSSL • Java FTP client • RPM
ProFTPD	• proftpd
SourceForge.net	• Expat • Net-snmp
Oracle	• Oracle client • Oracle server
--	• bootp-DD
Continuous Computing Corporation	• UpSuite • UpLink
--	• Net-snmp
Courtesan	• Sudo
tcl developers xchange	• tcl • tk
Interhack	• rotatelog
Comprehensive Perl Archive Network	• Perl • Perl modules
DeleGate	• DeleGate
TrustICE	• Syslog client
NIST	• Expect
ILOG	• JTGO • JViews

System and database backup

SSPFS lets you backup and restore the system and database. The information is backed up on a Digital Audio Tape (DAT) or a DVD-RW.

System backup

Applications and the system have several sets of configuration files with static information about the system configuration and operating parameters. This information is backed up in-service using standard Unix commands and a Solaris 8 feature called SNAPFS which takes a snapshot of the file system.

The file system layout for SSPFS-installed machines is as follows:

Note: File systems "/", "/var", "/data", "/opt", and "/opt/nortel" are available on every system. The other file systems vary according to the applications installed on the system.

File system	Types of information stored in file system
/	operating system software and administrations
/var	operating system software and administrations
/data	application data in flat files
/opt	third-party software as Platform common services
/opt/nortel	Nortel applications
/data/oradata	Oracle data files (only present with the CS2M and APS)
/data/qca	QoS Collector Application (QCA) data (only present with the CS2M)
/data/mg9kem/logs	MG 9000 Manager logs (only present with MG 9000 Manager)
/PROV_data	audio transaction files before they are sent to the UAS (only present with APS)
/user_audio files	audio uploaded from the user desktop prior to its import into the database (only present with APS)
/audio_files	audio data that has been imported into the database (only present with APS)

Database backup

The Oracle database includes its own utilities to perform live backup and restore of the database. The database information is maintained on a Digital Audit Tape (DAT) or Digital Video Disk-Re-Writable (DVD-RW).

Backup schedules and recommended policies

This section contains backup schedules and recommended policies.

Application data in the Oracle database

The application data in the Oracle database is not automatically backed up. You can enable automated Oracle data backups, where the system backs up all application data in the Oracle database on a daily basis at a specified time to a DAT or DVD-RW. Refer to procedure “Configuring automated Oracle data backups” in the Configuration Management document.

Data on a DVD cannot be overwritten, therefore, you must insert a blank DVD prior to the next scheduled backup.

If you leave the same DAT in the drive, the contents of the DAT will be replaced with the new backup data when the backup is scheduled to run. If you want to preserve the daily backup of your application data, remove the DAT from the drive and insert a new one prior to the next scheduled backup. It is recommended that you label the DAT with the date, time and content (oracle backup data). You can restore all application data from this DAT at any time. Refer to procedure “Restoring application data to the Oracle database” in the ATM/IP Security and Administration document, NN10402-600.

ATTENTION

In order to maintain network functionality, the CS 2000 Management Tools persistent data in the Oracle database and the associated CORE/CM tables must match at all times. Therefore, it is recommended that the CS 2000 Management Tools support person modify the automated oracle data backup schedule to run in parallel to the customer's CORE Image Dump schedule. This will ensure that there are always CORE Images and CS 2000 Management Tools database backups that are 100% identical in configuration information.

To view or change the current configuration settings for automated backup of Oracle data, refer to procedure Refer to procedure “Configuring automated Oracle data backups” in the Configuration Management document.

File systems

It is recommended you back up file systems after installing a new release of SSPFS software and all the Nortel Succession application software.

CS2000 Management Tools application

Overview

The CS2000 Management Tools application is a web-based GUI (graphical user interface) that provides the following capabilities:

- provision gateway controllers (GWCs), audio provisioning servers (APSs), universal audio servers (UASs), media gateways, carriers, media proxies, Network Address Translators (NATs), Policy Enforcement Point (PEP) servers, Quality of Service (QoS) collectors, and V5.2 interfaces (only in international version)
- view the topology and system faults, query and perform certain change operations
- perform line, trunk, and CS2K data integrity audits

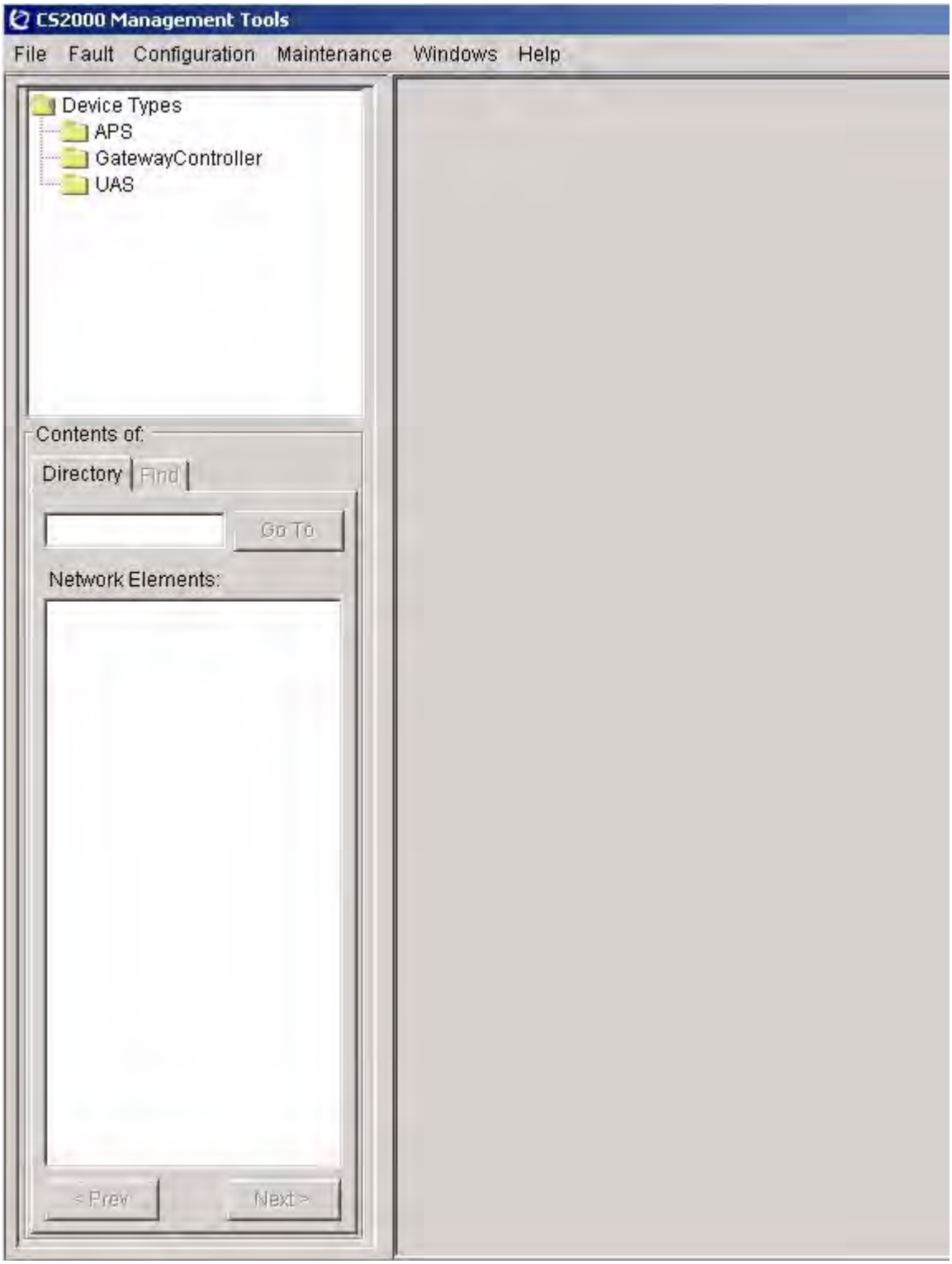
Note: To determine if this application is supported for your solution, refer to the table titled Application to solution mapping on page 211.

User interface

The CS2000 Management Tools application GUI is accessed through the common launch page as previously described under Common launch page on page 209. To access the CS2000 Management Tools application GUI, refer to procedure “Launching the CS 2000 Management Tools client applications” in the ATM/IP Security and Administration document, NN10402-600.

When the CS2000 Management Tools application is launched, a window, similar to the following is displayed:

CS2000 Management Tools GUI



Selecting a device under Device Types displays any provisioned network elements for that device under Contents of:.

Search capabilities for network elements of the selected device type, are provided through the Find tab and the Go to button, and scrolling capabilities are provided through the Prev (previous) and Next buttons.

The pane on the right side of the CS2000 Management Tools application GUI is a display area for device and network element information. The display varies according to the device type and associated network element selected. For details on each device type, refer to Audio Provisioning Server Manager application on page 229, CS 2000 GWC Manager on page 231, or Universal Audio Server Manager on page 239 in this document.

The sections that follow briefly describe the options available under each menu in the CS2000 Management Tools GUI.

Note: Some of the options in the menus are available only when a device that uses the function is selected.

File

The File menu contains the options to view the software version information, and Exit the CS2000 Management Tools GUI.

File menu

Fault

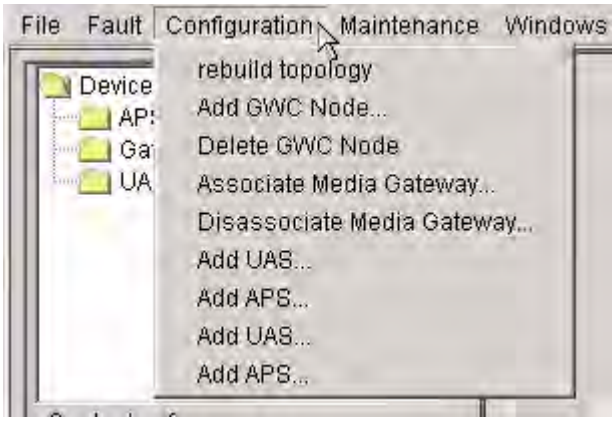
The Fault menu contains the options to open the Alarm Manager window and the Alarm History window used to manage alarms on the system. For more information, refer to the ATM/IP Solution-level Fault Management document, NN10408-900.

Fault menu

Configuration

The Configuration menu contains the options to rebuild the topology, add or delete network elements (GWC, UAS, and APS), associate or disassociate media gateways to or from GWCs, and manage V5.2 interfaces (only in international version).

Configuration menu



Maintenance

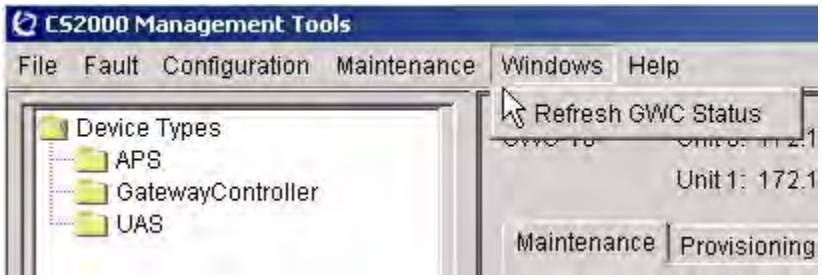
The Maintenance menu contains the Audit System option used to perform a line data integrity, trunk data integrity or CS2K data integrity audit. The audits track the integrity of line-specific, trunk-specific, and node-specific data shared between the XA-Core and CS 2000 GWC Manager data in the database. Refer to procedure “Performing an audit” in the Fault Management document.

Maintenance menu

Windows

The Windows menu contains the option to refresh the status of a network element when one is selected. The example below shows the Windows menu option when a GWC network element is selected and displayed.

Windows menu



Help

The Help menu contains the option to display help information on the Gateway Controller.

Help menu

Audio Provisioning Server Manager application

Overview

The Audio Provisioning Server (APS) Manager application is available to view alarms and logs sent by the APS network elements (NEs). No management functionality is available from this application.

> ***Note:*** To determine if this application is supported for your solution, refer to the table titled Application to solution mapping on page 211.

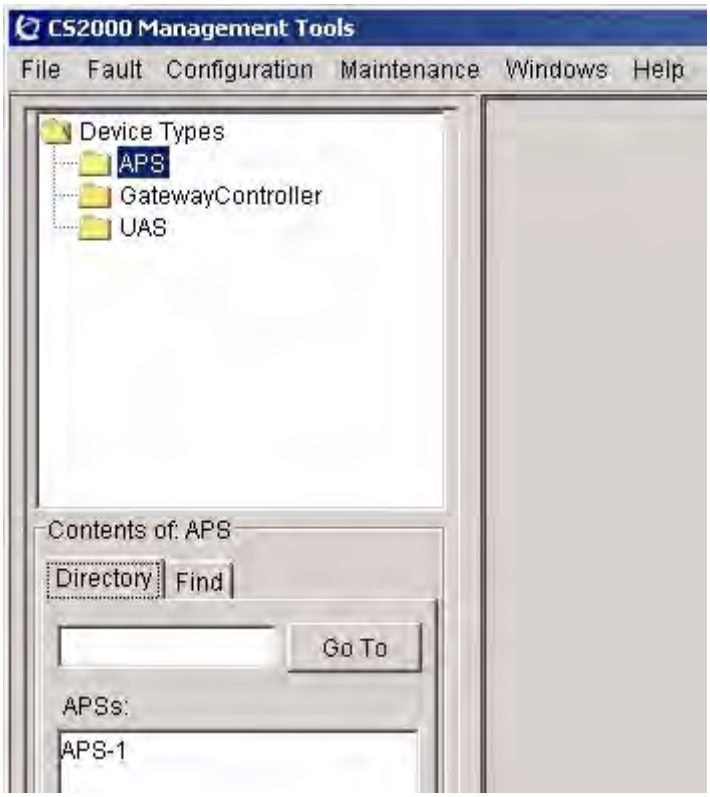
For procedures on how to provision and maintain APS NEs, refer to the UAS documentation suite.

User interface

The APS Manager application is a component of the CS2000 Management Tools application GUI (graphical user interface), which is accessed through the common launch page as previously described under Common launch page on page 209. To access the CS2000 Management Tools application GUI, refer to procedure “Launching the CS 2000 Management Tools client applications” in the ATM/IP Security and Administration document, NN10402-600.

When the APS device type is selected, a window, similar to the following is displayed:

Selecting APS



Adding or deleting an APS device to or from the network topology is done through the CS2000 Management Tools Configuration menu. Once an APS device is added to the topology, users can view APS alarms and logs through the Alarm Manager and Alarm History, which are accessed through the Fault menu. Refer to the ATM/IP Fault document, NN10325-900.

CS 2000 GWC Manager

Overview

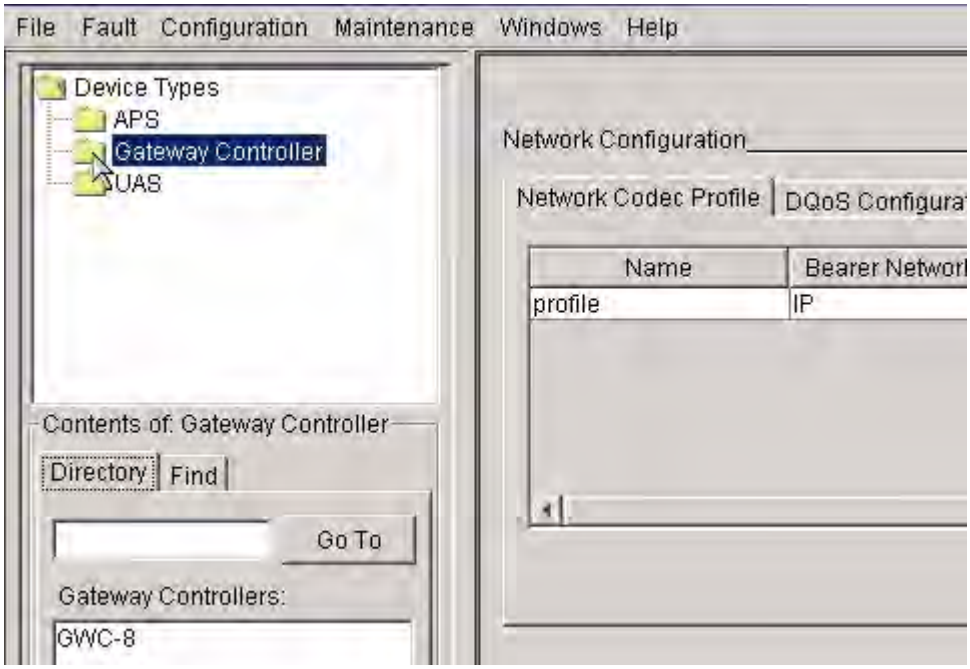
The CS 2000 GWC Manager is used to manage the GWC network elements (NEs) within a Succession Network.

This section provides a brief overview of the CS 2000 GWC Manager. For procedures on how to provision and maintain GWC NEs using the CS 2000 GWC Manager, refer to the GWC documentation suite, or the GWC online help.

User interface

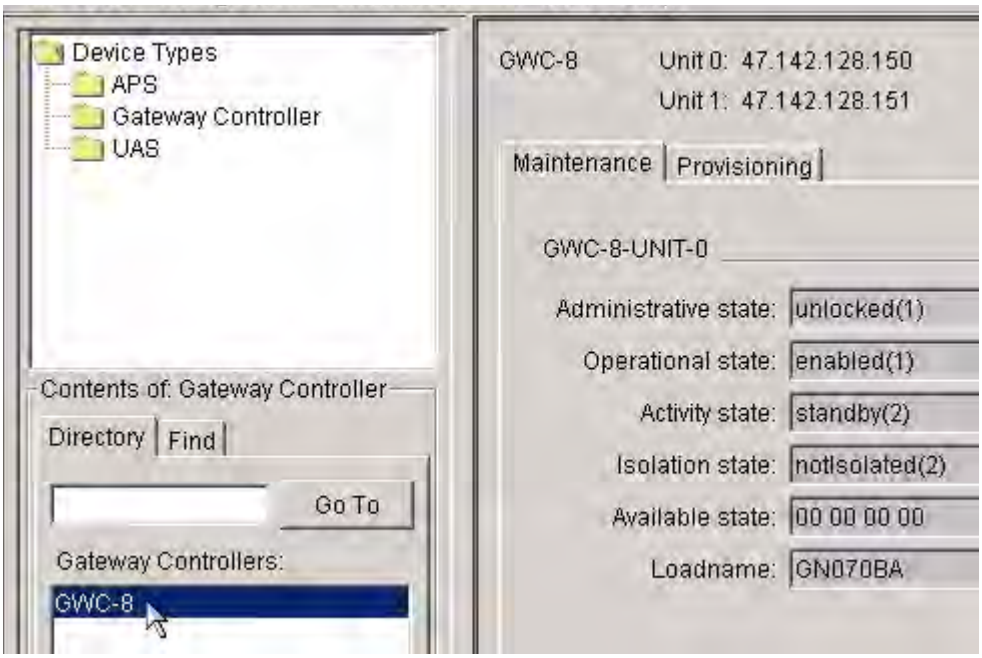
The CS 2000 GWC Manager is a component of the CS2000 Management Tools application GUI (graphical user interface), which is accessed through the common launch page as previously described under Common launch page on page 209. To access the CS 2000 GWC Manager, refer to procedure “Accessing the GUI for the CS 2000 GWC Manager” in the ATM/IP Security and Administration document, NN10402-600.

Selecting the “GatewayController” device type as shown in the figure below, displays network configuration information in the right pane (network view). The information applies to all GWC NEs in the network.



Network view

Selecting a specific GWC network element (NE) under “Contents of: GatewayController” as shown in the figure below, displays information about the selected GWC NE in the right pane (node view).

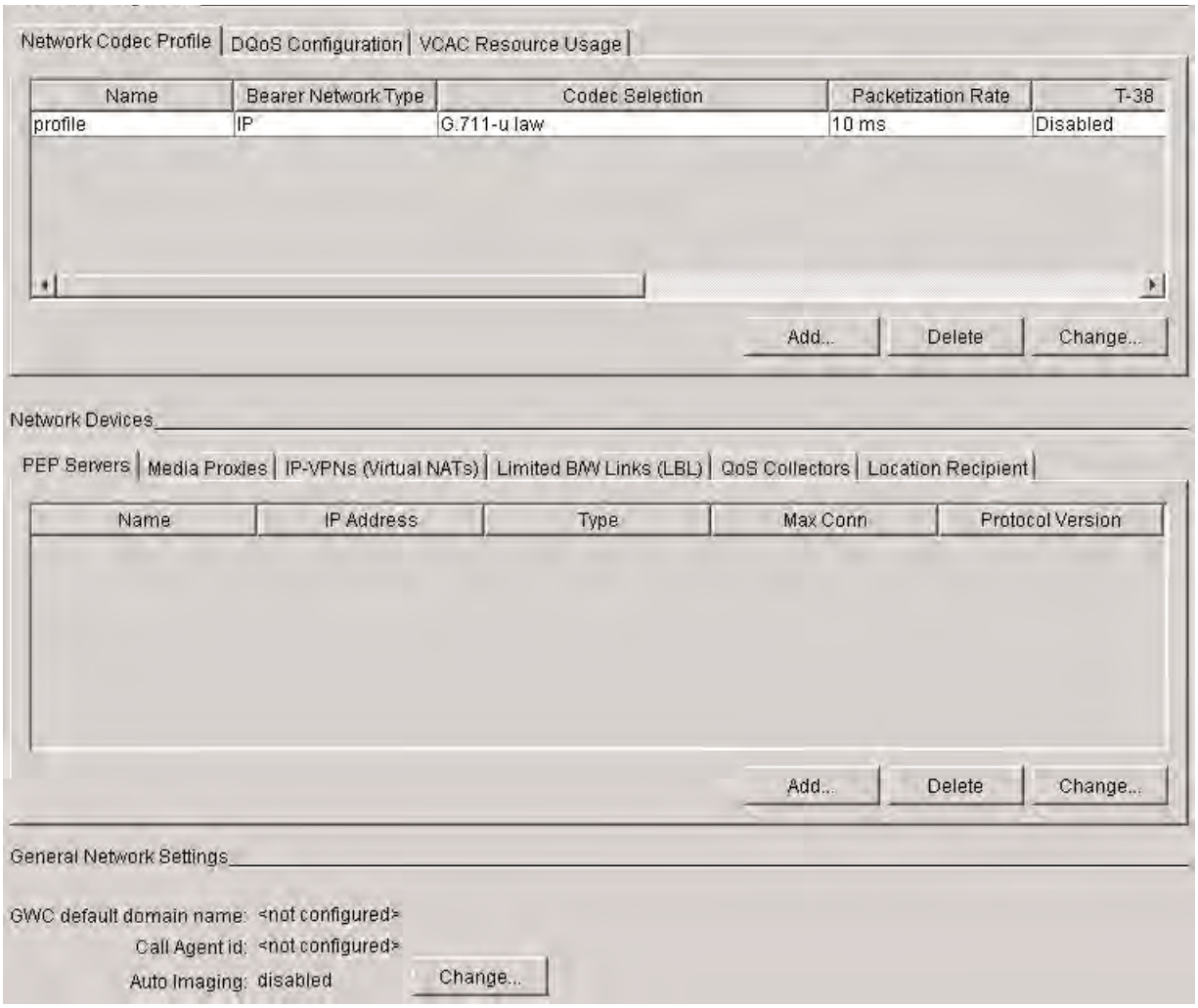


Node view

Managing the GWC NEs is done through the Network view and Node view of the CS 2000 GWC Manager, and some menu options in the CS2000 Management Tools application GUI as previously mentioned in ., CS2000 Management Tools application, on page 223

Network view

The Network view, similar to the following, displays information related to all GWC NEs in the network.



From the Network view, you can perform any of the following activities:

Network Configuration

- Network Codec Profile tab - Add or delete a codec profile to or from the network, or change information for an existing codec profile.
- DQoS Configuration tab - Change the dynamic Quality of Service (DQoS) system policy data for the GWCs in the network.

- VCAC Resource Usage tab - Add or delete resource usage data for use in the Virtual Connections and Admissions Control (VCAC) function of a limited bandwidth link (LBL), or change the resource usage data.

