Solution basics

Introduction

This Solution-level Basics document gives an overview of the Nortel Networks Universal Access - IP Solution, for voice over . The overview is intended to provide a high-level description of the Universal Access - IP Solution. It is not intended to provide an in-depth description of components or procedures.

The detailed information on components and procedures is contained in a wide range of supporting documentation. Most sections of the overview contain references to the relevant documents. The Helmsman solution CD-ROM contains both the overview itself and all the supporting documentation.

> ***Note:*** Throughout the overview, the solution is referred to as 'the UA-IP Solution'.

Audience

This document is intended for customers who need to understand, operate, and maintain the UA-IP Solution.

Quick Reference Guide

The Quick Reference Guide (NN10262-001) can be found on the documentation CDs and provides a very high level overview of all Solutions. It also contains a road map of documentation for all solution supporting equipment and their associated document numbers.

What's new in this release

The table below lists the new features in (I)SN08 release.

> ***Note:*** The terms Succession, Preside MDM and Passport 8600 have been re-branded in conjunction with the new Nortel Networks' brand simplified naming format. Succession is now Carrier Voice over IP (CVoIP), Preside MDM is now referred to as MDM, and Passport 8600 is now Ethernet Routing Switch 8600.

Feature Description				
CS 2000 features				
A00006657 -- EADAS trunk group buffer expansion				
Affecting	PT-AAL1	UA-AAL1	NA PT-IP	NA UA-IP

Feature Description

Engineering and Administrative Data Acquisition System (EADAS) is an operational support system that provides near real time data collection and surveillance from many central offices. The EADAS package has two components, EADAS/DC (Data Collection) and EADAS/NM (Network Management). This feature deals with the EADAS/DC component.

EADAS/DC has three OM (operational measurements) classes, and each class is divided into 255 sections. Each section is defined by a set of OMs which collectively form the standard set. The standard set is defined by Telcordia for each software release.

The report and accumulation for each section is stored in an internal buffer. In the case of section 112, this buffer size is not adequately large enough to support the number of trunk groups (TG) required by the customer. The current limit for this section is 727 TGs.

This feature will alter the internal memory architecture to support up to 1024 TGs so that it is consistent with TR-746 requirement. This increase will apply to all 255 sections.

A00006780 -- Trimodal Call Server OAM&P enhancements

Affecting NA IAW UA-AAL1 NA UA-IP

The Trimodal Call Server is a Nortel Networks Call Server which supports all the following three Bearer Network Fabric types: ATM, IP and TDM. It is a solution being provided by Nortel Networks to its customers who want to make a smooth transition from VoATM Carriers to VoIP network solution and move into the IP Space, leveraging the already existing ATM equipment at their premises.

The (I)SN08 Trimodal Enhancements include the following changes:

- OAM&P Enhancements
- TRK2NET2 and TRK2NET1 OM Tuple allocation enhancement.
- Enhancements to include Bearer Network information on the following MAPs
  - SPM PM, Carrier and Perfmon MAPs
  - ABI XPM MAPs
  - TTP, LTP MAPs
  - DPT MAPs
- Enhancements to the Servord Query Commands QDN, QLEN, QLENWRK, QDNWRK, QHASU, QGRP, QLT and QCUST command outputs to include Bearer Network Information.
- When a tuple is added in table NETBRDGE, a Bridge Pool without members is allocated.
- Introduce restriction in table NETBRDGE to the DISPLAY field contains unique and non-null values, as these values are used in the MAP display and query command enhancements.
- New table OFCVAR parameter OSS_PROV_VERSION is added to enable/disable the Servord Query Command enhancements.
- Tool QOSSVER is introduced to print out list of activity IDs of features delivered in various loads which have OSS impact.
- Integration of H.323 and Centrex IP agencies into the Trimodal solution
- Strategy for upgrading a PT-AAL1 office to UA-Trimodal

A00006979 -- Synchronized Backup Manager

Affecting NA IAW UA-AAL1 NA PT-IP NA UA-IP

Feature Description

The feature provides a centralized mechanism allowing the user to initiate a synchronous backup for the core components of the Call Server. Providing this capability reduces the possibility of error caused by manual backup procedures on the various component platforms spread across the Call Server solution.

In (I)SN08, the Backup Manager will provide synchronous centralized control of the backup functionality resident within the following Call Server components:

- Communication Server 2000 Management Tools server
- MG 9000 Manager server
- Supernode Data Manager (SDM) / Core and Billing Manager (CBM) server
- Integrated Element Management System (EMS) server
- Session Server

Note: The Integrated EMS may reside with the CS 2000 Management Tools (and other applications) on the CS 2000 Management Tools server.

A00006901 - Missing Patches Robustness

Affecting	NA PT-IP	NA IAC	NA UA-IP	NA UA-AAL1

This feature aids the customer in obtaining and applying patches in a timely and routine fashion. The feature also provides facilities in aiding the customer in maintaining data during an upgrade, as well as providing several clean-up mechanisms.

CS 2000-Compact features

A00008431 -- System Mastership for CS 2000-Compact Geographic Redundant configuration

Affecting	NA IAC	NA IAW	NA PT-IP	NA UA-IP	Intl IAC	Intl IAW	Intl PT-IP	Intl UA-IP

This activity supports the Geographic Redundant (GR) configuration of the CS 2000-Compact by modifying the mastership selection algorithm to obtain better performance during normal and disaster scenarios.

The GR configuration splits the control components between 2 physically separate sites, using a highly available Optical transport system to connect the 2 sites.

In normal mode, each of the components maintains communication with its mate in the other site, and they decide and negotiate activity between the two components using their existing mastership algorithm. This is the default behavior when communications are up between the two sites, and maintains the current non-GR behavior when inter-building communications is present.

The enhanced mastership algorithm is used primarily in disaster scenarios, that is, when the communications between the buildings is lost, or either an entire site, or portions of it are down. The mastership algorithm detects what portions of the system are still active and reconfigures the system in an optimal mode to maintain services with the remaining inservice components.

Shelf Controller features

A00007423 -- Support for new hardware

Affecting	PT-AAL1	UA-AAL1	NA IAC	NA IAW	NA UA-IP	Intl IAC	Intl IAW	Intl PT-IP	Intl UA-IP

Feature Description

In (I)SN08, new hardware, Motorola MCPN905, for the Gateway Controller (GWC), Universal Signalling Point Compact (USPc) and Call Agent (CCA) is being introduced. The new GWC, USPc and CCA Hardware will follow the maintenance system used for the old GWC, USPc and CCA Hardware however the underlying actions will be different.

It allows the customer to manage the various cards in the SAM21 via the CS 2000 SAM21 Manager and the SAM21 Shelf Controllers. Currently, all non-system slot blades have full support for the various maintenance actions available via the shelf controller.

This includes the following actions:

- Detection of board removal and insertion from the SAM21
- Detection of board type, MAC address(s), memory size, Power-On-Self-Test errors, and firmware version
- Provisioning of IP Address, Gateway IP Address, load path and name, and application specific firmware settings.
- Unlocking (Booting) and Locking (halting) of the provisioned application
- Automatic firmware flash of board
- Out-of-Service Diagnostics (brief and full)

A00007424 -- Critical application and network health monitoring

Affecting	PT-AAL1	UA-AAL1	NA IAC	NA IAW	NA UA-IP	Intl IAC	Intl IAW	Intl PT-IP	Intl UA-IP

This feature covers the SAM21 SC software robustness on following areas:

- Critical Application Health Monitoring
- Network Health Monitoring
- Alarming of locked IO cards
- Alarming of recovering IO cards
- State clean of removed IO slots

Gateway Controller features

A00006987 - GWC Real-time and Memory Recovery

Affecting	NA PT-IP	NA IAC	NA UA-IP	NA UA-AAL1	intl PT-IP	intl PT-AAL2	intl IAC	intl IAW	intl UA-IP

This feature optimizes the protocol engine within the GWC to provide performance and memory improvements.

A00007054 -- H.248 Protocol Compliance enhancements for GWC

Affecting	PT-AAL1	UA-AAL1	NA UA-IP	Intl PT-AAL2	Intl UA-IP

This feature enhances the compliance of the GWC implementation of H.248 to the H.248.1 version 1 specification.

A00007100 -- Next Generation GWC card

Affecting	NA IAC	NA IAW	NA PT-IP	NA UA-IP	Intl IAC	Intl IAW	Intl PT-IP	Intl UA-IP

Feature Description

The purpose of this feature is to provide an increase to the overall hardware performance over that of the current MCPN750 platform while maintaining the current software functionality. Key areas of performance and capabilities increases are CPU clock speed, and RAM. Additionally, on board Flash memory of 32Mb or greater is being added.

A00007101 -- GWC Telnet authentication

Affecting	NA IAW	NA PT-IP	NA UA-IP	Intl IAW	Intl PT-IP	Intl UA-IP

In SN07, a GWC allows serial port access with no login, telnet access from the SESM with no login, and telnet access protected by (a single hard-coded) password from any device. There is no idle timeout and no logging of access or commands used. Any user who learns to access PMDebug has full access to tools which range from viewing provisioning data to altering of memory contents on the device, and this can represent a security vulnerability.

This activity adds to the secure-ability of the solution by providing a standardized user-id/password based login for the GWC devices. Central account management via the Integrated EMS allows existing defined accounts to be used, as authorized, instead of a separate password management strategy. Additional standard services like idle timeout and security logging are also provided.

A00007102 -- Dual C-side IP for GWC

Affecting	NA IAC	NA IAW	NA PT-IP	NA UA-IP	Intl IAC	Intl IAW	Intl PT-IP	Intl UA-IP

This feature will eliminate the requirement to provision a default gateway IP address when provisioning a GWC. The gateway IP will be automatically provisioned for all GWCs. This eliminates provisioning errors. When the call server is an XA-Core, the two available core IP addresses will be automatically distributed across the GWCs.

A00007113 -- GWC External interface robustness

Affecting	NA IAC	NA IAW	NA PT-IP	NA UA-IP	Intl IAC	Intl IAW	Intl PT-IP	Intl UA-IP

This feature is aimed at enhancing error reporting of external communication paths from the Gateway Controllers (GWCs) and External hosts such as gateways, peer GWCs and USP. New alarms are added to report communication path lost and new Operational Measurements (OMs) are collected by Integrated EMS every 5 minutes.

The customer will use the existing SESM alarm manager for the new alarms. Integrated EMS will be configured to receive the new OMs every 5 minutes. Only the Active GWC will report the OMs, while the inactive will report no OMs found in table.

A00007135 -- GWC DPT audits and counter drift prevention

Affecting	NA IAW	NA PT-IP	NA UA-IP	Intl IAW	Intl PT-IP	Intl UA-IP

This feature addresses two areas of weakness in the existing DPT application:

- Counter drift.
- Trunk OM anomalies

A00007300 -- Enable by default IPSec on all GWC profiles

Feature Description

Affecting NA PT-IP NA UA-IP

This (I)SN08 activity enables IPSec on all GWC profiles that do not currently have the IPSec capability. As a result of enabling IPSec on all remaining GWC profiles, the IPSec provisioning tab will now be available in the CS 2000 Management Tools GUI for all GWC profiles.

Session Server features

A00006893 - TLS Security on Session Server

Affecting NA
UA-IP

This feature ensures that TLS version 1.0 (RFC 2246) is utilized for secure SIP message communication for inter-call server communication. With support of TLS by the Session Server, connections to a SIP-enabled server can be secured over a non-secure network.

A00008349 - Session Server: Provide Support for the SCTP Protocol IN 2.4.22 Kernel

Affecting NA
UA-IP

This activity provides support for the Stream Control Transmission Protocol (SCTP) in the IN 2.4.22 kernel

Multiple Session Server nodes per CS 2000

Affecting NA IAC NA IAW NA PT-IP

Currently in (I)SN08, each CS 2000 can support a pair of Session Servers running the SIP Trunking application and another pair of Session Servers running the SPC application.With this feature, a single CS 2000 will be able to support up to a maximum of 3 pairs of Session Servers running SIP Trunking applications in addition to a pair of Session Servers running SPC.

The current capacity of each pair of SIP Trunking Session Servers is as follows:

- 900K BHHCA SIP and SIP-T over UDP
- 500K BHHCA SIP over TCP
- Total ports supported at 40K-50K ports depending on traffic

With this feature, the total SIP/SIP-T capacity of each CS 2000 will be 3 times the above capacity numbers.

Session Server mount in Call Control Frame

Affecting NA IAC NA IAW NA PT-IP NA UA-IP

When the Session Server was introduced in SN07, the pair of SAM-XTS (HW platform of the Session Server) can only be mounted on the SAMF frame. This is not an issue with CS 2000 because there will always be a SAMF frame. However, for a small CS 2000-Compact installation, there may not be a SAMF frame. In this case, when the Session Server is introduced, a new SAMF frame will have to be added just to house the new pair of SAM-XTS.

This feature will allow mounting of the pair of SAM-XTS on the CCF frame.

Feature Description

Universal Signaling Point features

A00007359 -- USP log delivery stream to Integrated EMS

Affecting	NA IAC	NA IAW	NA PT-IP	NA UA-IP	Intl IAC	Intl IAW	Intl PT-IP

Currently, the USP only sends Alarms via the SNMP interface (integrated into Integrated EMS, Micromuse and some customer OSS's). This feature enhances the functionality of USP by supporting the delivery of security and audit logs to the Integrated EMS syslog server or any other application. USP log data is sent to Integrated EMS in unformatted manner using syslog.

A00007368 -- 16 simultaneous GUI sessions

Affecting	NA IAC	NA IAW	PT-AAL1	UA-AAL1	NA PT-AAL2	NA PT-IP	NA UA-IP

The Universal Signaling Point (USP) is centrally managed through a workstation, either a Windows 2000 PC or a SUN Solaris platform that provides a Graphical User Interface (GUI) for Operations Administration Maintenance & Provisioning (OAM&P).

This feature increases the number of simultaneous GUI sessions on a USP system to sixteen. Each GUI session is two CLI connections, one each to the two Real Time Controller (RTC) cards of a USP system.

At any given instance, the total number of connections to an RTC, GUI sessions and CLI connections together, cannot exceed sixteen. The user-session form on the GUI displays the number of GUI sessions established and their details.

IW-SPM features

A00004741 -- Enabling TRKGRP OMs on GEM and support nodal OMs

Affecting	NA PT-IP	NA UA-IP

This feature provides Nodal Based Operational Measurements for MG 4000-IP and IW-IP nodes. These nodal statistics are necessary for Link Bandwidth Engineering and to determine the network usage and transmission errors. The Nodal Based Operational Measurements includes the statistics for Gigabit Ethernet Link usage Bearer traffic injected in to the network.

A00007121 -- IW Bridge MAP maintenance for deload

Affecting	PT-AAL1	UA-AAL1	NA PT-IP	NA UA-IP

This feature introduces the BRGmtce MAP level to manage the state of the IW-SPM bridge terminals. It also introduces the deload status for bridge terminals.

Media Gateway 15000 features

Hi/Lo Continuity test tones

Affecting	NA PT-AAL1	NA UA-AAL1	NA UA-IP

Feature Description

The Media Gateway 15000 is deployed in solutions that require connection to the public network through RBOCs that deploy legacy equipment such as 1A ESS. RBOCs will not provide/change switch configuration for competitors such as Cable Multiservice operators. For example the 1A switches do not flexibly support continuity test tone signals and are currently incompatible with Media Gateway 15000. Continuity tones are used to confirm media path integrity before presenting a call.

The Media Gateway 15000 is required on the TDM interface to detect a high tone and respond with a low tone or vice versa. Currently Media Gateway 15000 detects high and transmit a hi tone. This feature implements the termination of COT tones of the Media Gateway 15000 by detecting high (2010 Hz) tones and send low (1780 Hz) tones while an incoming ton is present. This feature is only applicable on the VSP3-o using the H.248 media gateway control protocol. It is provisionable on a DS-1 basis.

Recurring fan alarm state preserved over CP SWACT

Affecting	NA PT-AAL1	NA UA-AAL1	NA UA-IP

[Description to be completed]

T&C for patch automation for non-disruptive patches

Affecting	NA PT-AAL1	NA UA-AAL1	NA UA-IP

[Description to be completed]

Succession IP Software Migration (SISM)

Affecting	NA UA-IP

A software migration on Multiservice Switch 15000 and Media Gateway 15000 nodes can be performed using the command console or the MDM GUI tool called Succession IP Software Migration (SISM) tool. SISM automates the HSM process. Using the SISM tool reduces the chance of errors and increases the speed and efficiency of the software migration.

Autopatching of Multiservice Switch 15000 and Media Gateway 15000

Affecting	All

The auto-patching of Multiservice Switch 15000/Media Gateway 15000 nodes feature allows the system to download and apply eligible non-disruptive patches from your MDM Software Delivery Server (SDS) to each of your switches, automatically. The eligible patches are downloaded and applied to the Software patchList using a script that is triggered to run at a scheduled time from the MDM Server. Only non-disruptive patches are eligible for auto-patching.

IP Security (IPSec) for Media Gateway 15000 control connection traffic

Affecting	NA PT-IP	NA UA-IP

Feature Description

This feature enables IP Security (IPSec) protocols to be used to secure the H.248 call control connection between the Communication Server 2000 (CS 2000) and the Media Gateway 15000 using VSP3-o FPs.

Media Gateway 9000 features

A00006865 -- HAL for GigE interface

Affecting	UA-AAL1	UA-IP	Intl UA-IP

A new Supercore card with 4 Gigabit Ethernet ports (SCG - Supercore Gigabit Ethernet, PEC code NTNY4540 / NTNY45FA) will be introduced in (I)SN08.This feature will implement the necessary device drivers (MAC drivers, GigE HAL, etc) and mesh design (network processor, switch fabric, host side code, etc) to support Gigabit Ethernet.

A00006894 -- Internodal Emergency StandAlone for MG 9000

Affecting	UA-AAL1	UA-IP	Intl UA-IP

This feature provides the ability to make calls while in ESA between MG 9000 nodes. In doing so, the Telco’s will also be provided the ability to provision a “Community of Interest” (COI) which defines which MG 9000 nodes can make ESA calls between one another. Calls can not be made between the two communities, only within a given community. If an MG 9000 does not have access to a LAN Switch, it will operate in the pre-SN08 manner of routing calls between VMGs within a single MG 9000 node. Also, although a Community of Interest is defined, each node must be in ESA for it to participate in the community. Nodes are not forced to enter ESA.

A00006906 -- (I)SN08 Clock synchronization enhancements

Affecting	UA-AAL1	UA-IP	Intl UA-IP

This Feature covers the software development on the MG 9000 node and specifically on the DCC and ITP cards. The clock sync code on the DCC is used to recover a synchronization signal from a Building Integrated Timing Source (aka. BITS, BITS is North American usage) or a Synchronization Supply Unit (aka SSU, International usage) signal. This signal is forwarded to the MG 9000 ITP card which uses the signal to synchronize the MG 9000 node. Prior to (I)SN08, the MG 9000 only supports the North American standard timing reference (BITS). This system uses DS-1 interfaces which are incompatible with the international standard 2048kHz interface. Lack of 2048kHz interfaces complicates the introduction of MG 9000 into international markets. This feature introduces the capability for the NY45FA GiGE DCC circuit pack to connect to an International standard Synchronization Supply Unit (SSU) using 2048kHz interfaces. The NY45FA can use an SSU or BITS signal as a timing reference

A00007053 -- MG 9000 Patch speed-up

Affecting	UA-AAL1	UA-IP

The purpose of this feature is to significantly reduce the amount of time it takes to patch an MG 9000 ITP device. The goal is to reduce patching activity to less than 30 seconds. Since most of the time spent patching takes place within the LPM, this feature’s primary focus involves improving the LPM’s performance.

Feature Description

A00007074 - GigE Link Maintenance

Affecting	NA UA-IP

This feature introduces the Gigabit link maintenance subsystem for the new Gigabit Ethernet (GigE) cards supported on the MG 9000. The link maintenance subsystem includes the ability to provision, performance monitor, recovery and upgrade the GigE.

A00007107 -- MG 9000 5/30 minute Operational Measurements

Affecting	NA UA-AAL1	NA UA-IP	Intl UA-IP

The OM collector currently collects OM's from different tables on a fixed 15 minute schedule. The MG 9000 stores the previous 96 15 minute interval data so it covers 24 hours of information. This feature changes the timing of these intervals to be configurable from the EM. The user can select any number of minutes as the standard interval. Also, the MG 9000 will be changed to store only 48 of blocks of interval data for non RFC-driven MIB tables.

RFC-compliant tables will continue to have 96 blocks of intervals stored. The feature also provides for a second or extended OM interval. This extended interval is longer than the standard interval and is a time that is a multiple of the time in a standard interval. The data in the extended interval is computed based on the data for the appropriate number of standard intervals.

A00007108 -- MG 9000 support for large Session Descriptor Protocols

Affecting	NA UA-AAL1	NA UA-IP	Intl UA-IP

The purpose of this (I)SN08 activity is to provide some means of recovering memory and real-time on both the ITP and ABI cards. By doing so, the life expectancy of the older ITP and ABI boards can be extended. This provides our current customers with some added benefits and delays their need to upgrade to the newer boards that were introduced in SN07.

In addition, this feature is tasked with being able to provide support for longer SDP strings. This change will lay the foundation needed to support MCS and SIP interworking with MG 9000 lines. With the introduction of T.38 looming on the horizon, the need to support longer SDP strings is a must. This feature will increase the size to allow for SDP strings up to 1000 bytes in length.

Note: SDP strings in excess of 1000 bytes will result in an error code being returned to the GWC.

A00007115 -- MG 9000 In-service fault detection

Affecting	NA UA-AAL1	NA UA-IP

This activity improves fault detection and recovery of MG 9000 ITP DSPs (Digital Signal Processors). This activity raises 2 alarms under new conditions.

A00007116 -- MG 9000 Oscillation Phenomena Signal detection

Feature Description

Affecting	NA UA-AAL1	NA UA-IP

The Office Oscillation Phenomena Signal refers to the oscillation on the Talk Battery feeds in the Central Office. This oscillation occurs when there is to much current draw on the Talk Battery feeds.The new NTNY42BA Metallic Test Access (MTA) card will be used to detect the OOPS. The NTNY42BA has two new Analog to Digital Converters that are dedicated to Talk Battery A and B. It also has parity protection for the processor's external SDRAM.

There are version bits for distinguishing the BA from the AA version of the MTA card.The MG-MTA consists of a Motorola Power PC MPC855T processor and memory, one RS232 ports (Test Head interface), a serial port, a Field Programmable Gate Array (FPGA) block, a P Phone Power Circuit, Relay Drivers, Relay Matrix, Line Card Diagnostic Termination, Test Response Circuit Termination, Analog to Digital Converter block for the Test Response Circuit, Metallic Access Jacks, and Analog to Digital Converter block for the Talk Battery Feeds.

A00007263 - LCI for GigE

Affecting	NA UA-IP

This feature provides the necessary changes to the Local Craft Interface (LCI) to support the new Gigabit Ethernet (GigE) network interface for the MG 9000.

A00007749 - MG 9000 ABI Support for LGCO, LGCOI

Affecting	NA UA-IP

This activity provides the customer with the ability to host LGCO and LGCOi peripherals off the ABI DS-512 interface on the MG 9000 gateway. Hosting this type of peripheral is required for some customers in the International market. The activity also adds support for hosting of a Remote Maintenance Module (RMM) directly on a PLGC host peripheral.

A00008387 -- GLC-32 AB card support

Affecting	NA UA-AAL1	NA UA-IP

This feature introduces the NTNY53AB Global Line Card, a cost reduced version of the NTNY53AA. This cost reduced version uses a more cost effective LCAS part, a no-SLIC Hybrid, and a more cost effective, more efficient Vinetic Chipset. While the new LCAS and Hybrid are not expected to require any new support, the new Vinetic Chipset (4M part) will require a different loading procedure and electrical characteristics while maintain the existing functionality of its predecessor.

Packet Media Anchor features

A00007120 -- Packet Media Anchor introduction

Affecting	NA IAC	NA IAW	NA UA-IP	Intl IAC	Intl IAW	Intl PT-AAL2	Intl PT-IP	Intl UA-IP

Feature Description

This feature introduces the Packet Media Anchor for the Dynamic Packet Trunking SIP/SIPt application. The role of the Media Anchor is to provide tone, digit collection and bearer path anchoring capabilities for SIP/SIPt call types. The Audiocodes 2010/2020 has been chosen as the packet gateway to supply media anchoring functionality. The Packet Media Anchor solution uses the bearer channel tandeming (BCT) capability of the AMS to provide media stream anchoring functionality. The media anchor is directed by the CS 2000, which is responsible for managing call topology, resource allocation/deallocation and resource usage. Media anchoring through the AMS does not require conversion from packet to TDM back to packet again, thus impact on bearer path latency will be minimal.

Integrated Element Management System features

A00007024 -- Core Element Manager Patching

Affecting	NA IAC	UA-AAL1	NA UA-IP	NA PT-IP

In (I)SN08, the CEM will be integrated with the Integrated Element Management System (Integrated EMS) on Solaris. Integrated EMS is patched via the Network Patch Manager (NPM). It is required that one patch management system be used with all applications on the same node, therefore the CEM integrated with Integrated EMS will also be patched by the NPM.

A00007302 -- (I)SN08 Integrated EMS-CEM integration

Affecting	UA-AAL1	NA UA-IP

This feature integrates the functionality of CEM (Core Element Manager) to the Integrated EMS (Integrated Element Management System). This includes the Resource Discovery (RD), Fault Management (FM) and Performance Management (PM) support for the core (call server). The Core Element Manager system is the Nortel implementation of a Element Management System which provides the following:

- An interconnection between the specific management applications that are on workstations and operated by systems personnel, over a Local Area Network/Wide Area Network (LAN/WAN) using Transmission Control Protocol/Internet Protocol (TCP/IP).
- An exchange of management information (data) between the management applications and the various elements of the Core Network elements. In the Circuit Core Network, the management application is the Core Element Manager, installed on a PC or Sun platform.
- Mediation functionality (data accumulation, filtering, manipulation, and transfer) between the network elements and the Core Element Manager workstation.

A00007304 - CEM I&C On Integrated EMS

Affecting	NA UA-IP	NA UA-AAL1

Feature Description

The CEM server functionality will be provided in conjunction with the Integrated EMS server. CEM will be installed as an overlay on Integrated EMS and SSPFS.

The CEM server is an element manager for the DMS node. It provides powerful fault, performance and configuration management toolsets. This server works in conjunction with the CEM browser which will be integrated into the Integrated EMS product.

This feature covers the installation of the CEM server onto the Integrated EMS server. This feature also covers the installation of the CEM components on the SDM and CBM. This feature will also incorporate the Synchronized Backup Manager to be used by CEM

A00007341 - MS 2000 IEMS Configuration Integration

Affecting NA
UA-IP

This feature provides the Integrated Element Management Server (IEMS) with the ability to provision both the MS 2010 and MS 2020 media servers using the standard IEMS GUI. The existing command line interface to configure the MS 2000 is now discontinued in the SESM software.

A00007344 - Integrated EMS Southbound Event Throttling

Affecting NA
UA-IP

This activity provides improved robustness on the IEMS to prevent event storms from causing the IEMS to crash.

A00007347 - Integrated EMS - CEM Integration into Integrated EMS

Affecting NA
UA-IP

This activity merges the CEM and IEMS loads into a single load and provides additional interfaces on the IEMS.

A00007388 - Integrated EMS Performance Phase 2

Affecting NA
UA-IP

[Information not yet available]

A00007404 -- Integrated EMS Security Serialized Patching

Affecting NA UA-IP

This feature ensures that only one Integrated EMS security module component is restarted at a time with respect to patching. Specifically if a request is initiated from the NPM GUI, CLUI, or scheduler to restart all Integrated EMS security module components, separate requests will be queued and executed serially.

To ensure the NPM server serializes Integrated EMS security module restart requests for patching, a new platform type is implemented by this feature. The new platform type value is ‘SCTY’ and can be queried as part of report generation from the NPM GUI or CLUI.

Feature Description

A00008058 - Integrated EMS Migration of SN07.1 content to (I)SN08

Affecting	NA UA-IP

This activity ensures that the migration of SN07.1 content is correctly managed in the (I)SN08 Integrated EMS.

CS 2000 Core Manager/Core and Billing Manager features

A00008311 -- Password synchronization between HA nodes

Affecting	NA IAC	Intl IAC	Intl IAW	NA PT-IP	NA UA-IP

The initial architecture of the Core and Billing Manager (CBM) high availability model CBM850 was that the two servers that make up the high availability (HA) configuration require separate password changes. This limitation resulted in the inconvenience of having to change passwords twice and the possibility of error by entering un-matched passwords.

This feature addresses this limitation by introducing a capability where a single password change will be propagated from one CBM server to its mated CBM server automatically.

Media Gateway 9000 Manager features

A00006905 -- MG 9000 Manager recovery improvements

Affecting	UA-AAL1	UA-IP

The recovery time for the MG 9000 Manager at the 110,000 native SLoA line capacity is 25 minutes. Considering outage risks for our customers, there is a strong business need to limit downtime that may occur from an unplanned OAM&P outage. To this end, this feature will lower the MG 9000 Manager recovery to less than 15 minutes.

A00006944 - MG 9000 Manager - Subnet, Log adapter and EM Factory Collapse

Affecting	NA UA-IP	NA UA-AAL1

This feature has two functions, to:

- integrate the MG 9000 Subnet Manager server process into the MG 9000 Manager Factory process
- integrate the MG 9000 Manager Logs Adaptor into the frameworks of all other MG 9000 Manager processes, hence removing the need for a separate Logs Adaptor process.

A00006957 - MG 9000 Manager - Deserialize Patching

Affecting	NA UA-AAL1	intl UA-IP

[Information not yet available]

A00007000 -- MG 9000 GigE Network Interface support from MG 9000 Manager

Affecting	UA-AAL1	UA-IP

Feature Description

A new SuperCore card is being introduced in (I)SN08 release to support GigE configuration for IP connectivity to a router. Compared to the current ATM-based IP Network Interface, GigE Network Interface is more efficient as it eliminates the ATM and IP overhead associated with IPoAAL5. It has greater capacity of 1 Gb and is more cost effective.Although the new SuperCore card will support 4 GigE ports, only 1 port can be connected to the router.With the GigE Network Interface, MG 9000 can be used as a real VoIP gateway.

With this EM feature, the user will be able to view the GigE carrier configuration details from the Element Manager but the user will not be able to provision the carrier from the Element Manager. All the GigE alarms and performance parameters will be displayed to the user.The user will also be able to provision clock sync data and view the APS data for GigE port.

A00007213 -- MG 9000 Manager 5/30 minute Operational Measurements

Affecting	UA-AAL1	UA-IP

This feature modifies the MG 9000 Manager to support 5/30 minute Operational Measurements. These changes include the following:

- Adds a new configuration GUI
- Modifies the behavior of the OM Collector whenever collection intervals change
- Implements changes in the Performance browser
- Adds new tags for OM Collector-generated CSV filenames
- Integrates the configuration and starting/stopping of the OM Collector and the MG 9000 Manager server

A00007415 -- Internodal ESA for the MG 9000 Manager

Affecting	UA-AAL1	UA-IP

Internodal ESA will provide the ability to make calls while in ESA between MG 9000 nodes. In doing so, the Telco's will also be provided the ability to provision a "Community of Interest" which defines which MG 9000 nodes can make ESA calls between one another. A community must have access to a LAN Switch (i.e. Media Gateway or Multiservice Switch 15000 or equivalent) in order for Inter Nodal ESA calls to complete.

If an MG 9000 does not have access to a LAN Switch, it will operate in the pre-SN08 manner of routing calls between VMGs within a single MG 9000 node. Also, although a Community of Interest is defined, each node must be in ESA for it to participate in the community. Nodes are not forced to enter ESA.

The current implementation of ESA only allows calls between Virtual Media Gateways (VMG) within the same MG 9000 node. This feature will expand ESA's ability to make calls between a limited number of MG 9000 nodes termed a "Community of Interest". However, as with previous ESA releases, calls can only be made between VMGs that are in ESA.

Multiservice Data Manager features

Administration of MDM user privileges (Operator Client)

Affecting	NA PT-AAL1	NA UA-AAL1	NA UA-IP

[Description to be completed]

Feature Description

MDM Configuration Audit - Phase 1

Affecting NA PT-AAL1 NA UA-AAL1 NA UA-IP

[Description to be completed]

Audit logs real-time to the audit log syslog interface

Affecting NA PT-AAL1 NA UA-AAL1 NA UA-IP

[Description to be completed]

Solaris 9 Upgrade for MDM workstations

Affecting All

Solaris version 9 is the current operating system shipped on the Sun platform. MDMs in Carrier VoIP networks must be upgraded to Solaris 9 on all MDM workstations in all Carrier VoIP Solutions. Both Carrier VoIP releases targeted for upgrade in (I)SN08 (SN06 and SN07) are currently running Solaris 8. You will use Live Upgrade to upgrade to Solaris 9 from Solaris 6, 7, or 8.