Network Devices

- PEP Servers tab - Add or delete a Policy Enforcement Point (PEP) server to or from the network, or change the information of an existing PEP server. A PEP server communicates with the GWC to provide dynamic quality of service (DQoS) and other policy services for the associated gateways.
- Media Proxies tab - Add or delete a media proxy server to or from the network, or change the information of an existing media proxy server.
- IP-VPNs (Virtual NATs) tab - Add or delete a Network Address Translations (NATs) device to or from the network, change the information of an existing NAT device, and display the ID of a NAT device.
- Limited B/W Links (LBL) tab - Add or delete a limited bandwidth link (LBL) middlebox to or from the network, or change the configuration information for an existing LBL middlebox.
- QoS Collectors tab - Add or delete a Quality of Service (QoS) collector to or from the network.
- Location Recipient tab - Change the values of the location recipient. The values cannot be changed if “Location Identification Reporting” is enabled on one or more gateway controllers (see Provisioning tab on page 236)

General Network Settings

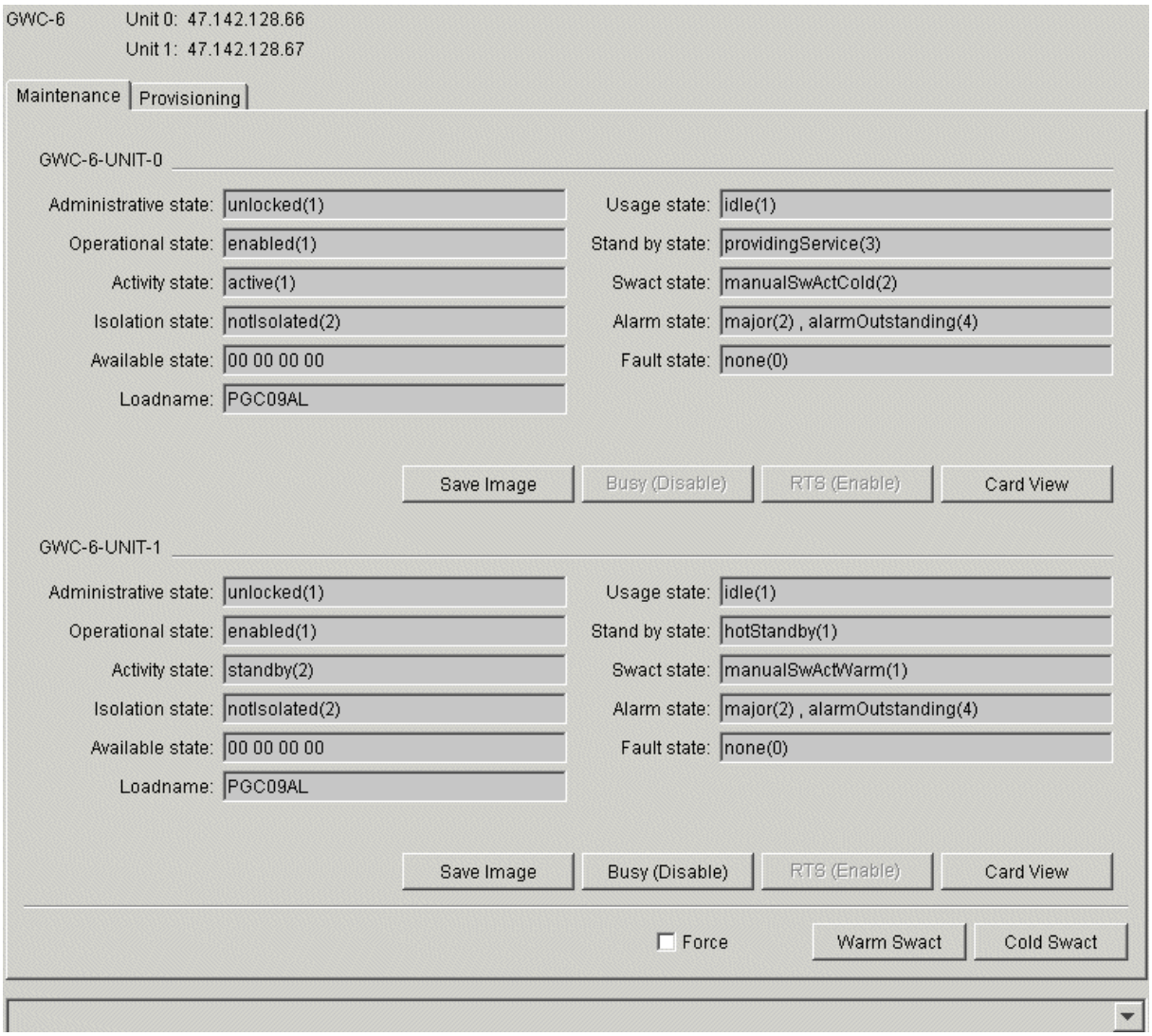
- Change button - Add, change, or delete the GWC domain name, change the call agent identifier, and enable or disable periodic auto-imaging of GWC loads. It is recommended that auto imaging be enabled in order to prevent potential losses of patching applications.

Node view

The Node view displays information related to individual GWC NEs in the network. The Node view consists of a Maintenance tab and a Provisioning tab, as well as a status bar, located at the bottom of the main panel, which displays operation messages. You can display the previous twenty messages from the drop-down list.

Maintenance tab

The Maintenance tab, similar to the following figure, displays the details related to each GWC unit.



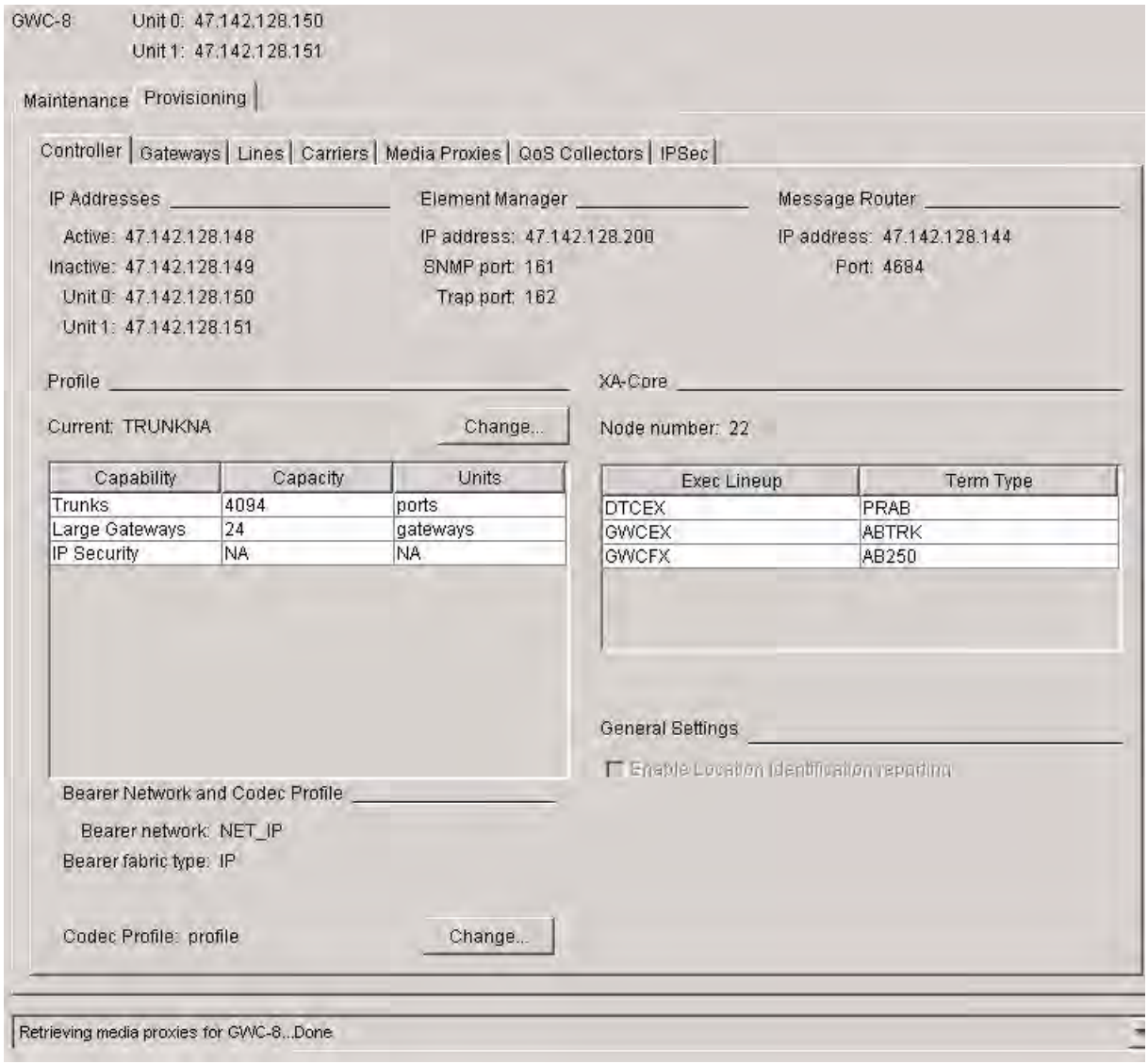
From the Maintenance tab you can perform any one of the following activities:

- Save Image button - save an image of each GWC unit
- Card View button - display the card view of each GWC unit
- Busy (Disable)/RTS (Enable) buttons - busy and return a GWC unit to service

- Warm Swact/Cold Swact buttons - perform a warm or cold switch of activity (Swact)
- Force option - give priority to the next maintenance request to override some pending operations

Provisioning tab

The provisioning tab, similar to the following figure, displays configuration data associated with a GWC NE.



From the Provisioning tab you can perform any one of the following activities:

- Controller tab - View the data specific to the selected gateway controller, including the gateway controller profile that is currently provisioned with a list of capabilities associated with that profile, change the gateway controller profile if the provisioned profile supports change, view and change the codec configuration, and enable or disable location identification reporting, which is only valid for gateway controllers with a “large line gateway” profile. Location identification reporting can only be enabled when the location recipient is configured (see Network view on page 233).
- Gateways tab - View a list of media gateways (MGs) associated with the GWC, associate or disassociate an MG to or from the GWC, or modify the MG configuration.
- Lines tab - View configuration data for lines associated with the selected gateway controller.
- Carriers tab - View configuration data for carriers associated with the selected gateway controller, add or delete a carrier to or from the selected gateway controller, and display the trunks for the selected carrier.
- Media Proxies tab - View configuration data for media proxies associated with the selected gateway controller, and associate or disassociate a media proxy to or from the gateway controller.
- QoS Collectors tab - View configuration data for the QoS collectors associated with the selected gateway controller, associate or disassociate a QoS collector to and from the gateway controller, and enable or disable QoS collection on the gateway controller.
- IPSec tab - View IP security configuration data associated with the selected gateway controller. Each tab shows the data that is currently provisioned, and each tab provides an Add, Change, and Delete button to perform various provisioning actions.

Universal Audio Server Manager

Overview

The Universal Audio Server (UAS) Manager application is used to manage the UAS network elements (NEs) within a Succession Network. With the UAS Manager application, users can view general information, perform various configuration and maintenance tasks, and view performance measurements for UAS NEs.

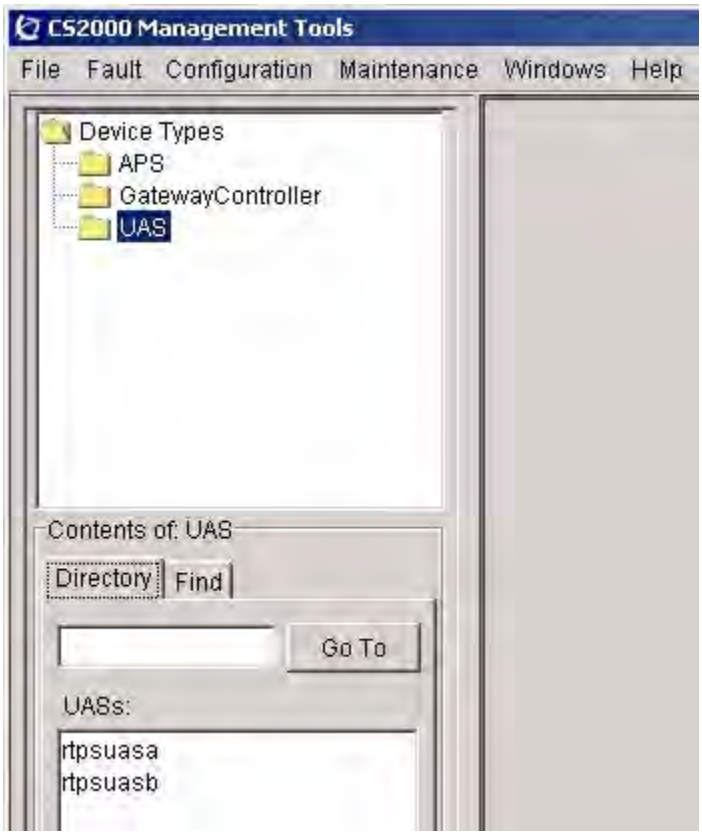
This section provides a brief overview of the UAS Manager. For procedures on how to provision and maintain UAS NEs using the UAS Manager, refer to the UAS documentation suite.

User interface

The UAS Manager is a component of the CS2000 Management Tools application GUI (graphical user interface), which is accessed through the common launch page as previously described under Common launch page on page 209. To access the CS2000 Management Tools application GUI, refer to procedure “Launching the CS 2000 Management Tools client applications” in the ATM/IP Security and Administration document, NN10402-600.

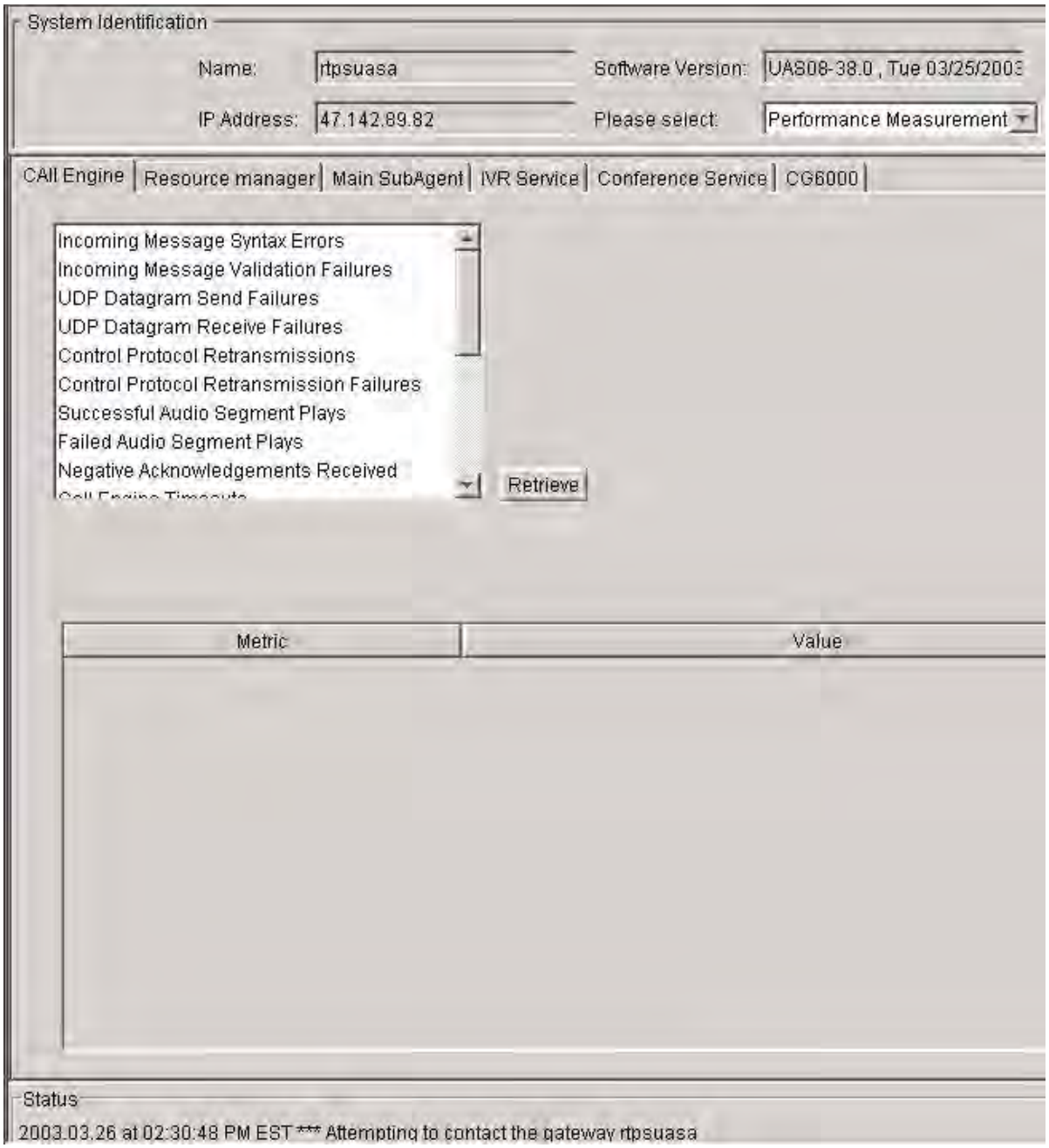
When the UAS device type is selected, a window, similar to the following is displayed:

Selecting UAS



Selecting a specific UAS network element (NE) under Contents of: UAS, displays information about that UAS NE in the right pane of the CS2000 Management Tools GUI as shown in the following example:

Selecting a UAS network element



The top portion of the pane displays information about the selected UAS network element and provides a drop down menu where you select one of the following options; Performance Measurement, Maintenance, Configuration or SNMP Configuration.

The middle portion of the pane varies according to the option selected, and the bottom portion of the pane displays operation messages.

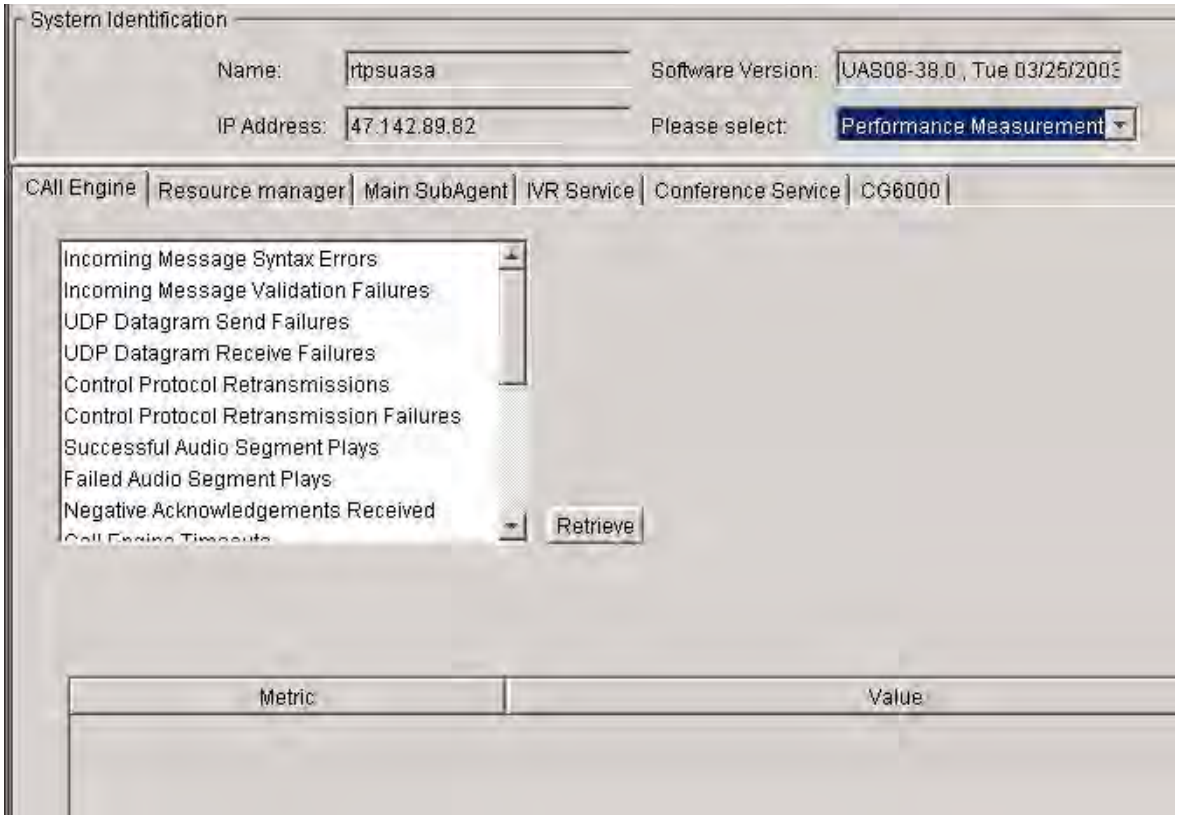
Managing UAS NEs is done through the Performance Measurement, Configuration, Maintenance, and SNMP Configuration options of the UAS Manager, and some menu options in the CS2000 Management Tools application GUI as previously mentioned in CS2000 Management Tools application on page 223.

The sections that follow briefly describes each of the options of the UAS Manager.

Performance Measurement

Selecting the Performance Measurement option from the drop-down menu, displays a window similar to the following.

Performance Measurement window

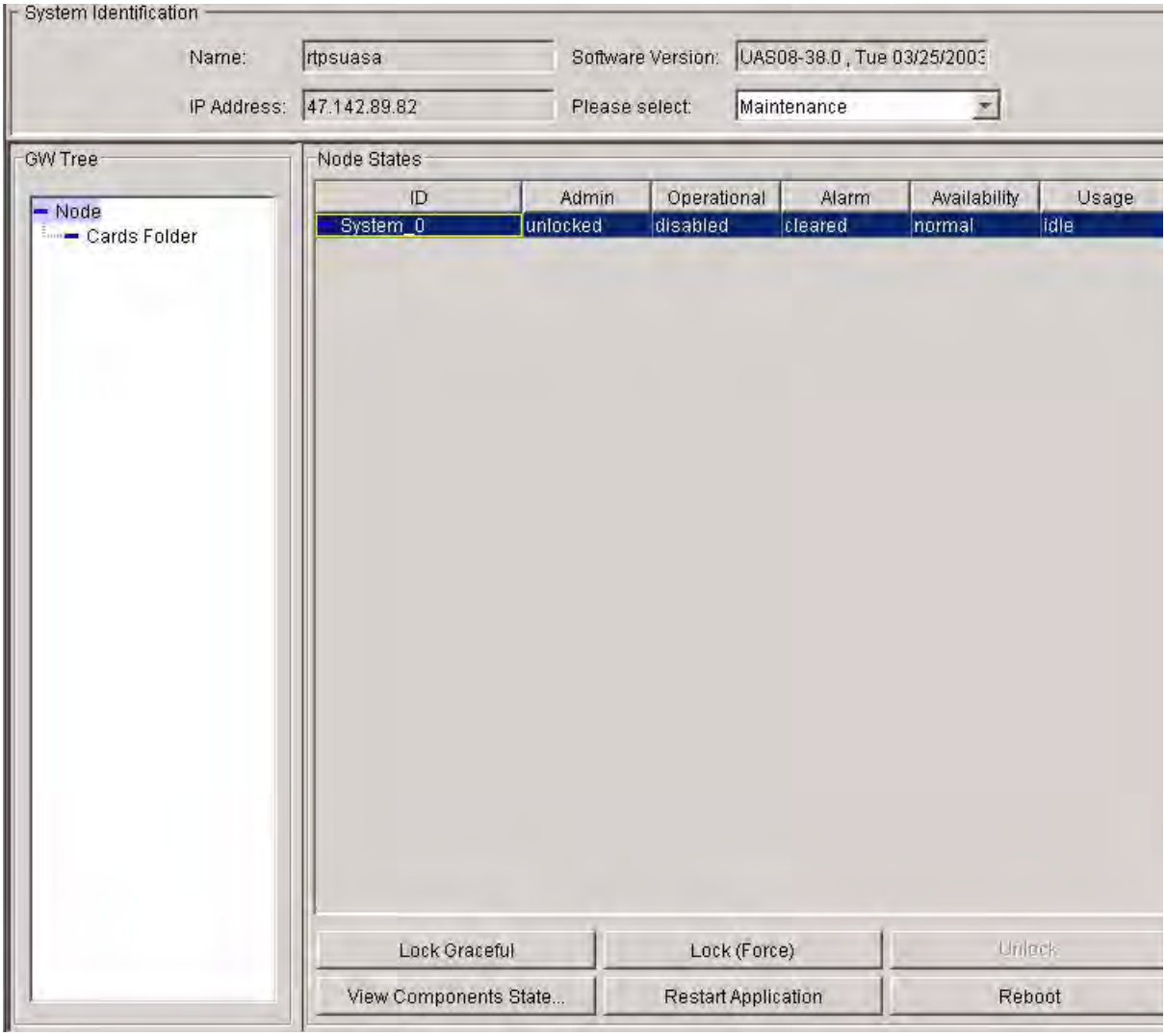


From this window, you can view the statistics collected for the selected UAS node. The types of statistics you can view are in individual tabs as shown above. For details on the statistics you can view in each tab, refer to the UAS Performance Monitoring document, NN10139-711.

Maintenance

Selecting the Maintenance option from the drop-down menu and selecting Node from the GW Tree, displays a window similar to the following.