MDM Operator Client

Affecting All

The Operator Client application permits the controlled access of the operator to the Operator Client tools that have been configured for the user from the MDM Toolset. The Operator Client desktop runs on either a Solaris workstation or on a PC that runs Windows 2000 or XP. With central AAA and the Operator Client application, access to Multiservice Data Manager (MDM) surveillance and configuration tools, and to the capabilities within these tools, is restricted. The tools are downloaded to the operator's desktop and run locally, thus off-loading the MDM server. The MDM Admin Server for VoA networks provides the point of user access administration and the Integrated EMS provides the point of user access administration for VoIP networks. This feature is optional for VoA networks but required for VoIP networks.

Security Audit Logs

Affecting NA PT-IP NA UA-IP

Feature Description

Security audit logs are generated by MDM applications and Multiservice Switch 15000/Media Gateway 15000 nodes to help monitor and audit configuration changes to the network elements and detect security issues such as unauthorized node access or configuration changes.

The Multiservice Data Manager Security Audit Log Collector (SALC) server provides real-time collection of security audit logs from Multiservice Switch 15000/Media Gateway 15000 nodes and the MDM workstation. This is done for local storage and for forwarding to another management system through UNIX's standard syslog process or through Nortel's internal custlog format. Multiple SALC servers can be run on an MDM workstation to handle security audit log feeds from different Multiservice Switch 15000/Media Gateway 15000 groups. An Multiservice Switch 15000/Media Gateway 15000 node can send security audit log feeds to multiple MDM workstations in real-time.

The security audit logs can be converted into custlog V2 format for delivery to a higher level element manager such as CS2000 Core Manager or Integrated EMS (that has been upgraded to (I)SN08) where they can be integrated into the SCC2 feed to the OSS. The security audit logs can also be written to a file on the MDM workstation for access by the Log Browser tool.

Central authentication, authorization, and accounting (AAA) through Integrated EMS

Affecting	NA PT-IP	NA UA-IP

Integrated EMS central AAA provides management of the Multiservice Switch 15000/Media Gateway 15000 and MDM users in a central office through a unified interface. Integrated EMS maintains a central repository of user information, and handles validation of userids and passwords (authentication), assignment of MDM and Multiservice Switch 15000/Media Gateway 15000 user access privileges through the use of groups and scopes to validated users (authorization), and general administration of userids, passwords, groups and scopes. Managing user access privileges is simplified by mapping job functions and access privileges onto groups and then associating userids to those groups. On the MDM workstation, PAM_RADIUS and PAM_NSSwitch interfaces are used to exchange login requests and access privilege information with the Integrated EMS. On Multiservice Switch 15000/Media Gateway nodes, a RADIUS interface is used for this purpose.

This feature is required for VoIP networks and is installed when the Operator Client feature is installed by selecting the JWS option and not selecting the Security package option.

Communications security

Affecting	NA PT-IP	NA UA-IP

The Secure Shell (SSH) protocol is used to authenticate and encrypt management data transmitted between MDM workstations and the Integrated EMS, and between remote operator desktops running the MDM Toolset and MDM workstations. The SSH software is installed on the MDM workstation as part of the Solaris 9 upgrade.

IP Security (IPSec) protocols are used to authenticate and encrypt management data transmitted between MDM workstations, and between an MDM workstation and an Multiservice Switch 15000/Media Gateway 15000 node. IPSec software for the MDM workstation is installed as part of the Solaris 9 upgrade. IPSec encryption software for the MDM workstation must be installed separately. IPSec software for the Multiservice Switch 15000/Media Gateway 15000 is included in the (I)SN08 software installation.

Feature Description
MDM and Multiservice Switch 15000/Media Gateway 15000 platform security **Affecting** NA PT-IP NA UA-IP Platform security procedures improve the resistance of the MDM and Multiservice Switch 15000/Media Gateway 15000 operating systems and MDM applications to unauthorized access through the IP network. This includes the following • removing unused userids and system functions • enforcing timeouts of idle user sessions • restricting access to functions providing IP address information • restricting the remote users that can access the workstation or node • enforcing good password policies
Centrex IP Client Manager features

What's new in CS 2000 management tools

CS 2000 Management Tools

The CS 2000 Management Tools offers the following new features and functionality in (I)SN08:

- The CS2M software package includes backup manager software The backup manager software allows a backup initiated from the Integrated Element Management System (EMS), to occur on the CS 2000 Management Tools server.
- The user has the option to turn OSSgate password control on or off. When the option is turned on, the password is not echoed on the screen when the user logs in.
- The NTsam21em and NTsesm software included in the CS2M software package, each include an upgrade tool that provides upgrade functionality for the SAM21 Shelf Controller and the Gateway Controller (GWC) respectively.
- The CS 2000 GWC Manager GUI has been modified as follows:
    - A new "Session Policy Controller" tab has been added to allow provisioning of a Session Policy Controller (SPC), which provides call admission control capabilities, and enable or disable Virtual Connection Admission Control (VCAC) .
    - A new "ALGs" tab has been added to allow provisioning of an Application Layer Gateway (ALG) device, which provides NAT-type functionality in a PacketCable network.
    - The "IP-VPNs (virtual NATs)" and "Limited B/W Links (LBL)" tabs have been moved under a new a tab called "Network Zones",

which allows provisioning of Network Address Translation (NAT) devices and Limited Bandwidth Link (LBL) devices.

— The call agent IP address is automatically distributed to all gateway controllers, and is displayed in the lower right-hand corner of the Network Configuration window of the GWC Manager GUI. A new log, CMT30x is introduced to indicate when there is no available call agent IP address. With auto-provisioning of the call agent IP address, the Message Router IP address has been eliminated from all applicable GUI windows.

- The CS 2000 SAM21 Manager GUI is modified to include support of the new MCPN905 card.

Succession Server Platform Foundation Software

The Succession Server Platform Foundation Software (SSPFS) offers the following new features and functionality in SN08:

- The command line interface (CLI) is modified to add a menu option under the Login Session menu to configure a limit on login retries .
- Local user account information is automatically propagated from the Active to the Inactive unit in a cluster (server pair). Therefore, the administrator needs only to create, delete, or modify a local user account on the Active unit, and the action will automatically propagate to the Inactive unit.
- Upgrading the SSPFS requires three disks. In a two-server configuration, the user has the option to accept the upgrade environment or rollback to the previous upgrade environment after having upgraded one unit in the cluster.
- The CM CLLI is automatically retrieved from the Communication Server 2000 (CS 2000) through the SDM IP address.

Network Patch Manager

The Network Patch Manager (NPM) offers the following new features and functionality in SN08:

- Information for system and user-defined tasks, sets, alarms, plans, and reports is retained in the NPM database over an upgrade from SN08 onward.
- PFRS configuration is done from the NPM GUI and CLUI and no longer from the SSPFS CLI tool.
- Two system-defined tasks have been added: PFRSGENREPORT, which generates a report specifying the patch and load content for each device in the site, and PFRSGETPATCH, which detects newly available patch files and transfers those patch files to the NPM database. Both tasks can be run on demand through the NPM GUI or CLUI, or can be scheduled to run through a user-defined plan or the system plan.

- A new option is introduced to delete patches from the drop box following the execution of the PFRSGETPATCH task, which transfers the patches to the NPM database. This new option is available under the Preferences window in the new Patch File Retrieval Preferences tab of the NPM GUI.
- A new system-defined task has been added: DELETREPORTS, which deletes reports that have been created and left in the "/data/npm/reports" directory.
- The audit of MG 9000 and GWC devices is now run immediately after reload as opposed to 20 minutes after reload.
- The NPM GUI has been modified as follows:
  - — A new View button is provided in the Task List, Report List, Alarm List and Plan List to view system-defined information, which can no longer be modified.
  - — A new refine button is provided in the Maintenance Task window to quickly determine which patch(es) are applicable to which device(s) and vice versa.
  - — The CM CLLI is now present at the top of each NPM GUI window.
  - — The progress of patching requests is now provided in the lower right-hand corner of the main NPM GUI window.
  - — The NPM now retains any previously entered criteria in applicable windows and dialog boxes.
  - — A new field, Type, is added in task, alarm, plan, sets, and reports list windows, that indicate whether the data is system or user-defined.
- The NPM supports patching activities on two Integrated EMS security components, IEMSCSS and IEMSCSS_DS. The Integrated EMS security component was split into two components in SN08 to allow for continued service of the Integrated EMS security component in a cluster (two-server) configuration during patching activities.
- The NPM supports patching activities on the Core Element Manager (CEM).

Solution overview

This chapter provides an overview of the UA-IP Solution. The chapter contains the following sections:

Solution overview

The Universal Access - IP Solution (UA-IP) provides voice telephony and data services over Internet Protocol (IP) packet networks built around the Communication Server 2000 (CS 2000). It delivers the traditional voice service suite on a converged packetized IP network, enabling carriers to offer inter-office trunking, long-distance, tandem and gateway functionality, plus emerging IP services. In addition, this solution also provides analog lines access in a CVoIP networking using the MG 9000 Lines Gateway.

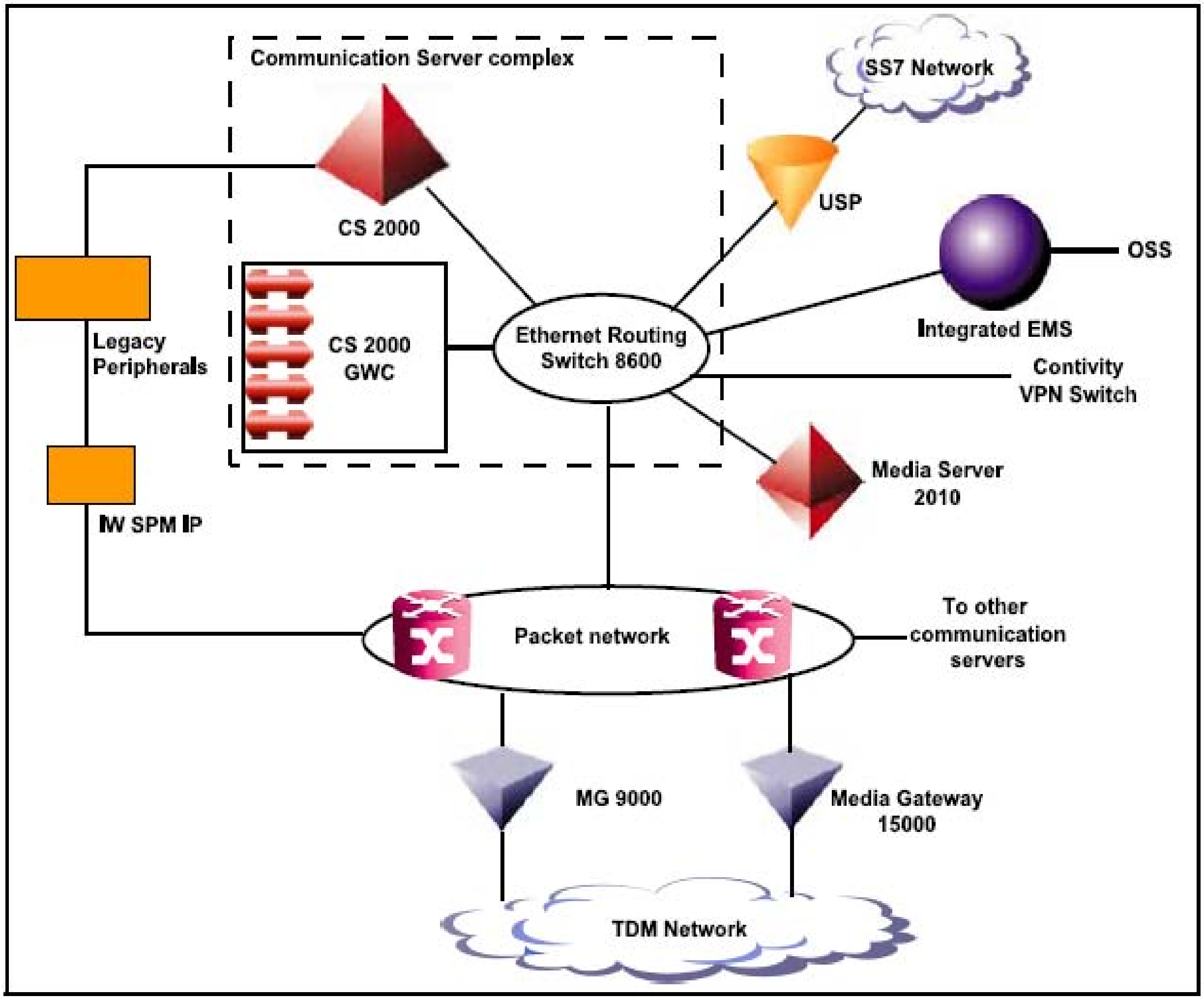
UA-IP supports the following time division multiplex (TDM) services:

- Line services
  - Plain old telephone services (POTS)
  - Digital Subscriber Line (DSL)
  - P-phone
  - Coin
  - Centrex
- 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 CVoIP Network nodes over an IP packet network.

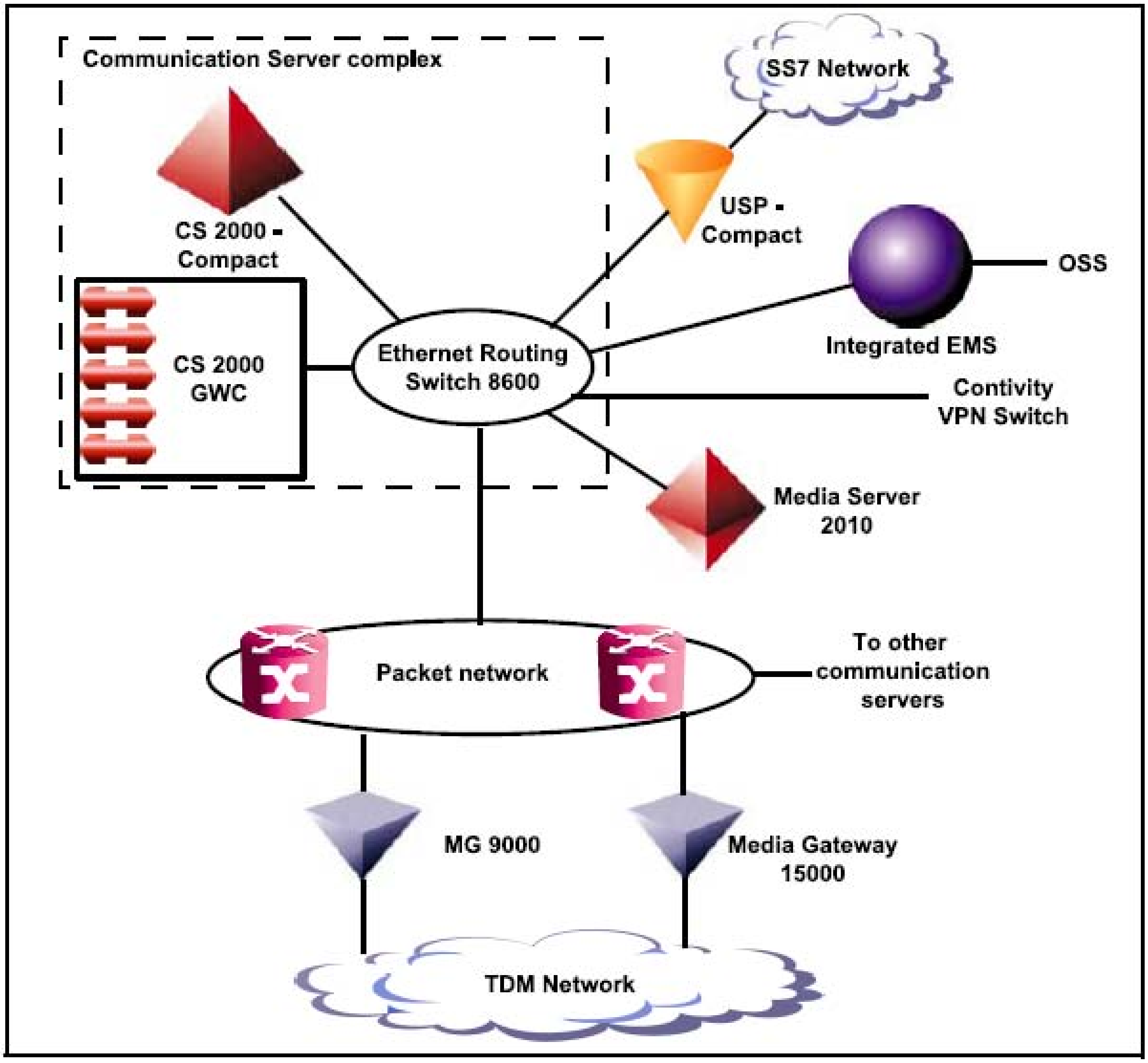
The figure below illustrates the UA-IP solution.

UA-IP solution architecture



The figure below illustrates the UA-IP-Compact solution.

UA-IP-Compact solution architecture



The role of each component in the UA-IP solution

The following table lists the components that make up the UA-IP solution 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 and CS 2000-Compact	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 and CS 2000-Compact	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, packetable DQoS COPS, and IPSec. 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 and CS 2000-Compact	Session Server 	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. The Session Server is the platform for the following applications: • SIP gateway application • Session Policy Controller
	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 and CS 2000-Compact	Media Server 2010 MS 2000 Series	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 • provides an important role in Nortel’s Lawful Interception facility

Components and their function (Sheet 6 of 22)

Components	Sub-component	Function
CS 2000 and CS 2000-Compact	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.
CS 2000 and CS 2000-Compact	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 and CS 2000-Compact	Universal Signaling Point (USP) and USP Compact USP	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 and CS 2000 Compact	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 Ethernet Routing Switch 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 IP solutions 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
Media Gateway 15000 		Media Gateway 15000 serves as a media gateway in the CVoIP Network. It supports the ASPEN2.1 and H.248 protocols for communication between the GWCs and Media Gateways. The Media Gateways 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 11 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

Components and their function (Sheet 12 of 22)

Components	Sub-component	Function
DPT Media Anchor		SN08 introduces the DPT Media Anchor as a replacement for the Anchor Packet Gateway (APG). SN08 does not support earlier versions of the APG that resided on the VSP card of the Media Gateway 7400/15000.The DPT Media Anchor resides on the Audiocodes Media Server and provides similar functionality as the APG. In addition, the DPT Media Anchor offers the following enhancements: • improved resource usage monitoring and troubleshooting for network operators • possible co-residency with announcement and conferencing resources • direct packet-to-packet forward capabilities, reducing speech path delay through the DPT Media Anchor to almost zero.
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. All cross-network OAM interfaces to and from the MG 9000 are secured with IPSec or SFTP. In addition, (I)SN08 extends the MG 9000's emergency stand-alone (ESA) reach to other MG 9000 nodes in a community of interest.

Components and their function (Sheet 13 of 22)

Components	Sub-component	Function
		The Keymile UMUX 1500 line gateway supports POTS and ADSL broadband data access to a backbone packet network for up to 300 users. Packet network connections are supported via STM-1 carriers (for IP/AAL5/ATM) or 10/100 BaseT Ethernet. Control connections between the UMUX 1500 and the CS 2000 GWC are based on H.248 signaling. The UMUX 1500 supports the following services: • traditional telephony • broadband Internet access: — optical Ethernet — ADSL — ADSL2+ — G.SHDSL • private circuits • next-generation services — Ethernet private lines — VoIP ***Note:*** The Keymile UMUX 1500 is only used in the International solutions.

Components and their function (Sheet 14 of 22)

Components	Sub-component	Function
Network management		
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, 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 • 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 CVoIP 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.
Integrated EMS	Multiservice Data Manager (MDM)	MDM allows you to manage Media Gateway 15000/7400. MDM allows you to perform fault management, configuration management, data collection, performance management, and security management. In addition, MDM forwards Media Gateway 15000/7400 performance management, and fault management information to the CS 2000 Core Manager. MDM resides on a Sun-based workstation.

Components and their function (Sheet 19 of 22)

Components	Sub-component	Function
Integrated EMS	MG 9000 Manager	The Media Gateway 9000 Manager (MG 9000 Mgr) allows technicians to remotely manage all MG 9000 components in a CVoIP 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.
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.

Components and their function (Sheet 20 of 22)

Components	Sub-component	Function
Integrated EMS	Device Manager (for Ethernet Routing Switch 8600)	The Device Manager (for Ethernet Routing Switch 8600) is a suite of GUI applications that allows you to manage and configure a Ethernet Routing Switch 8600 chassis. It can be launched independently or as part of Optivity.
Optivity		Optivity is a network management application capable of managing multiple Ethernet Routing Switch 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 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		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.

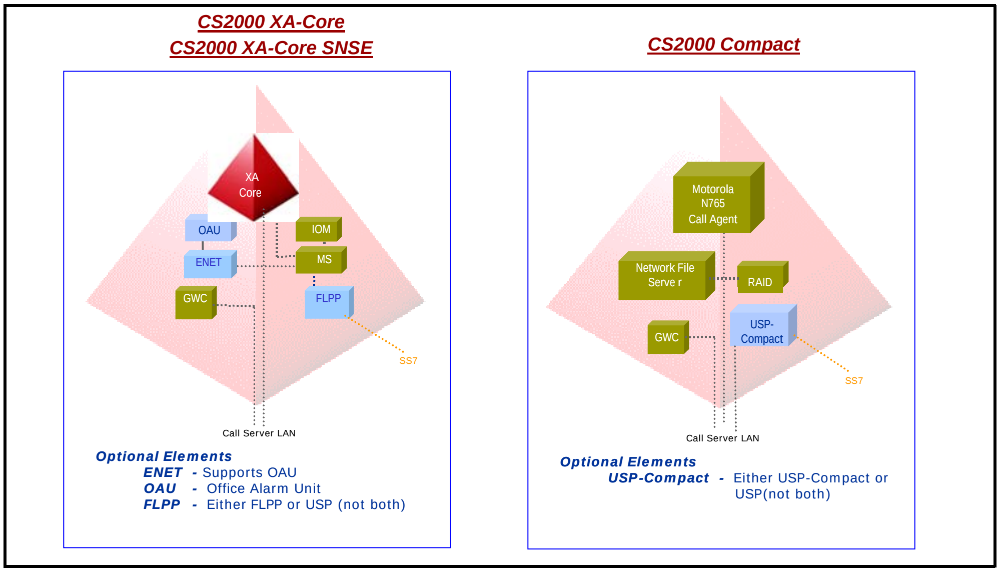
Components and their function (Sheet 22 of 22)

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. The 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

CS 2000 configurations

The UA-IP Solution offers two alternative CS 2000 components: the standard CS 2000, and the CS 2000-Compact - a small footprint softswitch for smaller communication server sites. The two CS 2000 configurations are functionally similar, but differ in the way they connect to the SS7 signaling network. Connection is via the FLPP or the USP for the standard CS 2000, and via the USP or the USP-Compact for the CS 2000-Compact. The figure CS 2000 configurations on page 47 shows the two CS 2000 configurations and their main subcomponents.

CS 2000 configurations



Hybrid configuration

A hybrid configuration comprises DMS-specific and CS 2000-specific hardware, as well as hardware that is common to both. Such a hybrid configuration can support circuit-based and packet-based capabilities simultaneously. For communication between the circuit and packet environments, the hybrid configuration uses one of the following:

- looparound trunks
- interworking Spectrum peripheral module (IW SPM)

Introduction

(I)SN software supports both conventional circuit-based switching capabilities and next-generation packet-based switching capabilities. Circuit-based capabilities are supported using the DMS legacy hardware platform. Packet-based capabilities are supported using the CS 2000 hardware platform. Some hardware is specific to DMS and some is specific to the CS 2000, but a number of major components are common to both. These common components include the XA-Core processor complex on which the (I)SN Product Computing-Module Load (PCL) is installed. It is this centrally loaded PCL that supports call processing agents, translations and routing, and service logic.

> ***Note 1:*** XA-Core is the only core that can be used to support hybrid CS 2000/DMS configurations. The older DMS-Core cannot be used with CS 2000 hardware. For the UA-IP solution, the CS 2000-Compact third-party core cannot be used with DMS hardware.
>
> ***Note 2:*** The hybrid solution supports all multi-market platform (MMP) hardware except JNET and BRISC.
>
> ***Note 3:*** The hybrid solution does not support the USP or USP-Compact.
>
> ***Note 4:*** In (I)SN07, the hybrid solution does not support mixed trunk subgroups (that is, trunk members on a legacy peripheral such as DTC or SPM in the same trunk subgroup as trunk members on a packet-based gateway such as PVG).

In a hybrid configuration, the XA-Core-based DMS switch runs an (I)SN07-based load. CVoIP network elements are added in-service. Alternatively, the CS 2000, which runs an (I)SN07 load, can have XPMs added to become a hybrid.

Solution description

A full hybrid CS 2000 solution implies full coexistence of TDM and packet switching, but also implies full interworking of TDM and packet networks through the use of an interworking peripheral/media gateway which can connect to both the ENET and the packet network.

‘Coexistence’ means a single CS 2000 which performs call processing with both TDM components (legacy XPMs) and packet components (gateway controllers (GWC) and media gateways). This does not imply interworking between the TDM and packet networks.

> ***Note:*** The implementation of coexistence does not introduce any new functionality to either side of the network. The existing range of legacy DMS XPMs and protocols is supported on the ENET side, and the existing range of CS 2000 gateways and protocols is supported on the packet side.

Looparound trunks

If no interworking gateway is available, the ENET cannot interwork with the packet bearer network. In such a configuration, the only way of connecting XPM-based calls and CVoIP media gateway calls is by using looparound trunks to provide a bearer path from ENET-based

XPMs and a CVoIP trunk gateway. From the CS 2000 perspective, an XPM-to-media gateway call is simply two separate TDM and packet-based calls.

Interworking SPM

The Spectrum peripheral module (SPM) is a peripheral which can connect to both the packet network and the ENET, thus providing a bearer path between CVoIP trunk gateways and ENET-based XPMs. The interworking SPM (IW SPM) is a version of the SPM with optical carrier connections that are used to support high-capacity links with the packet network rather than with circuit-based trunks.

The IW SPM provides GigE links with the packet network for packet-based connections, and DS512 links with the ENET for 64 Kb/s circuit-based connections. The IW SPM also supports interworking between the different connection types. In effect, the IW SPM is a media gateway that is internal to a CS 2000 hybrid configuration, performing circuit/packet conversion between conventional circuit connections on one side and streams of packetized voice on the other.

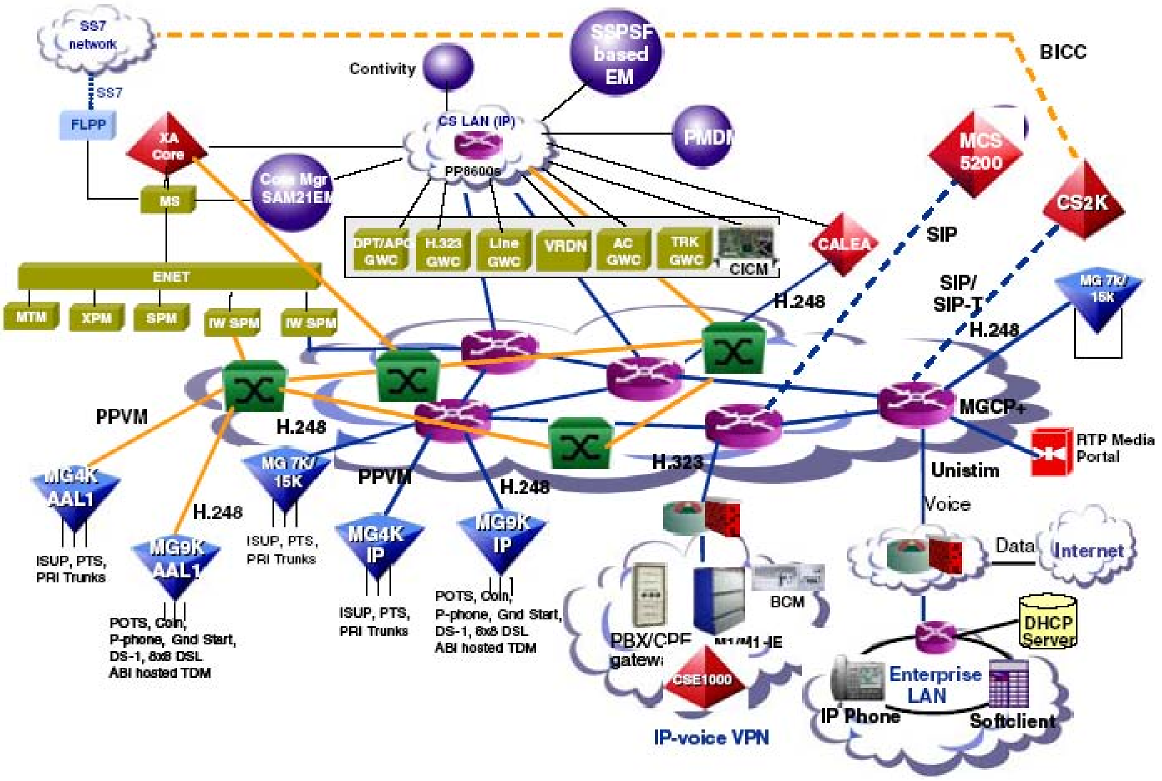
Trimodal network configuration

In the SN07 release, support was 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. 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	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
CHS	H.323 gateways	PRI trunks
	CICM	m5216 MBS lines
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 was introduced.

Control is given to the Carrier VoIP 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 SN08 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, Carrier VoIP 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 SN08 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).

Associated systems and services

CHS Services

The Carrier Hosted Services (CHS) Solution provides the following services:

- **Centrex IP Client Manager (CICM)**

  Associated hardware and functionality:

  — twin-card CICM unit (housed in the SAM21 shelf)

  — H.248 protocol

  — UniStim protocol for Centrex IP lines

  — support for new services (DPNSS over QSIG, DFT over IBN7, Centrex IP, multimedia (blended users), analog lines

  Note: Centrex IP clients are not controlled directly by GWCs, but by a CICM unit on the CS LAN. The CICM is controlled by a GWC.

- **H.323 Proxy**

Associated hardware and functionality:

— H.323 unit (housed in the SAM21 shelf)

— H.323 protocols (H.225, H.245)

— support for new media gateways (IP-enabled Meridian 1, IP-enabled BCM, Westell DPNSS, third-party H.323 gateways)

- **RTP Portal (RMP)**

  Associated hardware and functionality:

  — SAM16-based RMP unit

  — NAT traversal, MGCP+ protocol

Multimedia Communication Server 5200

The Multimedia Communication Server 5200 (formerly Interactive Media Server, IMS) is a peer MGC on a par with the CS 2000. It can be deployed in its own right as a stand-alone solution. However, it can also be deployed as part of a complete CVoIP solution together with the CS 2000. In this case, the Multimedia Communication Server 5200 LAN is typically co-located with the CS 2000 local area network (CS LAN), and is configured as an additional virtual LAN (VLAN).

The Multimedia Communication Server 5200 is part of the Multimedia Communications Portfolio (MCP). It integrates voice with video, collaboration, and presence services to deliver an integrated set of multimedia communications services: Broadband Multimedia Services, Personal Communication Services, and Multimedia Business Services.

Features and services

This chapter provides an overview of the features and services offered by the Lines-based solution.

IP solutions features and services

This section discusses the features and services that are common to the IAC, IAW, PT-IP, PT-AAL2, and UA-IP solutions. For information on features and services that are unique to the solution, see UA-IP features and services.

IP solutions Lawful Intercept

ATTENTION
The Lawful Intercept facility described here is not available in the International solutions. International customers should refer to their International Lawful Intercept CD, to be ordered separately.

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 Carrier VoIP switches that terminate lines, or lines and trunks, but is not applicable to Carrier VoIP 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 Carrier VoIP 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.

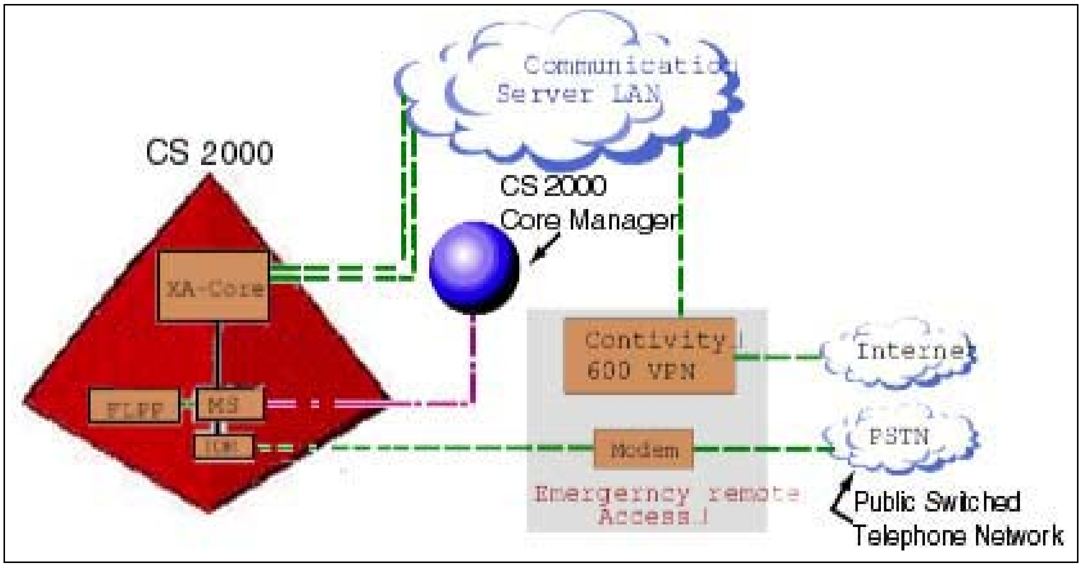
Note 2: The MARS (Meridian Automatic Route Selection) feature allowed calls that originated on a line to be rerouted by the system from ISUP IBNTO, or IBNT2 trunks. The Network Route Advance feature expands that functionality to include calls originating on trunks.

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 Carrier VoIP 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. Carrier VoIP 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 for narrowband PSTN/ISDN/VPN calls, including:

- Information database services: NXX toll free number services, authorization codes, calling card, account codes, debit/prepaid cards, operator services, and local number portability; either onboard or in an Intelligent Network configuration (via the INAP protocol to an external SCP)
- Routing and screening: CIC routing, time of day screening, CLI/ANI screening, and class of service screening
- Enterprise services: virtual private networks, ISDN PRI services

- Multiple dialing plans: support for multiple variable length dialplans for multiple PSTN and VPN customers, and speed dialing
- AMA format billing records
- support for IN services (via the INAP protocol to an external SCP)

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 for North American markets

> **ATTENTION**
> The following trunk types are supported in only the North American markets.

IP solutions support the following trunk types:

- Packet access on the Media Gateway 15000 for intra-Carrier VoIP Network and inter-Carrier VoIP Network calls
  - Inter ISUP IMT
  - Intra ISUP IMT
  - ISUP IT (for tandem)
- TDM access on the Media Gateway 15000 for intra-Carrier VoIP and intra-Carrier VoIP calls
  - ISUP FGD/EANT
  - Inter ISUP IMT
  - Intra ISUP IMT
  - ISUP ATC
  - ISUP IT
  - ANSI PRI variants
    - NTNAPRI
    - N449PRI
    - U449PRI
    - NIPRI
  - MF trunk groups for emergency services (ES) and operator services (OS)

IP solutions supported trunk types for International markets

ATTENTION
The following trunk types are supported in only the International markets.

National interfaces and services are supported for an extensive set of countries:

- ISUP, TUP (for UK and France) and PRI TDM trunk access
- SS7 signaling includes:
  - ETSI ISUP v1/v2
  - ANSI ISUP/IBN7
  - Argentinian ISUP v1
  - Australia Ie-ISUP ACIF G.500 (Interconnect ISUP)
  - Australian ISUP v2 (CA30)
  - Austrian ISUP v1
  - Belgian ISUP v2
  - Brazilian ISUP v1
  - Chilean ISUP v2
  - Chinese ISUP v2
  - Czech ISUP v1
  - Danish ISUP v1
  - German ISUP v2
  - Hong Kong ISUP v2
  - Hungarian ISUP v1
  - Israeli ISUP v2
  - Italian ISUP v1/v2
  - Japan Interconnect (unified ISUP)
  - Malaysian ISUP v1
  - Mexican ISUP v1
  - Norwegian ISUP v1
  - Polish ISUP v2
  - Portuguese ISUP v1

  - Singapore ISUP v2
  - Spanish ISUP v1/v2 with enhancements (functions Call_Ref, LNP, Transit Network Selection, Barring Rev-Charge)
  - SPIROU
  - SSUTR2 (FTUP)
  - Swedish ISUP v2
  - Telmex ISUP
  - Turkish ISUP v1/v2
  - UK ISUP
  - UK IUP (BTUP)
- PBX signaling includes:
  - ETSI PRI
  - ANSI PRI
  - China PRI
  - Hong Kong PRI (CR13)
  - Japan PRI (INS1500)
  - Spanish PRI
- support for up to 8 point codes for switch consolidation or multi-country point-of-presence

Dynamic packet trunks (DPT) are supported: packet connections between two gateways controlled by two different communication servers, using SIP-T call control signaling between the two communication servers.

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-IPPT-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

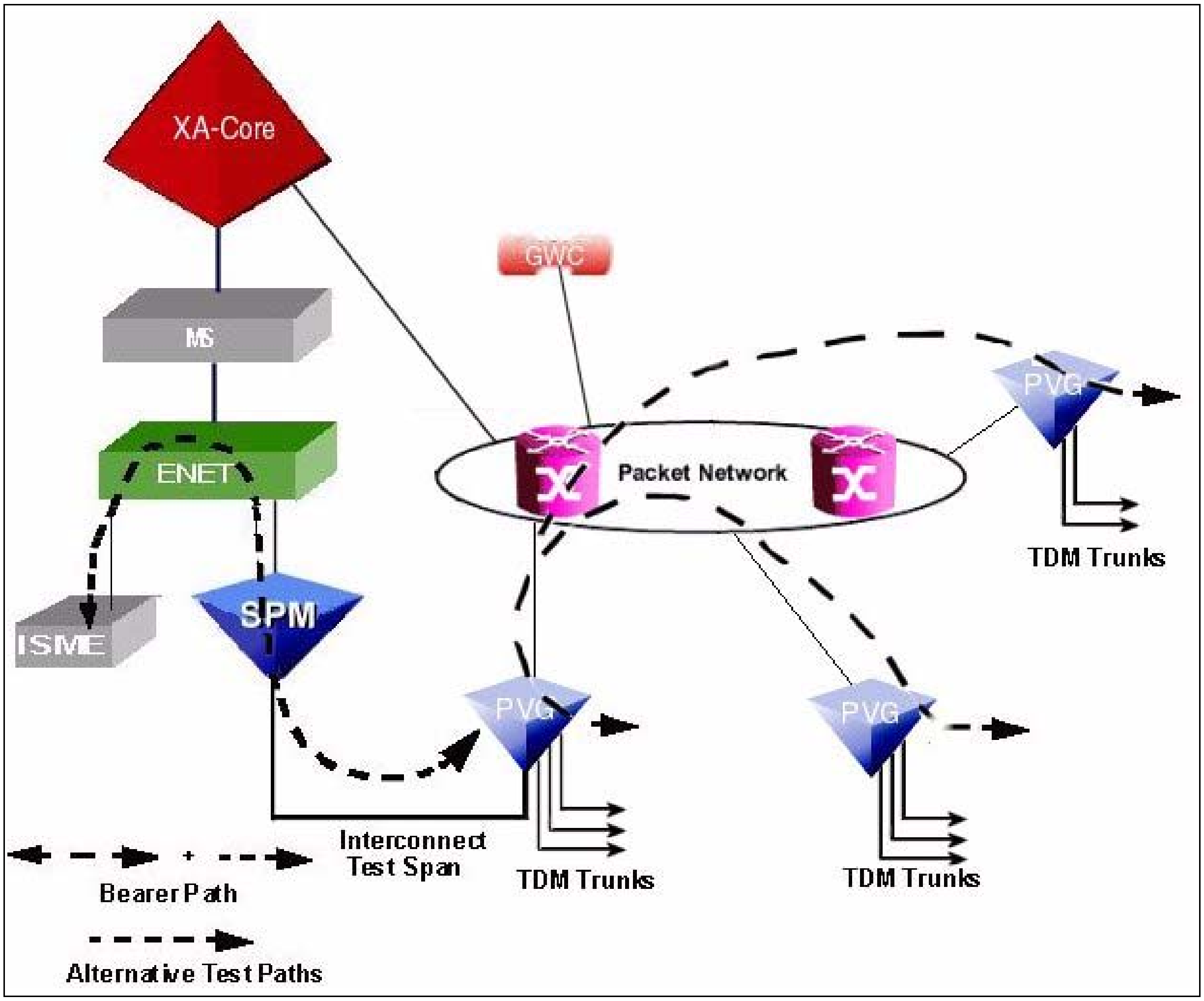
IP solutions interconnect span test trunking strategy

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 Media Gateway 15000s. 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 Media Gateway 15000 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 Media Gateway 15000. This functionality is accomplished through signaling control between the Gateway Controller (GWC) and the media gateways. Upon either originating or terminating COT requests, the Media Gateway 15000 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 Carrier VoIP 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

Carrier VoIP 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

UA-IP features and services

This section discusses the features and services that are unique to the UA-IP solution. The UA-IP 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

In addition, the UA-IP 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; either onboard or in an Intelligent Network configuration (via the INAP protocol to an external SCP)
- 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: support for multiple variable length dialplans for multiple PSTN and VPN customers, 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
- Support for IN services (via the INAP protocol to an external SCP)

The table Supported services: UA-IP line features lists the 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.

Supported services: UA-IP line features

Feature	Symbol	Capability	Description
Automatic CallBack	ACB	Supported	Allows a party to automatically redial the last number dialled on their station by dialling an access code.
Automatic Recall of Dialable Directory Number	ARDDN	Partially supported (no number, date, or time of last call is announced)	Delivers a dialable directory number to the Automatic Recall (AR) party. Also known as DDN AR Voiceback.
Anonymous Call Rejection	ACRJ	Supported	Allows parties to refuse calls from callers who choose to hide their directory number (CNDB) or name (CNAB)
Call Transfer	CXR	Supported	Allows a party to transfer a call to another station
Consultation on Hold		Supported	Allows a transferring party to talk in private with the party at the transfer destination. Part of the CXR functionality.
Call hold	CHD	Supported	Allows a calling party to temporarily place a call on hold
Call Restrict Area	-	Supported	Prevents calling parties from originating calls to a block prefix range of numbers
Call Park (PRK)	PRK	Supported	Allows a called party to place an incoming call on hold. The held call is available to any station in the customer group.
Directed Call Park	DPRK	Supported	Allows a called party to place an incoming call on hold on a user-selected station

Supported services: UA-IP line features

Feature	Symbol	Capability	Description
Call Waiting	CWT	Supported	Busy party is made aware that an incoming call attempt is being made
Cancel Call Waiting	CCW	Supported	Ability to cancel the Call Waiting feature
3-Way Call	3WC	Supported	Allows a party to add another party to an existing conversation and have a three-way conference call
Call Forward Universal	CFU	Supported	Diverts all calls to an alternate number
Call Forward Busy	CFB	Supported	Diverts calls to an alternate number when the called party is busy
Call Forward Don't Answer	CFD	Supported	Diverts calls to an alternate number when the called party does not answer
Call Forward Call Waiting Calls	CFCW	Supported	Diverts calls to an alternate number when the called party is busy
Call Forward Don't Answer Variable Timing	CFDVT	Supported	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 Indication	CFIND	Supported	
Call Forward Intragroup	CFI/CBI /CDI	Supported	Diverts calls to other directory numbers within a defined group
Call Forward Validation	CFWVAL	Supported	Allows a subscriber to check their current call forward settings
Last Number Redial	LNR	Supported	Allows the last number dialed to redialled automatically
Speed Calling, Individual Short List	SCS	Supported	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	Supported	Allows a party to store, delete and dial up to 70 directory numbers using only a few key presses
Call Completion to Busy Subscriber	CCBS	Supported	Allows a calling party to have a previously busy call attempt redialled when the called party becomes free.

Supported services: UA-IP line features

Feature	Symbol	Capability	Description
CEPT Call Completion to Busy Subscriber	CCBS	Supported	Allows a calling party to have a previously busy call attempt redialled when the called party becomes free. Conforms to the CEPT standard. ***Note:*** Only available on the International UA-IP solution.
Distinctive Ringing / Call Waiting	DRCW	Supported	Provides a terminating call a distinctive ring and gives busy calls a distinctive call waiting tone. The caller receives the standard audible ringback tone.
Secondary DN / Teen Service	SDN	Supported	Allows a single party to have additional directory numbers assigned to their line
Subscriber Activate Call Barring	SACB	Supported	Allows a subscriber to bar outgoing calls
CEPT International Line Restriction	ILR	Partially supported (calls to destinations barred by ILR cannot originate calls for roughly 30 seconds)	Allows a subscriber to bar outgoing calls. Similar to the SACB service, but conforms to CEPT standards. ***Note:*** Only available on the International UA-IP solution.
Calling Number Delivery	CND	Supported	Allows a called party to view the number of the calling party before they accept the call
Calling Number Delivery Blocking	CNDB	Supported	Allows a calling party to hide their directory number and cancel the effect of DDN
Calling Number Delivery Blocking Override	CNDBO	Supported	Allows a called party to view the number of the calling party before they accept the call, even if blocked by the caller using CNDB
Calling Name Delivery	CNAMD	Partially supported (only for intra-switch calls. No support via ETSI ISUP/SIP-T).	Allows a called party to view the name of the calling party before they accept the call
Calling Name Delivery Blocking	CNAB	Supported	Allows a calling party to withhold delivery of their calling name
Fixed Calling Number Delivery Blocking	SUPPR ESS	Supported	Allows permanent withholding of a calling party's directory number
Network-Wide Calling Name Delivery	-	Supported	

Supported services: UA-IP line features

Feature	Symbol	Capability	Description
Spontaneous Call Waiting with Identification	SCWID	Supported	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
CEPT Spontaneous Call Waiting with Identification	SCWID	Supported	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. Conforms to the CEPT standard. ***Note:*** Only available on the International UA-IP solution.
Delivery of Dialable Number	DDN	Supported	Allows presentation of a calling party's directory number for an incoming call
Message Waiting Indicator - Visual	MWT / CMWI	Supported	Lights an indicator lamp to indicate a message is waiting
CEPT Message Waiting Indicator - Visual	MWT / CMWI	Supported	Lights an indicator lamp to indicate a message is waiting. Conforms to the CEPT standards. ***Note:*** Only available on the International UA-IP solution.
Message Waiting - Audible	MWT (STD)	Supported	Provides an audible indication to indicate a message is waiting
Automatic Line / Hotline	AUL	Supported	Allows automatic dialing of a set number whenever the handset is raised or the DN key is pressed
Warm Line	WML	Supported	Allows a line to be associated with another directory number. If the subscriber goes off-hook and does not dial in a prescribed time, the call automatically routes to the associated directory number.
CEPT Warm Line	WML	Supported	Allows a line to be associated with another directory number. If the subscriber goes off-hook and does not dial in a prescribed time, the call automatically routes to the associated directory number. Conforms to the CEPT standard. ***Note:*** Only available on the International UA-IP solution.
Call Forward Remote Activation	CFRA	Supported	Allows a subscriber to remotely access call forwarding on a directory number different from which they are calling

Supported services: UA-IP line features

Feature	Symbol	Capability	Description
Do Not Disturb	DND	Supported	Allows an attendant to prevent call termination on a single station or group of stations
Announcement before Routing	ABR	Supported	
Call Forward Simultaneous/ Screening	CFS	Supported	Permits a user to forward more than one (up to a maximum of 256) calls through a station at a time. Conforms to the CEPT standard
Denied Call Forwarding	DCF	Supported	Allows a party to deny incoming forwarded calls. Conforms to the CEPT standard.
Call Pickup	CPU	Supported	Allows a station to answer incoming calls to another station in the same pickup group. Conforms to the CEPT standard.
Directed Call Pickup	DCPU	Supported	Allows a station to answer a ringing line in the same customer group before the called party answers the ringing line. Conforms to the CEPT standard.
Selective Call Acceptance	SCA	Partially supported (subscriber editing of the numbers not supported, E.164/ODP not fully supported, DNs only up to 10 digits supported)	Allows a called party to accept calls only from a group of definable directory numbers.
Selective Call Forwarding	SCF	Partially supported (subscriber editing of the numbers not supported, E.164/ODP not fully supported, DNs only up to 10 digits supported)	An incoming call management feature that allows subscribers to make a special list of telephone numbers and remote destination numbers.
Selective Call Rejection	SCRJ	Partially supported (subscriber editing of the numbers not supported, E.164/ODP not fully supported, DNs only up to 10 digits supported)	Allows a called party to automatically reject calls that arrive from a limited set of definable directory numbers.

Supported services: UA-IP line features

Feature	Symbol	Capability	Description
CEPT Call Waiting / Cancel Call Waiting	ICWT	Supported	Busy party is made aware that an incoming call attempt is being made. Conforms to the CEPT standard. ***Note:*** Only available on the International UA-IP solution.
CEPT International 3-Way Call and Call Transfer	I3WC	Supported	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 International Call Transfer	ICT	Supported	Allows a caller to transfer a call to a different International number. Conforms to the CEPT standard. ***Note:*** Only available on the International UA-IP solution.
CEPT Call Forwarding	CFx	Supported	Provides call forwarding functionality. Conforms to the CEPT standard. ***Note:*** Only available on the International UA-IP solution.
CEPT Calling Number Delivery	CND	Supported	Allows a called party to view the number of the calling party before they accept the call. Conforms to the CEPT standard. ***Note:*** Only available on the International UA-IP solution.
CEPT Calling Number Delivery Blocking	CNDB	Supported	Allows a calling party to hide their directory number and cancel the effect of DDN. Conforms to the CEPT standard. ***Note:*** Only available on the International UA-IP solution.
CEPT International Wake Up Call	IWUC	Supported	Allows a subscriber to program their telephones to ring at a specified time. Conforms to the CEPT standard. ***Note:*** Only available on the International UA-IP solution.

Supported services: UA-IP line features

Feature	Symbol	Capability	Description
CEPT Memo Box: Call Forward to Voice Mail		Supported	Diverts calls to a voice box. Conforms to the CEPT standard. ***Note:*** Only available on the International UA-IP solution.
Call Back to Last Received Call	AR	Supported	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.
Private Numbering Plan	PNP	Supported	Enables the use of private numbering plans provided all directory numbers within a VPN are the same length.
Automatic Call Distribution Observe	ACD OBS	Supported	Allows an ACD supervisor to monitor the quality of service offered to callers. An option exists to play an observation warning tone prior to the observation.
Automatic Call Distribution Emergency Key / Emergency Key Backup	ACD EMK	Supported	Allows an ACD agent to immediately conference in a supervisor and/or an auxiliary device in the event of threatening or abusive calls.
Camp-on for MDC lines	MBSCA MP	Supported	Similar to Call Waiting, allows an MBS set to camp-on to a busy group member
Music on Hold	LMOH, KSMOH	Supported	Provides an audio source to a line placed on hold.
Executive Busy Override	EBO	Supported	Allows a member of a customer group to override a busy indication from a called line and connect into the call in progress. The line can be connected as a third party, or can drop the extra party.
Requested Suspend Service	RSUS	Supported	Allows a party to request suspension of service. All incoming calls or attempted outgoing calls are routed to treatment
Wake-up Call Request	WUCR	Supported	Allows a subscriber to program their telephones to ring at a specified time
Bridged Night Number	BNN	Supported	Allows a different number for use during different time periods
Voice Band Data (Group 3 Fax and Modem)	FAX data	Supported	Allows transmission and reception of voice-band data services such as facsimile and modem

Supported services: UA-IP line features

Feature	Symbol	Capability	Description
Station Controlled Conference (6 pty)	SCC 6	Supported	
Distinctive Ringing	DRING	Supported	Allows a called party to have a distinctive ring on their telephone set
Preset Conference	-	Supported	Allows a conference to be initiated by dialing a single directory number, which in turn automatically dials up to a maximum of 25 other conference members. The conference begins when the first dialed party answers, and ends when all parties have disconnected.
MADN Multiple Call Arrangement	MCA	Supported	Allows multiple stations to have the same directory number. In the Multiple Call Arrangement, each station can communicate with a different calling party.
MADN Single Call Arrangement	SCA	Supported	Allows multiple stations to have the same directory number. In the Single Call Arrangement, one or multiple stations can communicate with a single calling party.
Make Set Busy	MSB	Supported	Allows a subscriber to manually make their directory number busy. All calling parties will then receive a busy tone (or appropriate action).
Ring Again	RAG	Supported	Allows the last number called by a phone to be redialed
Multicarrier	CARR	Supported	Allows multiple carriers to be used
Simultaneous Ring	SIMRING	Supported	Allows multiple directory numbers to ring during a single incoming call
Authorization Code	-	Supported	Allows the use of a security code to allow change of service privileges
Code Restrictions	NCOS	Supported	Allows Network Class of Service (NCOS) based call barring
Cut-off on Disconnect	COD	Supported	
Denied Origination	DOR	Supported	Allows a line to receive calls only. Also known as Outgoing Call Restriction by Administration.
Denied Termination	DTM	Supported	Allows a line to originate calls only

Supported services: UA-IP line features

Feature	Symbol	Capability	Description
Direct System Inward Access	DISA	Supported	Allows authorized callers to dial from switched networks directory into a private office. DISA also allows the caller to gain access to network facilities without the help of an attendant.
Essential Line	ELN	Partially supported (if V5.2 access is busy or all B-channels are in use, a prioritized user does not get priority access to the network)	When the system activates emergency cutoff, the system denies service to calls that originate from subscriber lines that are not provisioned as being essential lines. A line with the ELN option can originate non-local calls when the switching unit has network protection (NETPROT) active. When NETPROT is turned on, any subscriber can make local calls.
Hunting - Directory Number and Multi-line	DNH, MLH	Partially supported (hunt groups cannot span TDM and IP sides of a hybrid switch. V5.2 hunt group members must be on the same V5.2 interface)	Allows incoming calls to be directed to an idle line within a hunt group
Line Overflow to DN	LOD	Supported	Directs overflow calls to an defined directory number
Line Overflow to Route	LOR	Supported	Moves overflow calls to a route identified in one of the standard route tables
Line Reversal On Answer	LROA	Supported	
Line Reversal On Seizure	LRS	Supported	
Meet-me Conference (6 pty)	MM CONF	Supported	Allows a conference call to be established by all participants dialling a common DN
Networked Centrex		Supported	
Plug Up	PLP	Supported	Disables call terminations on single-line sets. Only originated calls can be made.
Suspend/Resume	SUS /RES	Supported	Temporarily suspends or resume telephony service
Second Language	SL	Supported	Allows voice prompts to be selected in a second language

Supported services: UA-IP line features

Feature	Symbol	Capability	Description
Uniform Call Distribution	UCD	Supported	Allows distribution of incoming calls evenly between the stations belonging to a UCD group. If not station is free when a call is received, an announcement is played to the calling party and the call is queued.
Wake-Up Call Request Universal Access	UAWUCR	Supported	
Calling Line Flash (for malicious call identification)	CLF	Supported	The facility for a called party to hold a connection with a switch-hook flash. Can be used to aid the tracing of malicious calls. Also known as Malicious Call Trace (MCT).
CEPT Call Diversion to Announcement	CDTA	Supported	***Note:*** Only available on the International UA-IP solution.
CEPT Call Forward Fixed	CFF	Supported	***Note:*** Only available on the International UA-IP solution.
Emergency Call Routing	-	Supported	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.

TL-1 Line Test Interface

ATTENTION
The TL-1 Line Test Interface has only been tested on North American solutions, although designed for use in all markets.

The TL-1 messaging interface on the CS 2000 Management Tools server allows third-party test systems to perform external loop tests on specified MG 9000 lines. The test interface supports narrowband testing for traditional voice services and wideband test access for DSL lines.

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.

Interfaces and protocols

This chapter provides an overview of the solution interfaces and protocols. The chapter contains the following sections:

- IP network on page 82
- Physical interfaces on page 82
- Protocols on page 88

IP network

The CS 2000 and CS 2000-Compact provide control to allow media carried in TDM networks (via the Media Gateway 15000) or in subscriber lines (via the MG 9000) to be carried across an IP network. The communication server processes the incoming call information (that is, signaling) and sends control commands to the Media Gateway 15000 or MG 9000 gateways. The gateways process the commands from the communication server to set up call connections.

Typically, more than one gateway is associated with each communication server, and calls can start and terminate on the subnetwork controlled by a single server. If more than one communication server is involved, the servers communicate using SIP-T across the packet network to set up the call.

Physical interfaces

This section identifies the physical interfaces and protocols that are associated with each of the components within the 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 Ethernet Routing Switch 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 Ethernet Routing Switch 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.

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, and IUA protocols support messaging between a GWC and Media Gateway. 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. M3UA supports messaging between a GWC and USP.

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.

> ***Note:*** Although still supported, the UAS has been replaced by the MS 2000 series of audio servers.

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.

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.

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.

Ethernet Routing Switch 8600 physical interfaces

The Ethernet Routing Switch 8600 terminates all 10/100 BaseT Ethernet links, and all Gigabit Ethernet links from other components on the CS LAN. In addition, Ethernet Routing Switch 8600 supports Gigabit Ethernet links to the backbone packet network.

Protocols supported by Ethernet Routing Switch 8600

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

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 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 MS 2000/UAS) on the bearer traffic network.

> ***Note:*** ASPEN is still supported but has been superseded by the standard H.248 protocol for most purposes. However, ASPEN remains the only protocol verified for control of trunk gateways supporting QSIG access.

Media Gateway 7480 physical interfaces

There are asynchronous transfer mode (ATM) interfaces from the VSP2 card of the Media Gateway 7480. In addition, there is a 10/100 BaseT Ethernet link to the CS LAN.

Protocols supported by Media Gateway 7480

ASPEN, SCTP, IUA, and H.248 support messaging between GWCs and Media Gateway 7480s. RTP and RTCP support the transmission of audio (from the MS 2000/UAS) on the bearer traffic network.

> ***Note:*** ASPEN is still supported but has been superseded by the standard H.248 protocol for most purposes. However, ASPEN remains the only protocol verified for control of trunk gateways supporting QSIG access.

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.

Ethernet Routing Switch 8600 physical interfaces

The Ethernet Routing Switch 8600 terminates all 10/100 BaseT Ethernet links, and all Gigabit Ethernet links from other components on the CS LAN. In addition, Ethernet Routing Switch 8600 supports Gigabit Ethernet links to the backbone packet network.

Protocols supported by Ethernet Routing Switch 8600

Ethernet Routing Switch 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 Ethernet Routing Switch 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 7480), 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 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.

MDM physical interfaces

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

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

Protocols supported by MDM

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

Protocols

A Carrier VoIP Network uses the following protocols.

ARP

Address Resolution Protocol (ARP) 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 2.1 is a legacy protocol used to communicate between the CS 2000 and the Media Gateways, that is, the gateway controller (GWC) to Media Gateway messaging to support VoIP. ASPEN 2.1 is based on the Simple Gateway Controller Protocol (SGCP) and includes modifications to support extensions that SGCP does not support. ASPEN is similar to the media gateway control protocol (MGCP) but is more explicit and specific than MGCP. The H.248 protocol has superseded ASPEN for most purposes.

> ***Note 1:*** ASPEN has not been supported for V5.2 access since ISN05. As of SN06, upgrade to the H.248 protocol is mandatory for all existing V5.2 interfaces. All new V5.2 interfaces must use H.248 and not ASPEN.
>
> ***Note 2:*** ASPEN is currently the only protocol that has been verified for control of trunk gateways supporting QSIG access.

DPNSS

Digital Private Network Signaling System (DPNSS) is a UK national common channel signalling system. It was initially used for interconnecting PBXs in private networks only, but is now also employed to give PBX access to VPN services offered by the PSTN.

Ethernet

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

FTP

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

H.248

Megaco/H.248 is an IETF protocol designed to support signaling between GWCs and the gateways they control. The CS 2000 uses H.248 for communication

- with Media Gateways configured as trunk gateways, as a preferred alternative to ASPEN in support of VoIP and VoATM
- between an audio control (AC) GWC and the UAS
- to support the MG 9000 media gateway

ICMP

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

IP

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

IPSec

Internet Protocol Security (IPSec) is a collection of IP security measures that define data privacy, integrity, authentication, key management, and tunneling methods. IPSec is a secure version of the Internet Protocol that provides optional authentication and encryption at the packet level. From SN08, IPSec provides additional security enhancements to the Media Gateway 7400/15000, and other media gateways (including small line gateways).

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.

MTP User Adaptation (M3UA and M2UA)

Message transfer part (MTP) User Adaptation is designed to support SS7 signalling over an IP network. It allows SS7 user part messages or MTP message signal units (MSU) to be conveyed between packet network nodes.

There are two types of MTP User Adaptation:

- MTP Layer 3 User Adaptation (M3UA)
  M3UA is used to convey SS7 MSUs between network nodes that share a SS7 point code. In a CS 2000 that uses the USP to terminate SS7 signalling, the USP and the Core share the same point code. The USP uses M3UA to distribute incoming SS7 messages to the Core and the GWCs.
- MTP Layer 2 User Adaptation (M2UA)
  M2UA is used to convey SS7 MSUs between network nodes with different SS7 point codes. A network of CS 2000s uses M2UA to convey MSUs between the CS 2000s (that is, between the USPs belonging to different CS 2000s).

NTP

Network Time Protocol (NTP) 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 or CS 2000 Core Manager.

Q.931 (over IUA)

Q.931 protocol is used for D-channel backhaul signaling between a GWC and a Media Gateway supporting PBX access over ETSI PRI trunks. ISDN User Adaptation (IUA) provides adaptation between PRI and the Stream Control Transmission Protocol (SCTP) layer used to provide reliable transport.

RTCP

Real-time Transfer 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.

SCTP

Stream Control Transmission Protocol (SCTP) is used to provide reliable ordered transport for call control messaging.

SDP

Session Description Protocol (SDP) session description signaling is used to complement GWC-to-gateway signaling and inter-CS signaling by specifying media stream characteristics and address information.

SIP

Session Initiation Protocol for Telephony (SIP-T) is used for inter-CS signaling (between CS 2000 and CS 2000, or CS 2000 and Multimedia Communication Server 5200). SIP-T allows inter-Carrier VoIP Network calls to be routed over the IP fabric instead of through traditional TDM access carriers. SIP-T messages convey encapsulated CCS7 messages; SIP-T therefore supports CCS7 (SS7) directly.

SNMP

Simple Network Management Protocol (SNMP) is used by network management applications to query a management agent using a supported MIB (management information base).

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

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

TFTP

The Trivial File Transfer Protocol (TFTP), an IETF standard, is used to transfer the software loads.

VRRP

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

TDM telephony interfaces

The following sections give brief descriptions of the TDM telephony interfaces.

SS7 trunk interfaces

The CS 2000 includes support for generic ETSI ISUP and variants, IBN7 (ANSI ISUP) and TUP interfaces. For details of the national variants supported, refer to the chapter [Features and services].

ISUP supports not only basic telephony, but also ISDN data calls, and a range of supplementary services based on the exchange of information using out-of-band messages.

Intelligent network (IN) interface

The Intelligent Network Application Part (INAP) protocol is used for peer-to-peer communication between IN functional elements. The CS 2000 SSP uses INAP to support IN queries from the SSP to an SCP, typically to allow IN service logic to be involved in call completion.

PRI access interface

PRI and variants are the interfaces used mainly for point-to-point communication between digital PBXs and CS 2000 gateways. For details of the national variants supported, refer to the chapter [Features and services].

Note: In ISN07, the CS 2000 does not support PRI user mode. Only network mode is supported.

Call processing

This section discusses the call processing operations applicable to Lines-based solutions.