Maintenance (Node view)



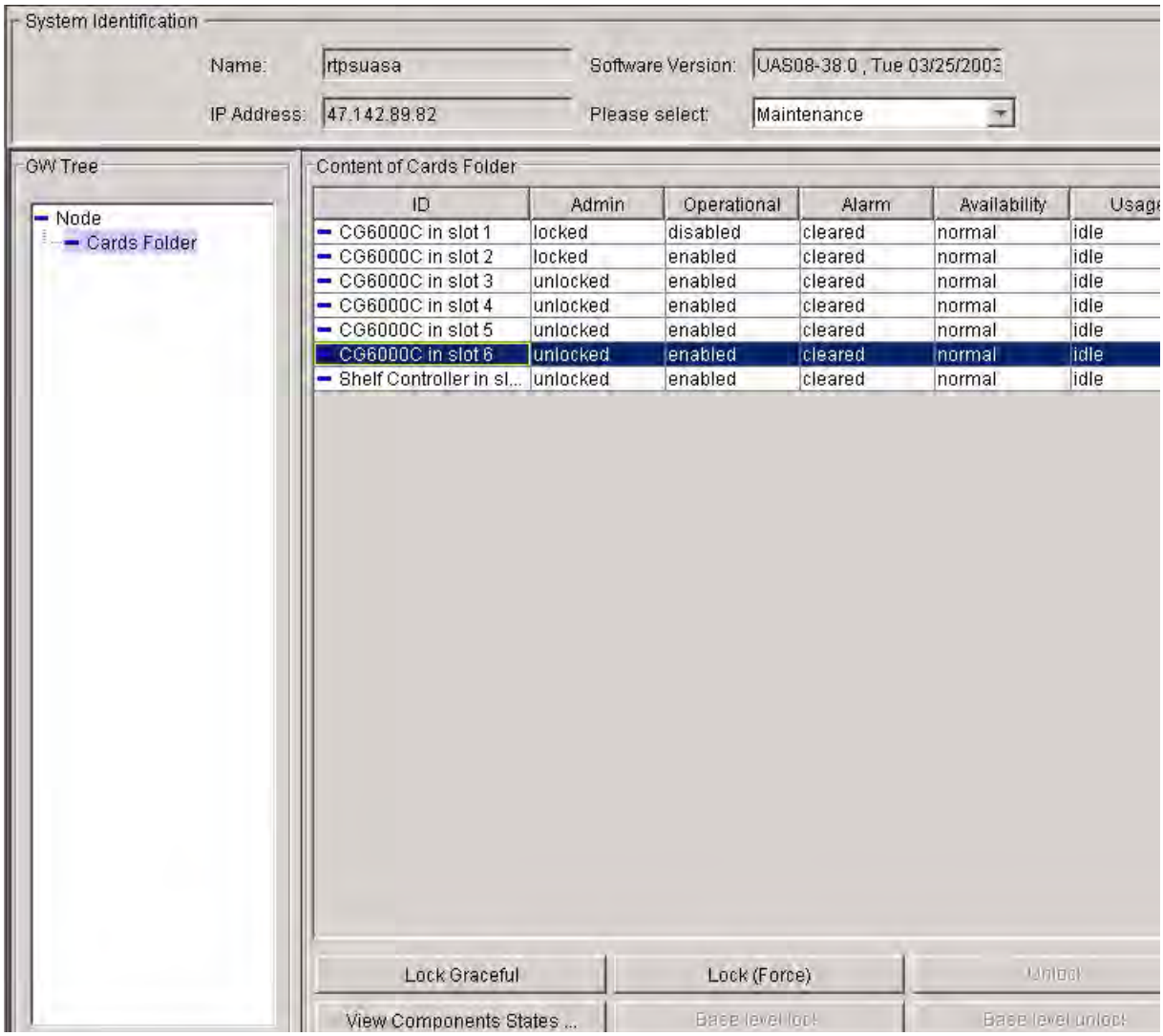
From this window, you can perform any one of the following activities: reboot the UAS, restart the UA

- Lock Graceful button - lock a UAS node
- Lock (Force) button - lock a UAS node (overriding any pending operations)
- Unlock button - unlock a UAS node

- View Component States... button - view component states associated with the selected UAS node
- Restart Application button - restart the UAS server application
- Reboot button - reboot the UAS node

Selecting Cards Folder from the GW Tree, displays a window similar to the following:

Maintenance (card view)



From this window, you can perform any one of the following activities: reboot the UAS, restart the UA

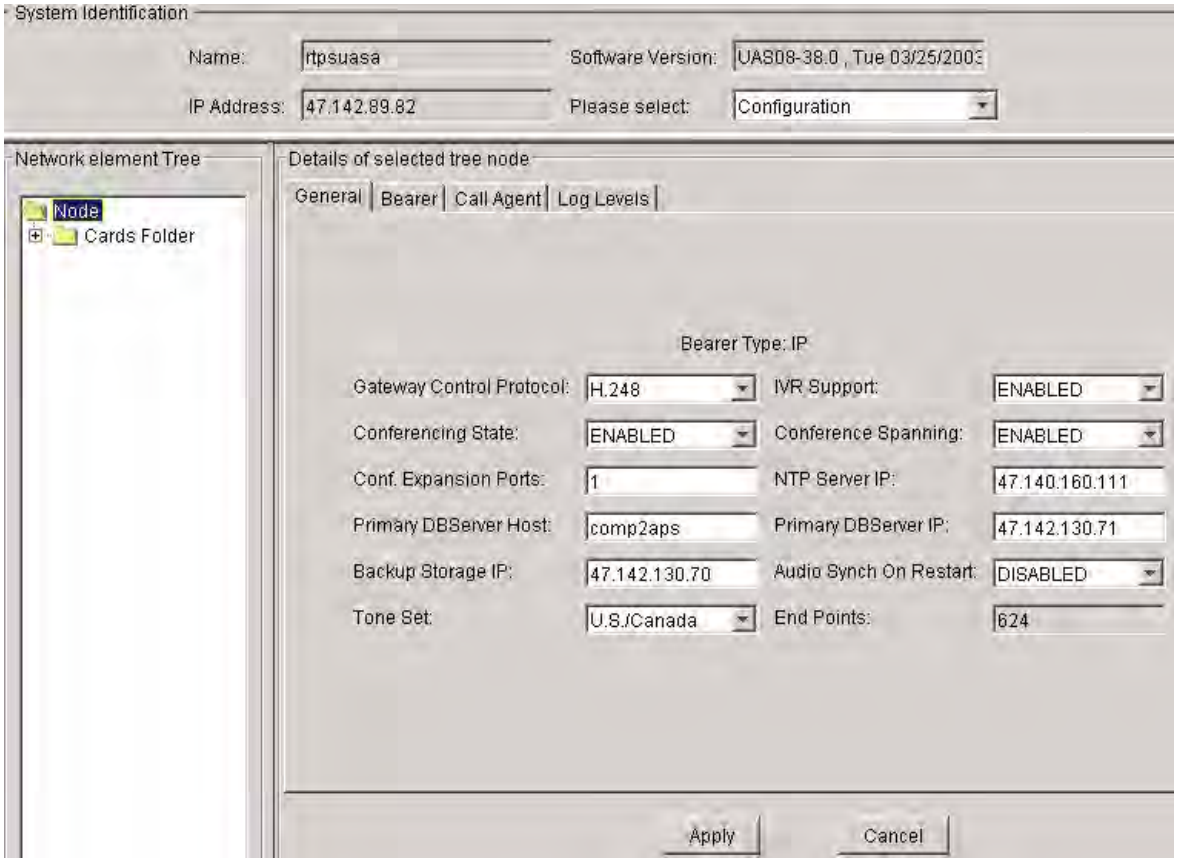
- Lock Graceful button - lock a card but not completely shut it down (used to perform some administrative tasks on the card)
- Lock (Force) button - lock a card (overriding any pending operations)
- Unlock button - unlock a card
- View Component States... button - view component states associated with the selected UAS node
- Base level lock button - lock a card and completely shut it down (used to replace or remove the card)
- Base level unlock button - unlock a card from a complete shut down

Note: The lock and unlock functions are only available for the CG6000 card type.

Configuration

Selecting the Configuration option from the drop-down menu and selecting Node from the Network element Tree, displays a window similar to the following.

Configuration (node view)

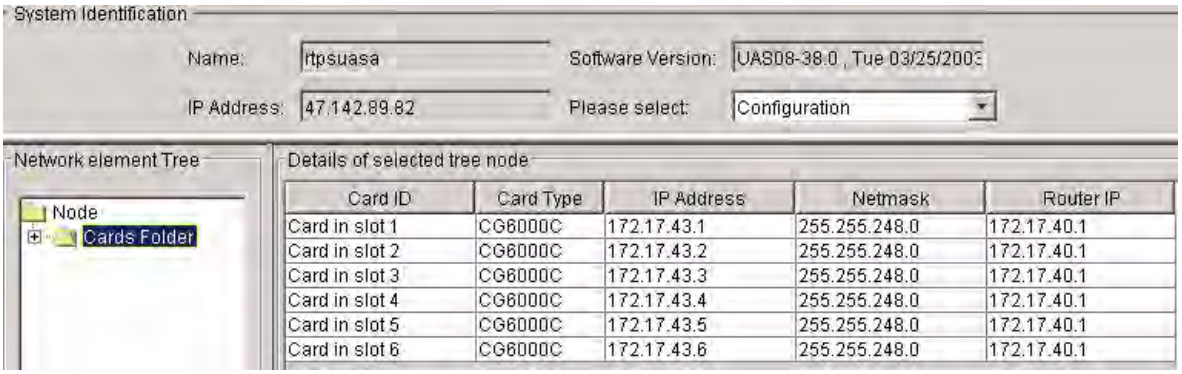


From this window, you can perform any one of the following activities:

- General tab - modify configuration data for the UAS node
- Bearer tab - modify configuration data for the bearer card associated with the selected UAS node
- Call Agent - modify the configuration data for the call agent associated with the selected UAS node
- Log Levels tab - modify the logs you want to have sent to the element management station
- Apply button - apply the configuration changes you made
- Cancel button - cancel the configuration changes you made and return the fields to their original value

Selecting Card Folder from the Network element Tree, displays a window similar to the following:

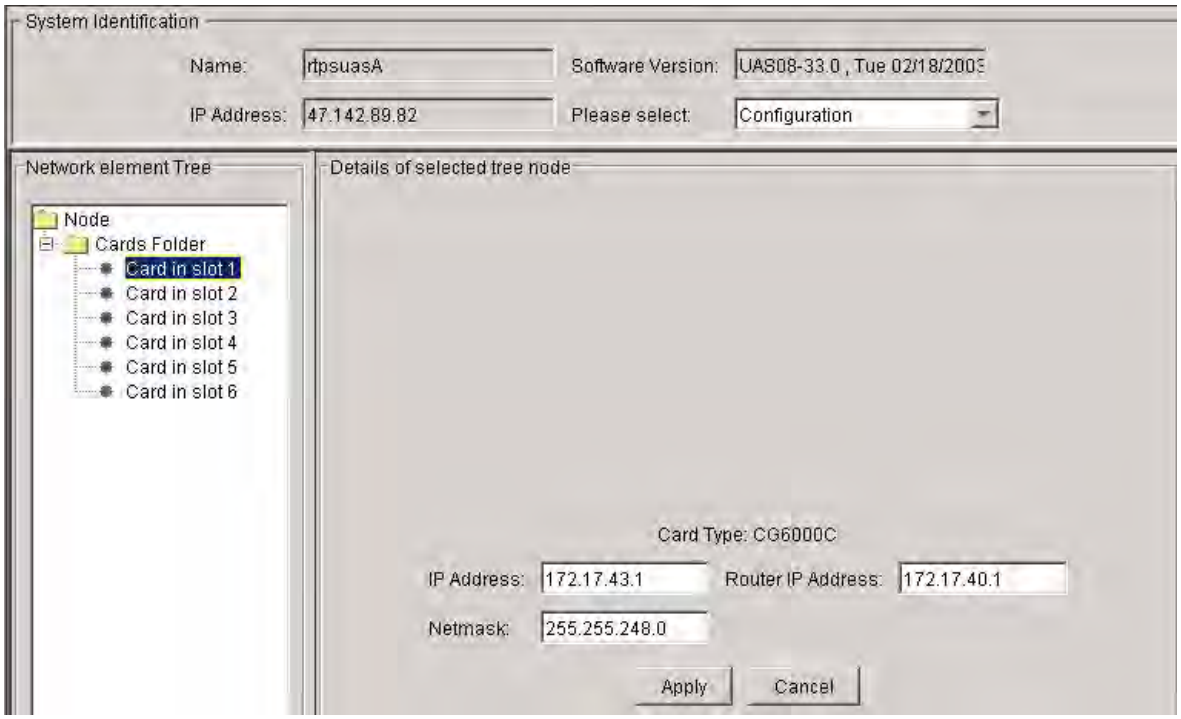
Configuration (card folder view)



From this window you can view the configuration data for all the cards.

Expanding the Card Folder and selecting a card, displays a window similar to the following:

Configuration (card view)

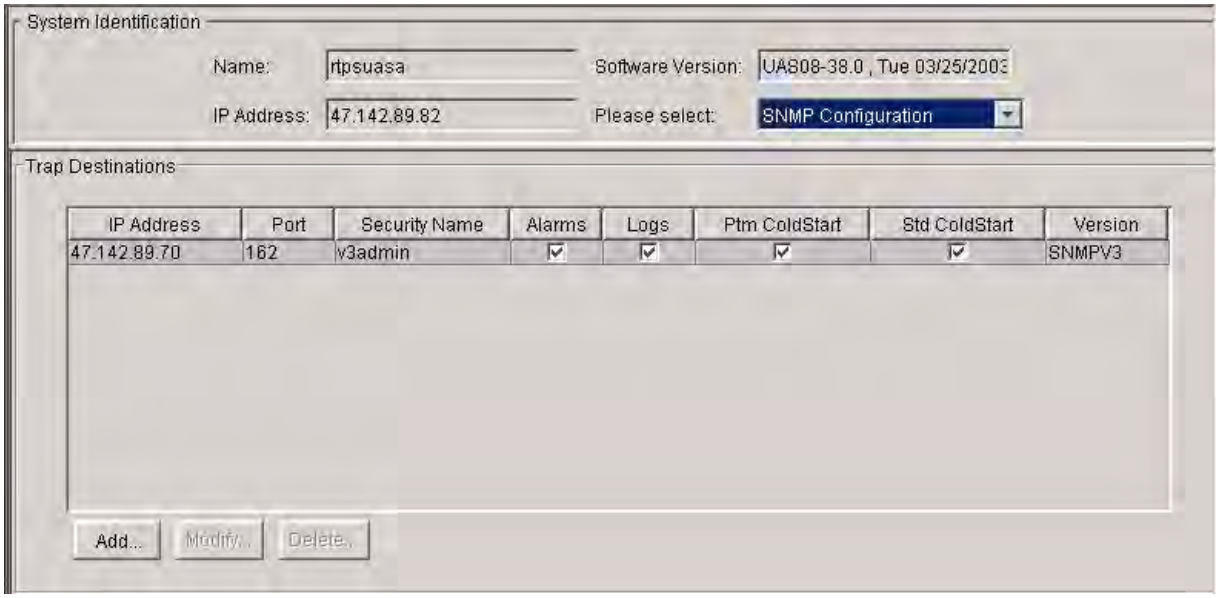


From this window you can modify the configuration data for the selected card.

SNMP Configuration

Selecting the SNMP Configuration option from the drop-down menu, displays a window similar to the following.

SNMP Configuration window



From this window, you can add, modify, or delete an SNMP trap destination for the selected UAS node.

Line Maintenance Manager

Overview

The Line Maintenance Manager (LMM) application is used to post lines and perform maintenance activities on them.

Note 1: To determine if this application is supported for your solution, refer to the table titled Application to solution mapping on page 211.

Note 2: The LMM does not currently support hunt groups.

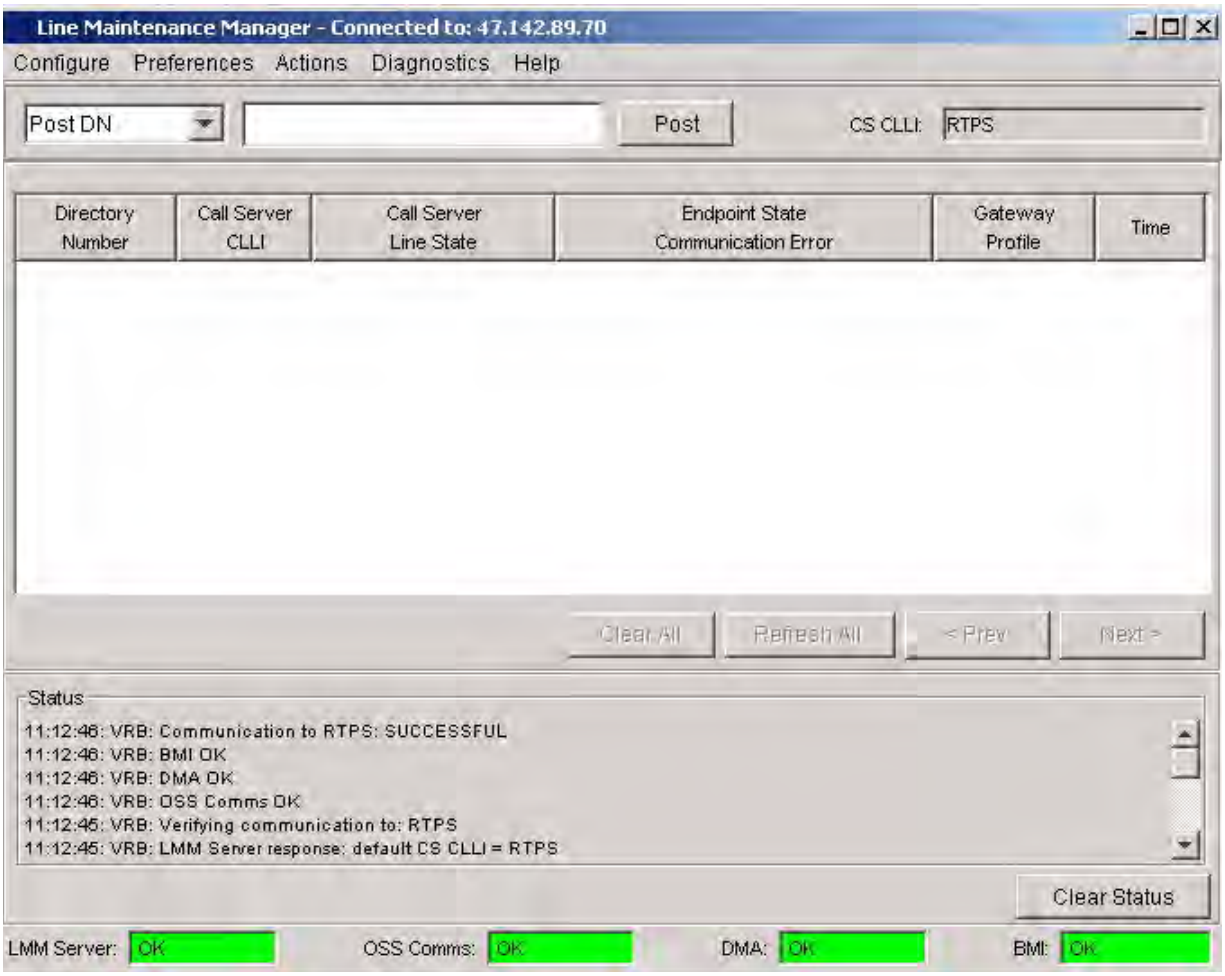
This section provides a brief overview of the LMM. For procedures on how to perform line maintenance activities using the LMM, refer to the Fault document.

User interface

The user interface for the LMM application is a web-based GUI (graphical user interface), which is accessed through the common launch page as previously described under Common launch page on page 209. To access the LMM GUI, refer to procedure “Launching the CS 2000 Management Tools client applications” in the Security and Administration document.

When the Line Maintenance Manager is launched, a window, similar to the following is displayed:

Line Maintenance Manager GUI



The main panel displays the following information:

- **CS CLLI** - The CLLI for the Communication Server 2000
- **Status** - Operation messages
- **LMM Server** - Status of the link between the LMM client and LMM server
- **OSS Comms** - Status of the OSS Comms Svcs application on the core manager.
- **DMA** - Status of the DMS Maintenance Application on the core manager
- **BMI** - Status of the Base Maintenance Interface application on the core manager

From the main panel, you can perform any of the following activities:

- **Post** - Post the lines according the selection in the pull down menu. Selecting Post DN, displays a line by its directory number (DN). Selecting Post by Gateway, displays the lines associated with the specific gateway.
- **Clear All** - Remove all posted lines from the display.
- **Refresh All** - Manually refresh the posted lines in the display, when auto-refresh is disabled.
- **Prev/Next** - Navigate from the current page to the previous or next page, respectively, when multiple screens are needed to show all the posted lines
- **Clear Status** - Clear the status information that is reported in the Status area

The sections that follow briefly describe the options available under each menu in the Line Maintenance Manager GUI.

Configure

The Configure menu contains the options to reconnect to the LMM server (used when the connection times out), set the CS CLLI, and exit the Line Maintenance Manager GUI.

Configure menu

Preferences

The Preferences menu contains the options to turn Auto refresh on or off and set the Auto refresh value, turn Auto Termination on or off and set the Auto Termination timeout value, disable Auto refresh, cancel pending CPD requests, and display a fixed number of lines.

Preferences menu

Actions

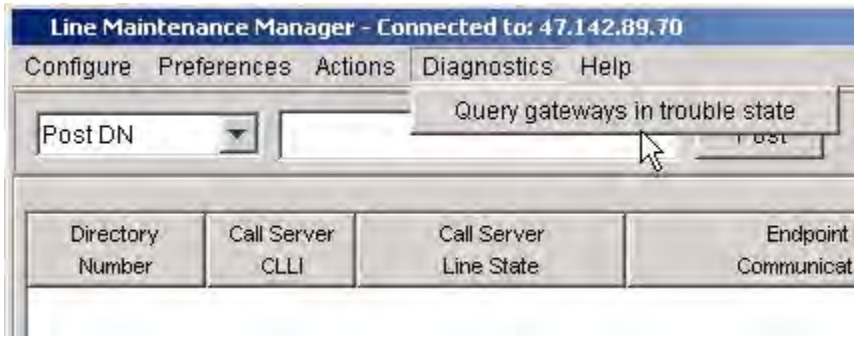
The Actions menu contains the options to busy and return lines to service, force release a line, installation busy (INB) a line, clear or refresh the display of the posted lines, and display the properties of a line.

Actions menu

Diagnostics

The Diagnostics menu contains the option to query gateways in trouble state.

Diagnostics menu



Help

The Help menu contains an option to display LMM troubleshooting tips.

Help menu

Trunk Maintenance Manager

Overview

The Trunk Maintenance Manager (TMM) application is used to display trunks and perform maintenance activities on them.

Note: To determine if this application is supported for your solution, refer to the table titled Application to solution mapping on page 211.

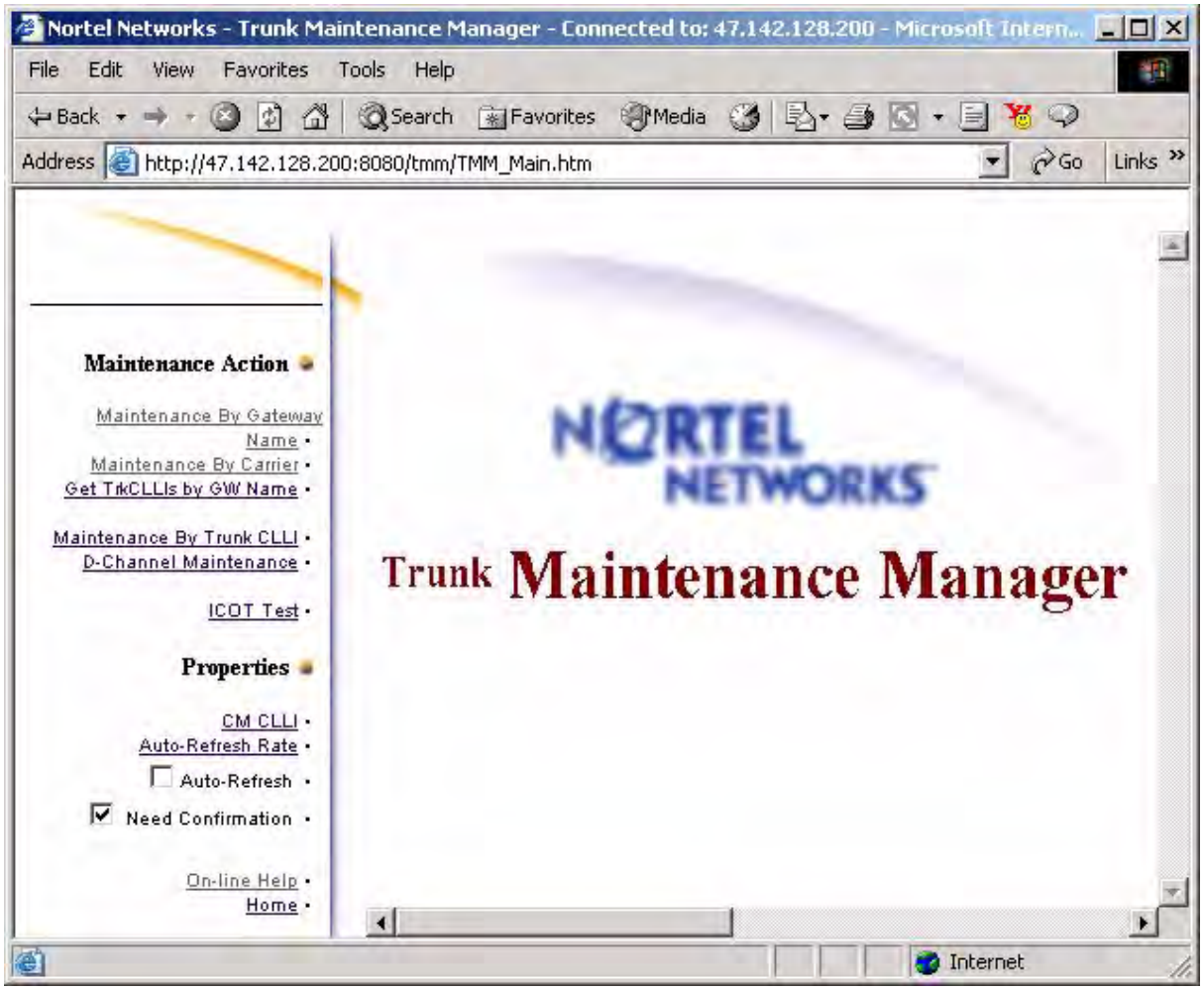
This section provides a brief overview of the TMM. For procedures on how to perform trunk maintenance activities using the TMM, refer to the ATM/IP Solution-level Fault Management document, NN10408-900.

User interface

The user interface for the TMM application is a web-based GUI (graphical user interface), which is accessed through the common launch page as previously described under Common launch page on page 209. To access the Trunk Maintenance Manager, refer to procedure “Launching the CS 2000 Management Tools client applications” in the ATM/IP Security and Administration document, NN10402-600.

When the Trunk Maintenance Manager is launched, a window, similar to the following is displayed:

Trunk Maintenance Manager main window



Using the Trunk Maintenance Manager GUI, you can perform any of the following activities:

- **Maintenance By Gateway Name** - Perform the following maintenance actions on all endpoints or a range of endpoints of a selected gateway:
  - query endpoint states
  - post endpoints
  - busy endpoints
  - return endpoints to service
  - force release endpoints
  - installation busy endpoints
- **Maintenance By Carrier** - Perform the following maintenance actions on all carriers or specific carriers of a selected gateway:
  - query carrier states
  - post carrier
  - busy carrier
  - return carrier to service
  - force release carrier
  - installation busy carrier
- **Get TrkCLLIs by GW Name** - Display a list of trunk CLLIs for a selected gateway.
- **Maintenance By Trunk CLLI** - Perform the following maintenance actions on all trunk members or a range of trunk members of a selected trunk group:
  - post trunks
  - busy trunks
  - return trunks to service
  - force release trunks
  - installation busy trunks
- **D-Channel Maintenance** - Display statistics on D-channels for a selected PRI trunk.
- **ICOT Test** - Perform an ISUP (Integrated Services Digital Network User Part) continuity test on a selected trunk group or trunk member.
- **CM CLLI** - Set the CM CLLI.

- **Auto-Refresh Rate** - Set the auto refresh rate, and enable or disable the auto refresh rate. The default is disabled (unchecked).
- **Need Confirmation** - Enable or disable confirmation on a request to busy an entire posted endpoint set. The default is enabled (checked), which indicates confirmation following a busy request is required.
- **On-line Help**- Open a separate window that contains help information for the TMM GUI.
- **Home** - Return to the main window.

Batch provisioning tool

Overview

The batch provisioning tool (BPT) provides users with the following capabilities:

- perform bulk configuration of Succession lines
- perform bulk flow through configuration of ADSL for MG 9000
- view the log and output files associated with each batch provisioning process
- delete the log and output files associated with each batch provisioning process

The batch provisioning commands are executed using a single OSSGate connection.

To perform provisioning activities using BPT, a user must be belong to user group “lnssprov”. Refer to procedure “Setting up users on a Sun server” in the ATM/IP Security and Administration document, NN10402-600.

For information on how to provision lines using the BPT, refer to the OSSGate User’s Guide, NE10004512.

User interface

The BPT is a command line user interface (CLUI). To access the BPT Refer to procedure “Starting the batch provisioning tool” in the ATM/IP Security and Administration document, NN10402-600.

Once logged in to the BPT, the Main menu, similar to the following, is displayed.

```
------------------------------------------------
        ================================
        Batch Provisioning Tool (BPT V1.0)
        ================================

Username:ptm
Password:

Loging in process...

You are currently logged in as : ptm!

==========
Main Menu:
==========

     (1) Execute Batch File
     (2) Display Output
     (3) Display Logs
     (4) Delete Output or Log Files
     (h) Help

     (x) Exit

Selection: [1/2/3/4/h/x:1]
------------------------------------------------
```

Execute Batch File

The Execute Batch File option allows you to execute batch provisioning commands. When you select this option, the Provisioning Input Entry Menu, similar to the following, is displayed.

```
------------------------------------------------
================================
Provisioning Input Entry Menu:
================================


     (1) Lines
     (2) ADSL
     (3) Go to shell prompt
     (r) Return to the main menu.
     (x) Exit BPT.

Selection: [1/2/3/r/x:1]
------------------------------------------------
```

- Lines - allows you to batch provision lines
- ADSL - allows you to batch provision ADSL
- Go to shell prompt - brings you to the command line where you can execute unix commands
- Return to the main menu - brings you back to the Main menu
- Exit BPT- exits the Batch Provisioning Tool CLUI

Display Output

The Display Output option allows you to view the output file associated with each batch provisioning process. When you select this option, the Display Output Menu, similar to the following, is displayed.

```
-------------------------------------------------
================================
Display Output Menu:
================================


     (1) Lines
     (2) ADSL
     (3) Go to shell prompt
     (r) Return to the main menu.
     (x) Exit BPT.

Selection: [1/2/3/r/x:1]
-------------------------------------------------
```

- Lines - allows you to view the output files that are currently in the Lines output directory
- ADSL - allows you to view the output files that are currently in the ADSL output directory
- Go to shell prompt - brings you to the command line where you can execute unix commands
- Return to the main menu - brings you back to the Main menu
- Exit BPT- exits the Batch Provisioning Tool CLUI

Display Logs

The Display Logs option allows you to view the log files associated with each batch provisioning process. When you select this option, the Display Log File Menu, similar to the following, is displayed.

```
-------------------------------------------------
=================================
Display Log File Menu:
=================================


     (1) Lines
     (2) ADSL
     (3) Go to shell prompt
     (r) Return to the main menu.
     (x) Exit BPT.

Selection: [1/2/3/r/x:1]
-------------------------------------------------
```

- Lines - allows you to view the log files that are currently in the Logs directory for lines
- ADSL - allows you to view the log files that are currently in the Logs directory for ADSL
- Go to shell prompt - brings you to the command line where you can execute unix commands
- Return to the main menu - brings you back to the Main menu
- Exit BPT- exits the Batch Provisioning Tool CLUI

Delete Output or Log Files

The Delete Output or Log Files option allows you to delete one or more output or log files from the Lines or ADSL directory. When you select this option, the Delete Files Menu, similar to the following, is displayed.

```
-------------------------------------------------
=================================
Delete Files Menu:
=================================


     (1) Lines
     (2) ADSL
     (3) Go to shell prompt
     (r) Return to the main menu.
     (x) Exit BPT.

Selection: [1/2/3/r/x:1]
-------------------------------------------------
```

- Lines - displays a menu with options to delete lines output files or lines log files
- ADSL - displays a menu with options to delete ADSL output files or ADSL log files
- Go to shell prompt - brings you to the command line where you can execute unix commands
- Return to the main menu - brings you back to the Main menu
- Exit BPT- exits the Batch Provisioning Tool CLUI

Help

The Help option displays information on the BPT, its menus and options.

Batch Configuration Monitor

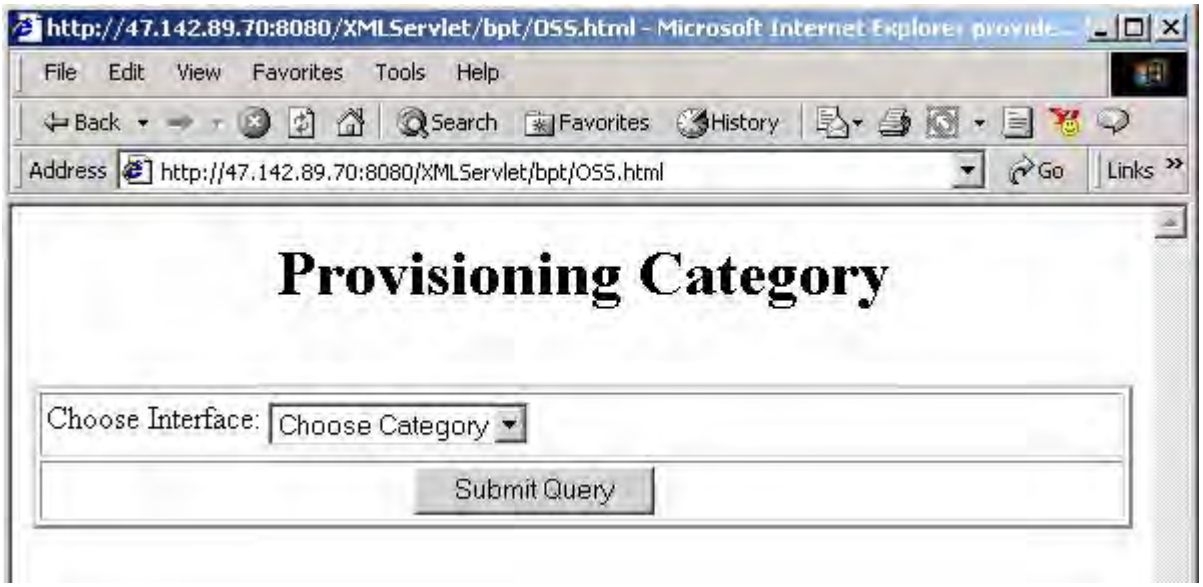
Overview

The Batch Configuration Monitor is a web browser interface to view provisioning output files in an easy readable format.

Note: To determine if this application is supported for your solution, refer to the table titled Application to solution mapping on page 211.

The Batch Configuration Monitor is accessed through the common launch page as previously described under Common launch page on page 209. To access the Batch Configuration Monitor interface, refer to procedure “Launching the CS 2000 Management Tools client applications” in the ATM/IP Security and Administration document, NN10402-600.

The web browser window is similar to following.



From this window, you can select an interface and display a list of provisioning output files that are available in the output directory for the selected interface.

Note: ADSL is the only supported interface at this time.

Network Patch Manager

Overview

The Network Patch Manager (NPM) is a patch management solution for Nortel Networks network-based products. Patching using the NPM is supported for the following components:

- CS 2000 Gateway Controller (GWC)
- Media Gateway 9000 (MG 9000)
- Media Gateway 9000 Manager (MG 9000 Manager)
- CS 2000 SAM 21 Element Manager (SAM21 EM)
- Patching Server Element (PSE)
- Succession Element and Sub-network Manager (SESM)
- QoS Collector Application (QCA)
- Succession Server Platform Foundation Software (SSPFS)
- Integrated Element Management System (EMS) and Integrated EMS security component
- Network Patch Manager (NPM)

The NPM software package is delivered with the Succession Server Platform Foundation Software (SSPFS).

Only one instance of the NPM can be installed and enabled in an office. Depending on your office configuration, your choices are as follows:

- Integrated Element Management System (EMS), which is the most preferred location
- CS 2000 Management Tools server (CS2M) when Integrated EMS is not present in the network

The NPM uses the Patch File Receipt System (PFRS) and the Patching Server Element (PSE) device.

Patch File Receipt System

The Patch File Receipt System (PFRS) provides an automated means of interacting with an upstream patch administration and delivery system, for example, the Regional Patch Selector (RPS), to make new patch files available to the NPM.

When installed, PFRS runs each of two tasks once every 24 hours. One task generates a report specifying the patch and load content for each device in the site (report). A second task detects newly available patch files and brings those patches into the NPM system (getpatch). You can schedule these two tasks, report and getpatch, to run at any given time on a daily basis. However, the intent is to schedule the report task at an early time so that the site patch contents are returned to Nortel, and to schedule the getpatch task at a later time to pick up new patch files based on the report information that was returned during the report task.

The PFRS 24-hour cycle typically uses the following schedule:

- PFRS generates the report showing the patch status of the site and puts the report file in the designated dropbox.
- Some time later, the upstream patch administration system gets the report from the dropbox.
- The upstream patch administration system uses the report to "calculate" which newly available patches are needed by the site.
- The upstream patch administration system downloads new patches to the site's dropbox.
- Some time later, PFRS executes the getpatch task which makes the new patches known to the NPM server and database, puts a copy of the each patch file in NPM's "Au" directory, and determines which devices can use the patch (i.e., creates a VA status where appropriate).

Note: PFRS does not automatically apply any patches.

The PFRS has the following requirements for use in the NPM:

- An interface server hosting an FTP server that is accessible using a userid and password with full read, write, and overwrite access, must be available.
- The default directory of the FTP user (1 unique user per site recommended) on the FTP server must provide the location from which patch files are retrieved and to which reports are written.
- The PFRS can be configured at any time after the NPM is installed, configured and running, using the command line interface (CLI) tool.
- A CLLI name is required to configure PFRS. You can retrieve the CLLI name from table OFCENG.
- The IP address or host name of the interface server is required to configure PFRS.

Patching Server Element Device

The patching server element (PSE) device enables communication between the NPM and OAM devices to be patched on the SSPFS platform. The PSE also tracks patch data and information on each OAM device.

User interface

The NPM provides a graphical user interface (GUI) and a command line user interface (CLUI). Both interfaces offer the same functionality. Using the NPM GUI or CLUI, you can

- apply and remove patches
- audit devices
- activate and deactivate patches
- restart OAM devices
- image select MG 9000 devices automatically
- perform file management, tracking, and reporting

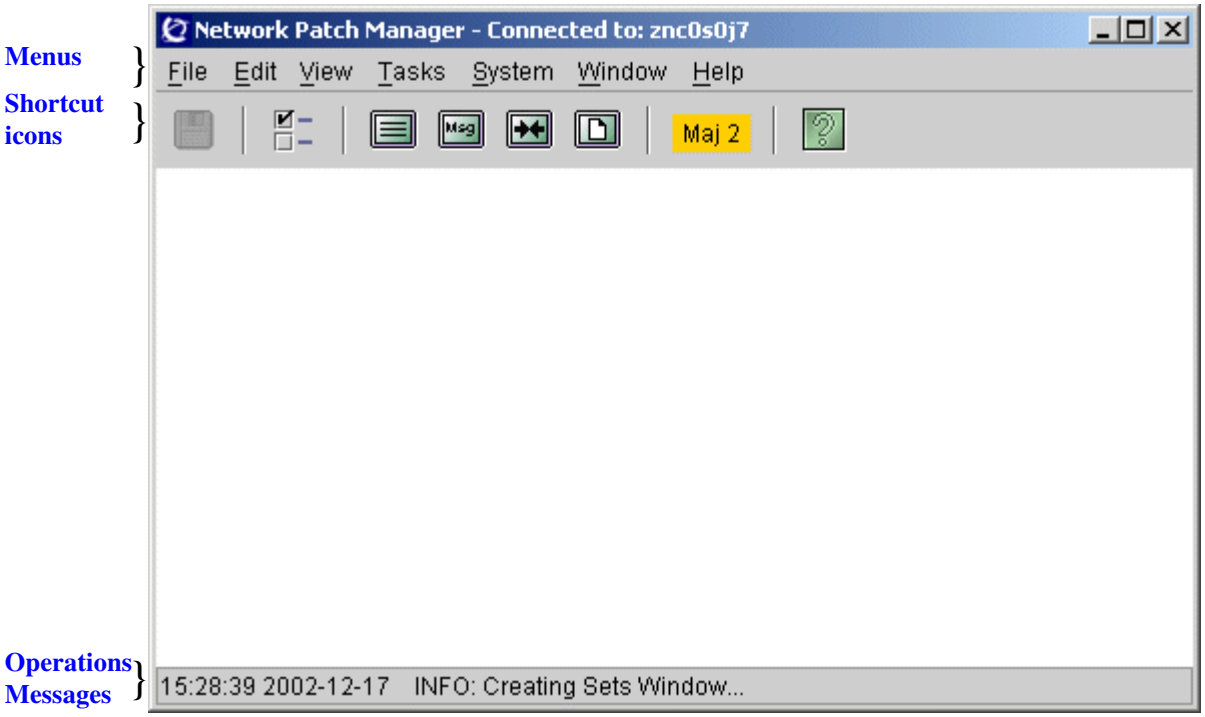
Users who need to perform patching activities using the NPM GUI or CLUI, need to belong to user group “emsadm”. Refer to procedure “Setting up local user accounts on a Sun server” in the ATM/IP Security and Administration document, NN10402-600.

NPM GUI

The NPM GUI is a Java™ Web Start (JWS) application delivered through a web browser that provides full access to all patching functionality. The NPM GUI is accessed through the common launch page as previously described under Common launch page on page 209.To access the NPM GUI, refer to procedure “Launching the CS 2000 Management Tools and NPM client applications” in the ATM/IP Security and Administration document, NN10402-600.

The following figure shows an example of the NPM GUI.

The NPM GUI



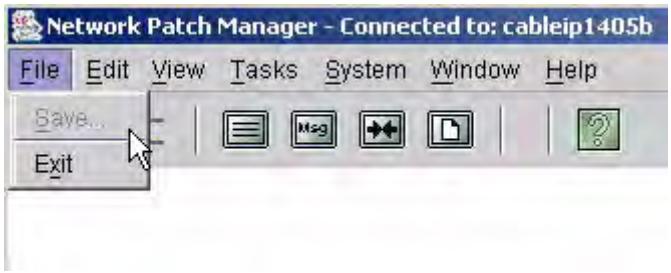
The GUI provides menus along the top with shortcut icons for some of the menu items below. Placing your cursor over an icon indicates its function. Operation messages are displayed at the bottom of the window.

The sections that follow briefly describe the options available under each menu. More details are provided in the online help for the Network Patch Manager (see Help on page 274).

File
The File menu contains the following options:

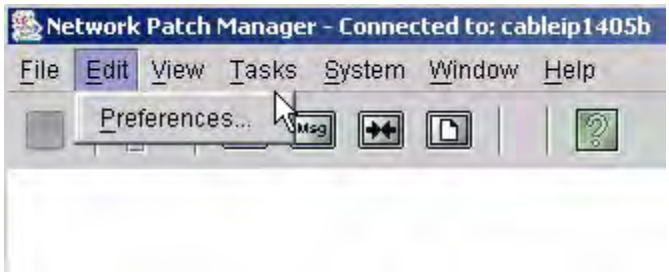
- **Save** - save the data of the currently active window to a file
- **Exit** - exit the Network Patch Manager GUI

File menu



Edit
The Edit menu contains the **Preferences** option used to enable or disable the display of patching activity results, and enable or disable debug messages.

Edit menu

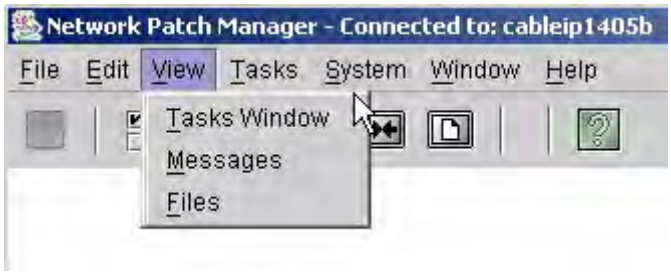


View

The View menu contains following options:

- **Tasks Window** - display maintenance tasks (apply, remove, and audit) and their current status
- **Messages** - display all system messages and responses received during the current session
- **Files** - view details of patch files

View menu



Tasks

The Tasks menu contains the following options:

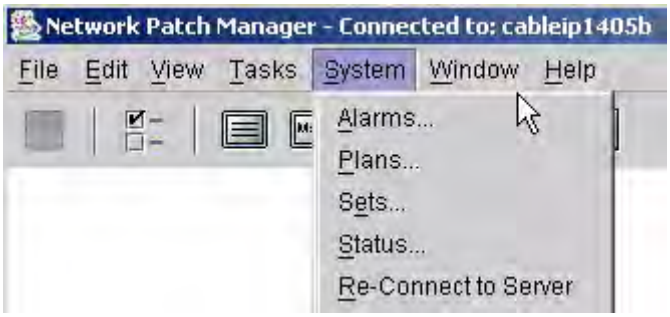
- **Maintenance** - initiate patching tasks such as apply, remove, audit, activate, deactivate, restart, and smartimage
- **Set Field Values** - set database field values such as PATCH.HOLD, and DEVICE.HOLD
- **Reports** - define and generate reports

Tasks menu

System
The System menu contains the following options:

- **Alarms** - define and manage alarms
- **Plans** - define, modify or delete a plan, which is a list of one or more tasks such as apply, remove, audit, reports, that can be executed according to a specified schedule
- **Sets** - define sets, which are groupings of patches and devices used in routine patching tasks
- **Status** - view details for currently active alarms
- **Re-Connect to Server** - reconnect to the server in the event the connection is lost

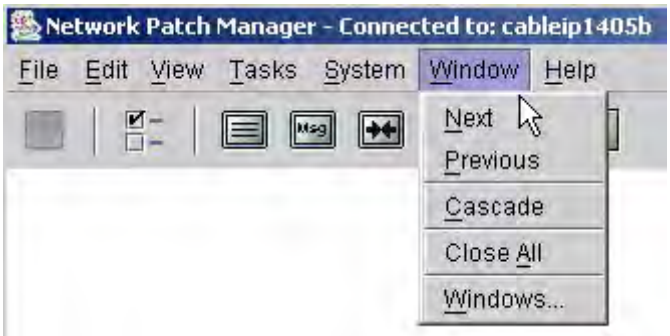
System menu



Window
The Window menu contains the following options:

- **Next/Previous** - activate the next or previous open window
- **Cascade** - auto-arrange all open windows on the desktop
- **Close All** - close all open windows
- **Windows** - view all open windows, and switch to or close an open window

Window menu

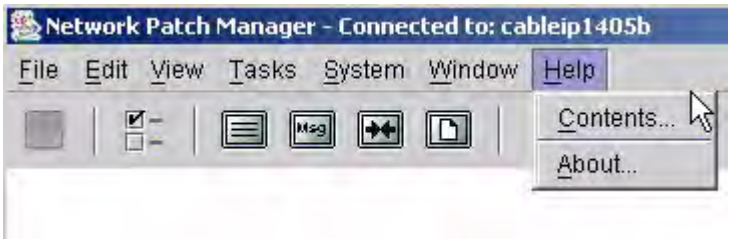


Help

The Help menu contains the following options:

- **Contents** - display online help information for the NPM
- **About** - display the version of the NPM GUI, NPM server application, and NPM database schema

Help menu



NPM CLUI

The CLUI offers the same functionality as the GUI, but in a command-line approach. Additionally, the CLUI services can be used as an Application Programming Interface (API) for scripts that need to access patching information or functions.

Alarms

The Network Patch Manager (NPM) includes a set of pre-defined system alarms at install. You cannot remove or modify these alarms, however, you can disable them (refer to procedure “Enabling and disabling alarms using the NPM” in the ATM/IP Fault Management document, NN10408-900). By default, all system alarms are enabled.

Each time an alarm is raised, log NPM360 is generated. For more details on the alarms that are reported through log NPM360, refer to the Succession Fault Management Logs Reference document, NN10275-909.

In addition to the pre-defined system alarms, you can create your own alarms to match your specific criteria. Refer to procedure “Defining alarms using the NPM” in the ATM/IP Fault Management document, NN10408-900.

Logs

The NPM logs are saved into a local file “/data/npm/logs/custlogs”, but you can also send them into the customer’s log system through an Operations Support Systems Interface (OSSI).

The NPM logs are grouped into logical sets based on the log number as follows:

- NPM300 to NPM399 - Trouble logs
- NPM400 to NPM499 - Service summary logs
- NPM600 to NPM699 - Information logs

Log severity is indicated by a number of asterisks at the beginning of the log.

- <none> - information
- * - minor
- ** - major
- *** - critical

For details on each of the NPM logs, refer to the Succession Fault Management Logs Reference document, NN10275-909.

CS 2000 SAM21 Manager

Overview

The CS 2000 SAM21 manager is a client-server application. The client application runs on either a Solaris or a Windows platform, and the server application runs on the CS 2000 Management Tools server (SSPFS platform).

Note: Depending on your office configuration, there may be two clients; one that is used with the core manager during the upgrade only, and the other that will be used with CS 2000 Management Tools server (SSPFS platform) after the upgrade.

The CS 2000 SAM21 Manager is used to manage the SAM21 network elements within a Succession Network. The SAM21 Manager allows remote device management of multiple SAM21 network elements at the card level through a single graphical user interface (GUI).

Note: To determine if this application is supported for your solution, refer to the table titled Application to solution mapping on page 211.

User interface

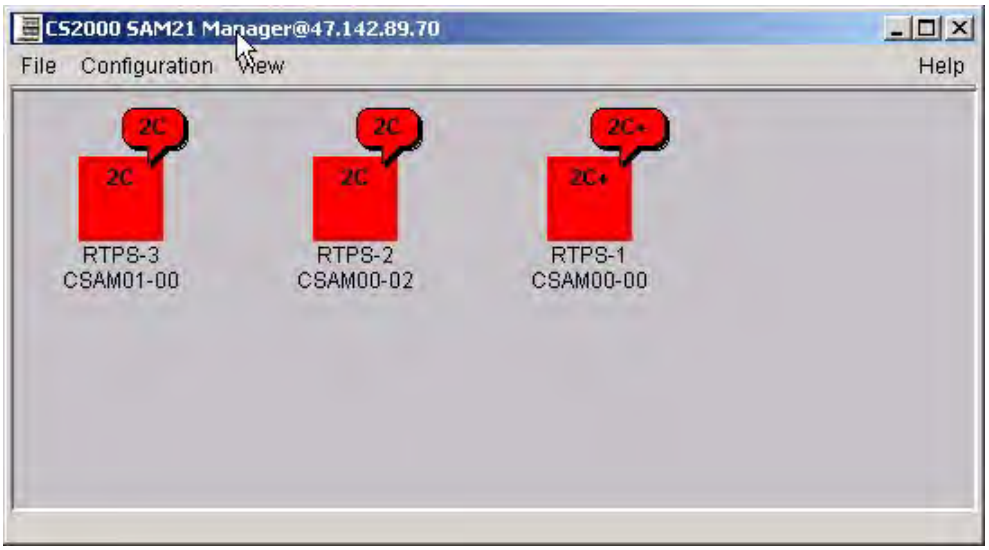
The user interface for the CS 2000 SAM21 Manager application is a web-based GUI (graphical user interface), which is accessed through the common launch page as previously described under Common launch page on page 209. To access the CS 2000 SAM21 Manager GUI, refer to procedure “Launching the CS 2000 Management Tools client applications” in the ATM/IP Security and Administration document, NN10402-600.