Call processing for IP

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

- the SIP-T protocol for set up and take down of dynamic packet trunks between Carrier VoIP 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

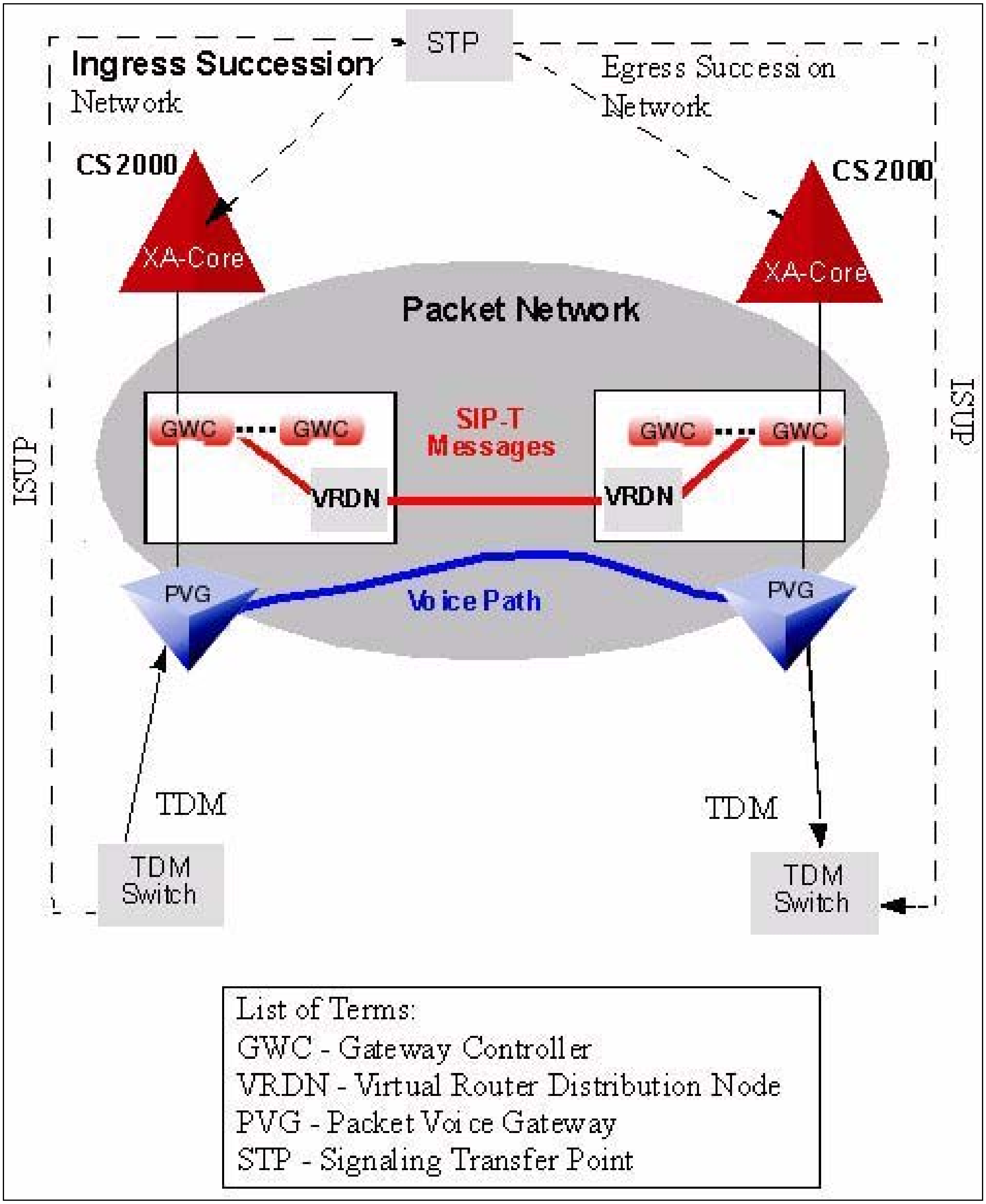
SIP-T introduces the following concepts to Carrier VoIP Call Processing:

- Dynamic Packet Trunks (DPTs). Represent a bearer path connection across a packet network. DPTs allow connections to other Carrier VoIP 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 Carrier VoIP Network receives the appropriate SIP-T message, the Egress Carrier VoIP Network can use the information in the SIP-T message to establish a bearer path across the packet network.

For the Carrier VoIP 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

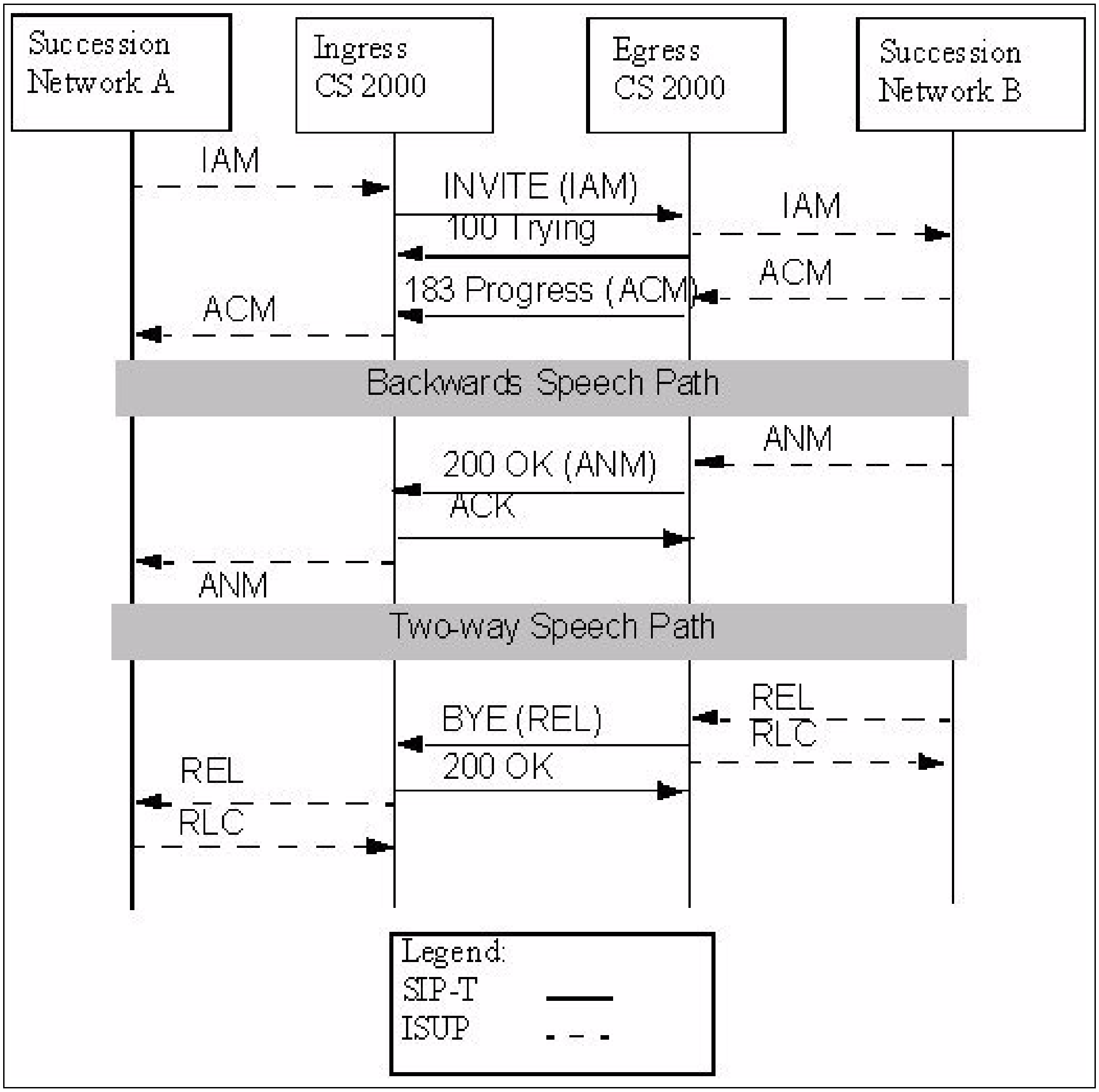


List of Terms:
GWC - Gateway Controller
VRDN - Virtual Router Distribution Node
PVG - Packet Voice Gateway
STP - Signaling Transfer Point

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:

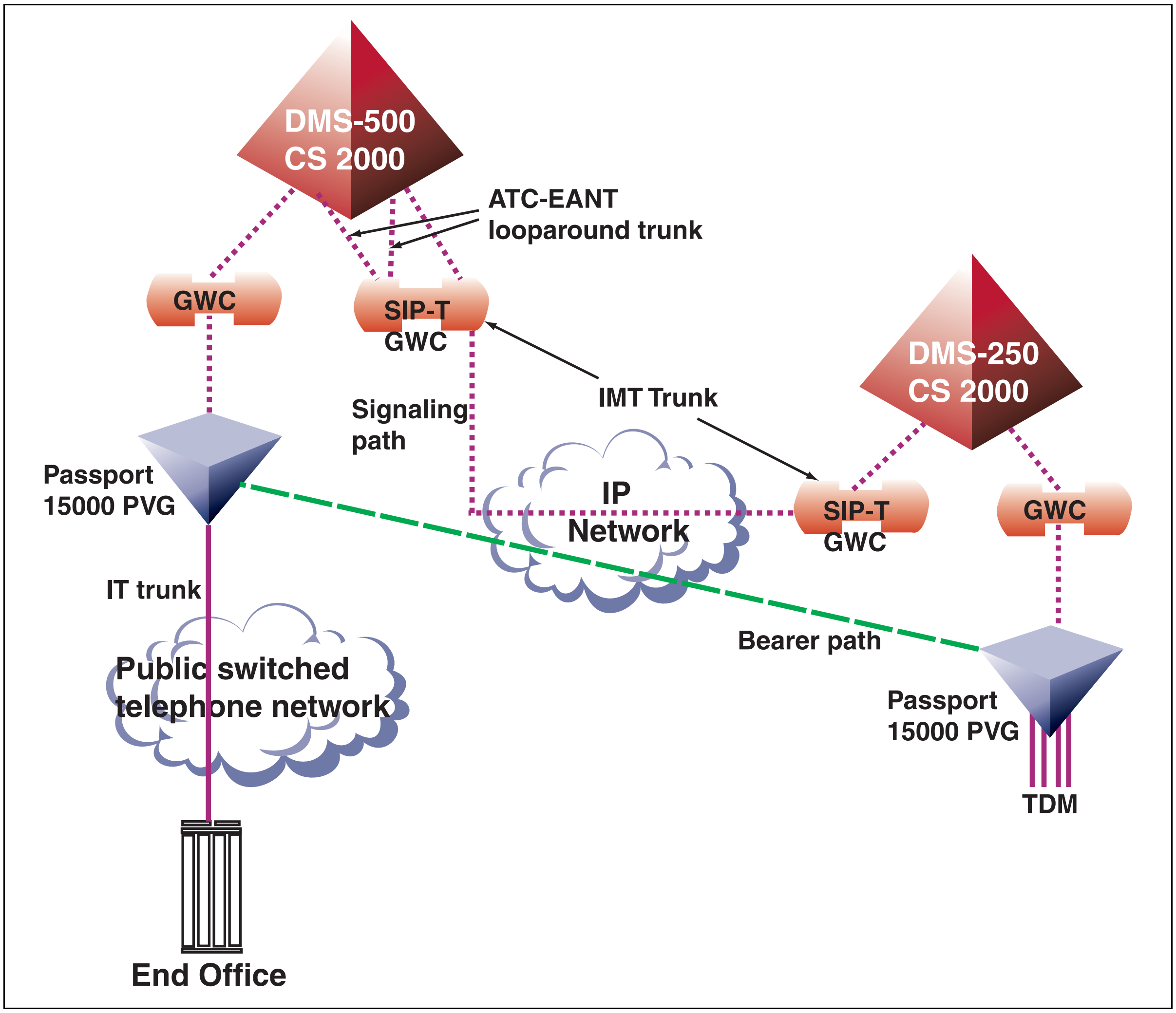
- Mechanized Calling Card Services (MCCS)
- Reorigination
- Auth Codes/PIN Codes/Account Codes

- 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 looparounds. 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.

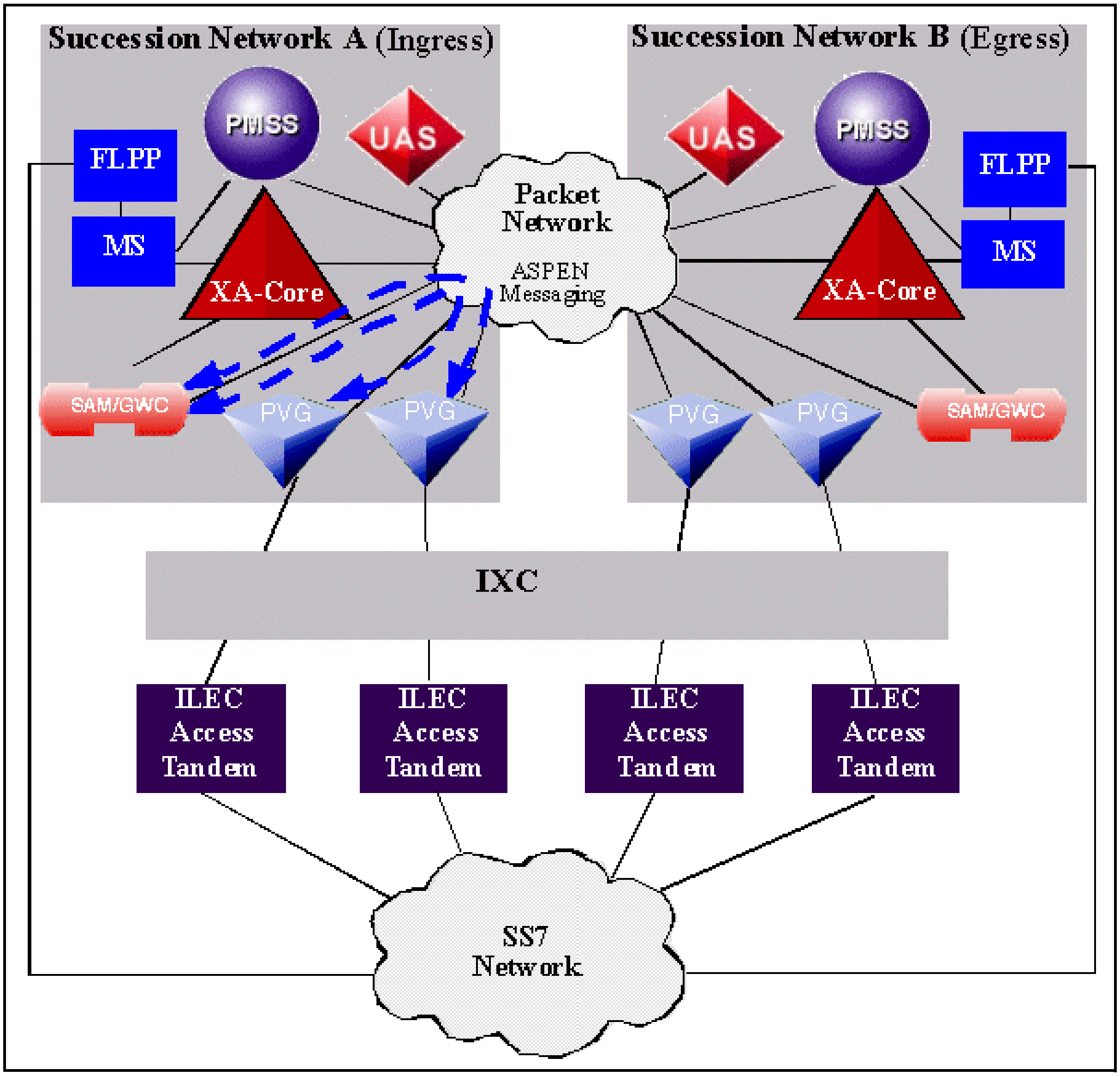
DMS-500 CS 2000 SIP-T with looparound trunks



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



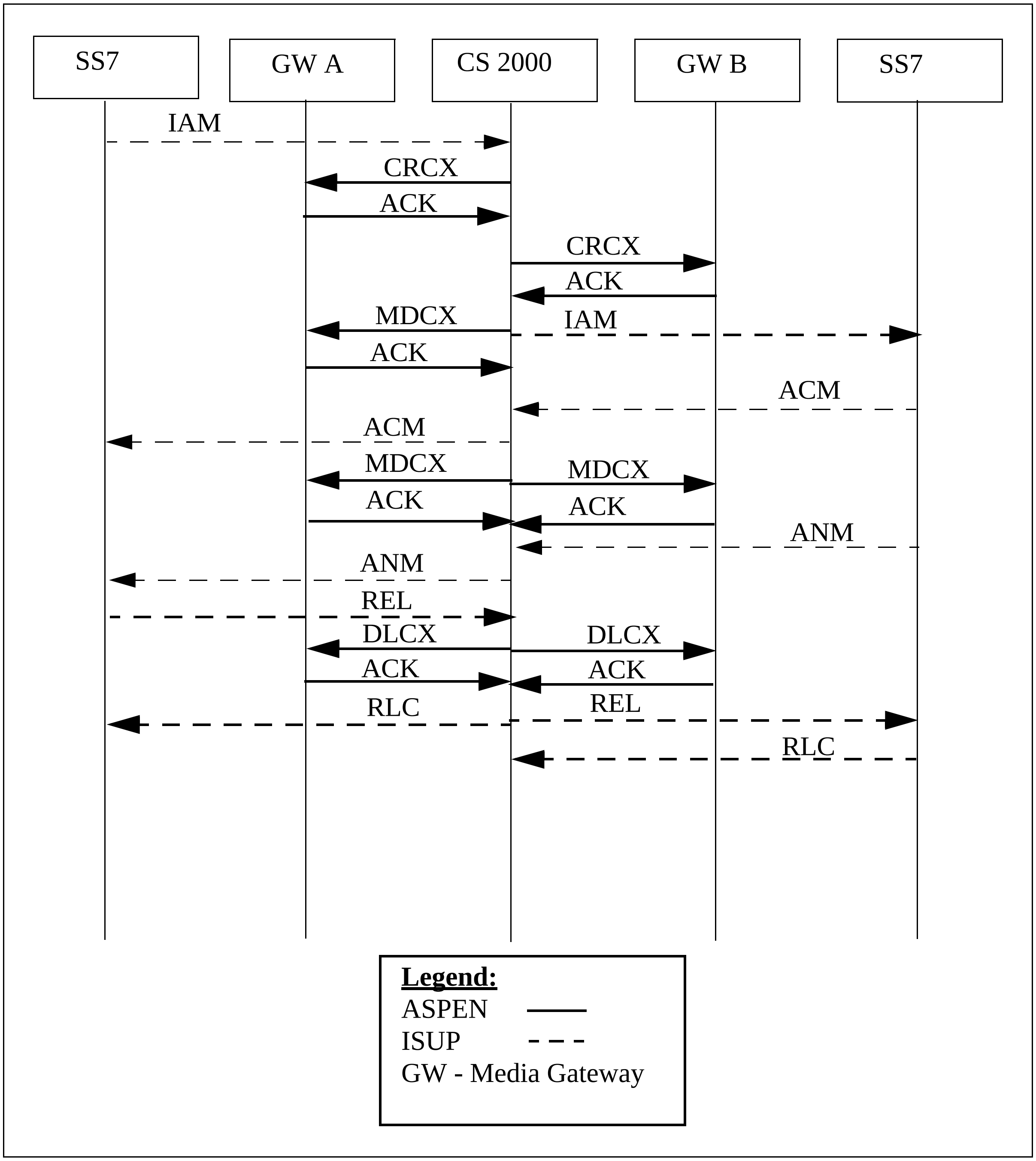
ASPEN messages are transmitted over User Datagram Protocol (UDP) across the packet network. The port number for the GWC and the controlled Media Gateway 15000/7400s should be set up by means of provisioning on both components. Since UDP is subject to losses, all commands are assigned timers and will 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.

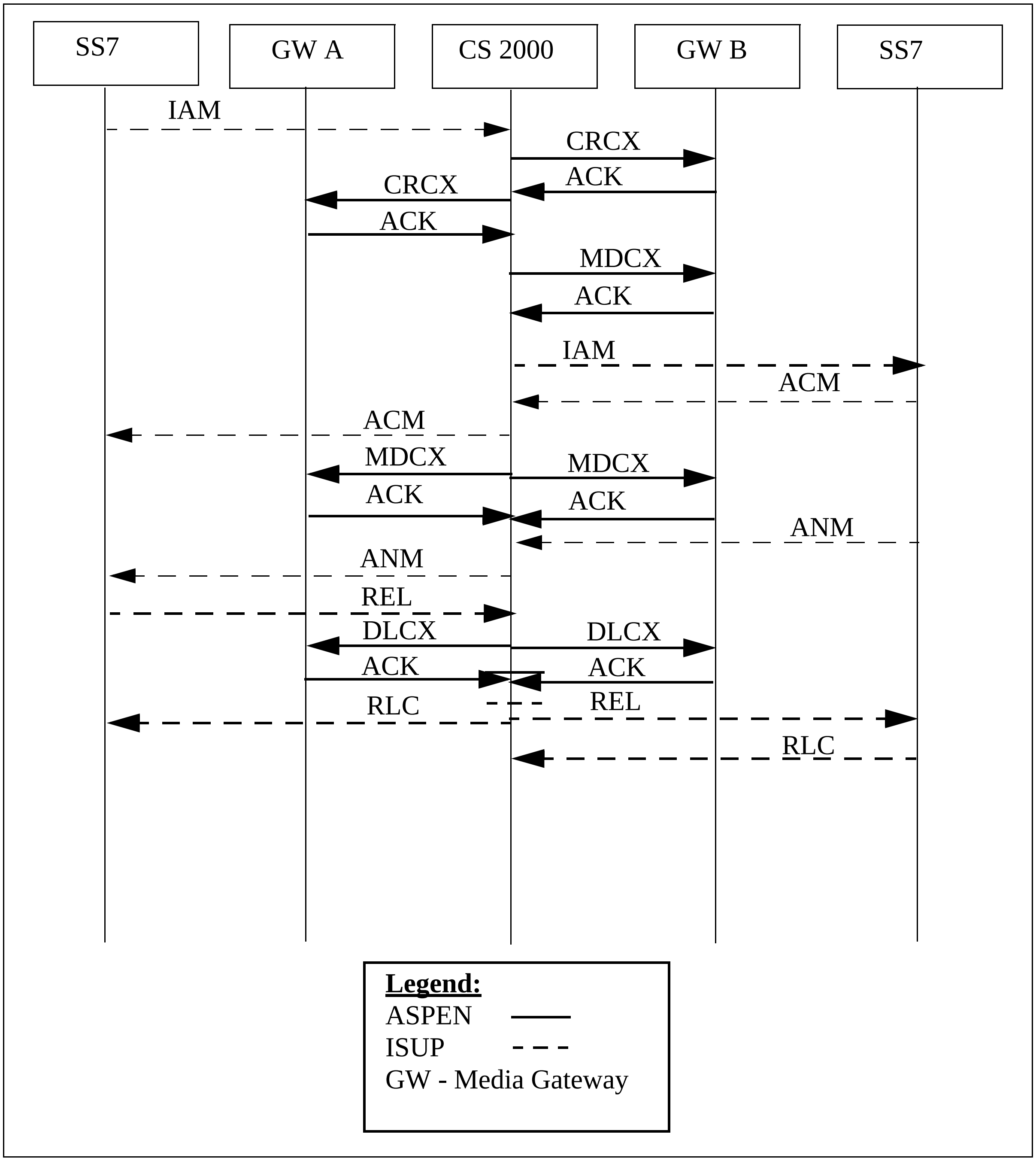
ASPEN Messaging (the CRCX is being sent to the incoming GWC first)



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.

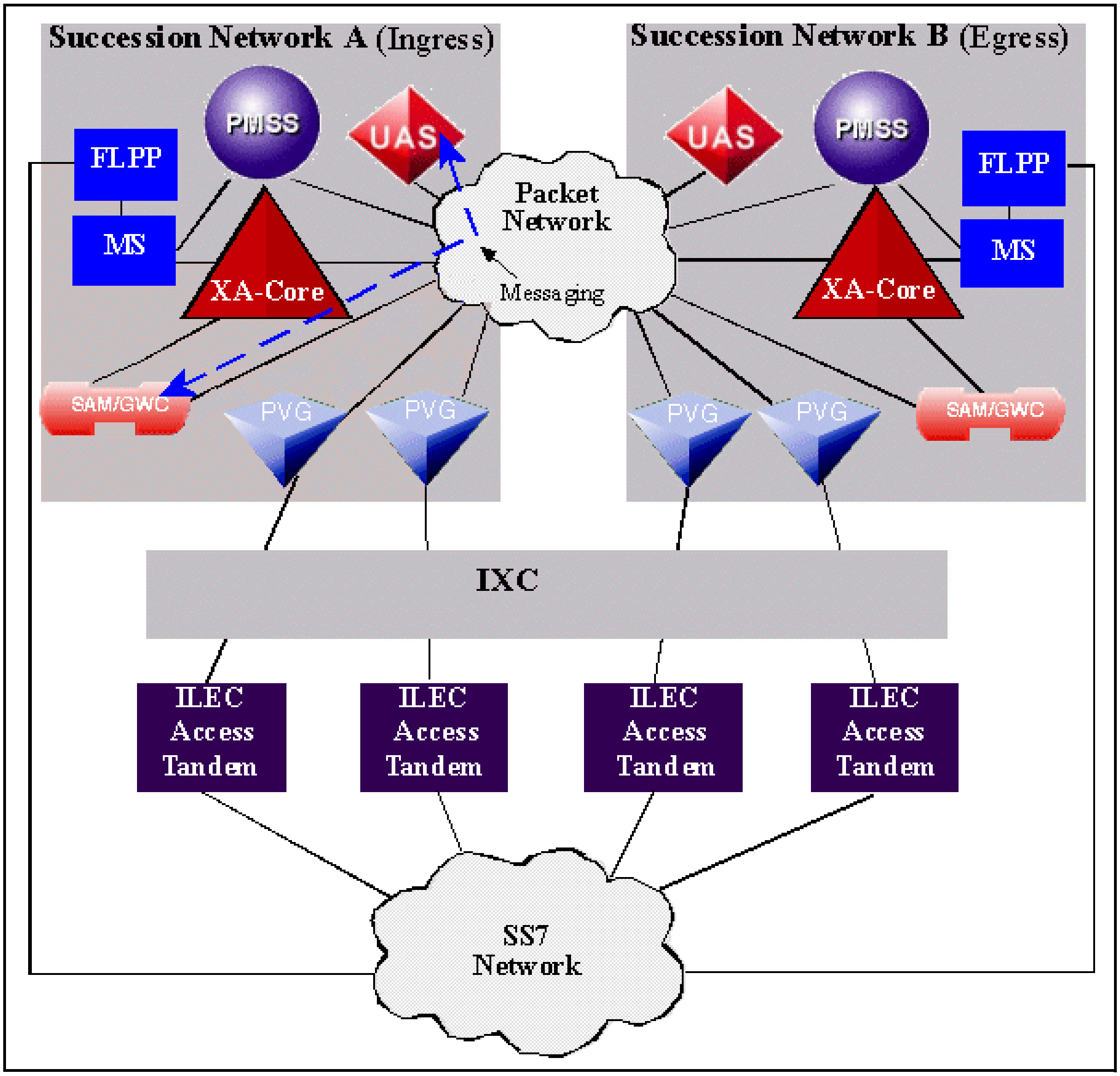
ASPEN Messaging (the terminator gets the first CRCX)



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

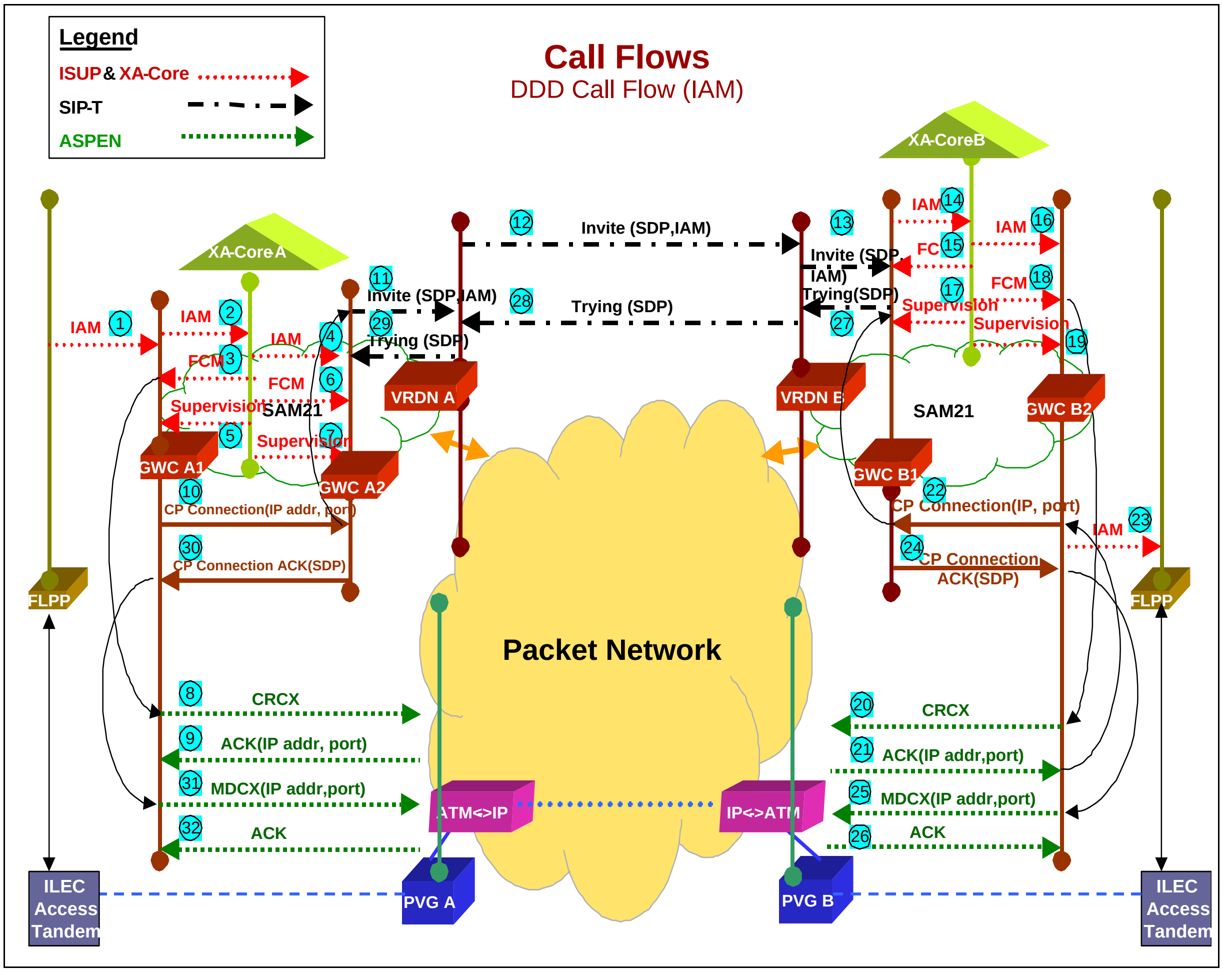


The UAS sends a response to each message it receives from the GWC. The response may indicate the result of processing the command.

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 Carrier VoIP 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 Carrier VoIP Network. Based upon data from table C7TRKMEM, the FLPP maps the CIC of the IAM to the corresponding DS0 circuit on Media Gateway-A and forwards the IAM message to the GWC controlling Media Gateway-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 Media Gateway-A to establish a bearer connection across the packet network.
9. Media Gateway-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 Carrier VoIP Network to another Carrier VoIP 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 Carrier VoIP Network, within the SIP-T Invite message, to an IP address, so that the SIP-T Invite message is routed to the correct egress Carrier VoIP 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.