The CS 2000 SAM21 Manager GUI provides a Subnet view, a Shelf view, and a Card view.

Subnet view

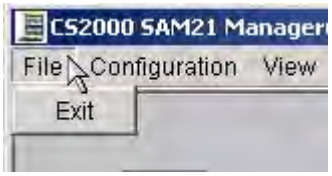
The subnet view, similar to the following, is displayed when the CS 2000 SAM21 Manager GUI is launched.

CS 2000 SAM21 Manager subnet view



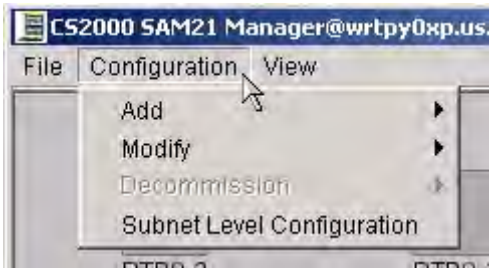
File menu

The File menu provides the options to Exit the CS 2000 SAM21 Manager.



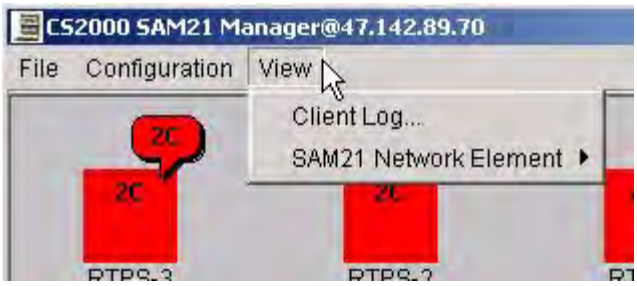
Configuration menu

The Configuration menu provides the options to Add, Modify, or Decommission a SAM21 network element, and provision or modify the IP address where the SNMP poller application for the MIB reader resides.



View menu

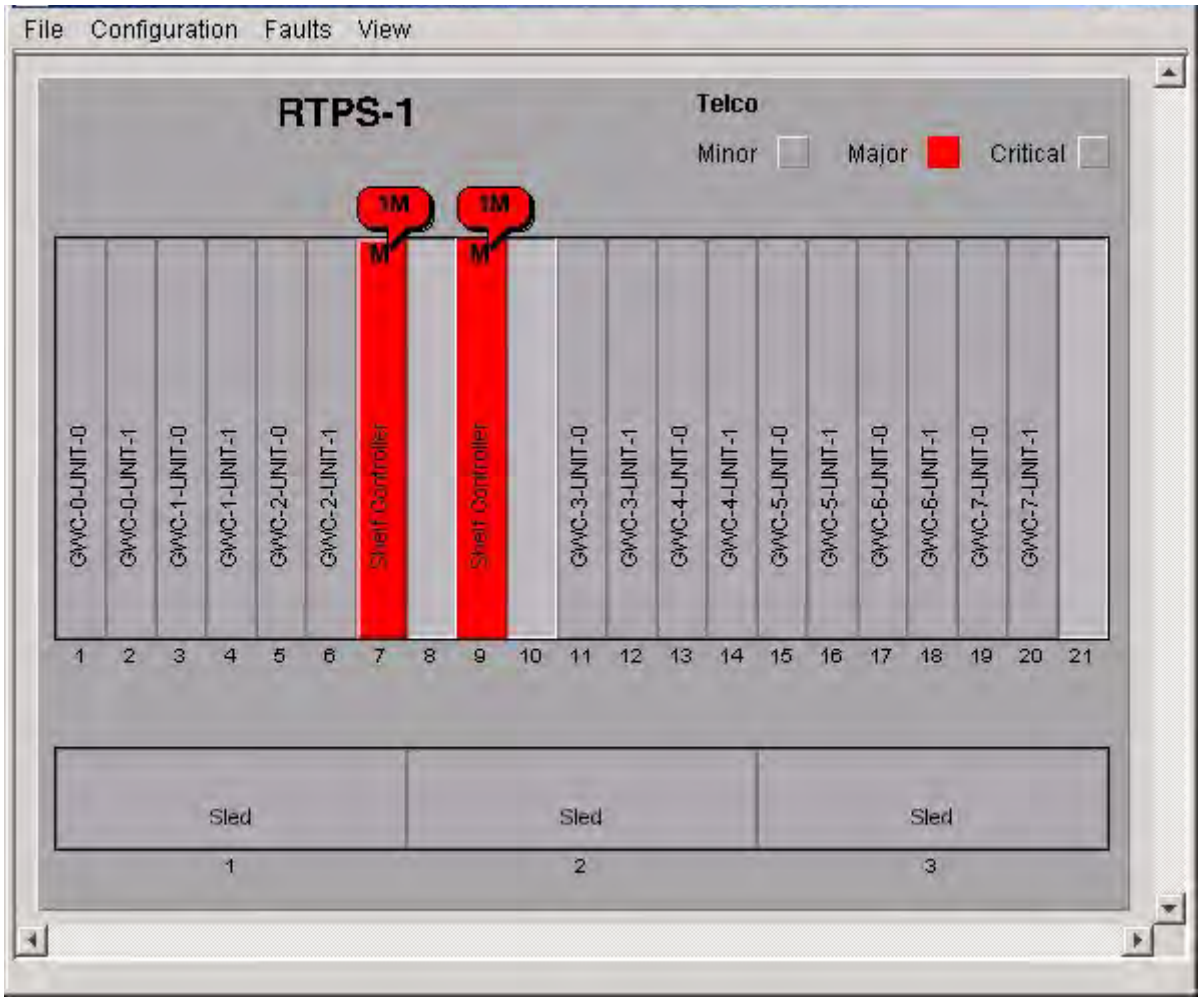
The View menu provides the options to view the client log and display the shelf view of a SAM21 network element.



Note: You can also display the shelf view of a SAM21 network element by double clicking on the SAM21 network element icon in the GUI window.

Shelf view

The Shelf view, similar to the following, is displayed by selecting the SAM21 Network Element option from the View menu of the Subnet view.



The Shelf view displays Telco alarms, which provide an indication of the overall condition of the shelf, excluding the SAM21 Shelf Controllers (SCs). Examples of Telco alarms include power feed failure, diagnostic failure and high temperature. A Telco alarm can have a severity of Minor, Major, or Critical. For more information on Telco alarms, refer to the SAM21 Shelf Controller Fault Management document, NN10089-911.

File

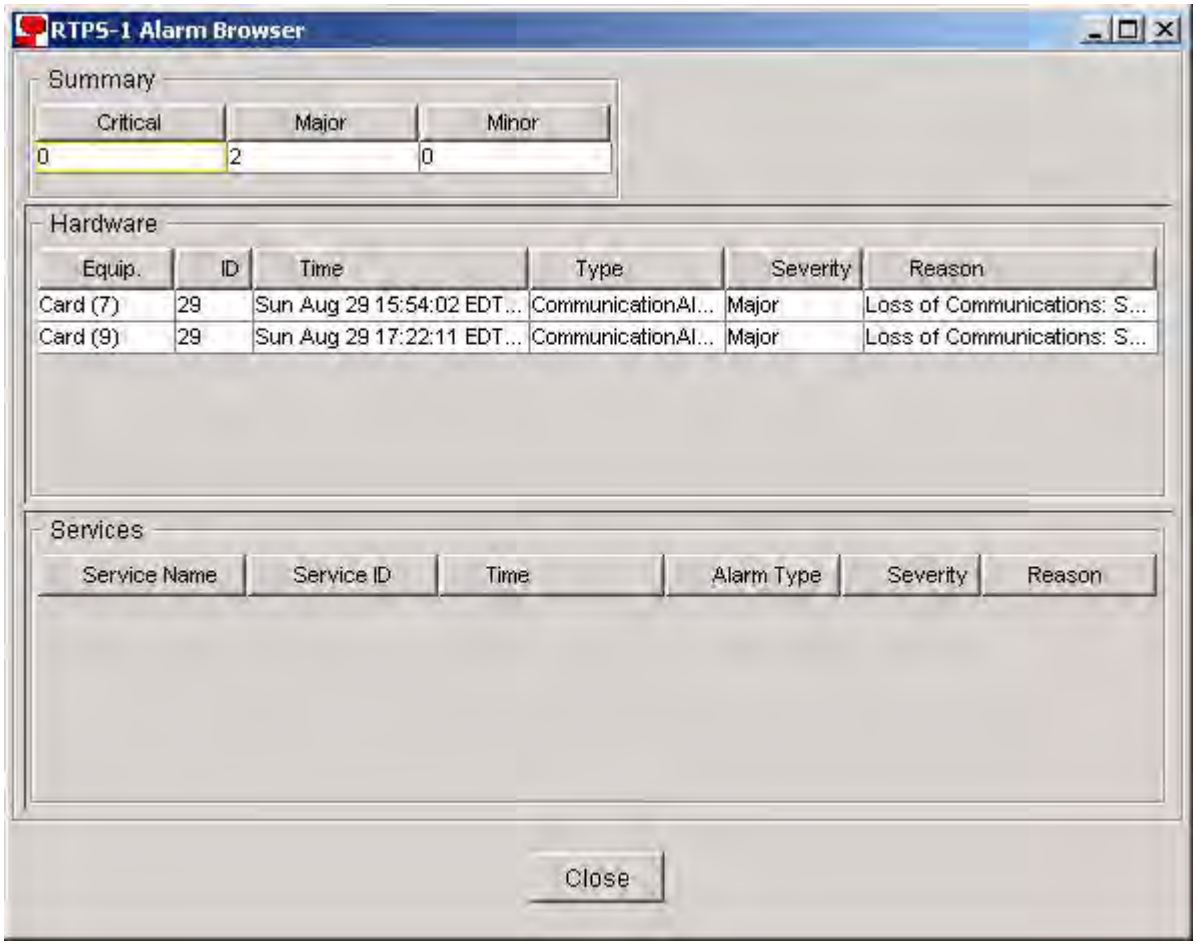
The File menu provides the option to close the shelf view.

Configuration

The Configuration menu provides the options to configure IPoA services and ATM PMC addresses.

Fault

The Fault menu provides the option to display the alarm browser, which shows alarm information for all cards in the SAM21 shelf. When the option is selected, a window similar to the following is displayed.

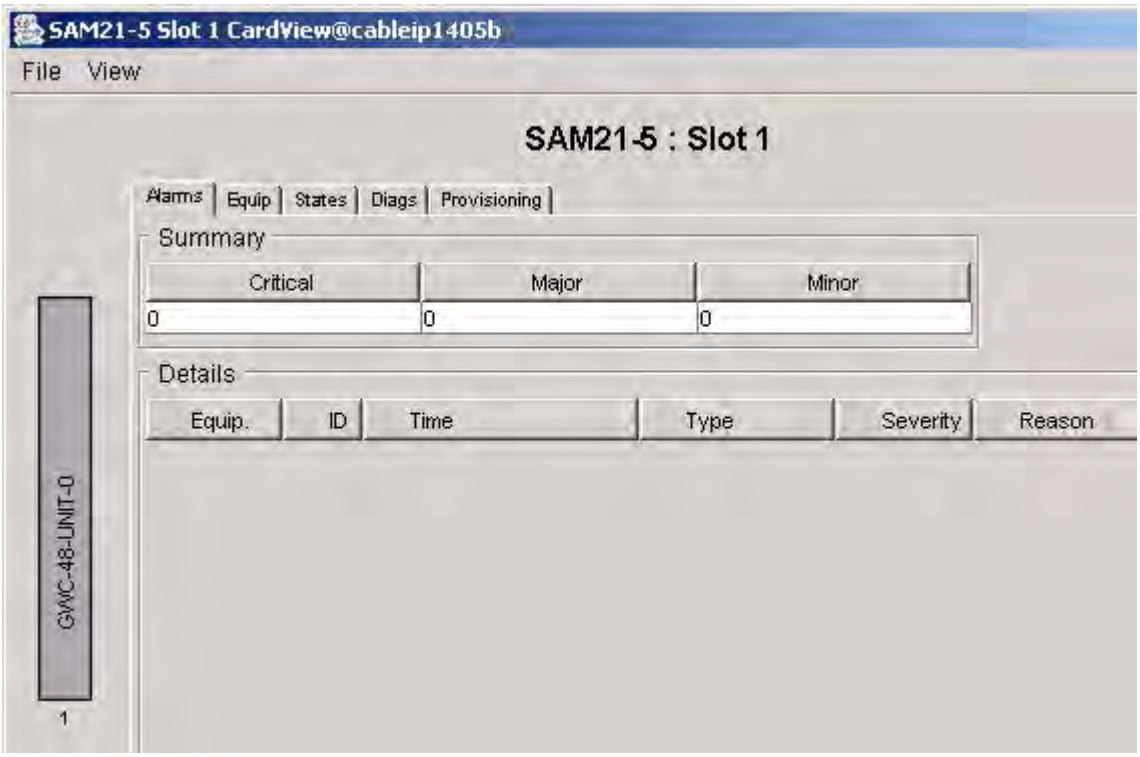


View

The View menu provides the options to display the client log, the card view, or the subnet view.

Card view

The Card view, similar to the following, is displayed by selecting the Card Views option from the View menu, by double clicking a card, or by right-clicking a card from the Shelf view and selecting the Card View... option.



Alarms tab

The Alarms tab displays the number of alarms on the card and the details on each alarm.

Equip tab

The Equip tab displays the type of card and memory size.

States tab

The States tab displays the current state of the card as well as a history of its state.

Diags tab

The Diags tab allows a user to perform brief or full diagnostics on the card and view status messages.

Provisioning tab

The Provisioning tab displays the provisioning details for the card.

QoS Collector application

Overview

The Quality of Service (QoS) Collector Application (QCA) collects QoS records and stores them. QoS records contain a set of QoS parameters collected on a per-call basis. The QoS parameters that are collected are

- packets sent
- packets received
- packet loss
- octets sent
- octets received
- inter-arrival latency
- jitter

The QCA receives binary QoS records from the Gateway Controllers (GWCs), converts these records to QCA Internet Protocol Detail Records (IPDRs), and stores them in a file. The OSS can obtain these QCA IPDRs and process them.

> ***Note:*** For details on the required disk space to store QCA data, refer to section Required disk space to store QCA data on page 285 in this document.

The configuration details for the QCA are contained in a properties file on the CS 2000 Management Tools server. Users can modify the configuration details for the QCA through the QCA properties. The QCA must be stopped and restarted for any changes in the properties file to take place.

The Quality of Service (QoS) Collector Application (QCA) is installed when the the CS2M software package is installed on the CS 2000 Management Tools sever. The procedures available for the QCA are as follows:

- "Installing the QCA software package on a separate server" in the ATM Upgrades document, NN10261-461 or IP Upgrades document, NN10344-461.

  Note: Nortel Networks recommends that you install a second instance of the QCA on another dedicated Sun server to support in-service upgrades without loss of records.

- "Configuring the QoS Collector Application" in the Configuration Management document.
- "Starting the QoS Collector Application" in the Security and Administration document.

To add a QoS collector to the network and associate it with a gateway controller, refer to the GWC documentation suite.

Restriction and limitations

QoS reporting is applicable to more than just VoIP networks. It can also be used in ATM and hybrid networks. However, to date, QoS reporting has only been validated to GWC-driven GWs in Succession Cable solutions.

Note: QCA is not applicable to AAL2 solutions.

If you are interested in using QoS reporting in your non-Cable solution, please contact your Nortel Networks account prime for more information.

All gateways in VoIP solutions will report these statistics via end-of-call reporting mechanisms specific to the protocol used for MGC - VMG communication.

The GWs that are supported are listed below.

- UAS (H.248)
- Motorola CG4500 (NCS)
- PVG (Aspen/VSP2)
- PVG (Aspen/VSP3)
- PVG (H.248)
- Mediatrix (MGCP)

- Arris PacketPort (MGCP)
- Askey

Required disk space to store QCA data

The following table provides guidelines for the required disk space to store QCA data for one day.

Estimated average traffic rate (BHCA)	Minimum disk space required to store QoS records for 1 day (GB)
250K	0.504
500K	1.008
750K	1.512
1M	2.016
1.25M	2.52
1.5M	3.024
1.75M	3.528
2M	4.032

The required disk space indicated in the table, was calculated as follows:

- BHCA = 500K
- Calls per day = 10 hours of traffic per day x BHCS = 5M
- QoS records per day = 2 x calls per day = 10M
- Record size = 840 bytes
- Compression ratio = 88%
- Required disk space for 1 day = 10M x 840 = 8.4GB
- When using compression = 8.4GB x 0.12 = 1GB

Note: If the storage period is greater than one day, the disk space must be increased accordingly.

To increase disk space of “/data/qca”, refer to procedure “Increasing the size of file systems” in the ATM/IP Solution-level Configuration Management document, NN10409-500.

OSSGate

Overview

OSSGate is an application that provides a machine interface for provisioning components within Succession. The main functionality of OSSGate is to act as a gateway to the Node, Carrier, Trunk, Line, ADSL Provisioning applications and the Trunk Maintenance application. It provides the end user with an alternative to the GUI (graphical user interface) as a method for provisioning succession components.

For detailed information on OSSGate, refer to the OSSGate User's Guide, NE10004512.

PM poller

Overview

The Performance Monitoring (PM) Poller is delivered as a sub-package within the Succession Server Platform Foundation Software (SSPFS). The PM poller provides a simple network management protocol (SNMP)-based system to gather performance information from the gateway controller (GWC), Universal Audio Server (UAS), SAM21 shelf controller, Media Server 2010 (MS 2010), and the Succession Server Platform Foundation Software (SSPFS).

The PM poller is configured with server information that provides system attributes for the system to be monitored. The poller is also configured with a number of profiles that determine data collection. Profile information can include the type of data collected, how often the data is collected, and the device from which the data is collected. The PM poller can have many profiles, each defining a distinct set of polling characteristics.

To set up SNMP polling in your network, refer to procedure “Setting up the PM poller” in the Configuration Management document.

Data collection output

The data collected by the PM device pollers is output in Comma Separated Value (CSV) files to the “/data/oms” file output directory. The oms directory contains seven sub-directories (named 1 through 7), which in turn contain a day’s collection of CSV output files. The current day’s output files are always written to sub-directory ’1’. File rotation occurs just prior to midnight every 24 hour period. When file rotation occurs, the files in sub-directory ’7’ are removed, and the contents of each sub-directory are moved up one sub-directory. For example, the contents of sub-directory 6 are moved up to sub-directory 7.

Viewing output files

The CSV files can be loaded into a customer supplied text viewer or spreadsheet software to browse the raw data.

Note: The CSV file format is not intended to be a user-friendly format for viewing the output using a standard text editor.

We recommend that you use an OSS tool to view the CSV output files. If you require a product to analyze and view performance data, contact your Nortel Networks account prime to allow Nortel staff to review and recommend a commercial solution.

Logs

The PM Poller uses the SSPFS syslog interface to log internal poller events. These events include the starting and stopping of the poller, polling session activities, and internal poller errors. These logs can be extremely useful in debugging PM Poller related issues. The command to monitor the PM poller syslog stream is as follows:

tail -f /var/adm/messages

Note: PM poller logs are preceded by “SNMPP”.

User interface

User interface tools, “snmpp_ctl” and “snmpp_cfg” are provided as part of the PM Poller package to control the state of the PM Poller, query configured data, and add or modify polled device configuration data attributes.

OMPUSH application

Overview

The OMPUSH application is delivered as a sub-package within the Succession Server Platform Foundation Software (SSPFS). The OMPUSH application is used to make scheduled OM (CSV/SSV) file transfers to predefined remote servers using File Transfer Protocol (FTP) or Secure FTP (SFTP).

The OMPUSH application does not create the OM files, but transfers them. The OMPUSH application can transfer two types of OM files:

- MG 9000 OM files, which are collected by the MG 9000 OM collector
- SSPFS, GWC, UAS, and SAM21 SC OM files, which are collected by the SNMP PM poller.

Note: All OM files to be transferred must reside on the server where OMPUSH is installed.

User interface

The OMPUSH application is a command line user interface (CLUI) with the following tools:

- OMPUSH application control tool on page 291.
- OMPUSH session configuration tool on page 292.

OMPUSH application control tool

The OMPUSH application control tool (**ompush_ctl**) is used to start, stop, and query the state of the OMPUSH server application. When the OMPUSH server application is running, the query also returns the status of existing OMPUSH sessions.

For a list of the sub-commands available with this tool, refer to Commands for the OMPUSH application control tool on page 292.

Commands for the OMPUSH application control tool

The following table lists the tasks you can perform with the OMPUSH application control tool, and their associated command.

Task	Command
Start the OMPUSH server application.	**ompush_ctl -start**
Stop the OMPUSH server application.	**ompush_ctl -stop**
Re-synchronize the OMPUSH server application with the configuration data. ***Note:*** You can also re-synchronize by stopping and starting the OMPUSH server application.	**`ompush_ctl -sync`**
Query the status of the OMPUSH server application, as well as the status of existing OMPUSH sessions (only provided when the OMPUSH server application is running)	**`ompush_ctl -status`**
Display help information for the OMPUSH application control tool	**`ompush_ctl -help`**

OMPUSH session configuration tool

The OMPUSH session configuration tool (**ompush_cfg**) is used to

- create a new session
- modify a session
- query a session
- delete a session
- activate or deactivate a session

Only one instance of the OMPUSH session configuration tool (ompush_cfg) is supported at one time.

The OMPUSH session configuration tool provides the following two interface types:

- full-screen menu mode that steps you through the provisioning process
- a command line interface (CLI) for provisioning data with batch scripts

  For a list of the sub-commands available from the command line, refer to Commands for the OMPUSH session configuration tool on page 293.

Commands for the OMPUSH session configuration tool

The following table lists the tasks you can perform with the OMPUSH session configuration tool CLI, and their associated command.

Note: It is recommended not to use the “Home”, “End”, “Insert”, “Delete”, and “Break” keys when using the OMPUSH session configuration tool CLI, as they may have a different function for different terminals and cause some unexpected errors.

Task	Command
Access the OMPUSH full-screen configuration mode.	**ompush_cfg -menu**
Create a new OMPUSH session.	**ompush_cfg -create <SessionName> <Attribute=Value ... >**
Modify an OMPUSH session.	**ompush_cfg -modify <SessionName> <Attribute=Modify ... >**
Activate an OMPUSHsession.	**ompush_cfg -activate <SessionName>**
Deactivate an OMPUSH session.	**ompush_cfg -deactivate <SessionName>**
Display details of an OMPUSH session.	**ompush_cfg -query <SessionName>** ***Note:*** If no value is entered for <SessionName>, all sessions will be displayed.

Task	Command
Delete an OMPUSH session.	**ompush_cfg -delete <SessionName>**
Display help information for the OMPUSH session configuration tool.	**ompush_cfg -help**

Logs

The OMPUSH application uses Syslog to log events such as starting and stopping the OMPUSH server application, configuration file errors, file push session activities, and internal push errors . All OMPUSH logs are preceded by "OMPUSH". To view OMPUSH logs, refer to procedure "Viewing OMPUSH logs" in the Fault Management document.

Additional information

The following procedures are available for the OMPUSH application:

- "Starting the OMPUSH server application" in the ATM/IP Security and Administration document, NN10402-600.
- "Stopping the OMPUSH server application" in the ATM/IP Security and Administration document, NN10402-600.
- "Creating an OMPUSH session" in the ATM/IP Configuration Management document, NN10276-500.
- "Modifying an OMPUSH session" in the ATM/IP Configuration Management document, NN10276-500.
- "Deleting an OMPUSH session" in the ATM/IP Configuration Management document, NN10276-500.
- "Activating or deactivating an OMPUSH session" in the ATM/IP Configuration Management document, NN10276-500.
- "Querying OMPUSH session attributes" in the ATM/IP Configuration Management document, NN10276-500.
- "Viewing OMPUSH logs" in the ATM/IP Fault Management document, NN10325-900.

Resource monitor

Overview

The resource monitor (RESMON) application is included with the Succession Server Platform Foundation Software (SSPFS). It is automatically started when the SSPFS server is started.

The resource monitor can detect the following hardware and software faults:

- fan failure
- disk failure
- loss of network connectivity
- power supply unit (PSU) failure
- temperature exceeding a defined threshold
- file system usage exceeding a defined threshold
- CPU load exceeding a defined threshold
- memory usage exceeding a defined threshold
- swap space usage exceeding a defined threshold
- file system not mounted
- file system write or read failure

In the (I)SN07 release, the resource monitor is integrated with the AlarmD utility, which is a utility that keeps track of alarms on the SSPFS platform, lights a light when an alarm is raised or cleared, and writes a customer log that corresponds to the state of an alarm .

The faults detected by the RESMON application are flagged through logs SPFS310 and SPFS350. For log details, refer to the Succession Fault Management Logs Reference document, NN10275-909.

You can query the state of the SSPFS platform , which displays faults detected by the RESMON application, and you can enable or disable local logging of RESMON faults. The corresponding procedures are provided in the ATM/IP solution-level Fault Management document, NN100408-900.

IP solutions features and services

This section discusses the features and services that are common to the IAC, PT-IP, PT-AAL2, and UA-IP solutions. For information on features and services that are unique to the four IP solutions, see IAC features and services, PT-IP and PT-AAL2 features and services, and UA-IP features and services.

IP solutions Lawful Intercept

The Lawful Intercept feature allows you to perform lawful electronic surveillance of voice and voice-band data traffic in the network. Lawful surveillance is the process of identifying traffic from or to a subject, and delivering data or content relating to that traffic to a remote law enforcement agency. In the IP solutions, the Lawful Intercept feature is implemented using the UAS.

Lawful Intercept works in conjunction with the USNBD (United States Network Broadcast Delivery) feature which was first released for DMS-100 in LEC0013. Lawful Intercept is applicable to Succession switches that terminate lines, or lines and trunks, but is not applicable to Succession switches that terminate trunks only. Both USNBD and Lawful Intercept are fully compliant with the Communication Assistance for Law Enforcement Act (CALEA).

From the perspective of the operating company, Lawful Intercept is identical to the USNBD feature. Therefore, you should use the existing USNBD documentation in order to perform all tasks relating to the Lawful Intercept feature.

For additional information on USNBD, see the *Lawful Intercept documentation*, NN10190-113.

IP solutions Multiple Point Code (MPC) support

Advanced Intelligent Network (AIN) applications using the SS7 network support both Single Point Code (SPC) and Multiple Point Code (MPC) formats for node addressing. The MPC functionality provides a CS 2000 switch with multiple SS7 node capability. Currently, 16 Point Codes for a SSP (service switching point) node are supported. MPC functionality is offered only on DMS100 and DMS250 applications. In the current release, the CS 2000 supports MPC functionality, and Translation Capabilities Application Part (TCAP) applications can work when more than one point code is provisioned on the CS 2000. However, for TCAP, only one point code is used for messaging.

IP solutions Network Route Advance

The Network Route Advance feature is the Succession implementation of the MARS (Meridian Automatic Route Selection) feature. Network Route Advance is a selection mechanism that provides a sequenced list of trunk groups over which a call is allowed to complete.

Network Route Advance allows you to provision alternate ISUP (ISDN User Part) trunks for outgoing calls that cannot complete because of congestion or failures (remote blocking) at the far-end switch. Network Route Advance can reroute calls from specific legacy ISUP trunks, terminating on DTC or SPMs (see previous list) as well as DPT IT trunks. This feature allows you to reroute calls to alternate trunk groups from the following trunk types:

- DPT IT (InterToll)
- ISUP (ISDN User Part) IT (InterToll)
- ISUP ATC (Access Tandem to Carrier)
- ISUP IBNTO (Integrated Business Network outgoing)
- ISUP IBNT2 (Integrated Business Network 2-way)

Note 1: For each of the trunk types in the previous list, the originating call can be either a line or a trunk.

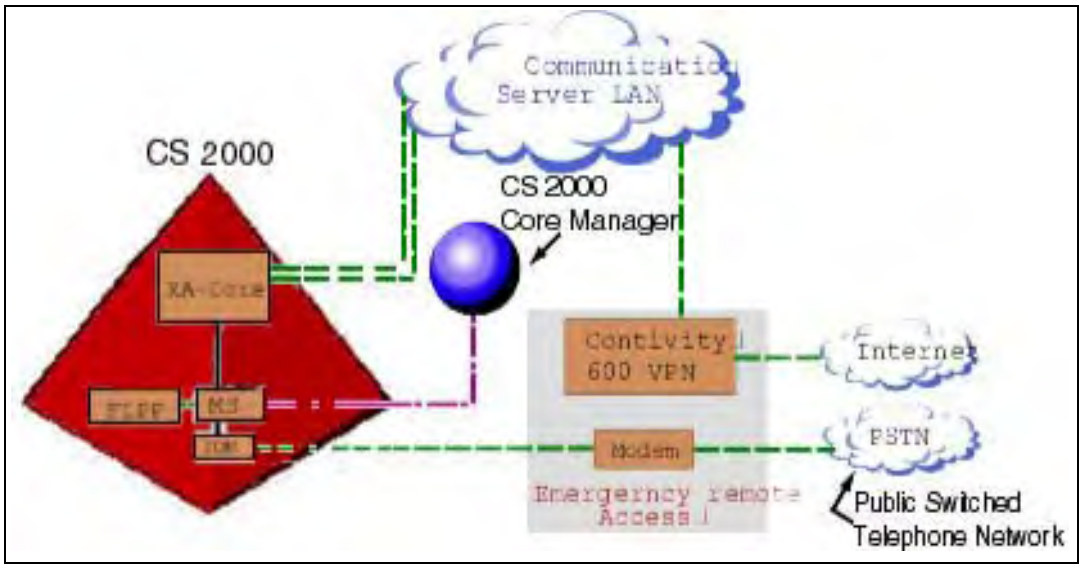
Note 2: The MARS (Meridian Automatic Route Selection) feature allowed calls that originated on a line to be rerouted by the system from ISUP IBNTO, or IBNT2 trunks. The Network Route Advance feature expands that functionality to include calls originating on trunks.

Note 3: Network Route Advance also supports alternate routing for calls that are forwarded over the trunk types in the previous list.

IP solutions emergency remote access

Under emergency conditions, Nortel Networks support personnel require remote access to the customers' network. This access can be provided by dial-up lines or terminal servers to the customer operations support system (OSS) network (see the figure Emergency remote access with Contivity 600 VPN). As part of the basic Succession solution offering, Nortel Networks offers an optional Contivity 600 VPN remote access solution. The Contivity 600 VPN switch enables virtual private network (VPN) tunneling from a remote location and is Simple Network Management Protocol (SNMP) manageable. Succession customers are responsible for providing the external analog or ISDN modems, and terminal servers required to access components without Ethernet connectivity

Emergency remote access with Contivity 600 VPN



IP solutions inter-exchange carrier (IXC) services

This solution provides a comprehensive set of inter-exchange carrier services widely deployed in the North American IXC network today. Services supported by this solution include the following:

- Information database services: NXX toll free number services, authorization codes, calling card, account codes, debit/prepaid cards, operator services, and local number portability
- Routing and screening: CIC routing, time of day screening, ANI screening, and class of service screening
- Enterprise services: virtual private networks, ISDN PRI services
- Multiple dialing plans: full 10 digit routing, 7 digit VPN routing, 15 digit international dialing, and speed dialing
- Billing: standard CDR and flexible CDR formats, and long call duration CDRs

In some deployments, interworking between a North America CS 2000 and an international CS 2000 is required. This should normally be achieved using trunks configured as IBN7 type ANSI ISUP trunks at both communication servers. The IBN7 trunks between the two communication servers may be SIP-T IP packet trunks or TDM trunks but not BCC trunks at present, as the international CS 2000 does not support BICC trunks yet.

Note: If the two communication servers serve different countries, the international CS 2000 will need to invoke international gateway

functionality by routing calls through loop around trunks configured as international ISUP trunks before connecting the call to/from the North America CS 2000.

IP solutions supported trunk types

IP solutions support the following trunk types:

- Packet access on the Passport PVG for intra-Succession Network and inter-Succession Network calls
  - Inter ISUP IMT
  - Intra ISUP IMT
  - ISUP IT (for tandem)
- TDM access on the Passport PVG for intra-Succession and intra-Succession calls
  - ISUP FGD/EANT
  - Inter ISUP IMT
  - Intra ISUP IMT
  - ISUP ATC
  - ISUP IT
  - ANSI PRI variants
    - NTNAPRI
    - N449PRI
    - U449PRI
    - NIPRI

IP solutions supported SIP Services

The following SIP services are supported by the IP solutions:

- EANT trunks and all FGD (Feature Group D) Dialing Plans, including Cut-through, Transitional, and Universal Access.
- Release Link Trunks
  - URLT0001
  - URLT0003
  - URLT0003
  - URLT0005

- MCCS trunks
  - CRDS001
  - CRDS002
  - CRDS003
  - CRDS004
  - CRDS005
- Network Route Advance
- Authorization Code, Account Codes, and PIN Codes
- Re-origination

IP solutions supported tandem trunk types

The IP solutions support the following trunk types for tandem services:

- ATC
- IT
- TO

IP solutions mixed trunk subgroups

IP solutions do not support trunk subgroups with both legacy and packet members. This restriction derives from the fact that all members in a given trunk subgroup share the same echo cancellation datafill via TRKSGRP. These values may be interpreted differently by packet and legacy peripherals.

For this reason, packet members should combined in one trunk subgroup and legacy members should be combined in a second trunk subgroup if both types are desired in the same trunk group. This requirement will not be enforced but a notification message will be generated during provisioning when both packet and legacy members are detected in the same trunk subgroup.

IP solutions test trunk services

This section describes how test trunking is accomplished through the SPM through an interconnect span. For information on how test trunking is accomplished using the IW SPM-IP, see PT-IP and PT-AAL2 test trunk services.

The test trunk services include the origination and/or termination of T100, T101, T102, T105, and T108 trunk tests and ISUP COT testing for commissioning trunks as follows:

- T100 Trunk Test Line

  T100 is also known as a quiet or balanced termination. It provides noise and loss measurements.

- T101 Trunk Test Line

  T101 is also known as Communication Test Line. It provides a two-way communication between a test position and an incoming or outgoing trunk.

- T102 Trunk Test Line

  T102 is also known as a Milliwatt Test Line. It provides far-to-near end transmission loss measurements for outgoing trunks.

- T103 Trunk Test Line

  T103 provides a connection to a supervisory and signalling test circuit of intertoll trunks. It performs supervisory checks over the DTU and detects the following supervisory signals:

  — Busy and re-order tones

  — Test progress tones

  — Milliwatt tones

  — Announcements signals

  — Ringing signals

- T104 Trunk Test Line

  T104 performs measurements of Two Way transmission loss, measurements of near-to-far noise, and a check of near-to-far noise. The types of measurements include:

  — Loss

  — Noise

  — Echo return loss

  — Transmission loss

  — Singing point return

  — High and low frequency measurements

- T105 Trunk Test Line

T105 provides two-way loss and noise measurement testing from the originating office.

Note: T105 tests run automatically.

- T108 Trunk Test Line

  The T108 test line is a dialable method for accessing the dialed loopback on trunks feature known as TRKLPBK. The T108 test line isolates trunk troubles and measures net loss, noise, and runs BERT for trunks at the DS0 rate.

- ISUP Continuity Test (COT)

  ISUP COT validates datafill and speech path on a trunk that uses CCS7 signaling.

- CVTEST

  Found in the TTP - C7TTP Level, CVTEST verifies the Trunk Datafill parameters including Glare

- QRYSIG

  Found in the TTP - C7TTP Level, QRYSIG displays the signaling status of the post CCS7 trunk

- TRKQRY

  Found in the TTP - C7TTP Level, TRKQRY displays the local or remote status of the posted trunk

IP solutions interconnect span test trunking strategy

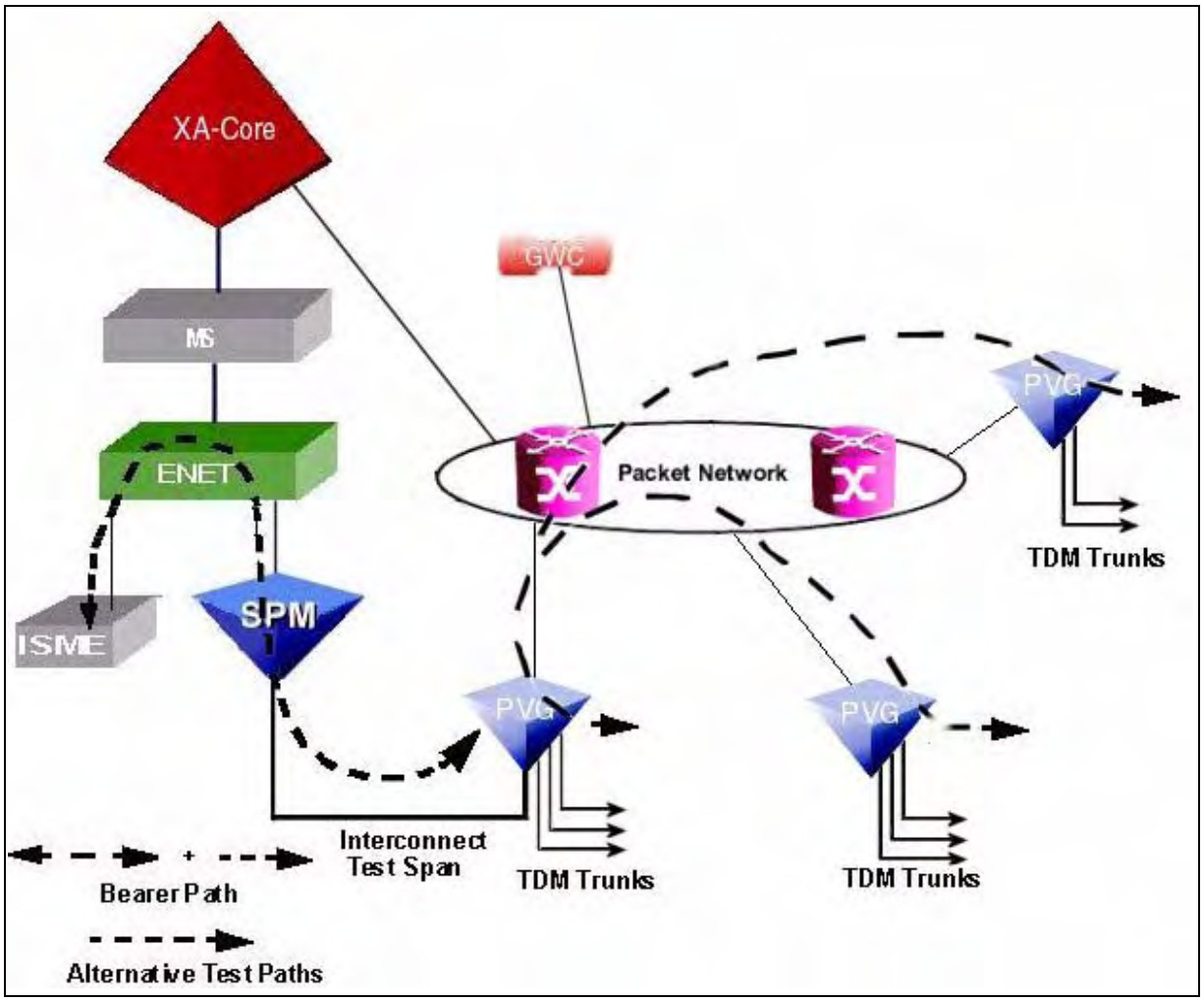
The figure Interconnect span test trunking strategy shows the configuration selected for T101, T102, and T105 test trunk services. The ISME in conjunction with an SPM-to-PVG trunk test connection executes the test trunk services across the media gateways. A span from the SPM is physically connected to one of the Passport 15000 PVGs. This arrangement can terminate any of the above trunk test requests onto the appropriate ISME service circuits. Through the use of datafill and translations, trunk tests are performed across any Passport 15000 PVG TDM trunk.

Note: The T108 test line can be conducted with or without the IW SPM-IP. For more information see, Terminating T108 test line support.

Both originating and terminating continuity tests (COT) are supported on the Passport 15000 PVG. This functionality is accomplished through signaling control between the Gateway Controller (GWC) and the media gateways. Upon either originating or terminating COT requests,

the Passport 15000 PVG ensures that COT tones are properly transmitted and received across the TDM interfaces.

Interconnect span test trunking strategy



IP solutions Network Management Controls

Network Management Controls provide a variety of mechanisms for limiting and/or balancing trunk traffic in order to handle special traffic circumstances.

- TID Limit provides an artificial limit to the number of DPT TIDs that can be used on a Call Server.This limit is in addition to the OFCVAR parameter DPT_MAX_PORTS and the sum of all TIDs enabled within the Terminal Resource Manager (TRM). If the limit is exceeded, egress (incoming DPT) calls are blocked and ingress (outgoing DPT) calls are “advanced”, i.e. the next route (if available)

is selected from the route list. In this case, the call will only succeed if one of the next routes is TDM based. This control is DPT-specific.

- Bandwidth Reservation provides an office-wide mechanism to reserve a percentage of DPT TIDs for outgoing calls. For example, in an emergency, the telephone service provider may want to ensure that calls can get out of the affected area, while potentially reducing the flow of incoming calls. Bandwidth Reservation never blocks outgoing DPT calls, but rather blocks incoming DPT calls once they reach the inverse (i.e. 100% - outgoing reserved %) of reserved DPT TIDs. This control is DPT-specific.
- Bandwidth Prioritization allows the telephone service provider to throttle call volume on a per-trunk-group basis. When the percentage of idle DPT TIDs in the office drops below a value specified against a trunk group, incoming calls are blocked on that group and outgoing calls are “advanced” to the next trunk group in the route list. This control is DPT-specific.
- CANT (Cancel To) limits the traffic offered to a specific trunk group to a percentage of total call attempts. This control is not DPT-specific and will work with any trunk group (DPT or TDM). The percentage of call attempts specified (both incoming and outgoing) are routed to an announcement, e.g. if 25% is specified, then 1 out of 4 calls are routed to an announcement.
- CANF (Cancel From) prevents a percentage of overflow traffic from a selected trunk group from advancing to the next route in the route list. This essentially prevents a route from being “advanced” under certain overflow conditions. E.g. is 25% is specified, then 1 out of 4 overflow calls will not be advanced to the next route. This control is also non DPT-specific.
- SKIP forces a specified percentage of traffic on a given trunk group to be ”advanced” to the next trunk group in the route list. This control is also non DPT-specific.
- FRR IRR (Flexible ReRoute Immediate ReRoute) allows the telephone service provider to force a given trunk group to be sent to an alternate trunk group or route. This essentially overrides the standard trunk “advance” mechanism through the route list. This control is also non DPT-specific.
- FRR RRR (Flexible ReRoute Regular ReRoute) allows the telephone service provider to force overflow traffic on a given trunk group to be sent to an alternate trunk group or route. This essentially overrides the standard trunk “advance” mechanism through the route list. This control is also non DPT-specific.

IP solutions Automatic Trunk Routing

Automatic Trunk Routing (ATR) is a mechanism to allow for trunk testing, for example, to test translations before new trunk groups are brought into service. Traditional ATR for TDM allows the selection of a specific trunk member to use for testing. In the DPT world, there is no concept of specific trunk members and trunk groups are also not associated with specific peripherals.

IP solutions GETS Support---circuit switched GETS

Government Emergency Telecommunications Service (GETS) is offered by the Office of the Manager, National Communications System (OMNCS), to meet NS/EP requirements for the use of public, defense, or Federal telephone networks by Federal, state, and local governments and other authorized users. The GETS feature for Succession is based on the GETS feature that was released earlier for time-division multiplex (TDM) switches.

GETS calls are initially identified by dialing pattern (normally 1+710-NCS-GETS), and when routed over networks using CCS7 signalling, identified by IAM attributes. IAM Calling Party Category (CPC) parameter National Security / Emergency Preparedness (NS/EP, decimal 226) and IAM message priority (usually 1, but controlled by office parameter) are used to identify GETS calls so that they may be provided a higher probability of completion (HPC).

GETS calls encountering all trunks busy or route list exhaust conditions may be queued (known as Trunk Queuing or Call Queuing) against eligible trunk groups and given First-In-First-Out (FIFO) priority over non-GETS calls for the next available trunk member. GETS calls are also exempt from Network Management controls that would otherwise inhibit call completion.

IP solutions packet switched GETS

Succession packet-switched support of GETS over LEC/IXC Dynamic Packet Trunks (DPTs), both VoA and IP, mirrors that of circuit-switched GETS in most respects.

Unlike circuit-switched trunk groups, packet-switched trunk groups (in other words, DPTs) do not have dedicated (static) bearer path resources. Packet-switched bearer path resources (for example, DPT TIDs, SVCs) are office-wide and shared among all DPT groups, dedicated only briefly during call processing (in other words, dynamic).

Furthermore, depending on the signaling protocol, additional resources (some dedicated, some not) may be required. For instance, BICC (Bearer Independent Call Control) protocol signaling utilizes Call

Instance Codes (known as CICs), which are dedicated to a DPT group and unique for a given routeset, to define a DPT group's bandwidth. Whereas, SIP-T (Session Independent Protocol - Telephony) protocol signaling utilizes a maximum call counter to define a DPT group's bandwidth.

It is the dynamic characteristics in which DPT groups share non-dedicated, office-wide bearer path resources that packet-switched and circuit-switched GETS functionality mostly differs. Other areas include supported trunk group types, signaling protocol, and Network Management (NWM) controls.

IP solutions supported trunk group types for packet switched GETS

Packet-switched GETS supports the following DPT trunk group types:

- LEC
  - IT (SIP-T supported, BICC supported)
  - ATC (SIP-T supported, BICC not supported
- IXC
  - IMT (SIP-T supported, BICC supported)
  - EANT (SIP-T supported, BICC not supported)

IP solutions idle trunk notification

Circuit-switched GETS calls, queued against Trunk Queue (TQ) or Call Queue (CQ) eligible trunk groups, are notified of idle trunk members as they become available from the Guard Queue, before being placed on the Idle Queue and made available to call processing. GETS calls are queued and dequeued against trunk groups on a First-In-First-Out (FIFO) basis.

DPT TIDs are briefly (dynamically) dedicated to individual DPT groups during call processing. Once released by call processing, DPT TIDs resume their role as an office-wide resource, requiring idle trunk notification to select a DPT group to be notified. DPT group selection occurs by selecting the first DPT group entry found in table DPTRKMEM with any GETS call(s) queued against it and available DPT CICs.

DPT CICs are dedicated (statically) to individual DPT groups at the time of provisioning. Once released by call processing, idle trunk notification occurs for any GETS calls queued on its DPT group, provided DPT TIDs are available.

Packet-switched GETs calls, queued against TQ or CQ eligible SIP-T DPT groups, are:

- notified of idle DPT TIDs before they are placed on Free Queue and made available to call processing.
- queued and dequeued FIFO against DPT groups, just as circuit-switched GETS.

Packet-switched GETs calls, queued against TQ or CQ eligible BICC DPT groups, are:

- notified of idle DPT TIDs before they are placed on Free Queue and made available to call processing, if DPT CICs are available.
- notified of idle DPT CICs before they are made available to DPT CIC Pool and call processing, if DPT TIDs are available.
- queued and dequeued FIFO against DPT groups, just as circuit-switched GETS trunk group queuing.

IP solutions IAM priority

IAM priority is part of the CCS7 message header and is used by CCS7 signaling to prioritize message handling. BICC signaling utilizes CCS7 signaling, allowing it to support GETS IAM priority. However, SIP-T signaling utilizes SCTP signaling, and therefore, does not support GETS IAM priority.

IP solutions network management controls with GETS

Packet-switched GETS calls are given a higher probability of completion by being exempt from the following Network Management (NWM) controls:

- Non-DPT Specific
  - CANT (Cancel To) limits the traffic offered to a specific trunk group to a percentage of total call attempts.
  - CANF (Cancel From) prevents a percentage of overflow traffic from a selected trunk group from advancing to the next route in the route list. LEC and IXC GETS calls are exempt when the percentage of control is not 100%. When percentage of control is 100%, IXC GETS calls will be exempt based on OFCENG parameter CGETS_BYPASS_SKIP_CANF_AT_100.
  - SKIP forces a specified percentage of traffic on a given trunk group to be “advanced” to the next trunk group in the route list. LEC and IXC GETS calls are exempt when the percentage of control is not 100%. When percentage of control is 100%, IXC

GETS calls will be exempt based on OFCENG parameter CGETS_BYPASS_SKIP_CANF_AT_100.

- DPT Specific
  - — Bandwidth Reservation provides an office-wide mechanism with which to reserve a percentage of DPT TIDs for outgoing calls.
  - — Bandwidth Prioritization provides a means with which to throttle call volume on a per-trunk-group basis. When the percentage of idle DPT TIDs in the office drops below a DPT group specific value, incoming calls are blocked on that group and outgoing calls are “advanced” to the next trunk group in route list.

Note: DPT GETS is not exempt from DPT TID Limit, as its use is expected to reflect the actual usable/available DPT bandwidth for an office. DPT TID Limit provides an artificial limit to the number of DPT TIDs that can be used on a Call Server. If DPT TID Limit is exceeded, egress (incoming DPT) calls are blocked and ingress (outgoing DPT) calls are “advanced” (in other words, the next route, if available, is selected from route list).

IP solutions MPC support

Advanced Intelligent Network (AIN) applications using the SS7 network support both Single Point Code (SPC) and Multiple Point Code (MPC) formats for node addressing. The MPC functionality provides a DMS switch with multiple SS7 node capability. Currently, 16 Point Codes are supported. MPC functionality is offered only on DMS100 and DMS250 applications. If a solution supports multiple point codes (MPC), each point code requires a unique set of resources, including SS7 link interfaces, linksets, and routesets.

One physical DMS switch can be datafilled to appear as several SS7 signalling nodes in an SS7 signalling network. Each of the nodes has its own unique point code, routesets, linksets, and links. In other words, all other nodes in the SS7 network need not be aware that the logical nodes are actually functioning on the same physical DMS switch.