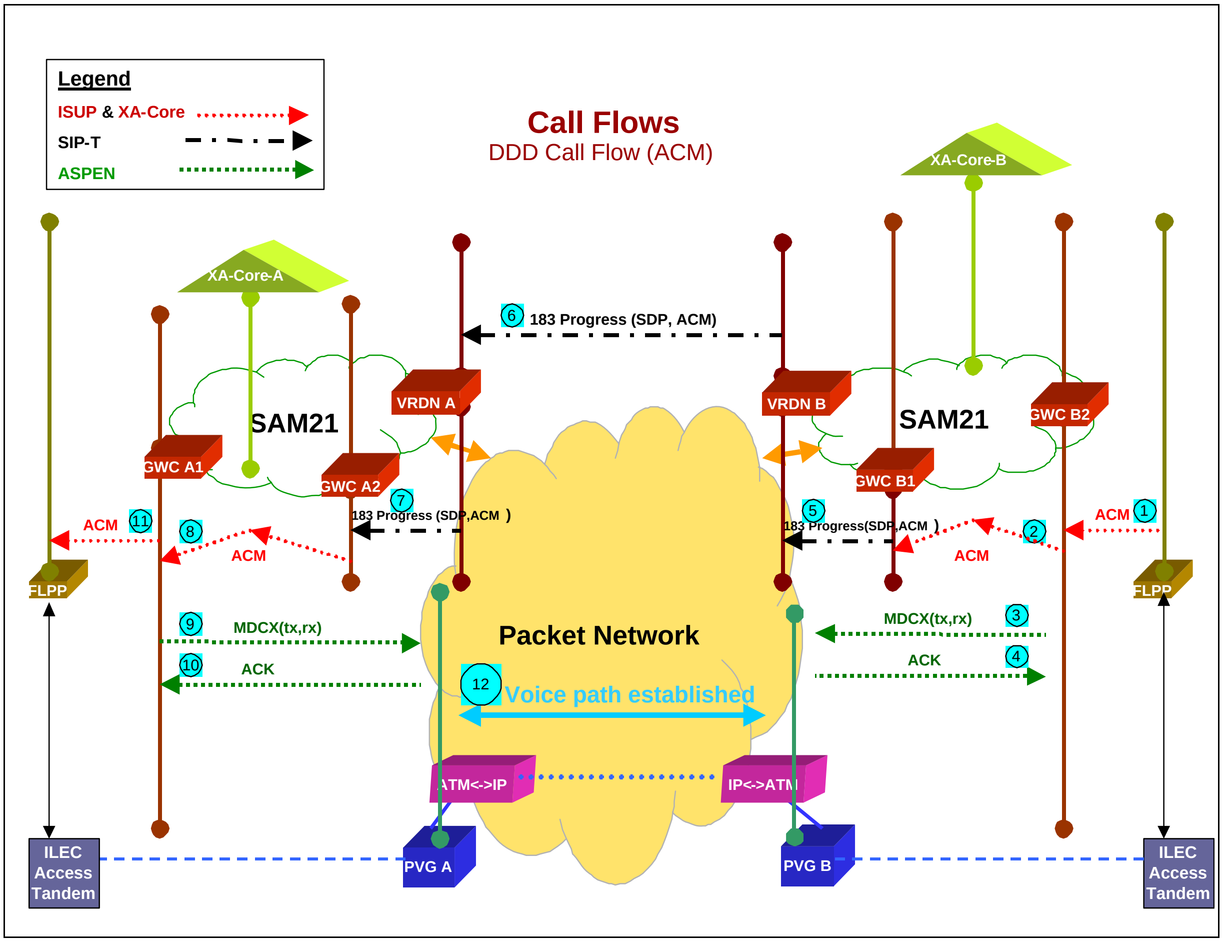
19. An ISUP supervision message is sent to the GWC-B2 to instruct it on how the terminating half call should behave.
20. Once GWC-B2 receives the FCM from XA-Core-B, GWC-B2 will send a create connection (CRCX) request to Media Gateway-B to establish a bearer connection across the packet network.
21. Media Gateway-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 Carrier VoIP Network to another Carrier VoIP 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 Media Gateway-B receives the ASPEN MDCX message, Media Gateway-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 Carrier VoIP Network, within the SIP-T Trying message, to an IP address, so the SIP-T Trying message is routed to the correct ingress Carrier VoIP 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 Carrier VoIP Network.
31. GWC-A1 sends an ASPEN modify connection (MDCX) message to Media Gateway-A.
32. Media Gateway-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)



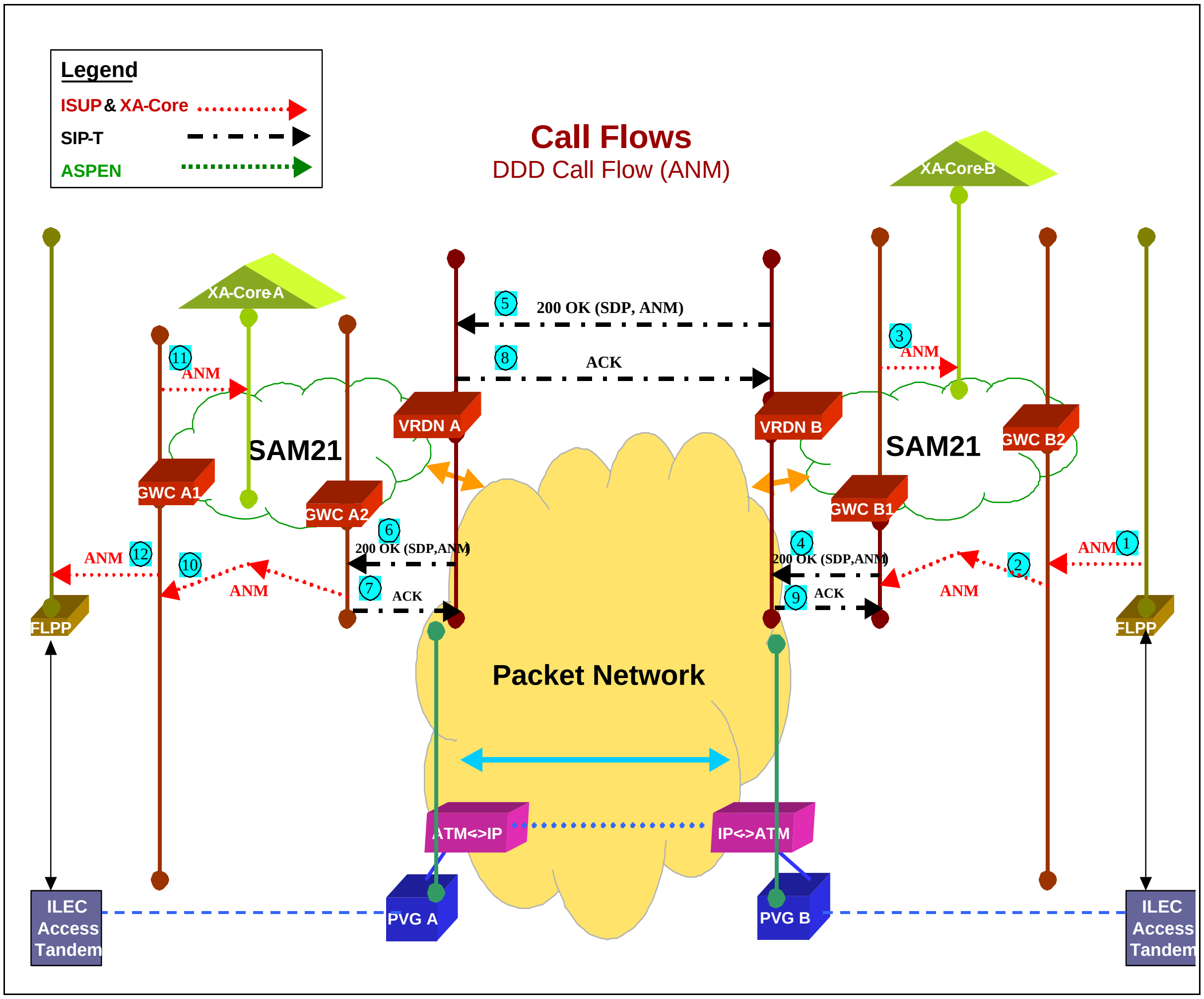
1. The terminating PSTN located on the egress Carrier VoIP Network sends an ISUP ACM through the SS7 network. The FLPP located in the egress Carrier VoIP Network forwards the ACM message to GWC-B2.
2. GWC-B2 forwards the ACM through the XA-Core to GWC-B1.
3. GWC-B2 sends an ASPEN modify connection (MDCX) message to Media Gateway-B.
4. Media Gateway-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 Carrier VoIP Network, within the SIP-T 183 Progress message, to an IP address, so the SIP-T Invite message is routed to the correct ingress Carrier VoIP 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 Media Gateway-A.
10. Media Gateway-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 Carrier VoIP Network sends an ISUP ANM through the SS7 network. The FLPP located in the egress Carrier VoIP 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 Carrier VoIP 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

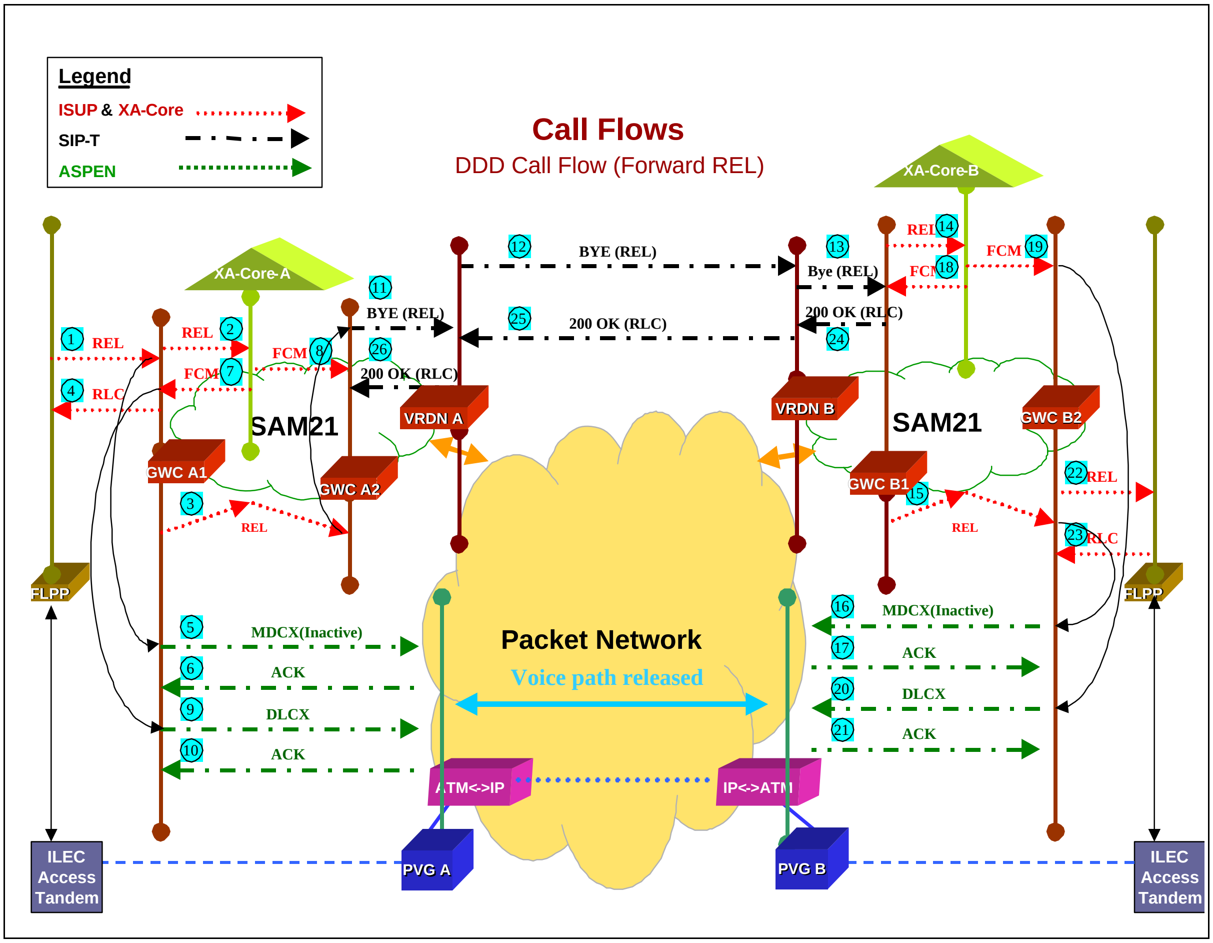
Carrier VoIP Network. VRDN-A receives the SIP-T 200 OK message.

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 Carrier VoIP Network.
8. VRDN-A translates the routing information of the egress Carrier VoIP Network, within the SIP-T ACK message, to an IP address so the SIP-T ACK message is routed to the correct egress Carrier VoIP 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 Carrier VoIP Network. Based upon data from table C7TRKMEM, the FLPP maps the CIC of the REL to the corresponding DS0 circuit on Media Gateway-A and forwards the REL message to the GWC controlling Media Gateway-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 Media Gateway-A.
6. Media Gateway-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 Media Gateway-A.
10. Media Gateway-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 Carrier VoIP Network, within the SIP-T BYE message, to an IP address, so the SIP-T BYE message is routed to the correct egress Carrier VoIP 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 Media Gateway-B.
17. Media Gateway-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 Media Gateway-B.
21. Media Gateway-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.

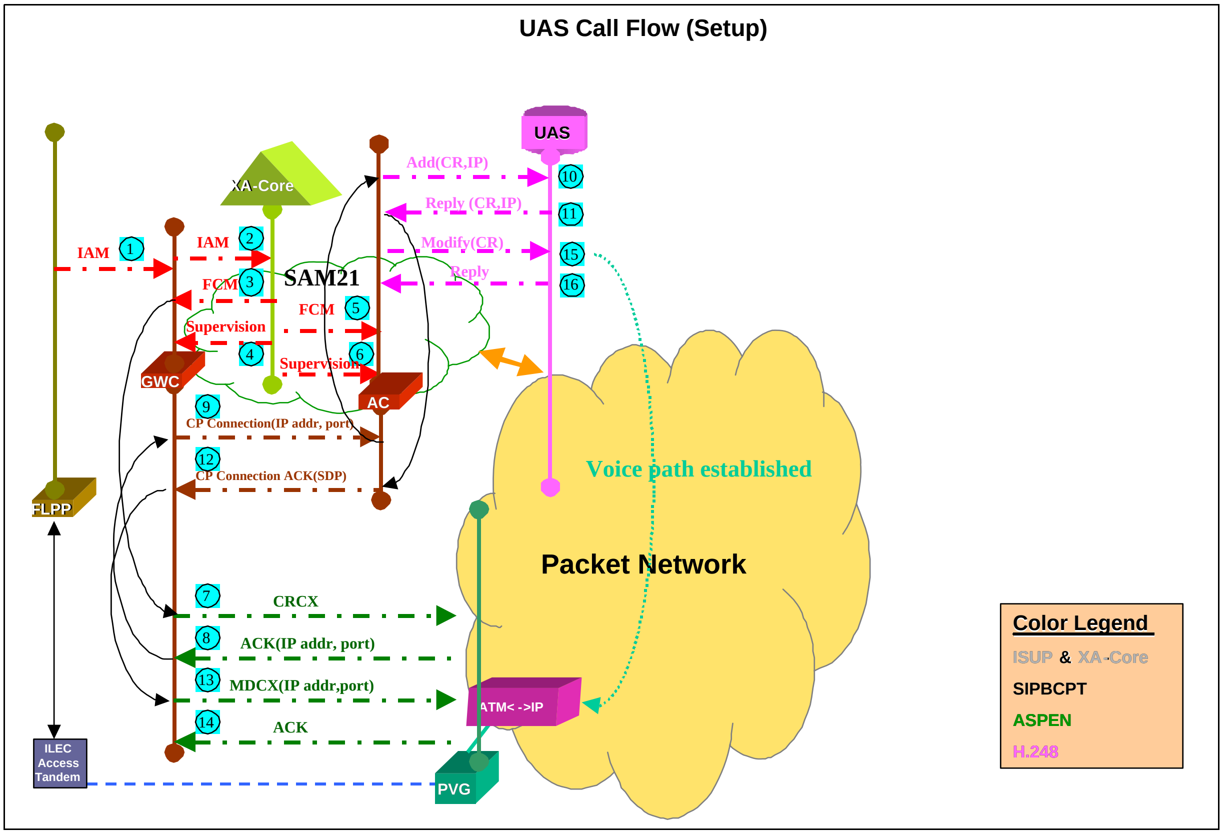
25. VRDN-B translates the routing information of the ingress Carrier VoIP Network, within the SIP-T 200 OK message, to an IP address, so the SIP-T 200 OK message is routed to the correct ingress Carrier VoIP Network. VRDN-A receives the SIP-T 200 OK message.

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 Carrier VoIP Network. Based upon data from table C7TRKMEM, the FLPP maps the CIC of the IAM to the corresponding DS0 circuit on the Media Gateway 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:

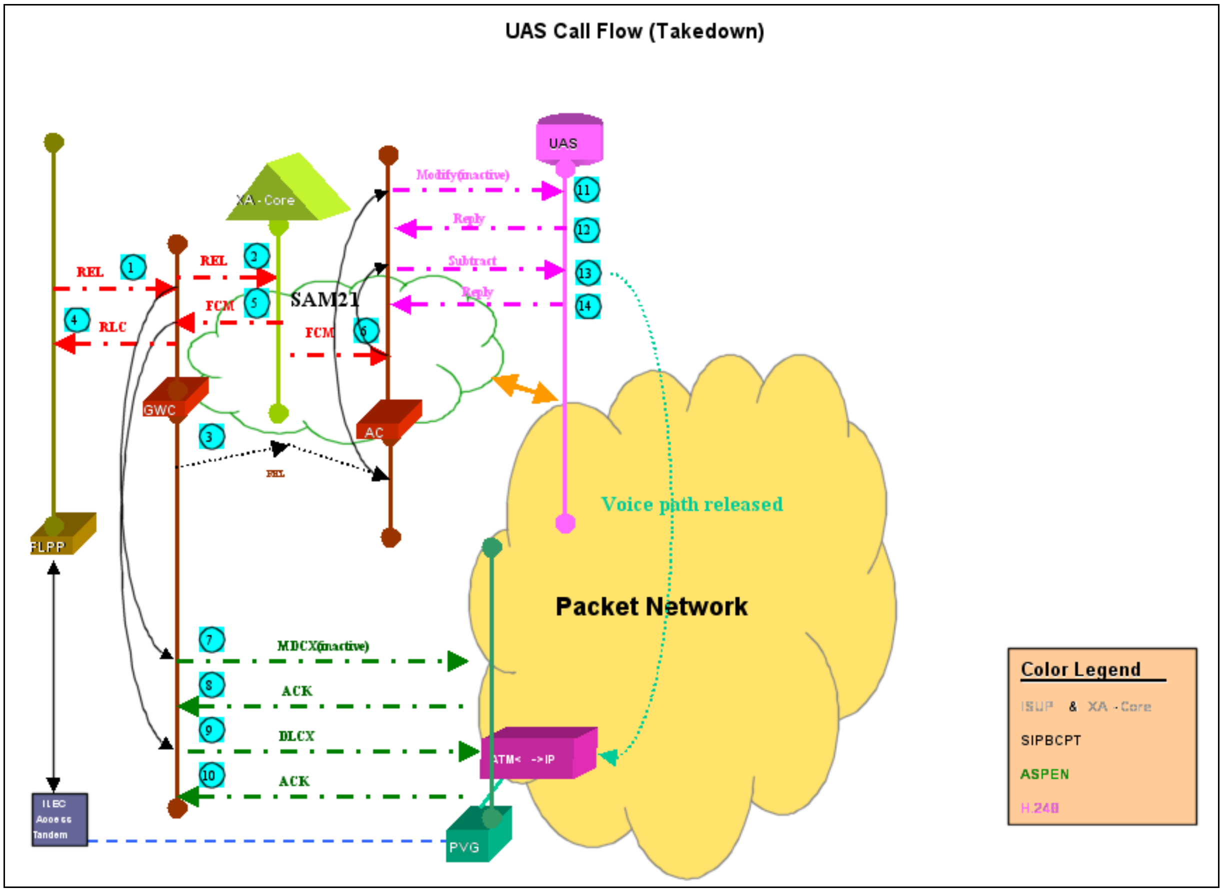
Announcements are provision in the translation tables in the same manner as existing TDM Announcements).

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 Media Gateway to establish a bearer connection across the packet network.
8. The Media Gateway 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 Media Gateway.
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 Media Gateway.
14. The Media Gateway 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 Carrier VoIP Network. Based upon data from table C7TRKMEM, the FLPP maps the CIC of the REL to the corresponding DS0 circuit on the Media Gateway 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 Media Gateway.
8. The Media Gateway 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 Media Gateway.
10. The Media Gateway 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.

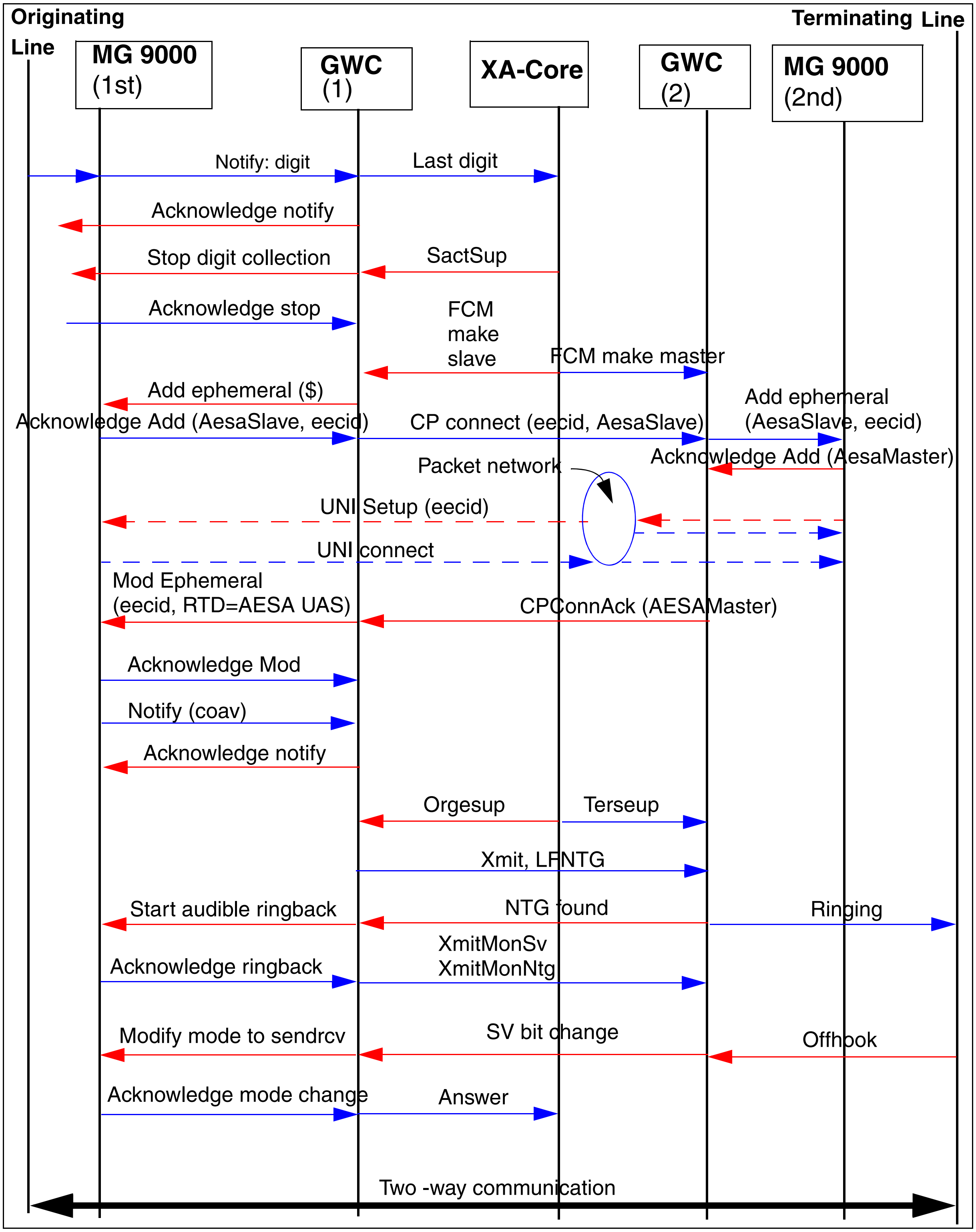
Call processing for UA-IP

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

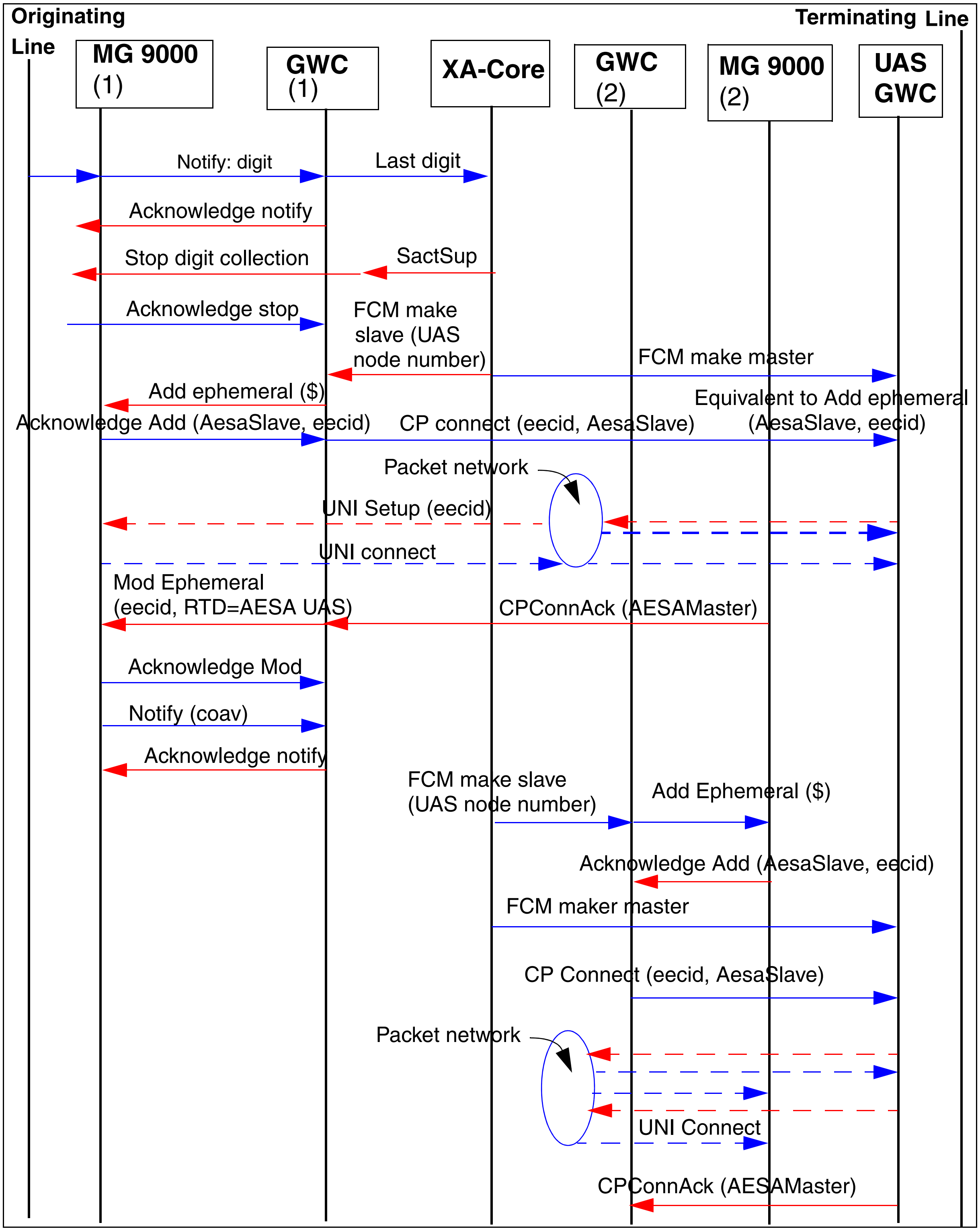
The figure MG 9000 to MG 9000 call setup shows a call walk through for a call that originates on one MG 9000 and terminates on another MG 9000.

MG 9000 to MG 9000 call setup

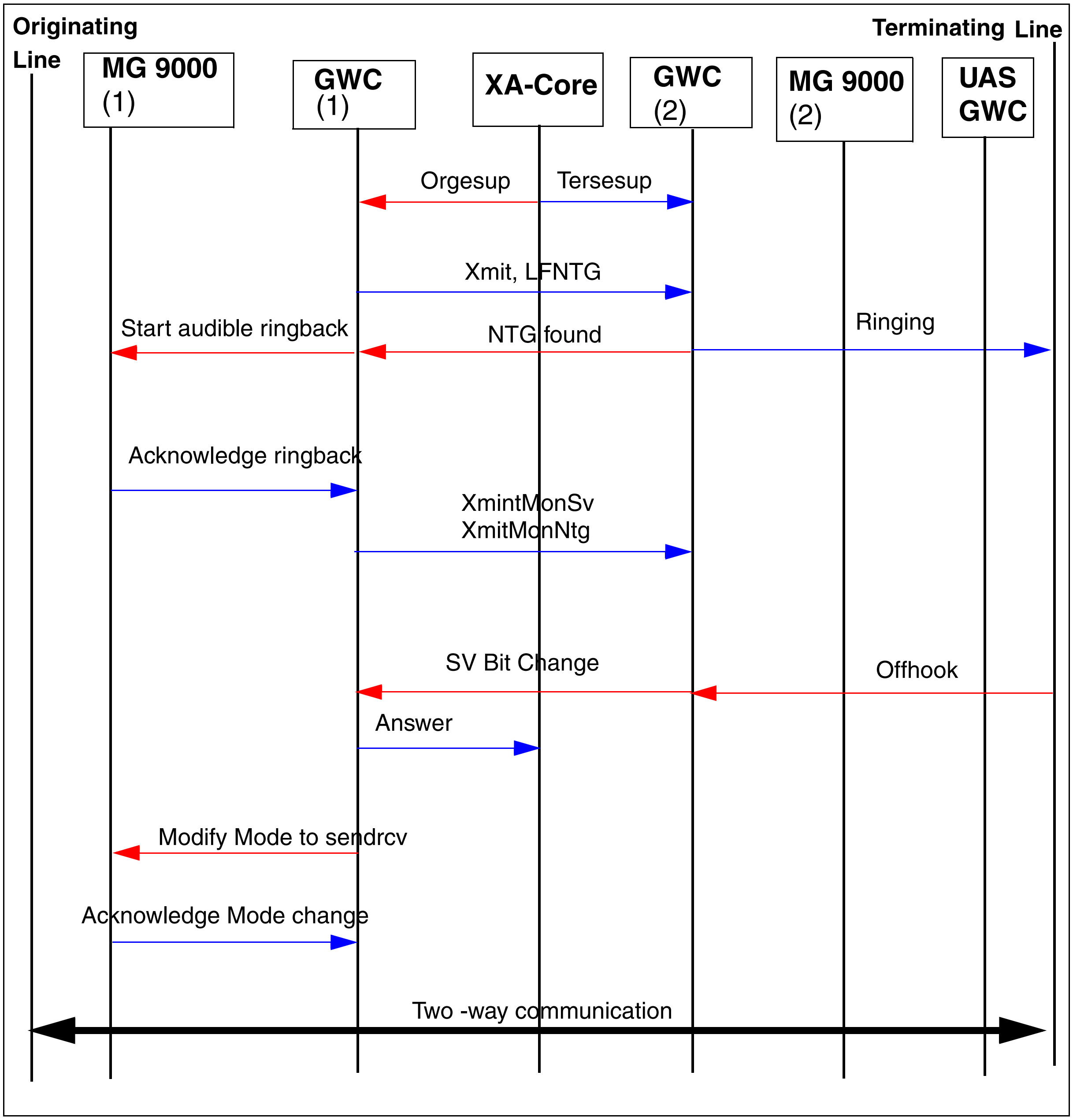


The figure MG 9000 to MG 9000 call setup with Lawful Intercept (part 1 of 2) shows a call walk through for an intercepted call (Lawful Intercept) that originates on one MG 9000 and terminates on another MG 9000.

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.