MPC functionality is offered for the following DMS100 applications:

- ACB
- AR
- SLE
- CNAMD
- E800
- PVN

- RAG/NRAG
- NACD via INTRWKSS
- SIGTRANS via INTRWKSS
- NMS via INTRWKSS

The following DMS250 Translation Capabilities Application Part (TCAP) applications are MPC compliant:

- N00 Number Translation
- Travel Card Validation
- Authcode Validation
- Account Code Validation
- Private Speed Number Translation

IAC features and services

This section discusses the features and services that are unique to the IAC solution. The IAC solution supports the following line services:

- Residential Enhanced Services (RES)
- Node-based services with advanced custom calling features designed for delivery from a single switching office.
- Network-based services that rely on multi-vendor switches to deliver network-wide services—including custom local area signaling services (CLASS)
- Display-based services
- Other switch services
- PacketCable™ Core features
- PacketCable™ Extended Features (limited set)
- PacketCable™ Signaling Security
- PacketCable™ NCS protocol

Note: Only the G.711 Codec is supported with the IAC solution. T.38 and DTMF Relay are not supported.

In addition, the IAC solution supports the following trunking services

- Information database services: toll free number services, authorization codes, calling card, account codes, debit/prepaid cards, operator services, and local number portability
- Routing and screening: CIC routing, time of day screening, ANI screening, and class of service screening
- Enterprise services: virtual private networks, ISDN PRI services
- Multiple dialing plans: full 10 digit routing, 7 digit VPN routing, 15 digit international dialing, and speed dialing
- Billing: standard CDR and flexible CDR formats, long call duration CDRs, and Bellcore AMA Format transported via Telecordia AMADNS
- MF ES/OP Trunks are supported for Operator and E911 services

Lastly, the IAC solution supports Dynamic Quality of Service (DQoS) (see IAC Dynamic Quality of Service (DQoS).

The table IAC node-based line services lists the node-based line services that are supported by the IAC solution.

Note: The ability to support these features is dependant upon the third-party equipment used.

IAC node-based line services

Feature	Symbol	Description
Call Forward Unconditional	CFU/CFW	Diverts all calls to an alternate number
Call Forward Call Waiting Calls	CFCW	Diverts calls to an alternate number when the called party is busy
Call Forward No Answer Variable Timing	CFDVT	Diverts call waiting calls to an alternate number if the called party does not respond to the call waiting signal within a variable time frame
Call Forward with Announcement	CFWANN	Diverts calls to an alternate number, with an announcement being played to the calling party
Call Transfer	CXR	Allows a party to transfer a call to another station
Cancel Call Waiting	CCW	Ability to cancel the Call Waiting feature
Code Restrictions	NCOS	Allows Network Class of Service (NCOS) based call barring
Denied Origination	DOR	Allows a line to receive calls only
Digitone	DGT	
Distributed Line Hunt	DLH	
Enhanced Secondary DN	ESDN	Allows a second directory number to be assigned to a single handset. It can function entirely separately from options assigned to the primary directory number.
Bridge Night Number	BNN	Allows a different number for use during different time periods
Call Forward Busy	CFB / CFBL	Diverts calls to an alternate number when the called party is busy
Call Forward Don't Answer	CFD / CFDA	Diverts calls to an alternate number when the called party does not answer
Call Forward Validation	CFWVAL	Allows a subscriber to check their current call forward settings
Call Waiting	CW / CWT	Busy party is made aware that an incoming call attempt is being made

IAC node-based line services

Feature	Symbol	Description
Circular Hunt	CIR	
Denied Termination	DTM	Allows a line to originate calls only
Directory Number Hunt	DNH	
Make Set Busy	MSB	Allows a subscriber to manually make their directory number busy. All calling parties will then receive a busy tone (or appropriate action).
Last Number Redial	LNR	Allows the last number dialed to redialled automatically
Line Overflow to DN	LOD	Directs overflow calls to an defined directory number
Meet-me Conference		
Plug Up	PLP	Disables call terminations on single-line sets. Only originated calls can be made.
Preferential Hunting	PRH	
Restore	RES	Resume telephony service
Simultaneous Ring	SIMRING	
Speed Calling - SC1, SC2, SC3	SCS	Allows a party to store, delete and dial up to 10 directory numbers using only a few key presses
Station Controlled Conference (6-port)	CNF	
Suspend	SUS	Temporarily suspends telephony service
Lawful Intercept / Call Monitoring (basic call)	LI	Ability to monitor incoming and outgoing calls, transparent to the parties involved in the call
Line Overflow to Route	LOR	Moves overflow calls to a route identified in one of the standard route tables
Multi-line Hunt	MLH	
Requested Suspend Service	RSUS	Allows a party to request suspension of service. All incoming calls or attempted outgoing calls are routed to treatment
Secondary DN / Teen Service	SDN	Allows a single party to have additional directory numbers assigned to their line

IAC node-based line services

Feature	Symbol	Description
Spontaneous Call Waiting Identification	SCWID	Allows delivery of calling party information, such as their directory number or name, and a call-waiting tone to the called party even when the called party is already busy
Subscriber Activated Call Blocking	SACB	Allows a subscriber to bar outgoing calls

The table IAC network-based line services lists the node-based line services that are supported by the IAC solution.

Note: The ability to support these features is dependant upon the third-party equipment used.

IAC network-based line services

Feature	Symbol	Description
Anonymous Call Rejection	ACR / ACRJ	Allows parties to refuse calls from callers who choose to hide their directory number (CNDB) or name (CNAB)
Automatic Recall / Call Return	AR	Allows a caller to automatically redial a previously busy dialed directory number when the called party becomes free
Calling Name Delivery Enhancements (includes Call Name Delivery Blocking and Calling Name/Number Delivery on individual call basis)	CNAB / CNNB	Allows a calling party to withhold delivery of their calling name
Calling Number Delivery	CND	Allows a called party to view the number of the calling party before they accept the call.
Customer Originated Trace with AMA	COTAMA	
Automatic Callback	AC / ACB	Allows a party to automatically redial the last number dialled on their station by dialing an access code
Calling Name Delivery	CNAMD, NDND	Allows a called party to view the name of the calling party before they accept the call
Calling Number Blocking	CNB, CNDB, CNNB	Allows a calling party to hide their directory number and cancel the effect of CND
Customer Originated Trace	COT	

IAC network-based line services

Feature	Symbol	Description
Distinctive Ringing / Call Waiting	DRCW	Provides a terminating call a distinctive ring and gives busy calls a distinctive call waiting tone. The caller receives the standard audible ringback tone.
Message Waiting Indicator - Audible	MWT / AMWI	Allows generation of a tone to indicate a message is waiting
Selective Call Acceptance	SCA	Allows a called party to accept calls only from a group of definable directory numbers.
Selective Call Rejection	SCRJ	Allows a called party to automatically reject calls that arrive from a limited set of definable directory numbers.
Voice Band Data: Modem and Group 3 Fax	n/a	Allows transmission and reception of voice-band data services such as facsimile and modem
Message Waiting Indicator - Audible or visible	VMWI	Allows generation of a tone or lights an indicator lamp to indicate a message is waiting
Selective Call Forward	SCF	An incoming call management feature that allows subscribers to make a special list of telephone numbers and remote destination numbers.

The table IAC display-based services lists the node-based line services that are supported by the IAC solution.

Note: The ability to support these features is dependant upon the third-party equipment used.

IAC display-based services

Feature	Symbol	Description
Automatic Recall of Dialable Directory Number	ARDDN	Delivers a dialable directory number to the Automatic Recall (AR) party. Also known as DDN AR Voiceback.
Delivery of Dialable Number	DDN	Allows presentation of a calling party's directory number for an incoming call

The table IAC other-switch services lists the node-based line services that are supported by the IAC solution.

Note: The ability to support these features is dependant upon the third-party equipment used.

IAC other-switch services

Feature	Symbol	Description
AIN 0.1	AIN, AINDN, AINMWT	
Emergency Call Routing	n/a	A facility which provides priority for emergency calls even if the backbone network is under heavy load. The dialed emergency number is specially translated to route the call to the nearest emergency bureau.
Local Number Portability (LAN based)	LNP / PORT	A network capability that allows a subscriber to change network operators (to be served by a switch belonging to a different operator) whilst retaining the same DN as before the move.
Primary InterLATA Carrier	PIC	
Carrier Selection / Equal Access	PIC, LPIC	Provides a subscriber the ability to choose a preferred carrier to route their long distance calls. Carrier selection can be used either via preselection or via call-by-call selection. Every network provider as assigned a unique Carrier Identification Code (CIC) which is defined and distributed by the regulatory authority amongst the German network providers.
IntraLATA Carrier PIC	LPIC	
Operator Services Access	n/a	

In the IAC solution, the CS 2000 is Packetcable 1.0 qualified as a Packetcable Call Management Server (CMS) and Media Gateway Controller (MGC).

The following Packetcable capabilities are supported:

- Network Call Signalling (NCS) Protocol
- Dynamic Quality Of Service (DQoS)
- Trunk Gateway Control Protocol (TGCP)
- Packetcable Signaling Security using IP Security (IPSec) to MTAs, CMTSs, and Trunk Media Gateways

The table PacketCableTM core features lists the node-based line services that are supported by the IAC solution.

Note: The ability to support these features is dependant upon the third-party equipment used.

PacketCable™ core features

Number ID	Requirement
12.1	PKT-TR-VOIPERF-R01-000615
PC2.1.1	Calling Number Delivery
PC2.1.2	Calling Name Delivery
PC2.1.3	Calling ID Delivery Blocking (default or per-call)
PC2.1.4	Calling ID Delivery on Call Waiting
PC2.1.5	Call Waiting
PC2.1.6	Cancel Call Waiting
PC2.1.7	Call Forward Variable and Usage-Sensitive Call Forward
PC2.1.8	Call Forwarding Busy Line
PC2.1.9	Call Forwarding Don't Answer
PC2.1.10	Selective Call Forwarding
PC2.1.11	Selective Call Rejection
PC2.1.12	Automatic Recall
PC2.1.13	Automatic Callback
PC2.1.14	Visual Message Waiting Indicator (CPE light, stutter dial tone)
PC2.1.15	Customer Originated Trace
PC2.1.16	Three-Way Calling and Usage-Sensitive Three-Way Call
PC2.1.17	Distinctive Ringing/Call Waiting
PC2.1.18	Speed Calling

The table PacketCableTM extended features lists the node-based line services that are supported by the IAC solution.

Note: The ability to support these features is dependant upon the third-party equipment used.

PacketCable™ extended features

Number ID	Requirement
PC Ext. Feat. -2.1.1	Residence Distinctive Alerting Service
PC Ext. Feat. -2.1.2	Remote Activation of Call Forwarding (RACF)
PC Ext. Feat. -2.1.5	Line Service Restriction (LSR) (known as SACB)
PC Ext. Feat. -2.1.10	Anonymous Call Rejection (*77/*87)

Note: Remote Activation of Call Forwarding (RACF) is not supported with TGCP.

IAC Dynamic Quality of Service (DQoS)

Resources may be constrained in segments of the network, requiring allocation of resources in the network. Dynamic Quality of Service (DQoS) assigns (on demand) resources for each communication, depending on the QoS requested. Simply put, DQoS is the allocation of QoS between the Multimedia Terminal Adapter (MTA) and Cable Modem Termination System (CMTS).

DQoS framework handles the coordination between signaling (which controls access to application specific services) and resource management (which controls access to network-layer resources). This coordination provides the following critical functions:

- ensures that users are authenticated and authorized before receiving access to the enhanced QoS associated with the service
- ensures that network resources are available end-to-end before alerting the destination MTA
- ensures that the use of resources are properly accounted for, consistent with the traditional voice-grade telephone service in which charging only occurs after the party receiving a communication picks up

The MTA dynamically reserves local QoS resources using mechanisms defined in DOCSIS (Data Over Cable System Interface System). The MTA directly signals for local access QoS using the MAC (Message Authentication Code) Control Service interface. When an MTA

determines that QoS resources need to be reserved or committed, it initiates DOCSIS Dynamic Service Flow signaling to create, change, and/or delete Service Flow(s) and allocates DOCSIS resources.

CALEA

IAC supports the following CALEA functionality:

- Timing Information, Content of subject-held conference calls, and Party hold, join, drop on conference calls
- Subject-initiated dialing and signaling information, In-band and out-of-band signaling, and dialed digit extraction

PacketCable signaling security

The security architecture for IAC closely follows PacketCable security specifications and concepts.

The CMTS and MTA have different architectures for encryption key management and initial authentication.

The MTA uses Kerberos/PKINIT. In SN07, MTA authentication with the CS 2000 requires a PacketCable KDC, which grants Kerberos call server tickets to the MTA. The KDC is third-party equipment provided by the customer that must be integrated by the customer, a third-party integrator, or Nortel Networks through the Nortel interoperability program.

The CMTS and trunk gateways use IPSec/IKE with pre-shared keys. These devices do not require a KDC.

Note: In SN07 the CS 2000 only supports the CMTS/trunk gateway architecture on third-party trunk gateways. The CS 2000 does not support the architecture on the Media Gateway 7400/15000.

Trunk Gateway Control Protocol

In SN07 IAC introduces support for the PacketCable Trunk Gateway Control Protocol (TGCP). TGCP is part of the suite of PacketCable 1.0 protocols and TGCP support is part of IAC PacketCable 1.0 compliance in SN07.

TGCP controls PSTN trunk gateways within the PacketCable architecture. Support is limited to the following trunks:

- SS7 ISDN user part (ISUP)
- MF
  - outgoing operator trunks
  - one-way incoming operator trunks for busy line verification (BLV)/Barge-in
  - E911 trunks for access to an E911 tandem

PT-IP and PT-AAL2 features and services

This section discusses the features and services that are unique to the PT-IP and PT-AAL2 solutions.

PT-IP and PT-AAL2 test trunk services

This section describes how test trunking is accomplished through the IW-SPM-IP. For information testing trunks using the SPM through an interconnect span, see IP solutions test trunk services.

IW-SPM-IP test trunking strategy

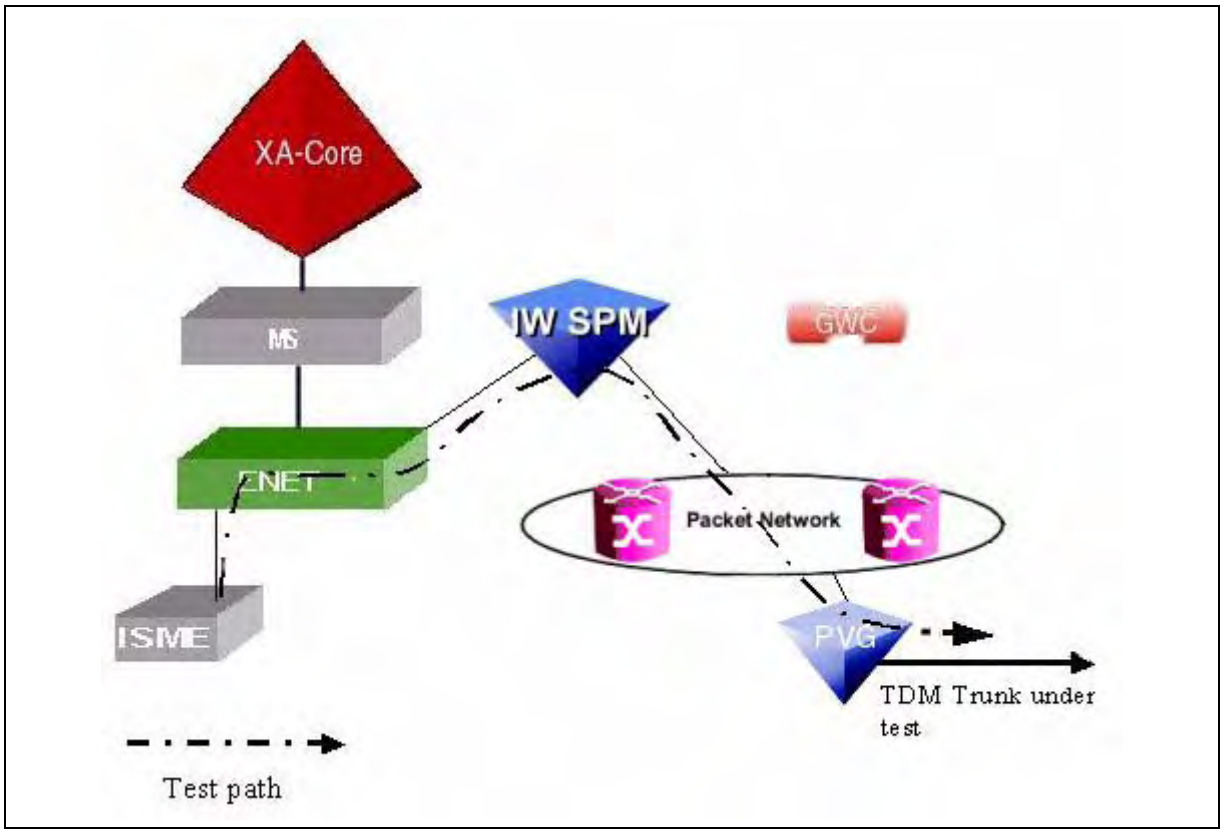
The IW-SPM-IP can be used to bridge the TDM side of the switch and the packet side or intra-switch traffic as well as inter-switch traffic. In other words, it supports trunk testing calls on the Gateway trunk using legacy MTM test circuits, legacy TDM trunk and Gateway TDM trunk interworking calls, and legacy TDM trunks.

Note: IW-SPM-IP test trunking is only available for the hybrid solution PT-IP solution.

The IW-SPM-IP provides the bridge between the Passport 15000 PVG trunk that requires testing and the test trunk hardware, enabling the user to directly conduct the test on the specific trunk. The figure Trunk test strategy with an IW-SPM-IP shows that the test is conducted directly using the IW-SPM-IP. The figure depicts a test path for a trunk hosted by a Passport 15000 PVG. The test path is bridged using the IW-SPM-IP to the trunk under test hosted by a Passport 15000 PVG.

The figure Trunk test strategy with an IW-SPM-IP shows the test trunking strategy with an IW-SPM-IP.

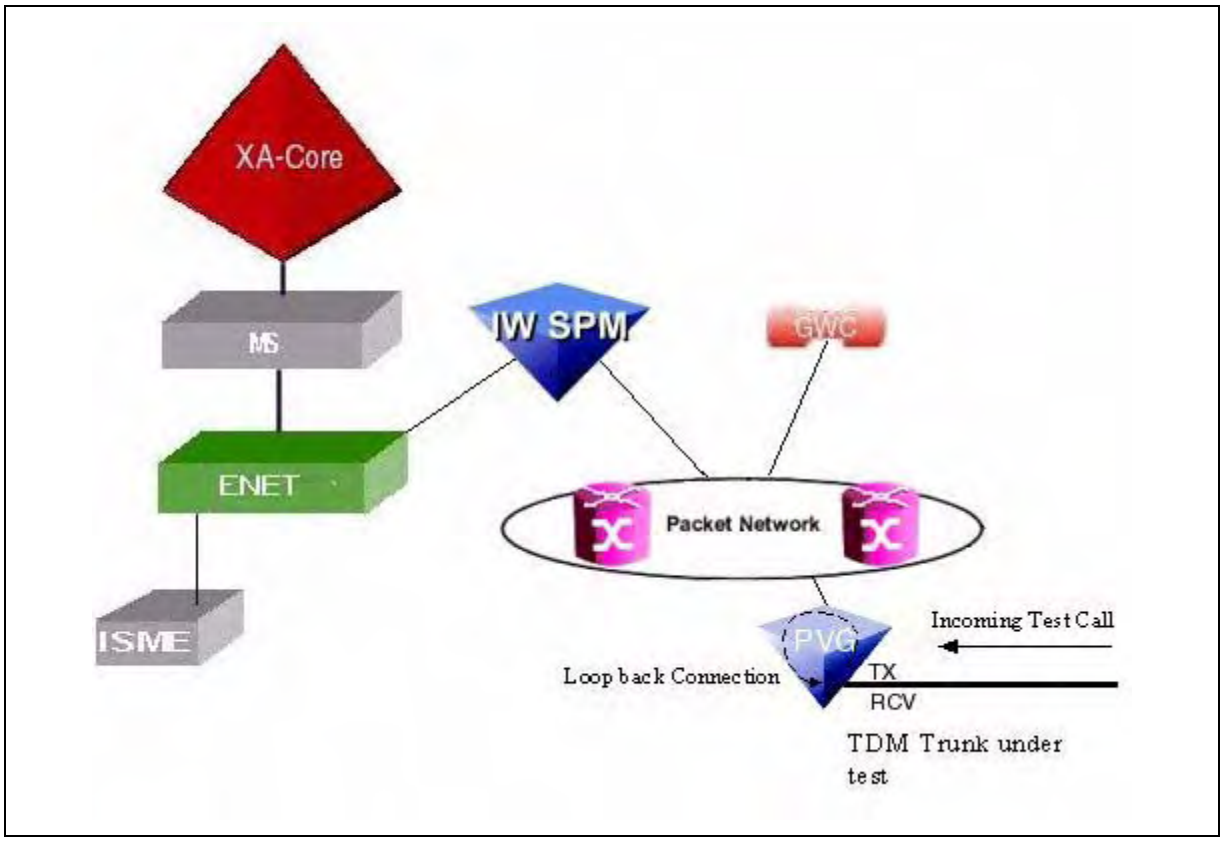
Trunk test strategy with an IW-SPM-IP



Terminating T108 test line support

The SN05 Release also provides terminating T108 test line test support. As mentioned earlier, the T108 test line is a dialable method for accessing the dialed loopback on trunks feature, TRKLPBK; however, it does not require IW-SPM-IP. In the SN05 Release, when the TRKLPBK feature is invoked for a trunk hosted by a Passport 15000 PVG, a loopback connection is established on the trunk at the DS0 level (transmit is connected to receive). This loopback connection isolates trunk troubles and measures net loss and noise and runs BERT for trunks at the DS0 rate. The figure Terminating T108 test line test support depicts the strategy for terminating T108 test line test support.

Terminating T108 test line test support



UA-IP features and services

This section discusses the features and services that are unique to the UA-IP solution.

The table UA-IP node-based line services lists the node-based line services that are supported by the UA-IP solution.

Note: The ability to support these features is dependant upon the third-party equipment used.

UA-IP node-based line services

Feature	Symbol	Description
Announcement before Bridging	ABR	[Description required]
Automatic Line / Hotline	AUL	Allows automatic dialing of a set number whenever the handset is raised or the DN key is pressed
Bridge Night Number	BNN	Allows a different number for use during different time periods
Call Forward Unconditional	CFU/CFW	Diverts all calls to an alternate number
Cancel Call Waiting	CCW	Ability to cancel the Call Waiting feature
Call Forward Busy	CFB / CFBL	Diverts calls to an alternate number when the called party is busy
Call Forward Don't Answer	CFD / CFDA	Diverts calls to an alternate number when the called party does not answer
Call Forward No Answer Variable Timing	CFDVT	Diverts call waiting calls to an alternate number if the called party does not respond to the call waiting signal within a variable time frame
Call Forward Remote Access	CFRA	Allows a subscriber to remotely access call forwarding on a directory number different from which they are calling
Call Forward Simultaneous / Screening	CFS	Permits a user to forward more than one (up to a maximum of 256) calls through a station at a time
Call Forward Validation	CFWVAL	Allows a subscriber to check their current call forward settings
Call Hold	CHD	Allows a calling party to temporarily place a call on hold
Call Pickup	CPU	Allows a station to answer incoming calls for another station in the same pickup group

UA-IP node-based line services

Feature	Symbol	Description
Call Waiting	CW / CWT	Busy party is made aware that an incoming call attempt is being made
Denied Call Forwarding	DCF	Allows a party to deny incoming forwarded calls
Directed Call Pickup	DCPU	Allows a station to answer a ringing line in the same customer group before the called party answers the ringing line
Subscriber Activated Call Baring	SACB	Allows a subscriber to bar outgoing calls
Speed Calling, individual short list	SCS	Allows a party to store, delete and dial up to 10 directory numbers using only a few key presses
Speed Calling, individual long list	SCL	Allows a party to store, delete and dial up to 70 directory numbers using only a few key presses
Lawful Intercept / Call Monitoring (basic call)	LI	Ability to monitor incoming and outgoing calls, transparent to the parties involved in the call
Requested Suspend Service	RSUS	Allows a party to request suspension of service. All incoming calls or attempted outgoing calls are routed to treatment
Secondary DN / Teen Service	SDN	Allows a single party to have additional directory numbers assigned to their line
Spontaneous Call Waiting Identification	SCWID	Allows delivery of calling party information, such as their directory number or name, and a call-waiting tone to the called party even when the called party is already busy
Warm Line	WML	Allows a line to be associated with another directory number. If the subscriber goes off-hook and does not dial in a predefined time, the call automatically routes to the associated directory number.

The table UA-IP network-based line services lists the node-based line services that are supported by the UA-IP solution.

Note: The ability to support these features is dependant upon the third-party equipment used.

UA-IP network-based line services

Feature	Symbol	Description
3-Way Call	3WC	Allows a party to add another party to an existing conversation and have a three-way conference call
Call Completion to Busy Subscriber	CCBS	Allows a calling party to have a previously busy call attempt redialled when the called party becomes free
Calling Name Delivery Enhancements (includes Call Name Delivery Blocking and Calling Name/Number Delivery on individual call basis)	CNAB / CNNB	Allows a calling party to withhold delivery of their calling name
Calling Number Delivery	CND	Allows a called party to view the number of the calling party before they accept the call.
Calling Name Delivery	CNAMD, NDND	Allows a called party to view the name of the calling party before they accept the call
Calling Number Blocking	CNB, CNDB, CNNB	Allows a calling party to hide their directory number and cancel the effect of CND
Do Not Disturb	DND	Allows an attendant to prevent call termination on a single station or group of stations
Distinctive Ringing	DRING	Allows a called party to have a distinctive ring on their telephone set
Voice Band Data: Modem and Group 3 Fax	n/a	Allows transmission and reception of voice-band data services such as facsimile and modem
Message Waiting Indicator - Audible or visible	VMWI	Allows generation of a tone or lights an indicator lamp to indicate a message is waiting
Wake-up Call Request	WUCR	Allows a subscriber to program their telephones to ring at a specified time

The table UA-IP other-switch services lists the node-based line services that are supported by the UA-IP solution.

Note: The ability to support these features is dependant upon the third-party equipment used.

UA-IP other-switch services

Feature	Symbol	Description
Local Number Portability (LAN based)	LNP / PORT	A network capability that allows a subscriber to change network operators (to be served by a switch belonging to a different operator) whilst retaining the same DN as before the move.
CEPT Call Waiting Indication	ICWT	Provides announcements to the calling party that the called party is engaged on another call. Diverts to treatment is the call is accepted (or after a thirty second timeout). Conforms to the CEPT standard. ***Note:*** Only available on the International UA-IP solution.
CEPT Call Forward Simultaneous / Screening	CFS	Permits a user to forward more than one (up to a maximum of 1024) calls through a station at a time. Conforms to the CEPT standard. ***Note:*** Only available on the International UA-IP solution.
CEPT Call Forward No Answer Variable Timing	CFDVT	Diverts call waiting calls to an alternate number if the called party does not respond to the call waiting signal within a variable time frame. Conforms to the CEPT standard. ***Note:*** Only available on the International UA-IP solution.
CEPT Call Pickup	CPU	Allows a station to answer incoming calls for another station in the same pickup group. Conforms to the CEPT standard. ***Note:*** Only available on the International UA-IP solution.

UA-IP other-switch services

Feature	Symbol	Description
CEPT Outgoing Call Barring	OCB	Allows an operator to bar outgoing calls according to specified rules. The rules can be modified by the operator. Conforms to the CEPT standard. ***Note:*** Only available on the International UA-IP solution.
CEPT International 3-Way Call and Call Transfer	I3WC and ICT	Allows a caller to establish a 3-party conference call. The initiator of the conference call can drop out leaving the remaining two callers connected (call transfer). Conforms to the CEPT standard. ***Note:*** Only available on the International UA-IP solution.
CEPT Call Back to Last Received Call	AR	Allows a called party to inquire into the number of the last received call that was not answered, as well as the date and time in which the call took place. The called party can, if desired, return the call to the original caller by pressing a single digit.

CLASS support for UA-IP

The MG 9000 line card has the ability to support different types of CLASS signaling, which can be configured through a provisioning feature to handle different markets.

Ringing support for UA-IP

To provide distinctive ringing, the MG 9000 supports the ability to indicate which ringing to use as part of the H.248 “alert” package.

Hook flash support for UA-IP

Hook flash has a default setting for hook flash time, but the setting may be provisioned on a per line basis to adjust for different markets that may have different hook flash considerations.

Customer Support

This section describes the range of services Nortel Networks offers:

- solution and customer support
- customer information
- customer responsibilities
- training and documentation
- professional services
- operation support services

Solution and customer support

Nortel Networks provides solution support using standard Customer Service Center (CSC) and Global solution Support (GPS) policies and procedures. For issues that cannot be resolved, contact Nortel Networks regional Customer Services Center and a representative will open a Customer Service Report (CSR). If the regional representative cannot resolve the problem, The Customer Service Center representative will refer the matter to the next level of support to provide either an answer to the problem or corrective action.

Corrective action can include the following:

- amendment in a future software release
- incremental software update (patch)
- customer information change
- request for feature development to address new or changed functionality

Once the problem is resolved, the customer is notified and the CSR is closed.

Software release and support policy

A Succession Software Release consists of the Call Server PCL (solution Computing load) and the Nortel Networks brand Component software loads that are required for the Packet Trunking-AAL1 solution. For Third Party Network Element software sold by Nortel Networks in conjunction with a Succession Software Release, the Third Party software support policy will be in effect.

Ordering and support overview

A Succession Software Release can be ordered either before or within 12 months after reaching First Volume Ship (FVS) status, and is priced

at the applicable contract terms for right-to-use and generic load insertion fees.

Nortel Networks does not recommend using retired (unsupported) software releases in existing offices and will not deploy a retired release to an initial (new) Succession installation or an extension. Therefore, each individual Succession Software Release application of a given software release must be scheduled to occur before the retirement of that release. This requirement must be considered when placing an order toward the end of the active stage of a particular release.

Full software support—including both emergency-outage and non-emergency support—will be available until 12 months after FVS of the release. Support is available for retired releases only under a separate service contract, and will be limited to support which does not require patching or other design effort.

Software upgrade path overview

Generally, Succession Software releases will reach FVS status about every six months. Thus, at the end of the six months after FVS of a Succession Software Release, another new release will be available for ordering and loading. The network provider can choose either to deploy this next Succession Software Release in sequence or to skip up to one release. If skipping more than one release is required, one or more of the skipped releases must be temporarily inserted (at extra cost) to enable loading of the desired release.

Note: Any updates or exceptions to the Succession Software Release and Support Policy must be made through solution/Service Update and/or solution/Service Information publications. For more information about Nortel Networks software development cycles and software administrative policy, please contact your Nortel Networks representative.

Optional support package overview

The table Standard software support policy lists the components that require optional support packages for software support. Some of these optional support packages will require the component to be upgraded

to the latest software release when the standard software support expires.

Standard software support policy

Component	Standard software support policy
Contivity 600	Software support is available for the last published software release and one release back (including their associated patches, fixes, and work a rounds).
Passport 8600/Device Manager	Software support is available for the last published software release and one release back (including their associated patches, fixes and work a rounds).
Media Gateway 15000	Media Gateway software releases are supported for 2 years (24 months) after declaration of General Availability (GA). This policy applies to PCR 3.0 and later software releases.
Preside MDM	MDM software releases are supported for 2 years (24 months) after declaration of General Availability (GA). This policy applies to MDM 13.3 and later software releases.

Note: In addition to the optional support packages, Nortel Networks can offer extended warranty support at an additional charge based on agreements with your account representative. For additional details on the software support policies available for these components, please contact your regional Nortel Networks representative.

Service bundling

Customers may purchase the following additional services:

- software upgrades
- technical support services
- emergency recovery services such as disaster recovery options
- hardware repair services outside of warranty coverage
- applications and migration support
- audits and evaluations
- operations training

- call response coverage
- electronic software delivery
- mentoring services

Web site information

Nortel Networks Web site, www.nortelnetworks.com is a valuable site for customer information, support, and services. From this site, the customer can get information on customer service, training, and documentation, professional services, and other areas of business.

Customer responsibilities

The information in this section is intended for use by Nortel Networks sales, Business and Development, and Marketing personnel who are responsible for ensuring that the customer is aware of and agrees with their responsibilities when discussing the Succession PT-AAL1 solution. Additionally, these responsibilities must be written into any subsequent contracts which result from such discussions or negotiations.

This section includes the following:

- Hardware baseline
- Electronic software delivery requirements

Hardware baseline

Unless stated otherwise, all classic Digital Multiplex Switch (DMS) equipment used for this Succession solution has the same hardware release lineup as that of the concurrent DMS17 release.

Electronic software delivery requirements

Information on electronic software delivery (ESD) patches is included in the document *Upgrading the Succession Network*, NN10344-450. Succession solution electronic software delivery requirements include:

- Media Gateway software delivery

  Software delivery for Media Gateway 15000, and Preside MDM software loads is done using BaaN 145 ordering system and the Software Tracking and Navigating (STAN) system. STAN is a powerful tool offered as part of the Performance On Line (POL) suite of services. This system allows customers to download software or request shipment of software CD ROMs and documentation. STAN is accessed, as part of the POL system, from the Nortel Networks

web-based center located at http://www12.nortelnetworks.com/cgi-bin/cnss/cs/main.jsp

- DMS and SPM software delivery

  In order to perform electronic software delivery, the software order codes that make up the Succession solution load will be retrieved from a software vault. The appropriate formatting (pre-mastering) will be applied and the load will be stored on a Nortel Networks electronic software delivery server.

  There are two main ways to employ electronic software delivery. Customers using the “pull” method will be notified and provided with the details and the directory structure of the load on the Nortel Networks electronic software delivery server. The customer can connect over to the Nortel Networks electronic software delivery server to pull the load.

  For customers requiring the “push” method, Nortel Networks will send the loads to the CS 2000 Core Manager repository server or drop box. The drop box can either be customer provided within the customer’s network or Nortel provided within Nortel’s network. The Nortel account team and Software Delivery will work with the customer to choose the best option based on their needs and security requirements. If a repository is set up in the customer’s network, it must be externally accessible to Nortel Networks. A customer E-mail address is required for subsequent notification of software load delivery.

  The loads are transmitted in a compressed form and after they are received at the destination, decompression of the load can take place.

  As an example of the load transmission time, if the available connectivity from the customer network to Nortel Networks is 1.544 Mbit/s (a T1 connection), then the transmission time for a 2 Gbyte load will be approximately 3 hours. The available data connection bandwidth will proportionately affect the transmission time.

  After the customer retrieves the load from the Nortel Networks electronic software delivery server, the load enters their LAN/WAN infrastructure and can be stored on their local server. Thereafter, an application on the CS 2000 Core Manager is used to pull the load. The customer is expected to have an application for security and authentication on the WAN to which the CS 2000 Core Manager is connected.

  For satisfactory performance, it is recommended that the customer LAN/WAN have a throughput of 300 Kbyte/s (or greater to transmit the load files to the destination CS 2000 Core Manager. With a throughput of 375 Kbyte/s and a load size of 2 Gbytes, it will take

approximately 1.5 hours to move a complete Succession load from the customer server to the CS 2000 Core Manager. The table Comparative transmission times for 100 Mbytes gives the approximate comparative download times for throughput over selected dedicated connection links. The customer must consider what transmission time is acceptable to their operations in order to determine the throughput requirements for their network.

Comparative transmission times for 100 Mbytes

Type of Data Link	Data Rate	Time
28 Kbit/s modem	28.8 Kbit/s	10+ h
56 Kbit/s modem, ISDN, EIU, X25, DataPac, ISDN	56-64 Kbit/s	5+ h
T1	1.5 Mbit/s	10+ min
10 base-T Ethernet	10 Mbit/s	80 s
OC-3	84 x T1 (155 Mbit/s)	6 s

The peak demand for network resource for electronic software delivery occurs when a milestone software upgrade is scheduled. A lesser demand occurs when an NCL or an MNCL is transmitted by electronic software delivery. The frequency of the former is approximately twice a year, and the later can have a frequency of approximately once a month.

In summary, requirements for electronic software delivery are:

- The customer must have their network engineer work with the Nortel Networks electronic software delivery engineer to discuss technical details.
- The link from the Nortel Networks electronic software delivery server to the customer LAN/WAN server must have a minimum throughput of 1.544 Mbit/s.
- The customer should have a storage of 36 Gbyte on their server.
- The CS 2000 Core Manager and the LAN/WAN server must be integrated into the DCE cell of the customer, if DCE is used for security.
- The customer LAN/WAN must have a minimum throughput of 300 Kbyte/s to transmit Succession Network loads in a reasonable time period.

Security requirements for DMS and SPM based-equipment software loads

Access from the Nortel Networks electronic software delivery server to the customers server will be over a switched circuit, and user identification and password are employed to provide security. When logging in from the Nortel Networks electronic software delivery server to the customer LAN/WAN, the security algorithm required by the customer will be used. For Media Gateway 15000, and Preside MDM software loads, the Nortel Networks electronic software delivery system uses a secure-access system; customer Login ID and passwords are managed as part of the POL (Performance On Line) suite.

Training and documentation

This section provides information about who to contact and where to get customer documentation and training.

Contacting Nortel Networks for help on customer information

You can contact Nortel Networks account prime for help on customer information.

Customer information

Nortel Networks provides customer information on a CD. The customer CD provides component-level as well as solution-level customer information, which includes information in the following areas:

- overview
- network upgrades
- fault management
- operational configuration
- accounting
- performance
- security and administration

Legacy information

For legacy information, refer to the DMS-100 Family suite of documents that are available through Helmsweb.

Where to get customer documentation

Documentation for each Succession Network solution is delivered on a CD ROM.

Nortel Networks Web site (www.nortelnetworks.com) is a valuable site for customer information, support and services. From this site, the

customer can get information on customer service, training and documentation, professional services, and other areas of business.

Where to get training information

All course descriptions, prerequisites, schedules, and locations can be viewed at www.nortelnetworks.com.

Note: For the most recent curriculum information, please contact Nortel Networks Training and Documentation representative. For enrollment assistance, please contact Training registration at 1-800-4-NORTEL, (1-800-466-7835), express routing code #280.

Professional services

An extensive set of professional services accompany the IP solutions. These services will be offered in addition to the engineering, installation, and commissioning services that are part of the base solution.

Services are defined and selected according to the needs of the customer and range from turnkey solutions to programs that assist the customer in specific tasks and in acquiring needed skills.

The initial set of services offered as part of the IP solutions are as follows:

- business and market planning services
- network planning and design to cover the packet network, TDM network, operations networks, and access networks
- operations planning realization
- business contingency and disaster recovery planning
- program and project management
- translations for Communication Server 2000 (CS 2000) and for the Media Gateway 15000
- packet configuration
- LAN design and setup and element manager setup
- Preside Management for Succession Solution (Preside MSS) and security planning, implementation, and integration
- network test and verification
- feature migration services
- facility cut-over services

- surveillance, maintenance, provisioning, and customer care services
- enhanced Technical Assistance Service (TAS) support services
- removal of old equipment

Additional services are available on a custom basis if required. For more details, please refer to the Service bundling section.

Operations support services

Nortel Networks provides Technical Assistance Service (TAS) and Emergency Technical Assistance Support (ETAS). The TAS and ETAS technical personnel investigate and resolve problems that customers encounter while operating the covered switching systems.

Requests and operational problems are classified according to severity and overall effect on the system.

Routine Technical Assistance Support (TAS), S1 and S2

The service provides the following help for customers:

- Coverage during Nortel Networks' business hours or as scheduled with a TAS supervisor.
- Response from Nortel Networks as soon as practical, according to the severity of the problem. Assistance through telephone and/or remote access.
- Diagnosis of cause and recommended actions to restore operational stability.
- TAS-initiated on-site assistance made necessary by non-emergency conditions and covered by the Service and Support Plan (S&SP).
- Customer-initiated on-site assistance, available through mutual agreement and dispatched within four hours of mutual agreement. Additional charges are billed for travel and per diem expense, plus the current hourly rate.

Technical Assistance Support (TAS) can be reached between the hours of 8:00 a.m. and 5:00 p.m. (CST), Monday through Friday.

Emergency Technical Assistance Support (ETAS), E1 and E2

This service provides the following help for customers:

- Coverage 24 hours a day, seven days a week
- Immediate assistance through telephone and/or remote access.

- Diagnosis of cause and recommended actions to restore operational stability
- ETAS-initiated on-site assistance made necessary by emergency conditions and covered by the S&SP.
- Customer-initiated on-side assistance, available through mutual agreement and dispatched within four hours of mutual agreement. Additional charges are billed for travel and per diem expense, plus the current hourly rate.

Emergency Technical Assistance Support (ETAS) can be reached 24 hours a day, seven days a week.

Escalation procedure

If customer needs are not met at the TAS representative level, the matter may be escalated by contacting the following persons, in sequential order:

- Manager, Technical Assistance Service
- Senior Manager, Technical Assistance Service
- Director, Technical Assistance Services
- Director, Service Operations

Glossary of terms

Terms and acronyms commonly used in Succession Networks are defined below.

3PC card
3rd Party Core card

AALn
ATM adaptation layer (where n is a number such as 1, 2, 5)

AAL2
ATM adaptation layer 2

AC
Audio Controller: is a type of Succession GWC

ADSL
asymmetrical digital subscriber line

AIN
Advanced Intelligent Network

AMA
Automatic Message Accounting

AMADNS
Automatic Message Accounting Data Networking System (AMADNS)

ANM
Answer Message

ANSI
American National Standards Institute

APS
Audio Provisioning Server

ARP
address resolution protocol

ATM
asynchronous transfer mode

BHCA
Busy Hour Call Attempts

BICC
bearer independent call control

BIP
breaker interface panel

CALEA
Communication Assistance for Law Enforcement Act

CAM
Communications Applications Module

CAN
Customer Access Network

CCF
Call Control Frame

CEM
common equipment module

CIC
Call Instance Codes

CISM
Cabinetized Integrated Service Module

CLLI
common-language location identifier

CLP
CS 2000 Management Tools Common Application Launch Point

CMTS
Cable Modem Termination System

CNAMB
Calling Name Delivery Blocking

CNAMD
Calling Name Delivery

CND
Calling Number Delivery

CNDB
Calling Number Delivery Blocking

CODEC
coder-decoder

Contivity 600 VPN switch
Contivity 600 Virtual Private Network switch

cPCI
compact Peripheral Component Interconnect

CPE
customer premises equipment

CSAM
Cabinetized Services Application Module

CRCX
CreateConnection - requests the establishment of a connection.

CS 2000
Succession Communication Server 2000:

CS 2000-Compact
Succession Communication Server 2000-Compact

CS 2000 Core Manager
Succession Communication Server 2000 Core Manager is the device manager of the CS 2000.

CS 2000 GWC
CS 2000 Gateway Controller

CS 2000 SAM21
CS 2000 Services Application Module 21

CS LAN
Communication Server Local Area Network: is the integrated component within Nortel Networks Succession CS 2000 and CS 2000-Compact that provides a secure environment for mission critical processing of message traffic between the CS 2000 components and other key network elements.

CSV
comma separated values

CTC
Centralized Translations Control

CUAS
Cabinetized Universal Audio Server cabinet

CUSE
Cabinetized Universal Server Extension

DPT
Dynamic Packet Trunking

DDD
direct distance dialing

DIRP
Device Independent Recording Package

DMS
Digital Multiplex System

DQoS
Dynamic Quality of Service feature: assigns (on demand) resources for each communication, depending on the QoS requested

DRAM
digital recorded announcement module, or dynamic random access memory

DS0
Digital Signal Level 0: the 64 Kbit/s channel that is the basic building block for a North American T1 transmission line

DS0A
Refers to a process where a subrate signal (2.4, 4.8, or 9.6 Kbps) is repeated 20, 10, or 5 times respectively to make a 64 kbps DS0 channel

DS1
Digital Signal Level 1: the North American Digital Hierarchy signaling standard for transmission at 1.544 Mbit/s.

DS30
Digital Signal Level 30: is the equivalent of 30 DS1s

DS512
a proprietary fiber optic transmission link that is the equivalent of 16 DS30 links

DSL
Digital Subscriber Line

DTC
Digital Trunk Controller

DTCI
Digital Trunk Controller with ISDN

DTM
Digital Trunk Module

DTMF
dual tone multi-frequency

EIU
Ethernet interface unit

ENET
is the enhanced network for the XA-Core

ESA
Emergency Standalone Support

FCAPS
Fault, configuration, accounting, performance, security

FCM
Fabric Control Message

FLPP
fiberized link peripheral processor

FRUs
Field Replaceable Units

FTP
file transfer protocol

GD
Genetic Digits

GETS
Government Emergency Telecommunications Service

GUI
graphical user interface

GWCEM
Succession Gateway Controller element manager

HFC
Hybrid Fiber Coax Cable System

HLR
Home Location Registration

HSC
hot swap controllers

HSL
high-speed links

IAC
Integrated Access Cable (a Succession solution)

ICCM
InterCAM Communication Medium

ICMP
Internet control message protocol

IETF
Internet Engineering Task Force

ILEC
incumbent local exchange carrier

I/O
input/output

IOM
input or output module: a peripheral that connects the XA-Core the message switch.

IP
Internet protocol

ISME
Integrated Service Module Enhanced

ISUP
integrated services digital network user part

ITU
International Telecommunications Union

IW SPM-IP
Interworking Spectrum Peripheral Module

IXC
Inter-exchange Carrier

JAAS
Java Authentication Authorization Service

JWS
Java™ Web Start

LAN
local area network

LD
long distance

LIS
link interface shelves

LIU7
link interface unit 7

LMM
Line Maintenance Manager

LPP
link peripheral processor

LTC
Line Trunk Controller

LTCI
Line Trunk Controller with ISDN

LTM
Line Test Manager

MAPCI
maintenance and administration position command interface

MARS
Meridian Automatic Route Selection

MG 9000
Succession Media Gateway 9000

MG 9000 Manager
Succession Media Gateway 9000 Manager

MGC
media gateway controllers

MPC
multiple point codes

MSO
multiple system operator

MTA
Multimedia Terminal Adapter

MTM
Maintenance Trunk Module

MTP
message transfer part

NCS
Network based Call Signaling

NEBS
North American New Equipment Building Standard

NFS
network file system

NGS
Nortel Networks Global Solutions.

NOCs
network operations centers

NPM
Network Patch Manager

NTP
network time protocol

PT-IP
Packet Trunking IP (a Succession solution)

nrt-VBR
non-real-time variable bit rate

OAM&P
operations, administration, maintenance, and provisioning

OAU
Office Alarm Unit

OC-3
optical carrier level 3 is the SONET transmission rate of 155.52 Mbit/s

OC-3c
concatenated OC-3

OM
operational measurement

OMD application
Operational Measurements Delivery application

OSI
Open Systems Interconnection

OSPFIGP
open shortest path first Internet gateway protocol

OSS
operations support system

OSSGate
is an application that provides a machine interface for provisioning components within Succession

PAM
Pluggable Authentication Module

Passport 7400 PVG
Passport 7400 Packet Voice Gateway

Passport 8600
expansion and definition

Passport 15000 PVG
Passport 15000 Packet Voice Gateway

PC
personal computer

PDS
persistent data storage

PM Poller
Performance Measurements Poller

POTS
plain old telephone service

PPC
PowerPC

PPVM
peripheral processor virtual machine

Preside MDM
Preside Multiservice Data Manager

Preside MSS
Preside Management for Succession Solutions. Preside MSS is a suite of element management software that runs on approved hardware platforms. Preside MSS provides the overall OAM&P functionality for Succession solutions.

PRI
primary rate interface

PSP
Product and Services Provisioning

PT-AAL2
Packet Trunking AAL2 (a Succession solution)

QCA
Quality of Service Collector Application

QoS
quality of service

QoSCA
Quality of Service Collector Application

RAM
random access memory

RAID
redundant array of inexpensive disks

RAS
Remote access server

REX
Routine EXercise

RMGC
Redirecting Media Gateway Controller

RMON
Remote MONitoring specification is a simple network management protocol

RTCP
real time control protocol

RTP
real-time transfer protocol

SAAL
signaling ATM adaptation layer

SBA
SuperNode Billing Application

SBC
Single Board Computer

SC
Shelf Controller

SCCP
signaling connection control part protocol

SCTP
simple control transmission protocol

SCWID
Spontaneous Call Waiting Identification

SDH
Synchronous Digital Hierarchy

SDM
SuperNode Data Manager

SDP
signal distribution point or Session Descriptor Protocol

SERVORD
service orders

SESM
Succession Element Sub-Network Manager: is a software package that includes several CS 2000 Management Tools applications

SFT
secure file transfer

SIP
Session Initiation Protocol

SIP-T
Session Initiation Protocol for Telephony

SMP
simplex multiprocessor

SNMP
Simple Network Management Protocol (SNMP)

SONET
synchronous optical network

SPC
Single Point Code

SPDC
Secondary Power Distribution Center

SPM
Spectrum Peripheral Module

SS7
signaling system number 7: is a family of signaling protocols used to set up, manage, and tear down connections, as well as to exchange non-connection associated information.

SSPFS
Succession Server Platform Foundation Software: is the NCL software package that contains base operating system and common tools, libraries and server functions used by element-management-level applications.

STORM
STOrage Management

STP
signaling transfer point: a node in the SS7 network

STORM
STOrage Management

STP
spanning tree protocol

Succession MG 9000
Succession Media Gateway 9000

Succession UAS
Succession Universal Audio Server

SWIM
SDM Software Inventory Manager

TCAP
transaction capabilities application part

TCP
transmission control protocol

TDM
time division multiplexing

TFTP
trivial file transfer protocol

TM8
Trunk Module 8-wire (TM8)

TM
transition module

TMM
Trunk Maintenance Manager

UA-IP
Universal Access IP (a Succession solution)

UAS
Universal Audio Server

UAS Manager
Succession Universal Audio Server Manager

UDP
User Datagram Protocol

USNBD
United States Network Broadcast Delivery

USP
Universal Signaling Point

USP-Compact
Universal Signaling Point–Compact

USP–Manager
Universal Signaling Point–Manager

VDRN
Virtual Routing Destination Node: is a type of Succession GWC

VPN
virtual private network

VRRP
virtual router redundance protocol

VSP
voice services processor card in the Passport 15000 PVG or the Passport 7400 PVG

XA-Core
Extended Architecture Core