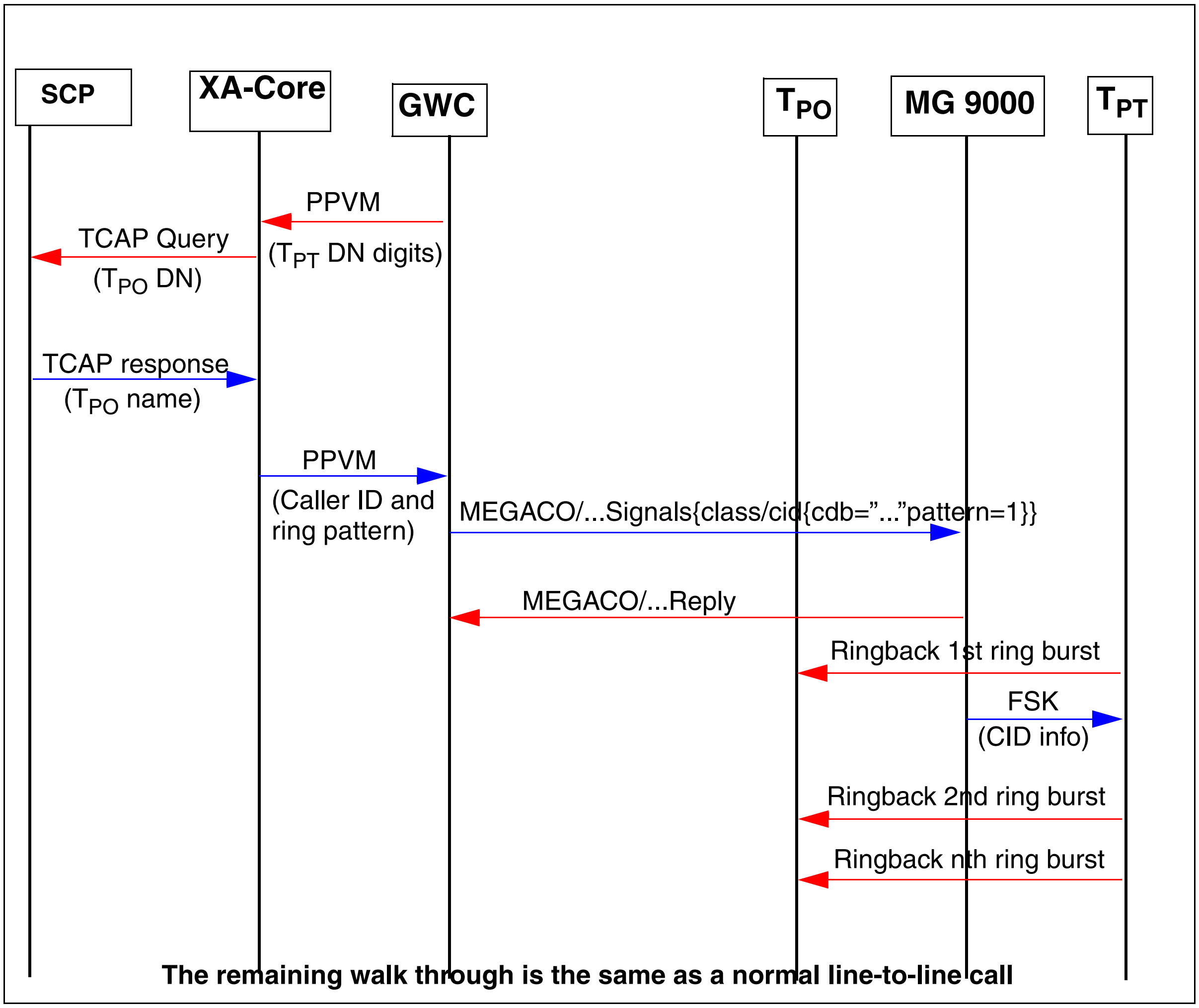
Note 1: The walk through for Calling Number Delivery (CND) or Calling Name Delivery (CNAMD), and Calling Number Delivery

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.

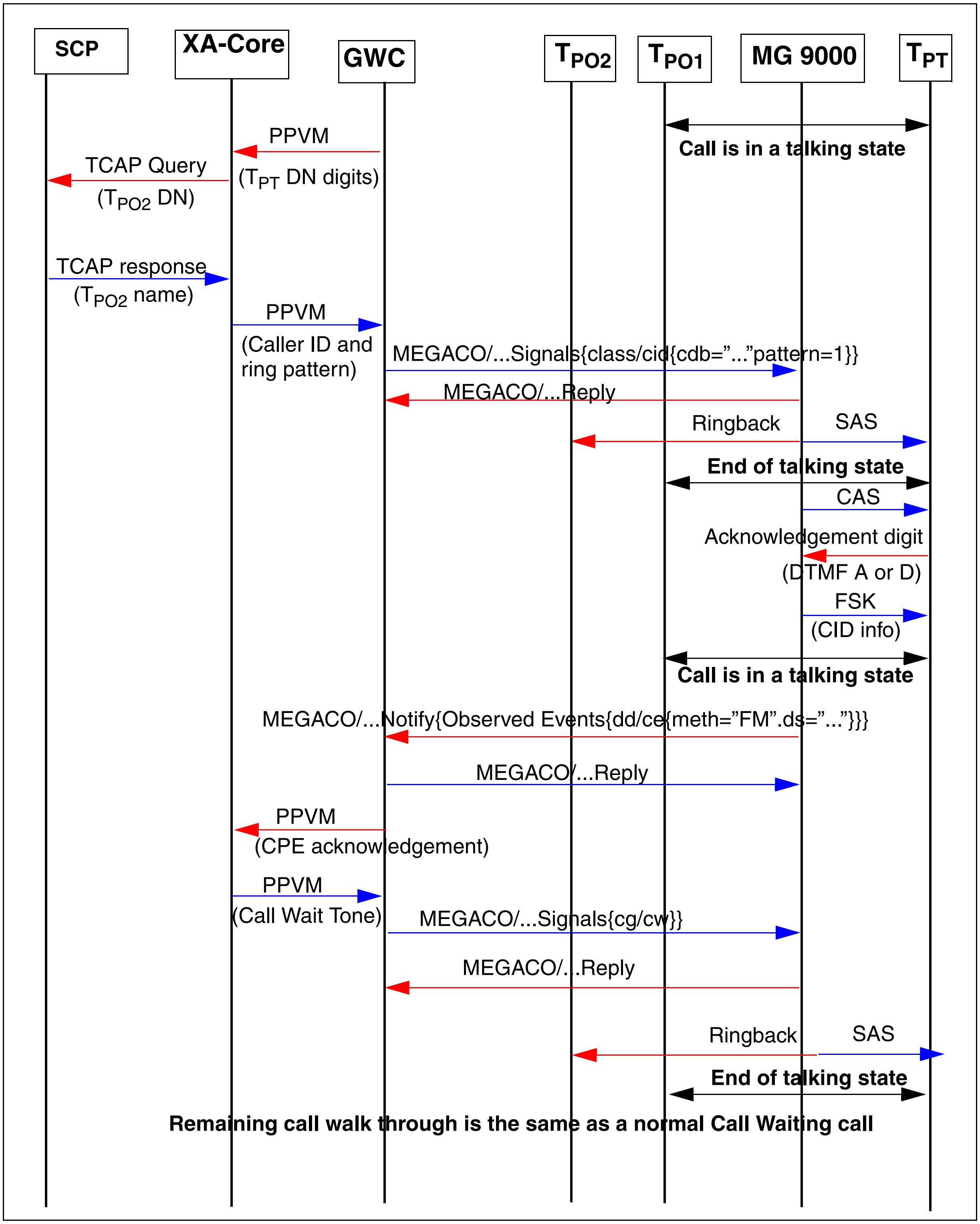
Note 1: The Megaco message for SCWID is identical to Caller ID. This Megaco message is distinguished by the MG 9000 by means of the switch hook status of the line.

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.

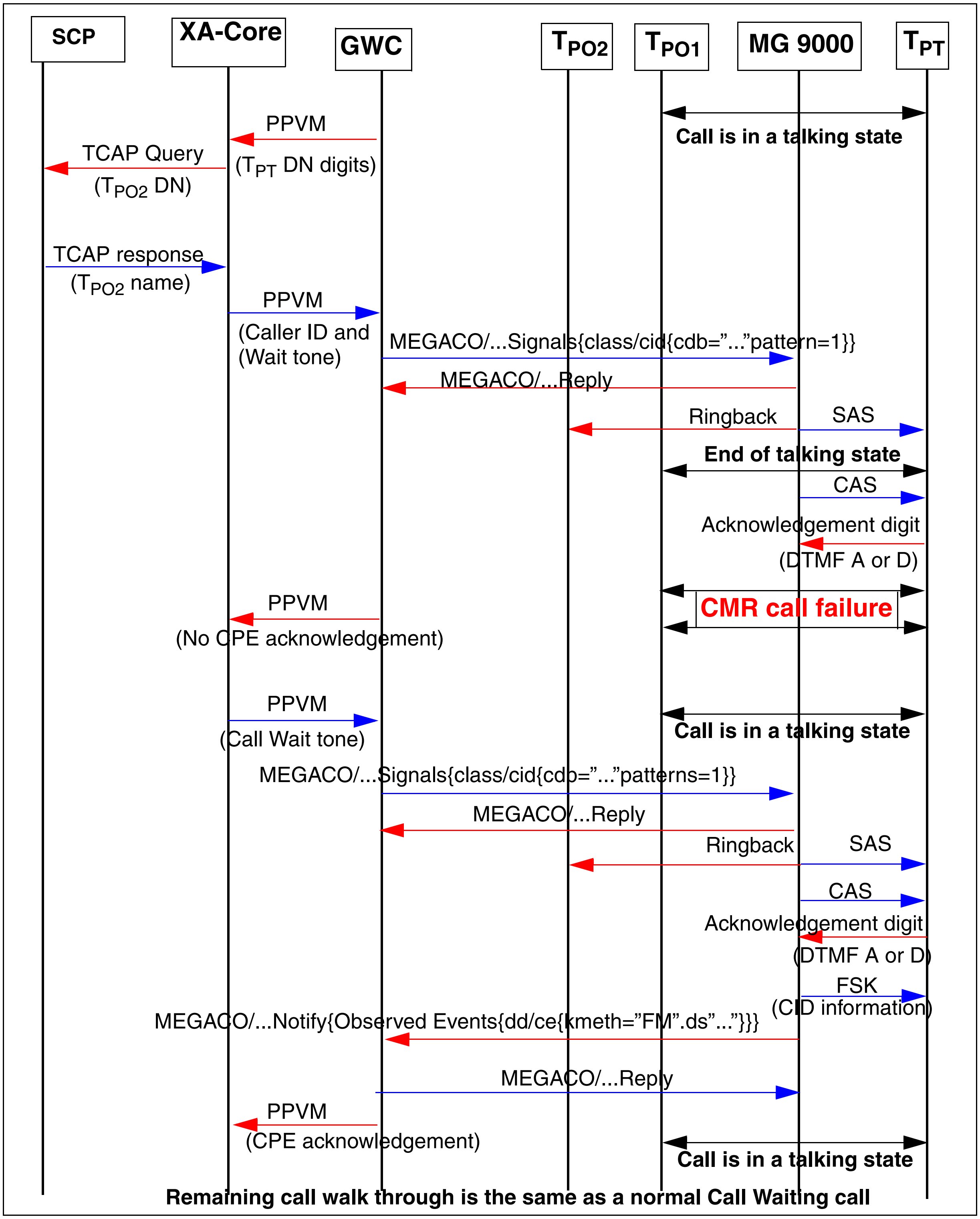
Intra MG 9000 POTS call involving SCWID



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.

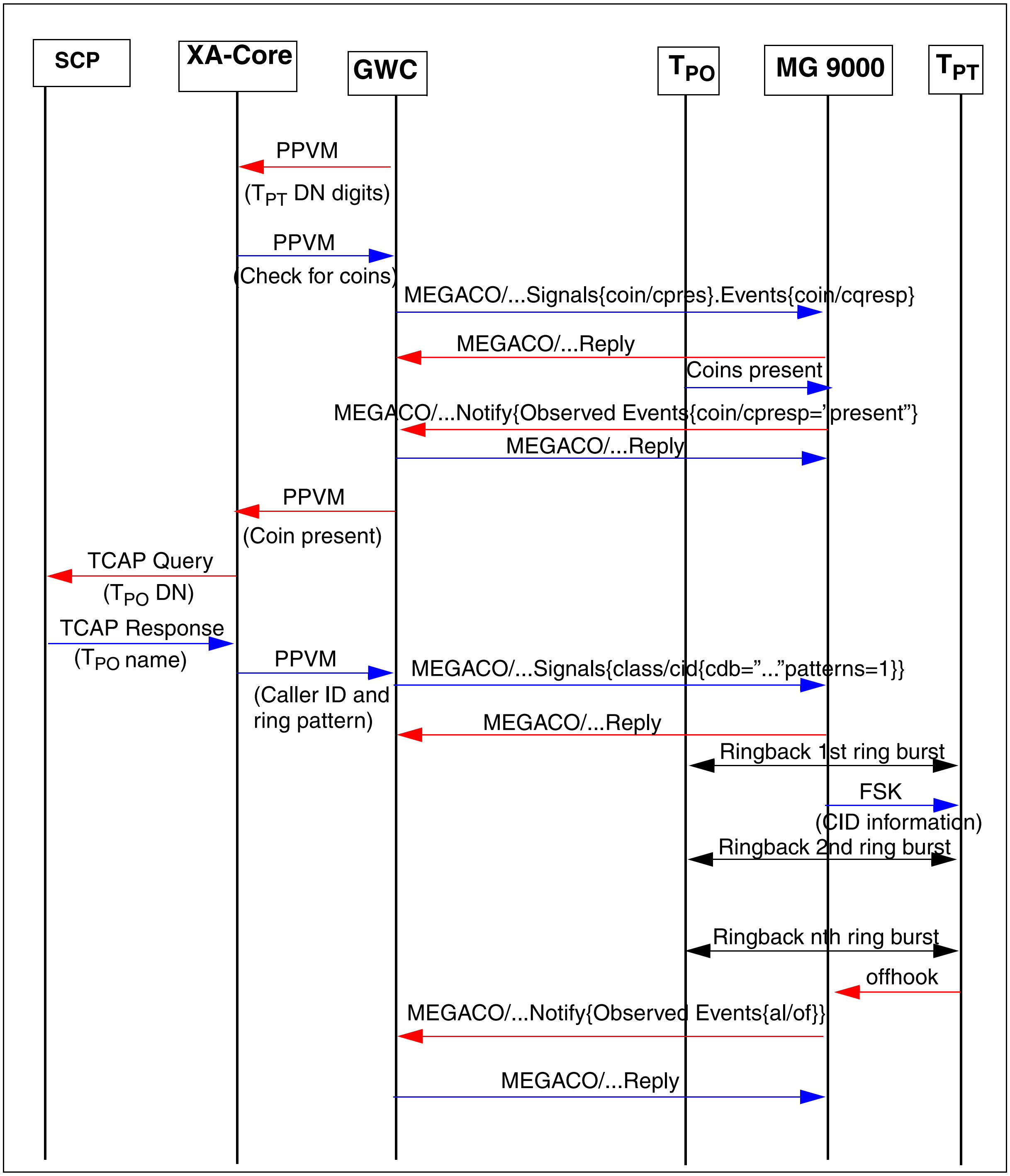
Intra MG 9000 POTS call failure involving SCWID



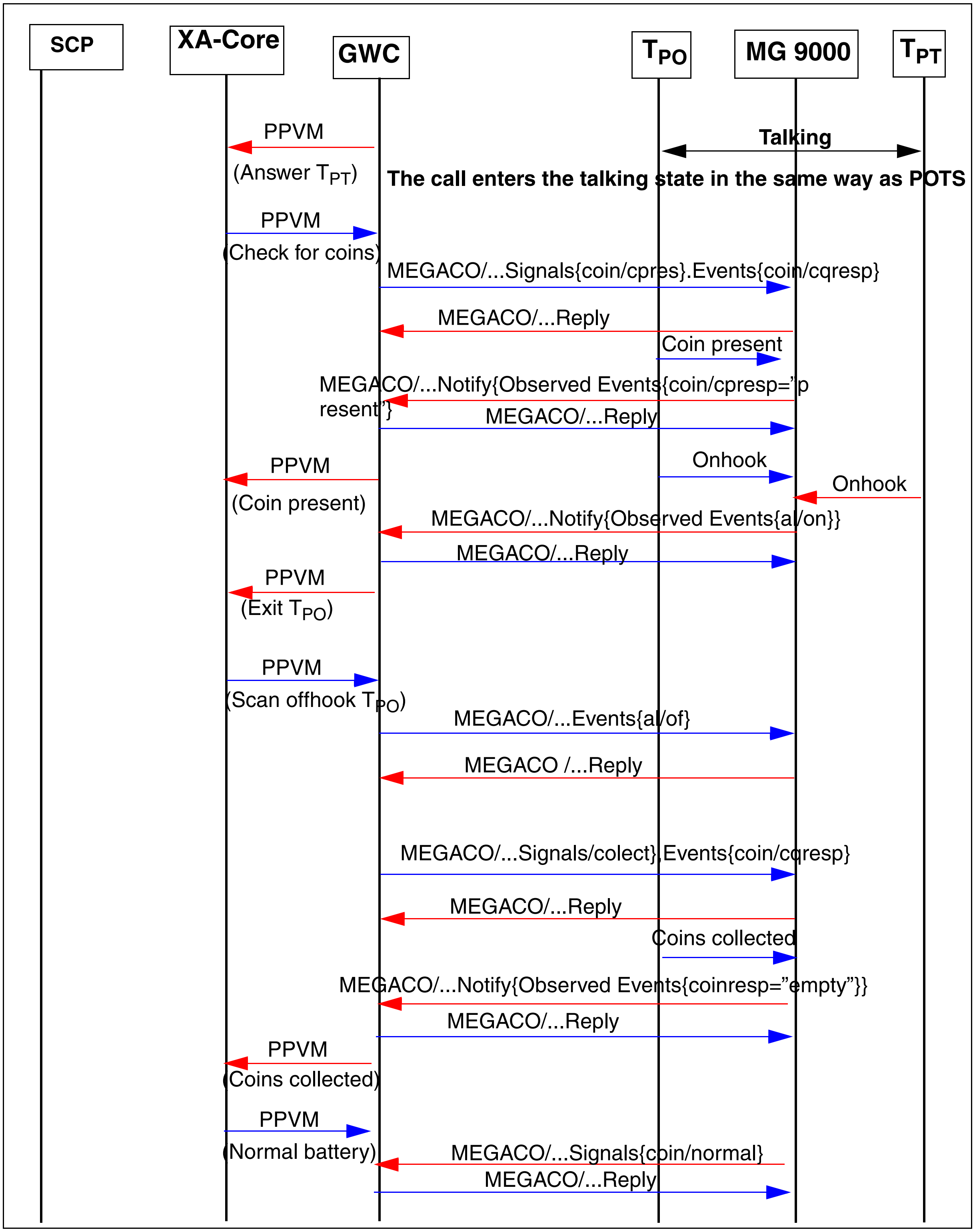
UA-IP Intra MG 9000 coin call

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)



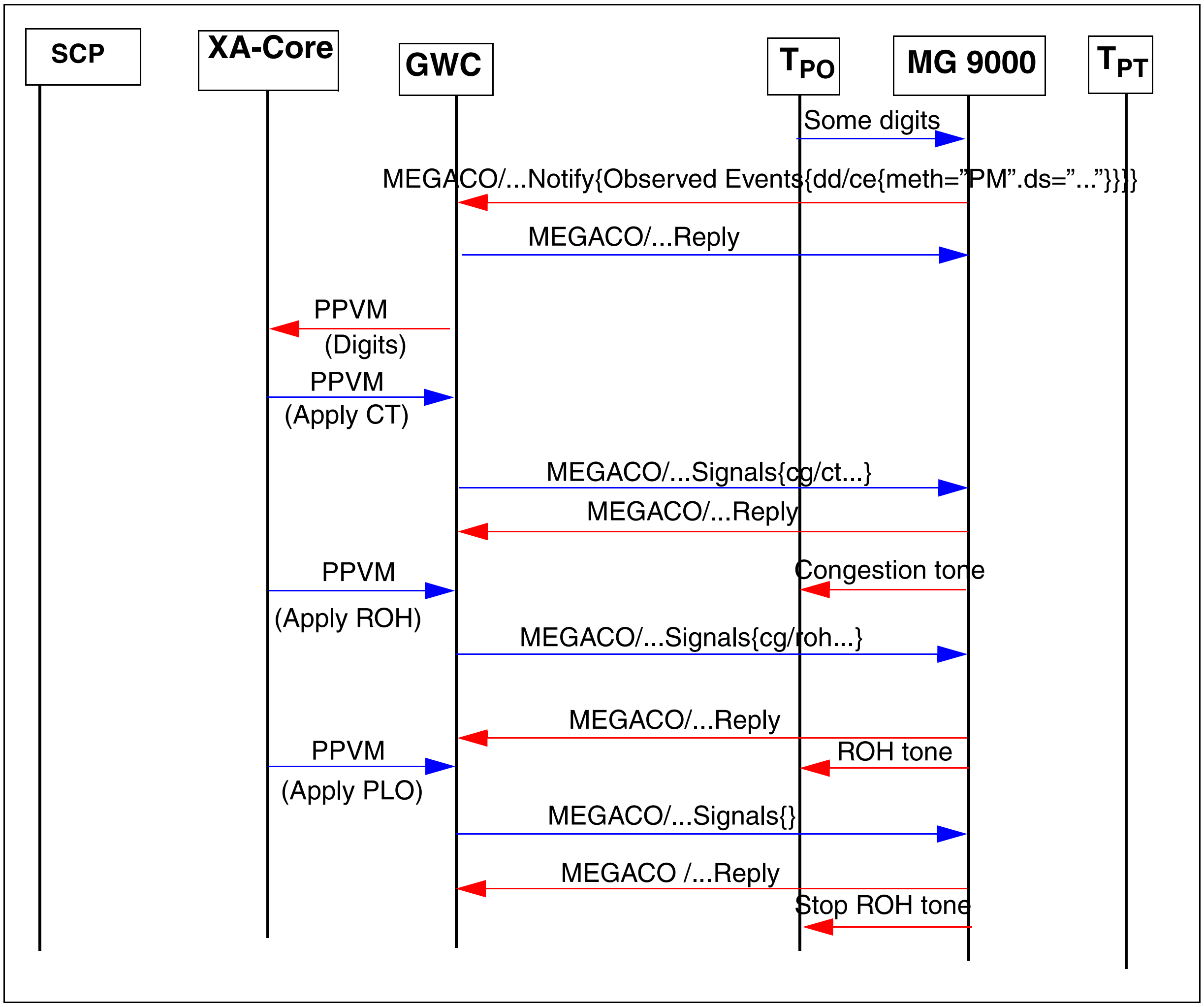
Intra MG 9000 coin call (part 2 of 2)



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

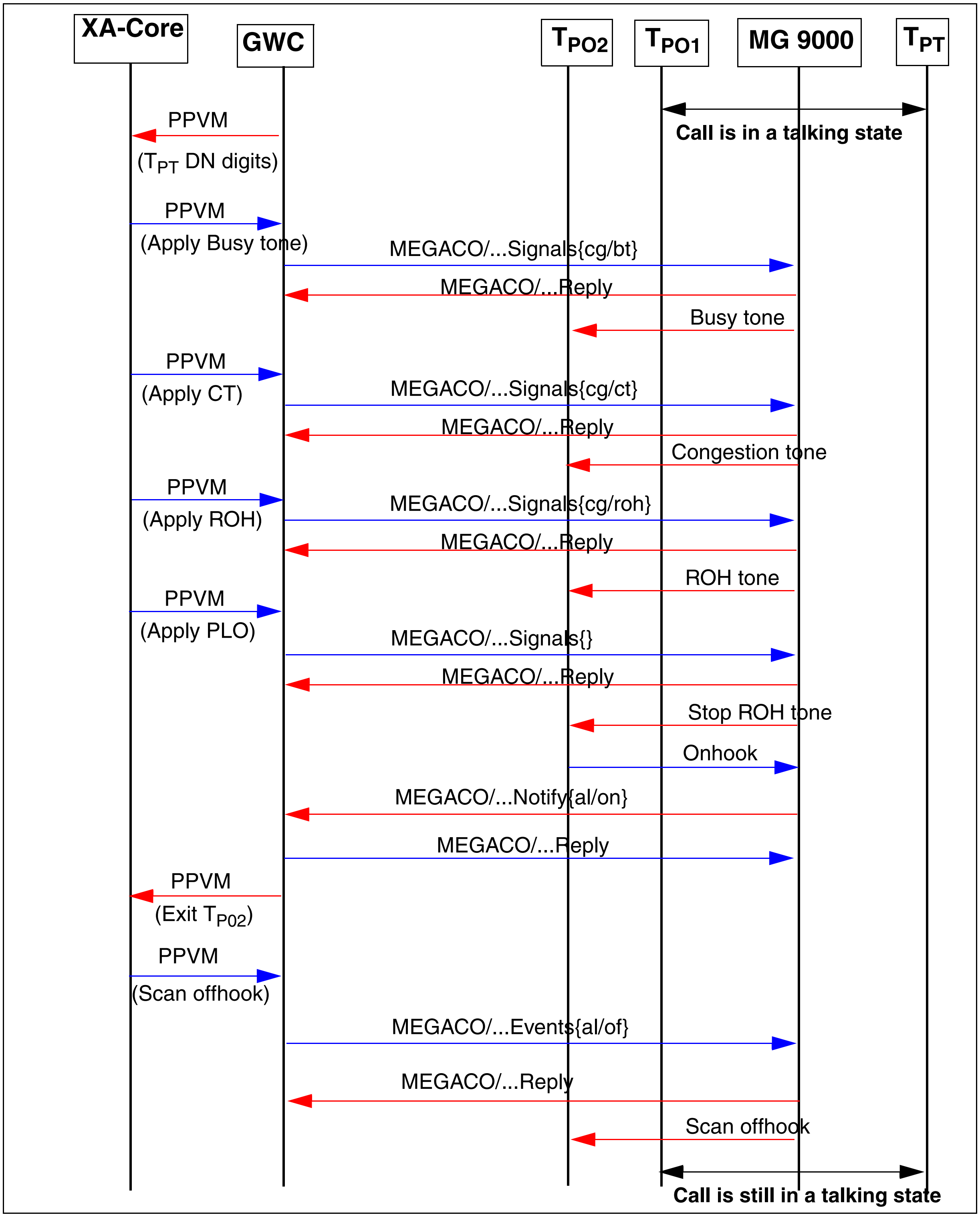
The figure Intra MG 9000 call involving routing to a local treatment shows a call walk through for a plain old telephone service (POTS) call involving a failure and partial dial treatment. This call originates and terminates on the same MG 9000 and uses three separate lines.

> ***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



Hardware

This chapter describes the UA-IP Solution hardware components. The chapter contains the following sections:

CS 2000 configurations

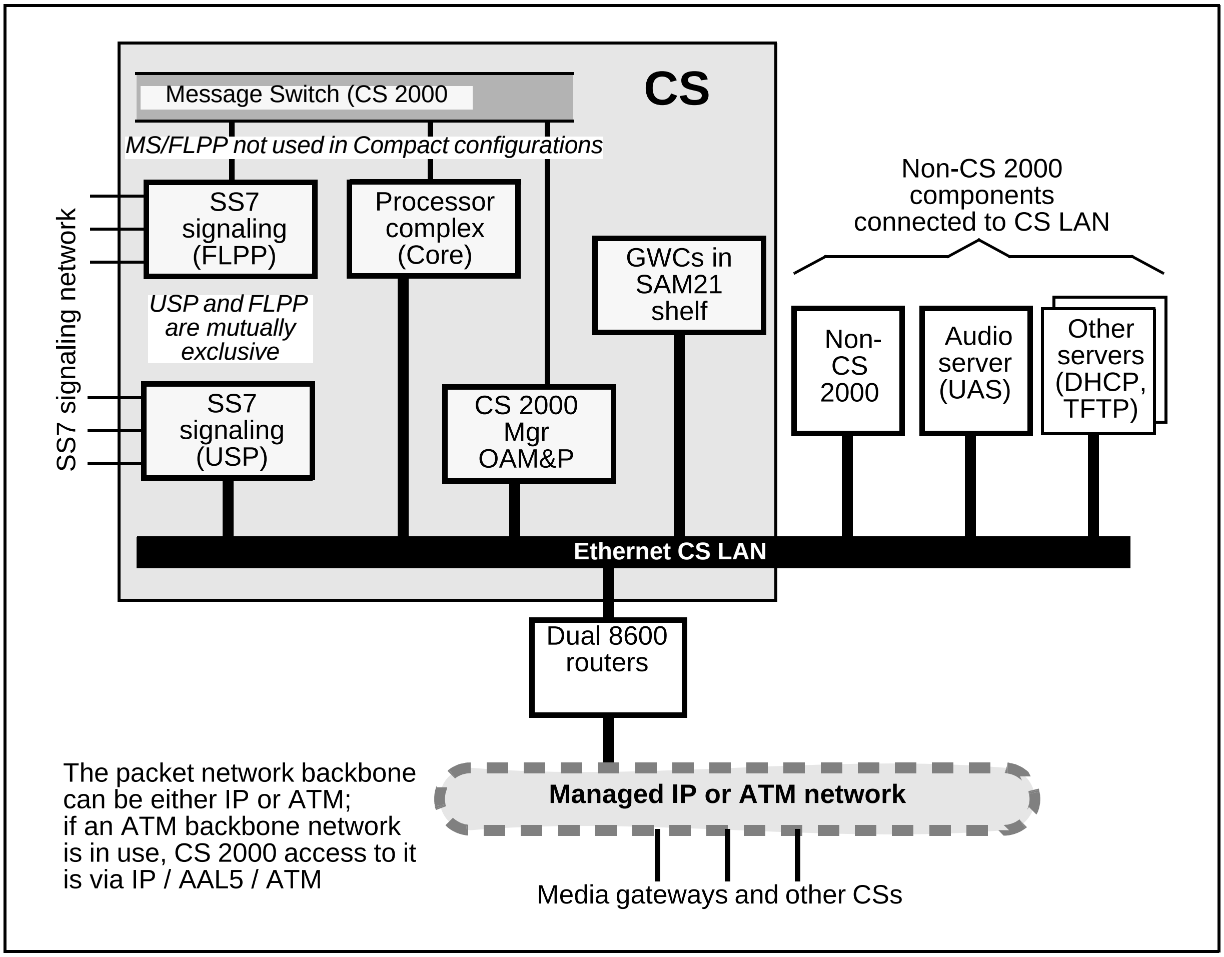
The UA-IP Solution supports two types of communication server: the standard CS 2000 configuration and the CS 2000-Compact. The two configurations are based on different processing platforms but have certain hardware items in common, as described in the following sections.

Standard CS 2000 configuration

In the standard CS 2000, most call processing and feature support is provided by the central XA-Core processor complex. Specialized processing is delegated where possible to peripherals and gateway controllers (GWC) ensuring that optimum use is made of XA-Core capacity.

The figure Functional overview of CS 2000 hardware and the CS LAN on page 134 provides a functional view of the interaction between the major hardware components that make up a complete CS 2000. As shown, most intra-CS 2000 communication uses the Communication Server (CS) LAN, a subnetwork that is connected to the external managed IP network via dual Ethernet Routing Switch 8600 routers (see section CS LAN and Ethernet Routing Switch 8600 routers on page 144).

Functional overview of CS 2000 hardware and the CS LAN


CS
Message Switch (CS 2000
MS/FLPP not used in Compact configurations
SS7 signaling network
SS7 signaling (FLPP)
USP and FLPP are mutually exclusive
SS7 signaling (USP)
Processor complex (Core)
CS 2000 Mgr OAM&P
GWCs in SAM21 shelf
Non-CS 2000 components connected to CS LAN
Non-CS 2000
Audio server (UAS)
Other servers (DHCP, TFTP)
Ethernet CS LAN
Dual 8600 routers
Managed IP or ATM network
Media gateways and other CSs
The packet network backbone can be either IP or ATM; if an ATM backbone network is in use, CS 2000 access to it is via IP / AAL5 / ATM

XA-Core

The Extended Architecture Core (XA-Core) is the CS 2000 central computing engine. The XA-Core software load contains call processing agents for supported TDM telephony interfaces, together with service logic for the delivery of value-added features and services over those interfaces. It also comprises software for controlling packet network bearer connections established via GWCs and gateways.

XA-Core design is based on the principle of using independently scalable subsystems to deliver call processing capacity. The XA-Core subsystems are:

- Processor subsystem
  (I)SN08 and up supports 3+1 XA-Core sparing, i.e. four active load-sharing processor elements (PE). This configuration leaves

any one PE theoretically spare and gives the system the ability to survive a PE failure.

- Shared memory
  Memory is provided by mated pairs of 32 Mbyte memory blocks, each storing duplicated data, so that one copy of the data is retained in the event of a memory failure. In (I)SN08 and up, the maximum XA-Core shared memory is 1728 Mbytes.
- Input/output processors
  - — Ethernet ports for TCP/IP communication over the CS LAN with SAM21 shelves housing GWCs. XA-Core is equipped with two HIOP (High-capacity IOP) cards, providing two pairs of active/standby Ethernet connections.
  - — disk storage with capacity of 4 Gbytes
  - — tape storage (DAT) with capacity of 1.3, 2 or 4 Gbytes

Links between subsystems (bus capabilities) are provided by a set of independent communication links known as the Extended Architecture Interconnect (XAI).

Message switch (CS 2000 bus)

The CS 2000 bus supports peer-to-peer messaging between XA-Core, the FLPP and the optional OAU (not between XA-Core and GWCs, which are connected via 100BaseT Ethernet). It also provides the TDM-side system clock and communication to the XA-Core manager (SuperNode Data Manager) via DS512. The bus consists of two identical load-sharing planes called Message Switches (MS) each with the capacity and connectivity to support the full internal messaging load if the other plane fails.

FLPP signaling peripheral

The Fiberized Link Peripheral Processor (FLPP) provides a platform for terminating TDM-side SS7 signalling links and extracting the contents of MTP Signalling Units (MSU) so that they can be appropriately handled by XA-Core and GWCs, e.g. extracting ISUP or TUP messages for translations and routing.

> ***Note 1:*** The FLPP is not involved in any way in the handling of call control signalling for PRI or lines.
>
> ***Note 2:*** The connection to the SS7 network can be via either the FLPP or the USP (see section Universal Signaling Point on page 139).

An FLPP cabinet houses two types of hardware unit:

- Up to three Link Interface Shelves (LIS) each providing 12 slots for housing Interface Units (IU). IUs are the circuit packs supporting the various applications on the FLPP, and are therefore also referred to as Application-Specific Units (ASU).
- A Link Interface Module (LIM) that supports
  - — direct high-speed communication between IUs
  - — SR128 subrate optical fiber links with CS 2000-bus for conveying signalling messages to and from the CM
  - — DS30 for non-fiberized LPP

A CS 2000 configuration can include up to five FLPP cabinets.

The FLPP supports circuit-oriented (includes a bearer channel) SS7 signalling terminations for ETSI ISUP, ANSI ISUP, national ISUP and national TUP interfaces. The FLPP also supports circuit-independent (no bearer channel) SS7 signalling terminations for TCAP interfaces.

Each signalling channel terminates on a Link Interface Unit for SS7 (LIU7) in an FLPP. The interface between the LIU7 and the external multiplexer is V.35, controlled by a 9X77 paddleboard in the FLPP.

All 12 slots on each FLPP shelf are available for LIU7s terminating external SS7 signalling links, which means that one FLPP cabinet can support a maximum of 36 signalling links. A CS 2000 can support up to 180 SS7 signalling links.

> ***Note:*** The channelized access configuration is also supported (with no external multiplexer, an NIU/MLIU interface and DS0), in addition to the non-channelized configuration described above.

Service Application Module Frame

The Service Application Module Frame (SAMF) is deployed in a PTE2000 equipment cabinet and houses the following equipment:

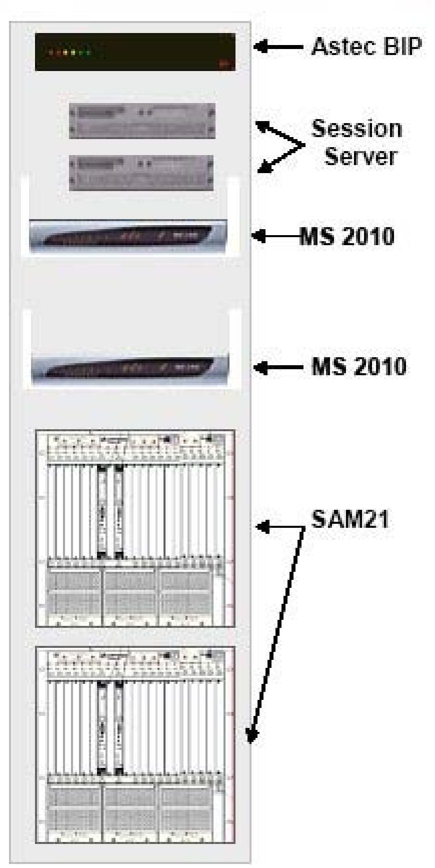
- Enhanced Breaker Interface Panel (EBIP) that provides the main power feed to the frame
- a mix of SAM16 chassis, SAM21 chassis, Media Server 2000 chassis, and Ethernet switches
-

The SAMF can house the following equipment configurations:

- 1 to 2 SAM16 chassis with up to three Ethernet switches
- 1 to 3 SAM21 chassis
- 1 to 2 SAM21 chassis with 1 SAM16 chassis
- 1 to 2 SAM21 chassis with up to 6 Media Server 2000 chassis

The following figure shows an example SAMF configuration.

Example SAMF configuration



SAM21 chassis

Each SAM21 chassis is a rack-mountable server based on a Motorola CPX8221 cPCI platform. The CPX8221 platform is a 21-slot shelf, managed by a resident pair of duplex redundant system slot CPU cards (shelf controllers). The SAM21 server for the CS 2000 contains the following cards:

- one pair of SAM21 shelf controller unit (SCU) cards

  The shelf controllers monitor the hardware state of all the cards in the shelf, and provide the mechanism for hardware diagnostics and maintenance activities on the hardware in the shelf. The shelf controllers also monitor the software state of the cards in the shelf and automatically recover cards that experience an application failure.

For more detailed information on the SAM21 SC, refer to *SAM21 Shelf Controller Basics*, NN10025-111.

- up to 8 pairs of GWC cards

  A GWC consists of two separate GWC cards, one active and one inactive. The two cards that make up a given GWC need not be adjacent. They can occupy any of the SAM21 shelf slots reserved for GWC cards, i.e. a GWC comprises two cards, but it is not physically a twin-card unit.

  For more detailed information on the GWC, refer to *GWC Basics*, NN10189-111.

Media Server 2000 chassis

The MS 2000 series 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.

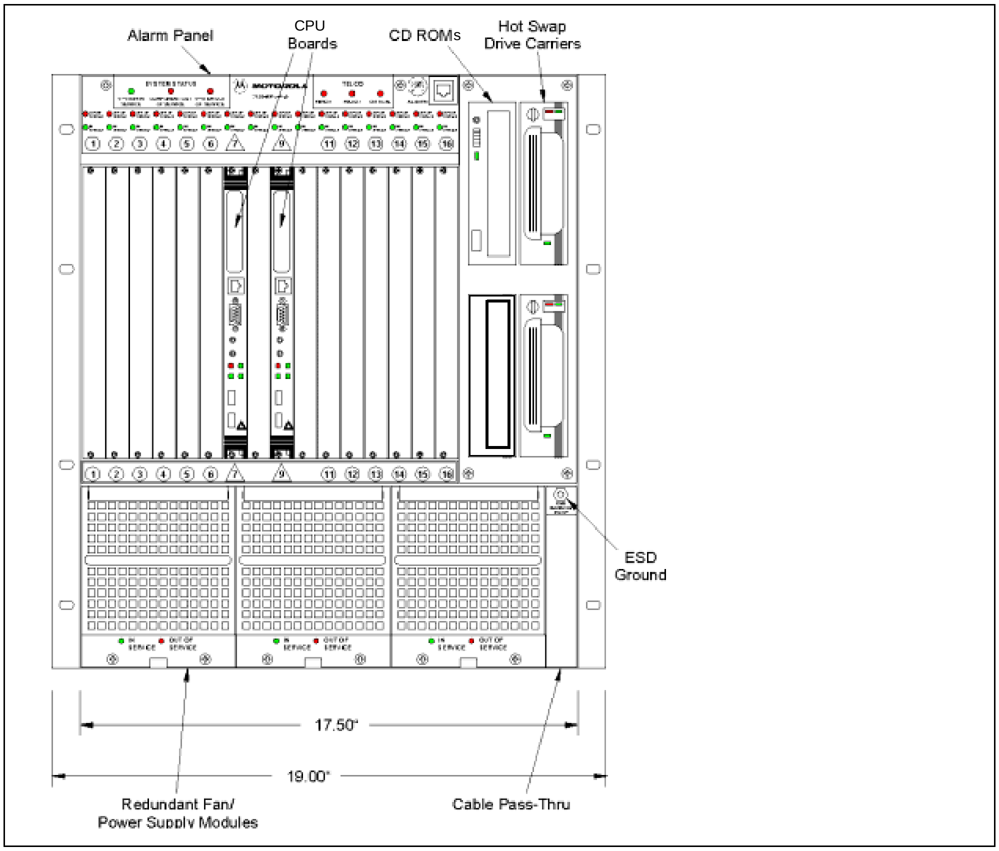
Although the MS 2000 Series IPM-1610 board occupies only one slot in the IPmedia 2000 chassis, it consists of two separate, logical media gateway modules from an OAM&P management perspective. Each module has its own MAC address and IP address. Both modules share a redundant LAN connection through an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

For more detailed information on the MS 2000 series, refer to *MS 2000 Series Basics*, NN10323-111.

SAM16 chassis

The UAS is housed in a SAM16 (16-slot chassis). The figure SAM16 chassis external components and functions - front view on page 139 shows a typical SAM16 chassis.

SAM16 chassis external components and functions - front view



Each chassis consists of two independent domains, which contain the following equipment:

- 8 card slots front and rear
- hard disk drive
- DVD drive
- floppy drive

For more detailed information on the SAM16 chassis, refer to *UAS Basics*, NN10010-111.

Universal Signaling Point

The Universal Signaling Point (USP) shelf can be housed either in an industry-standard 19” frame or in the same type of PTE2000 frame used to house CS 2000-Compact components.

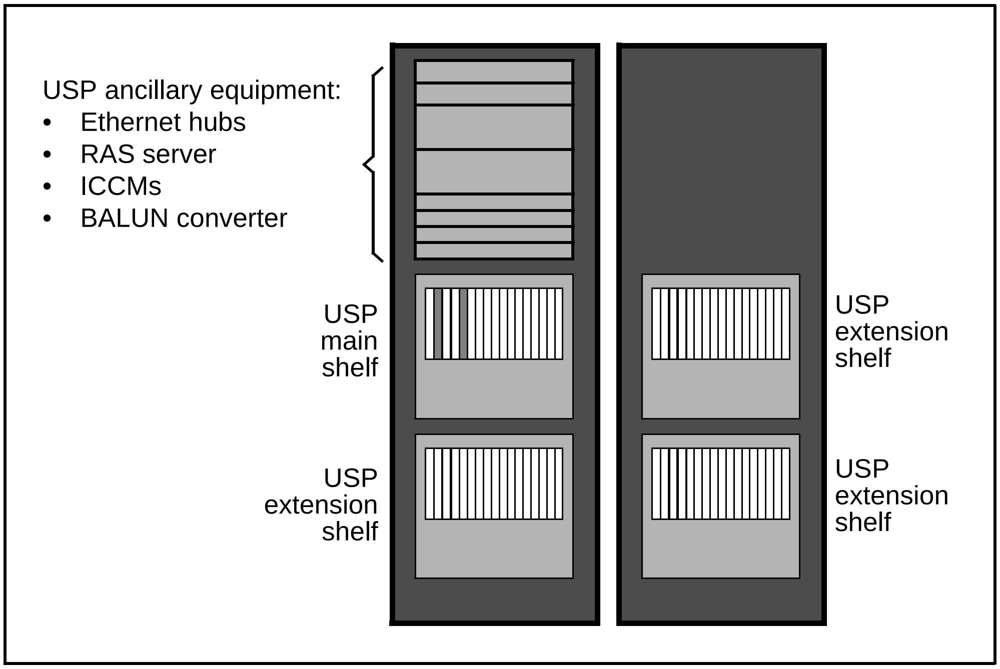
A CS 2000 supporting the maximum of 328 SS7 signaling links by means of the USP requires one USP main shelf and three USP extension shelves. These are housed in two adjoining frames, with two

USP shelves in each frame. The space above the USP shelves in the frame housing the USP main shelf contains:

- Twin 10BaseT Ethernet hubs, each with 12 ports
- Remote Access Server (RAS) supporting OAM&P access for the USP manager
- Twin ICCM (Inter-CC Modules) supporting communication between shelf CCs
- Balanced/Unbalanced (BALUN) line and impedance converter for coax cable termination, enabling E1s to be transported over coax.

The figure USP hardware packaging shows the above configuration example.

USP hardware packaging



For more detailed information on the USP, refer to *USP Basics,* NN10008-111.

Integrated Services Module (ISM)

The Integrated Services Module (ISM) is a specialized module designed to accommodate test and service circuit packs used in switch and facility maintenance. In a CS 2000 configuration, the ISM is used to house Input/Output Modules (IOM). These provide ports for serial input and output, enabling local and remote devices to communicate with the rest of the CS 2000 via the CS 2000 Message Switch. CS 2000

IOMs support the datalinks used to bring into service the SDM platform (for CS 2000 component managers) and the CS 2000.

An ISM cabinet has four shelves. In a CS 2000 configuration, two of these shelves provide slots to house IOMs (each shelf has 18 slots). The other two shelves are left empty unless the configuration includes the optional OAU, in which case they are used as follows:

- one shelf is used for the Office Alarms Unit (OAU)
- one shelf is used for the Alarms Cross-Connect Unit (AXU)

Optional CS 2000 hardware: the OAU

The Office Alarms Unit (OAU) can be used to connect a CS 2000 with the office alarm system to provide notification of physical or electrical problems.

The OAU is a single-shelf peripheral that is housed in an Integrated Service Module (ISM) cabinet. It is directly connected to the Enhanced Network (ENET), which is in turn connected to the MS to support communication between the OAU and XA-Core.

CS 2000-Compact

The Communication Server 2000-Compact (CS 2000-Compact) is a full-featured softswitch which provides call processing capabilities such as routing, translations, and centralized service delivery. Built on a compact PCI (cPCI) chassis, the CS 2000-Compact incorporates a Linux operating system. The cPCI shelves house blades, which perform call agent and gateway controller functions.

The CS LAN, implemented by dual Ethernet Routing Switch 8600 routers, provides the interface between the CS 2000-Compact and the IP bearer network (see section CS LAN and Ethernet Routing Switch 8600 routers on page 144 for details). The Universal Signaling Point (USP) or the USP-Compact connects the CS 2000-Compact to the SS7 signaling network (see section Universal Signaling Point on page 139 for details).

Call Control Frame

The Call Control Frame (CCF) is deployed in a PTE2000 equipment cabinet that houses the following equipment:

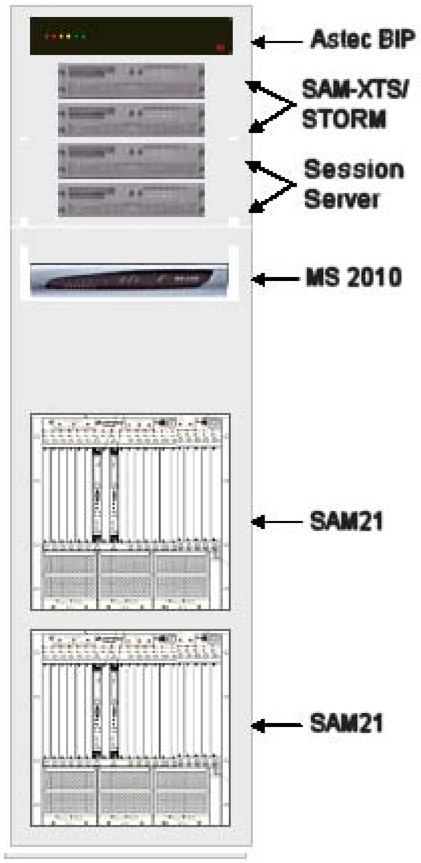
- Enhanced Breaker Interface Panel (EBIP) that provides the main power feed to the frame
- a mix of SAM21 chassis, Media Server 2000 chassis, and STORM chassis
-

The CCF can house the following equipment configurations:

- 1 to 2 SAM21 chassis
- 1 to 2 SAM21 chassis, 1 to 6 Media Server 2000 chassis, and 1 STORM chassis

The following figure shows an example CCF configuration.

Example CCF configuration



SAM21 chassis

Each SAM21 chassis is a rack-mountable server based on a Motorola CPX8221 cPCI platform. The CPX8221 platform is a 21-slot shelf, managed by a resident pair of duplex redundant system slot CPU cards (shelf controllers). The SAM21 server for the CS 2000-Compact contains the following cards:

- one Call Agent card

  The Call Agent card provides the call-processing services for the CS 2000-Compact. Each card has two 10/100 BaseT Ethernet ports.

  For additional information on the Call Agent, refer to *Call Agent Basics*, NN10023-111.

- one NFS card (STORM cPCI only)

  Each Call Agent writes data to both STORM units for redundancy.

  For more detailed information on the STORM, refer to *STORM Basics*, NN10024-111.

- up to seven pairs of GWC cards

  The GWC cards are responsible for communication between the CS 2000-Compact Call Agent software and the media gateways for call-processing control. Each card contains one 10/100 BaseT Ethernet port.

  For more detailed information on the GWC, refer to *GWC Basics*, NN10189-111.

- if the USP-Compact is used, one USP-Compact blade in each SAM21 shelf

  For more detailed information on the USP-Compact, refer to *USP-Compact Basics*, NN10009-111.

- one pair of SAM21 shelf controller unit (SCU) cards

  The shelf controllers monitor the hardware state of all the cards in the shelf, and provide the mechanism for hardware diagnostics and maintenance activities on the hardware in the shelf. The shelf controllers also monitor the software state of the cards in the shelf and automatically recover cards that experience an application failure.

  For more detailed information on the SAM21 SC, refer to *SAM21 Shelf Controller Basics*, NN10025-111.

Media Server 2000 series

The MS 2000 series 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.

Although the MS 2000 Series 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.

For more detailed information on the MS 2000 series, refer to MS 2000 Series Basics, NN10323-111.

STORM

The Storage Manager (STORM) provides persistent disk storage services for the Call Agent (and BOOTP service for the USP-Compact). STORM is available in two hardware implementations:

- STORM cPCI, which uses a Dothill disk array (RAID device) as the persistent data storage device. The disk array holds the Call Agent core load. STORM consists of two Motorola N750 network file server (NFS) cards, one in each Call Agent shelf. The NFS service running on the cards provides access to the RAID device.
- STORM SAM-XTS, which uses a pair of SAM-XTS servers instead of the Dothill disk array and NFS cards. The SAM-XTS servers hold the Call Agent core load. The services provided by STORM SAM-XTS are equivalent to those provided by STORM cPCI.

> ***Note:*** In (I)SN08 and up, two HP servers are used to implement the STORM SAM-XTS (eXtreme Thin Server) platform.

For more detailed information on the STORM, refer to *STORM Basics*, NN10024-111.

Common hardware

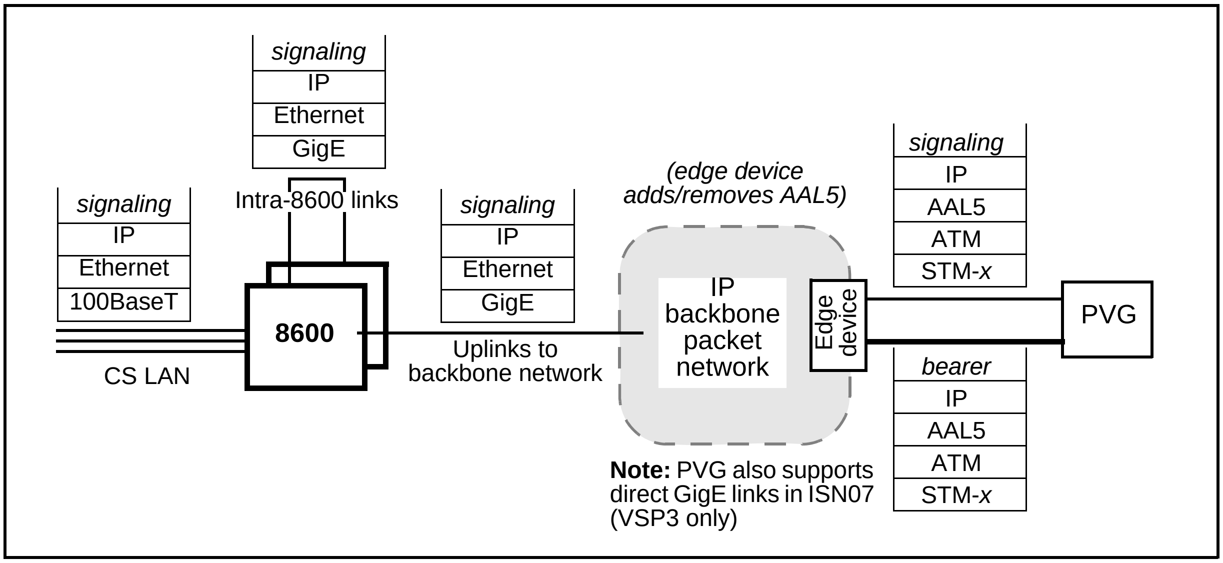
CS LAN and Ethernet Routing Switch 8600 routers

The CS LAN supports Ethernet communication between the GWCs and the other CS 2000 hardware components. The CS 2000 components connected via the CS LAN are:

- standard configuration - GWCs, XA-Core, SDM, USP (if used instead of the FLPP), MS 2000 Series, Session Server, CICM
- Compact configuration - GWCs, Call Agent, SDM, USP or USP-Compact, MS 2000 Series, Session Server, CICM

The CS LAN is based on the Ethernet Routing Switch 8600 router. Each CS LAN has two Ethernet Routing Switch 8600s for redundancy. The figure Connectivity provided by the Ethernet Routing Switch 8600 for the CS LAN on page 145 shows the Ethernet Routing Switch 8600s also provide the interface between the CS LAN and the external managed IP network.

Connectivity provided by the Ethernet Routing Switch 8600 for the CS LAN



Note: PVG also supports direct GigE links in ISN07 (VSP3 only)

For more detailed information on the Ethernet Routing Switch 8600, refer to *Installing Ethernet Routing Switch 8600 Switch Modules*, 312749-F.

Remote access server

A remote access server (RAS) provides the necessary signal format conversions to connect a remote OAM&P workstation to the CAM shelves via a dial-up phone connection.

Ethernet hubs

Two 10/100 BaseT Ethernet hubs provide connections between the CAM shelves and the OAM&P workstation.

Contivity 600

The Contivity 600 VPN switch enables VPN tunneling from a remote location for secure IP remote access. Contivity 600 provides a secure connection by authenticating users, protecting data in transit, and verifying data authenticity. It can provide up to 30 simultaneous authorized connections.

Two options are available for Contivity 600: 56-bit encryption and 128-bit encryption. For more detailed information on Contivity 600, refer to *Reference for the Contivity VPN Switch*, 311643-D.

Gateways

Trunk gateways

The (I)SN08 and up release supports one type of trunk gateway: Media Gateway 15000.

Media Gateway 7400/15000

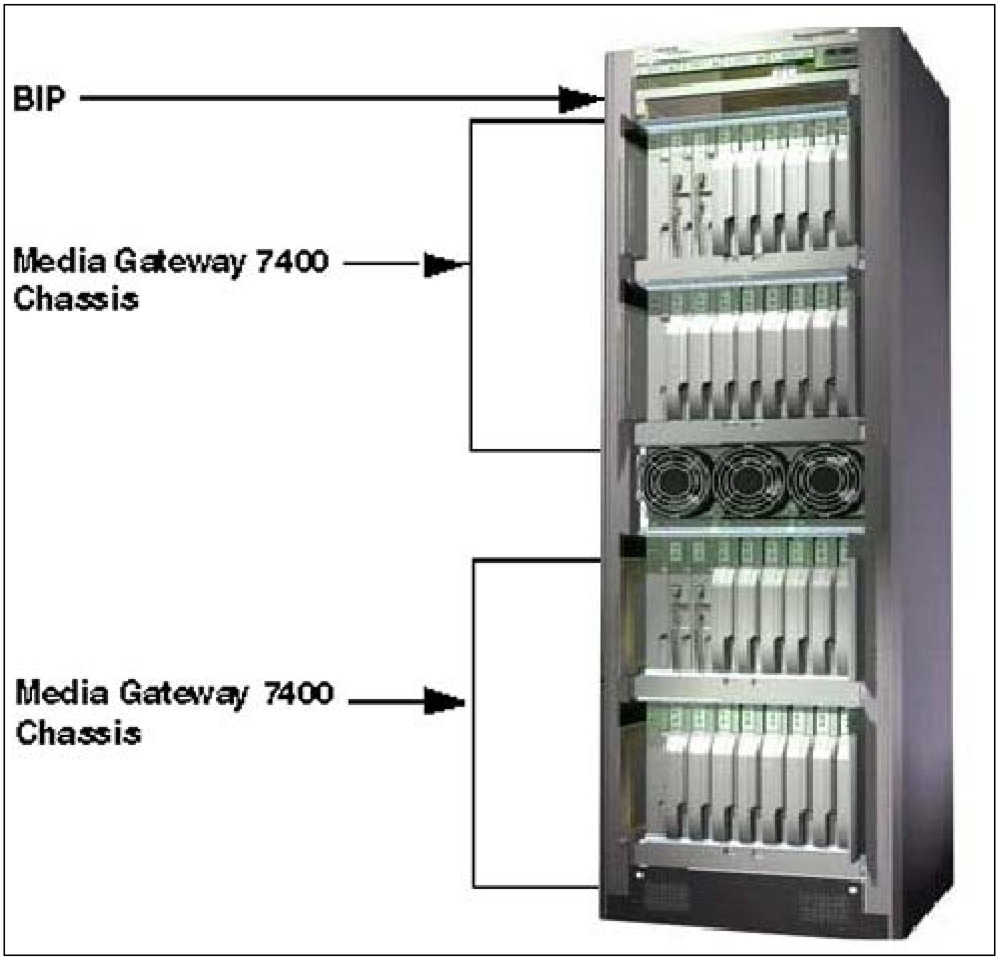
The Media Gateway 7400 is a medium-scale switch that supports up to 8,000 DS0s per frame. The Media Gateway 15000 is a large-scale switch that supports up to 38,000 DS0s per frame.

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



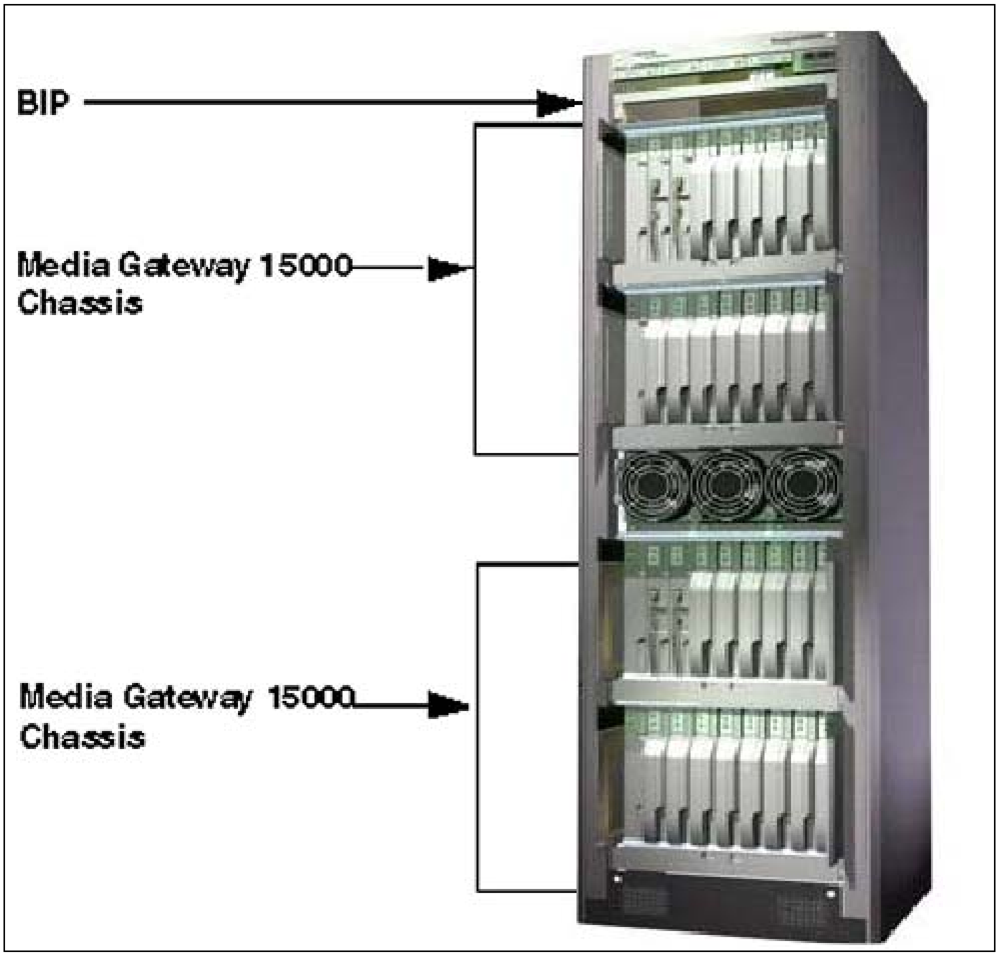
For more detailed information on the Media Gateway 7400, refer to *Nortel Networks Media Gateway 7480/15000 Technology Fundamentals*, NN10600-780.

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



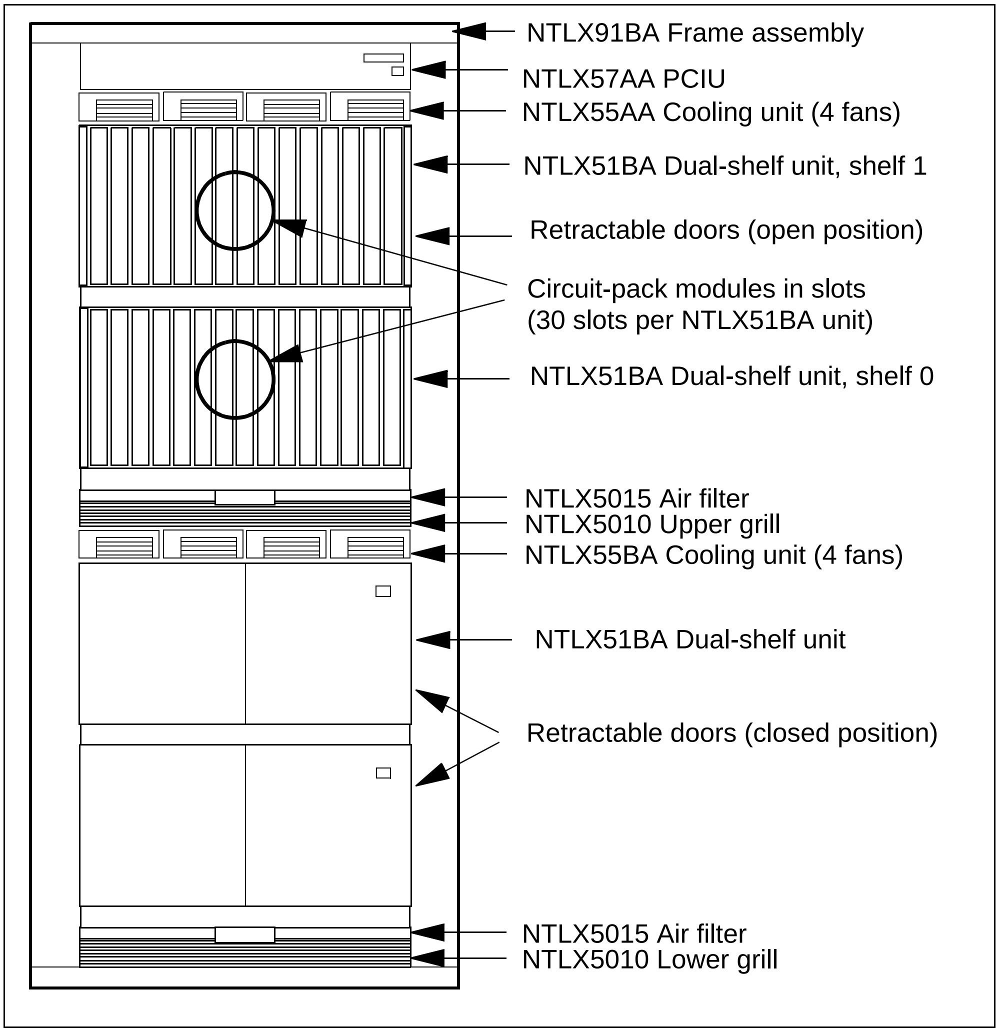
For more detailed information on the Media Gateway 15000, refer to *Nortel Networks Media Gateway 7480/15000 Technology Fundamentals*, NN10600-780.

IW-SPM-IP

The IW-SPM-IP uses the same backplane, shelf, and frame used for the Spectrum Peripheral Module (SPM).

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


NTLX91BA Frame assembly
NTLX57AA PCIU
NTLX55AA Cooling unit (4 fans)
NTLX51BA Dual-shelf unit, shelf 1
Retractable doors (open position)
Circuit-pack modules in slots
(30 slots per NTLX51BA unit)
NTLX51BA Dual-shelf unit, shelf 0
NTLX5015 Air filter
NTLX5010 Upper grill
NTLX55BA Cooling unit (4 fans)
NTLX51BA Dual-shelf unit
Retractable doors (closed position)
NTLX5015 Air filter
NTLX5010 Lower grill

For more detailed information, refer to *IW SPM-IP Basics*, NN10181-111.

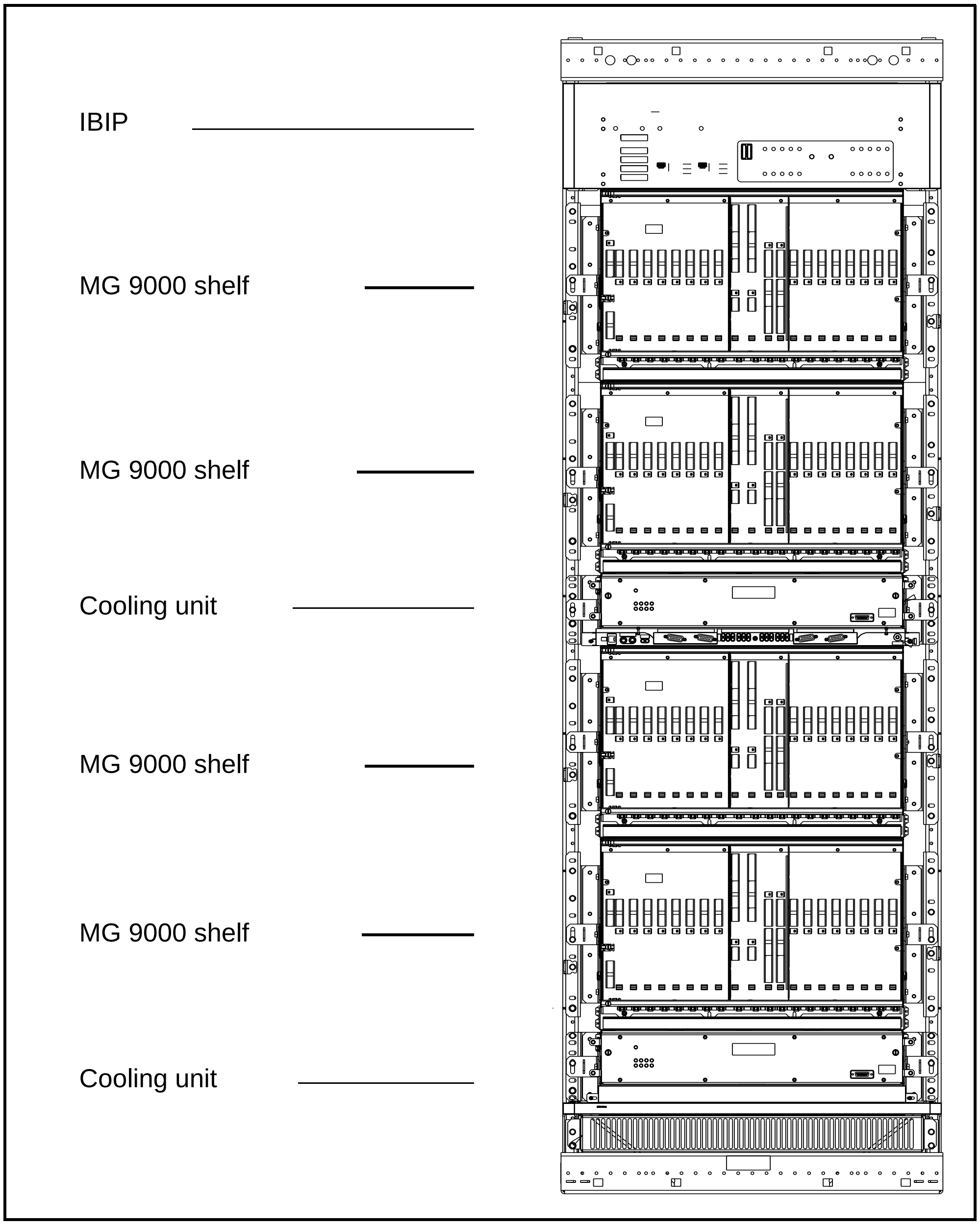
MG 9000

The MG 9000 media gateway can be housed in one of two frame configurations:

- NTNY01BB MG 9000 frame without DS1 sparing
- NTNY02BB MG 9000 frame with DS1 sparing shelf

The figure NTNY01BB MG 9000 frame without DS1 sparing on page 150 show the NTNY01BB frame without DS1 sparing.

NTNY01BB MG 9000 frame without DS1 sparing



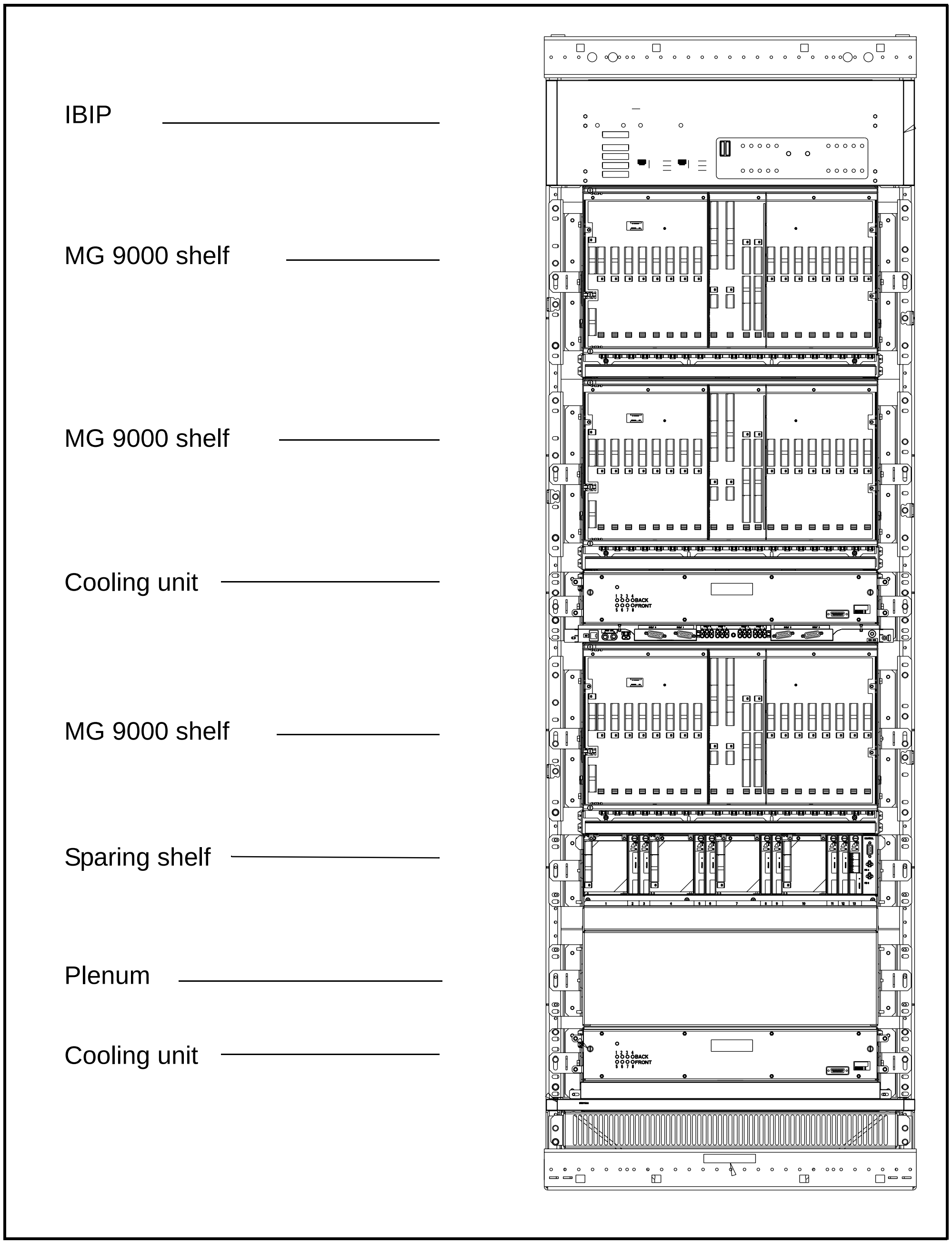
The table NTNY01BB frame components below lists the frame components for the NTNY01BB frame.

NTNY01BB frame components

Frame component	Description
IBIP	Intelligent bay interface panel
DCC, ITP, and ITX card	Data control card, Internet telephony processor card, and Internet telephony extender card (up to four sets)
Cooling units	Frame cooling units (x2)
MG 9000 shelves	Providing POTS/combination lines, supporting: • private lines (without sparing) • switched lines • xDSL services (in master shelf only) • DS512 (two pairs of cards) connection for up to two subtending XPMs (ESMA/LGCI) (in master shelf only)

The figure NTNY02BB MG 9000 frame with DS1 sparing shelf on page 152 shows the NTNY02BB frame with DS1 sparing shelf.

NTNY02BB MG 9000 frame with DS1 sparing shelf



The table NTNY01BB frame components below lists the frame components for the NTNY01BB frame.

NTNY01BB frame components

Frame component	Description
IBIP	Intelligent bay interface panel
DCC, ITP, and ITX card	Data control card, Internet telephony processor card, and Internet telephony extender card (up to four sets)
Cooling units	Frame cooling units (x2)
MG 9000 shelf	One MG 9000 shelf supporting: • private lines (without sparing) • switched lines • xDSL services (in master shelf only) • DS512 (two pairs of cards) connection for up to two subtending XPMs (ESMA/LGCI) (in master shelf only)
MG 9000 shelves	Two MG 9000 shelves providing POTS/combination lines, supporting: • private lines (without sparing) • switched lines • xDSL services (in master shelf only) • DS512 (two pairs of cards) connection for up to two subtending XPMs (ESMA/LGCI) (in master shelf only)
Sparing shelf	Provides sparing and DS1 protection to the system

In (I)SN08, a new Global Linecard 32 (GLC-32) is introduced for the MG 9000. The NTNY53AB supports the following functionality:

- International COIN
- International POTS
- North America POTS
- Ground start

- Loop reversal
- P-phone

For detailed information on the MG 9000, refer to *MG 9000 Basics*, NN10011-111.

Gigabit Ethernet

As from (I)SN08, the MG 9000 offers Gigabit Ethernet (GigE) interfaces as a new SuperCore card. The GigE interface card provides GigE for IP connectivity to the packet network. The GigE cards provide GigE link redundancy by being provisioned in pairs and 1+1 hot swappable.

> ***Note:*** In (I)SN08, the MG 9000 does not support DS-1 or DSL services with the GigE interface.

Network management hardware

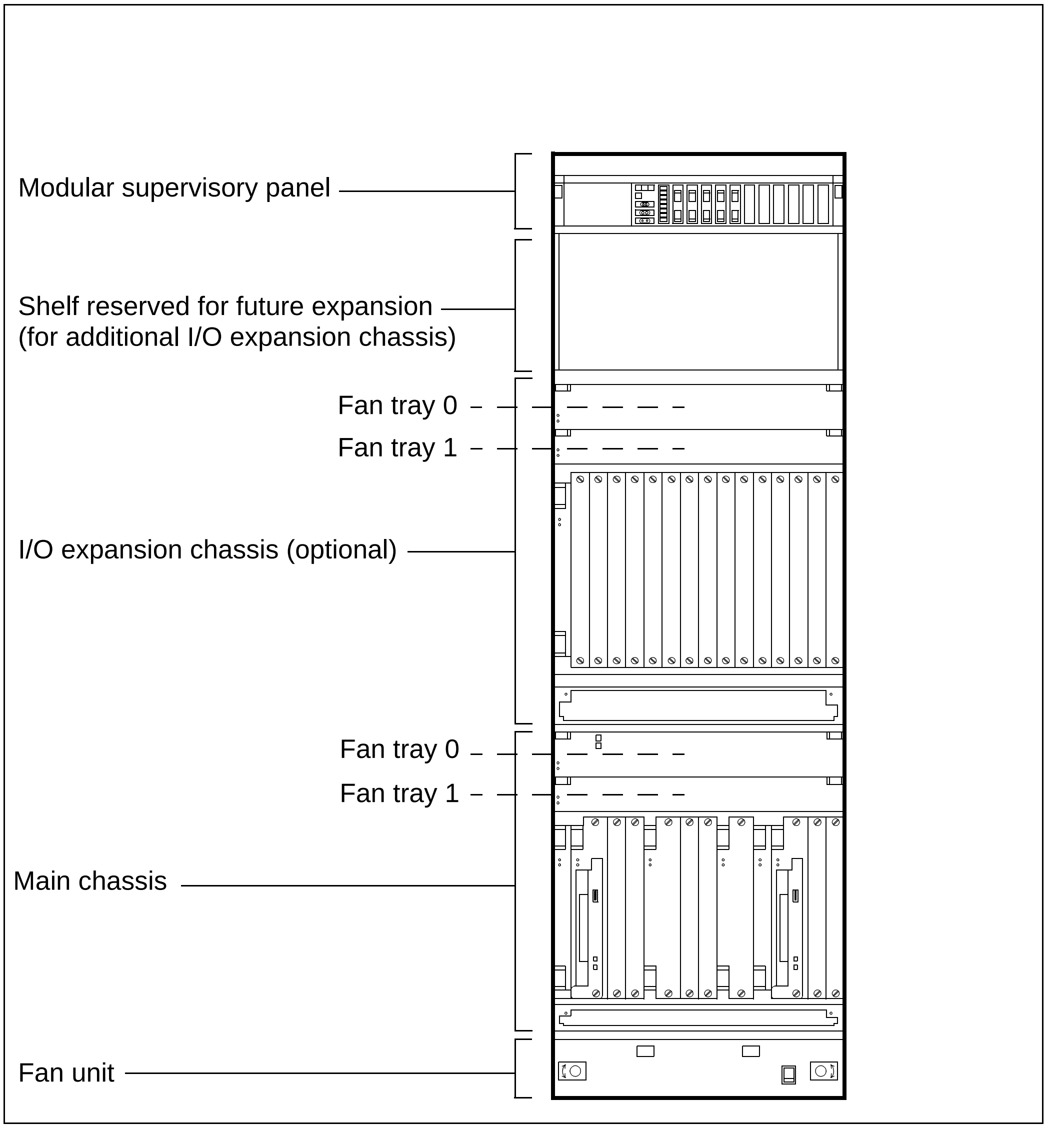
This section describes the hardware used in the Network management of CVoIP solutions.

CS 2000 Core Manager

The CS 2000 Core Manager is housed on the SuperNode Data Manager (SDM) platform. The SDM hardware is a Motorola Power PC Series FX system running AIX (the IBM version of UNIX). It is connected to XA-Core via DS-512 links to the CS 2000 MS, and to other CS 2000 components via the Ethernet CS LAN. The network connection between Integrated EMS applications and their OSS clients is provided by a managed IP network.

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


Modular supervisory panel
Shelf reserved for future expansion (for additional I/O expansion chassis)
Fan tray 0
Fan tray 1
I/O expansion chassis (optional)
Fan tray 0
Fan tray 1
Main chassis
Fan unit

Cabinetized Operations Administration and Maintenance

The Cabinetized Operations Administration and Maintenance (COAM) configuration consists of Sun Netra 240 servers (COAM servers) in a PTE 2000 cabinet. COAM supports the following Carrier VoIP applications

- Core and Billing Manager
- CS 2000 Management Tools
- APS
- SSPFS

- MG 9000 Manager
- Integrated EMS

COAM is available in simplex or high availability configurations:

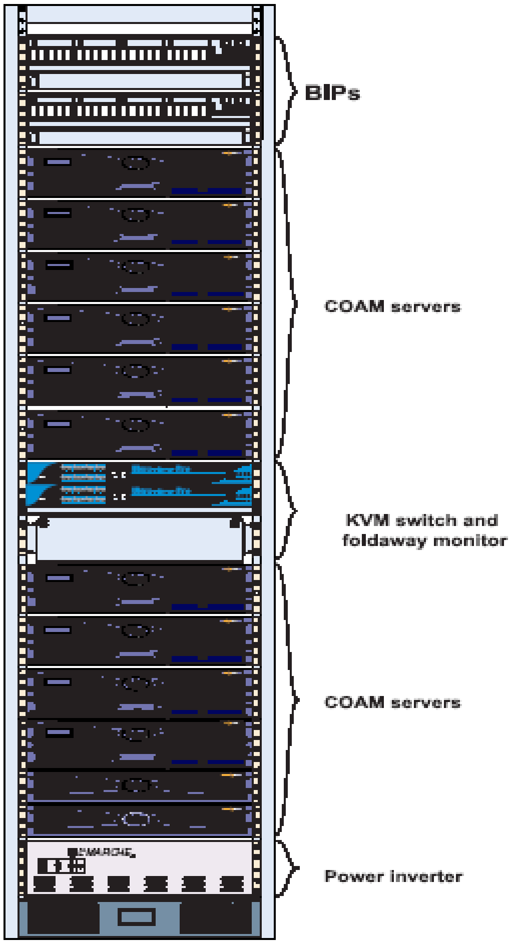
- simplex - one single Sun Netra 240 running CBM
- high-availability - two or four Sun Netra 240s

COAM cabinet
The COAM cabinet is a PTE2000 cabinet that houses the following components:

- two breaker interface panels (BIPs)
- slots for up to 10 COAM servers
- optional fold-away monitor and keyboard
- optional Keyboard Video and Mouse (KVM) switch that connects up to eight computers
- DC-AC power inverter

The following figure shows a COAM cabinet.

COAM cabinet



COAM servers

The COAM server is the Sun Netra 240 server. COAM servers can be provisioned as simplex units or High Availability (HA) pairs. Carrier VoIP products can be deployed on COAM servers in the following configurations:

- Integrated EMS co-resident with CS 2000 Management Tools
- Integrated EMS on standalone server

The table below lists the residency requirements for each configuration.

	Integrated EMS co-resident with CS 2000 Management Tools			Integrated EMS on standalone server			
Software	**Server #1**	**Server #2**	**Server #3 (see note)**	**Server #1**	**Server #2**	**Server #3**	**Server #4**
APS	X			X			
CBM		X				X	
CS2M	X			X			
Integrated EMS	X				X		
MG 9000 Mgr			X				X
MG 9000 Mid-tier			X				X
NPM	X				X		
SSPFS	X	X	X	X	X	X	X
USP Mgr	X			X			

Note: This only applies to the UA-AAL1, UA-IP, and Intl UA-IP solutions.

Core and Billing Manager The Core and Billing Manager resides on commercial off the shelf (COTS) hardware that uses the Solaris operating system. In (I)SN08, 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 a Sun Netra 240 server from SUN Microsystems.

APS The APS resides on a COAM 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
- redundant power supplies consisting of three units capable of hot swaps

SSPFS The Succession Server Platform Foundation Software (SSPFS) is installed on a Sun Netra 240 server from SUN Microsystems.

MG 9000 Manager

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

Integrated EMS The Integrated Element Management System (Integrated EMS) runs on Sun Netra 240 servers (alongside Core and Billing Manager).

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.

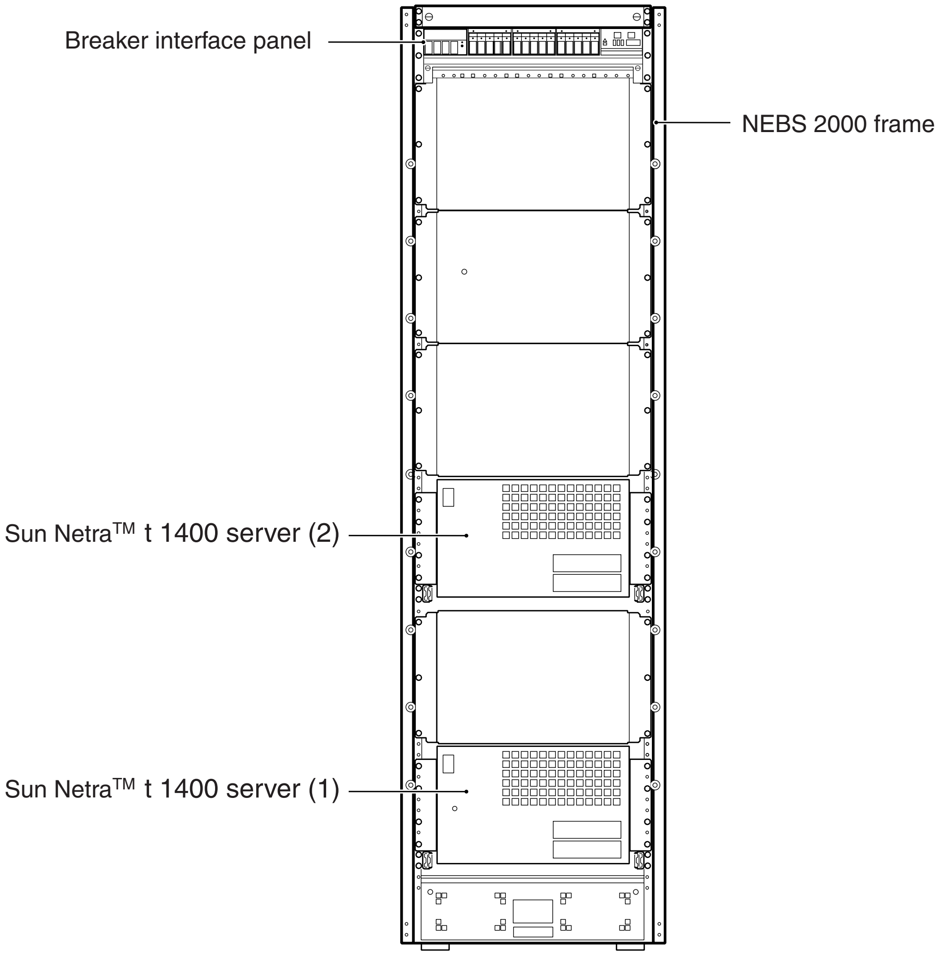
MDM

MDM software runs on dual Sun Netra^{TM} 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 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^{TM} 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^{TM} t1400 servers running MDM must be co-located with the Core Manager in the central office.

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

Sun Netra^{TM} t1400 servers mounted in NEBS 2000 frame



PPT 3054 007 AB

Device Manager

The Device Manager manages the Ethernet Routing Switch 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.

Additional hardware

Secondary Power Distribution Center

You have the option of using a Secondary Power Distribution Center (SPDC) to power your Carrier VoIP 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 1.2 GHz 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 interface 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

This chapter describes the UA-IP Solution software and how to order it. The chapter contains the following sections:

The capabilities of the UA-IP Solution are implemented by means of executable software assembled into several software components. These components consist of software loads (or in some cases, firmware) to support the corresponding hardware components, and managers for managing the hardware components.

The table [3] Software components below lists all the software components, with their corresponding page references. This chapter describes the software loads and other Carrier VoIP software such as Contivity 600. The next chapter,OAM&P strategy on page 184, describes the OAM&P managers and tools.

[3] Software components

Supporting software for...	Page	Element management software	Page
APS	170	APS Manager	
Contivity 600	172	n/a	
CS 2000 (XA-Core)	169	CS 2000 Manager	196
		CS 2000 Core Manager	196
		CS 2000 GWC Manager	196
		CS 2000 SAM21 Manager	196
CS 2000-Compact	169	CS 2000 Manager	196
		CS 2000 Core Manager	196
		CS 2000 GWC Manager	196
		CS 2000 SAM21 Manager	196

[3] Software components

Supporting software for...	Page	Element management software	Page
Call Agent	169	Call Agent Manager	196
STORM cPCI	169	STORM Manager	
		CS 2000 SAM21 Manager	196
STORM SAM-XTS	169	STORM Manager	
DCE Security	173	n/a ***Note:*** Some DCE management is done using the CS 2000 Core Manager (sdmmtc on the SDM); some is done on each network element. The console command is dcecp.	
Gateway controllers	170	CS 2000 GWC Manager	196
		CS 2000 SAM21 Manager	196
Integrated EMS	172	n/a	
MG 9000	170	MG 9000 Manager	192
Nortel Media Server 2000 Series	170	Nortel Media Server 2000 Manager	186
Multimedia Communication Server 5200	170	System Manager	186
Ethernet Routing Switch 8600	170	Device Manager	170
Media Gateway 7400	171	Multiservice Data Manager	193
Media Gateway 15000	171	Multiservice Data Manager	193
CS 2000 SAM21 shelf controller	170	CS 2000 SAM21 Manager	196
Session Server	171	Session Server Manager	196
UAS	171	UAS Manager	
USP	171	USP Manager	193
USP-Compact	171	USP Manager	193

[3] Software components

Supporting software for...	Page	Element management software	Page
		CS 2000 SAM21 Manager	196
UE3K			

Software loads

CS 2000 product computing-module load

The UA-IP Solution can be based on either a CS 2000 XA-Core or a CS 2000-Compact (which incorporates Call Agent, a third-party cPCI processor). Both configurations use a core software load, also known as the product computing-module load (PCL). For more information on the CS 2000-Compact core PCL, refer to the section CS 2000-Compact additional software loads on page 169.

Within the PCL, CS 2000 functionality and features are made available via the Software Optionality Control (SOC) mechanism. All customers receive the same load; it is the customer-specific combination of (de)activated SOC options that determines which features can actually be used (see section Software Optionality Control on page 183).

The *CS 2000 Software Portfolio,* NN10514-111, provides a comprehensive overview of the CS 2000 software options available to network operators. This guide gives an overview of all the software functionality and features available with the Carrier VoIP solutions, including the core software load and related solution component module loads.

CS 2000-Compact additional software loads

The CS 2000-Compact core PCL (see section CS 2000 product computing-module load on page 169) runs on the Call Agent under a combination of Linux operating systems, Protel Environment Emulation Layer (PEEL) and maintenance image (Call Agent Manager). The CS 2000-Compact software is packaged in two separate loads:

- System operating system (SOS) load; the PCL contains the SOS image.
- Linux/PEEL/maintenance load; the non-computing module load (NCL) contains the Linux operating system, PEEL and Call Agent Manager. NCL is installed using the SuperNode Data Manager (SDM) SWIM tool.

The Storage Manager (STORM) has separate loads for STORM cPCI and the lower-cost alternative STORM SAM-XTS. These loads support the Call Agent network file server (NFS) services.

Software loads for other components

Audio Provisioning Server

For information on the APS, refer to the section [APS on page 236 - CHECK REFERENCE!].

Gateway controllers

CS 2000 gateway controllers (GWC; housed in a CS 2000 SAM21 shelf) are configured to provide different services, but the same International software load is used for all of them. CS 2000 datafill is used to customize this load for each CS 2000 GWC, to equip the CS 2000 GWC for its intended role.

Nortel Media Server 2000 Series

ATTENTION
The MS 2010 is not applicable to the International AAL2 solution

For information on the Nortel Media Server 2000 Series refer to the documents listed in the chapter [About the documentation suite].

MG 9000

The UA-IP Solution uses the MG 9000 to provide voice and data lines to subscribers. The software includes the following functions

- SNMP master agent, to communicate to the Carrier VoIP Network through SNMP messaging
- card diagnosis, to diagnose the intelligent MG 9000 boards
- OAM&P, providing maintenance functions and MG 9000 management through SNMP
- shelf and frame management, to control card autodiscovery, alarms, LEDs, etc.
- Local Craft Interface (LCI), providing a local maintenance access point for initial installation, node and carrier maintenance
- synchronization, providing synchronization signals for use in the MG 9000 network-connected shelf and subtending shelves

Multimedia Communication Server 5200

The Multimedia Communication Server 5200 software consists of the Application Module and a number of other modules.

Ethernet Routing Switch 8600 and CS LAN

The Communication Server Local Area Network (CS LAN) is used to support redundant Ethernet communication between the network components in the CS 2000, especially communication between the XA-Core or Call Agent and the CS 2000 Core Manager. The CS LAN is based on the Ethernet Routing Switch 8600 router, which supports intra-CS 2000 communication and also provides the interface between the CS LAN and the external managed network.

Trunk gateways

The trunk gateways (Media Gateways 7400 and 15000) are supported by a Passport carrier release (PCR) load.

Session Server

The Session Server is introduced in ISN07 to support inter-CS communication across the packet network. It is the preferred implementation from release ISN07 onwards.

The HP-CC3310 hardware provides processing, memory and disk capacity for SIP-T and STORM applications. The base layer of the Session Server software uses the Nortel Carrier Grade Linux (NCGL) layer, which includes the Linux kernel.

Universal Audio Server

The Universal Audio Server (UAS) supports announcements and conferencing functionality. The UAS software layers include the following:

- external control interfaces
- audio server functions
- peripheral card functions

Universal Signaling Point

The Universal Signaling Point (USP) provides the signaling gateway for the network. The USP links the application server network to the SS7 network.

The USP software includes three components:

- Basic Signaling Server Platform
- Basic OAM&P
- Basic USP

USP-Compact

The USP-Compact may be used instead of the standard USP to provide the signaling gateway for a CS 2000-Compact network.

The software running on the USP-Compact blades derives directly from that on the standard USP.

Third-party components

For information on all third-party components, refer to the vendor-supplied documentation ().

Integrated Element Management System

The Integrated Element Management System (Integrated EMS) is an application which ties all the OAM&P managers into a single integrated desktop environment. It is distributed as a separate NCL and runs on a dedicated server.

Integrated EMS provides:

- graphical topology and inventory relationships between NEs and managers
- aggregation of all EMS/NE fault data
- integrated fault streams to NML
- customer choice of fault interfaces (SCC2, SYSLOG or SNMP)
- centralized fault viewer with filtering capability
- context-sensitive EMS launching, application launching (for example, TMM, LMM, V5.2), and NE CLUI launching
- enhanced security through a more centralized administration of user accounts and passwords for PAM-enabled systems

Other software

This section gives brief descriptions of various other items of Carrier VoIP software.

Contivity 600

Nortel Networks recommends the third-party Contivity 600 VPN switch to provide Nortel Networks support staff with secure remote access to the customer’s OSS network. Two options are available for Contivity 600: 56-bit encryption and 128-bit encryption.

The Contivity software (supplied on CD with the product) allows configuration and maintenance of the switch. Connection to the Contivity 600 is via a terminal emulation program (for example, HyperTerminal) running on a PC.

For further information on Contivity 600, refer to the FCAPS modules listed in the chapter [About the documentation suite].

DCE Security

Ethernet connectivity is required from Integrated EMS to the corporate TCP/IP WAN to support the operations support system (OSS). For XA-Core and SDM access, the optional DCE Security application provides a means of establishing the authenticity of users. Access is restricted based on privileges assigned by the administrator.

Customers can use an alternative security product for XA-Core and SDM access (see section [DCE cell hardware and software]).

> ***Note:*** An alternative authentication method is the Pluggable Authentication Module (PAM). The exact implementation of PAM authentication is the customer's choice.

Software baseline

The table below shows all the components of the UA-IP Solution, together with their order codes. The hardware items are shown in bold type, followed where relevant by the corresponding manager.

Component	Order code	Notes
APS APS Manager *	APS00100	
Carrier Endpoint Configuration *		
Contivity 600	n/a	third-party; two options available: 56-bit and 128-bit encryption
CS 2000 CS 2000 Management Components	SN000008 CS2M0080	
CS 2000 Core Manager	CS2E0080	AIX-based software
Core and Billing Manager	CBM00080	Solaris-based software
Note 1: The items marked * are components of the CS 2000 Management Components NCL (CS2M). ***Note 2:*** The following 'loads' are built from the PNM08 'DRU': SESM0008 (managers), NPMM0080 (NPM), SPFS0080 (tools), 9KEM0080 (MG 9000 manager).		

Component	Order code	Notes
CS 2000-Compact		
SOS load (PCL)	SWC00008	
PEEL/Linux /load	CCA00080	
3PC firmware	SAM20080	
STORM cPCI	STRM0006	
STORM cPCI firmware	SAM20080	
STORM SAM-XTS (HP server)	STRM0006	
STORM Manager		
CS 2000 Management Components	CS2M0080	
CS 2000 Core Manager	CS2E0080	AIX-based software
Core and Billing Manager	CBM00080	Solaris-based software
Call Agent Manager	included in 3pclinuximage_6.xx.x.0	
DCE security (optional)	n/a	customer-provided, must be ordered from IBM; supported and verified DCE server with IBM DCE v3.1 on Solaris 2.7
EMS Proxy Services		
CS 2000 GWC	GWCW0080	PGC load; delivered with Base PCL load
GWC080 firmware	SAM20080	delivered with Base PCL load
CS 2000 GWC Manager *		
Integrated EMS	IEMS0080	
Lines Configuration *		
LMM * (optional)		
LTM *		
Nortel Media Server 2010	MS200080	The MS 2010 is not applicable to the International AAL2 solution
Nortel Media Server 2000 Manager *		

Note 1: The items marked * are components of the CS 2000 Management Components NCL (CS2M).

Note 2: The following ‘loads’ are built from the PNM08 ‘DRU’:
SESM0008 (managers), NPMM0080 (NPM), SPFS0080 (tools),
9KEM0080 (MG 9000 manager).

Component	Order code	Notes
MG 9000	MG9K0080	The MG 9000 is not applicable to the PT-AAL1 solution
MG 9000 Manager	9KEM0080	The MG 9000 is not applicable to the PT-AAL1 solution
Multimedia Communication Server 5200	IMS 2.0	
System Manager		
Nodes Configuration *		
NPM	NPM08	NPMM0008
Ethernet Routing Switch 8600	P86S0070	CS LAN only (Release 3.7.2)
Device Manager	n/a	shipped with Ethernet Routing Switch 8600 (DVM 5.8.2.1)
PM Poller		
Media Gateway 7400	PCR6.1.2	
Media Gateway 15000	PCR6.1.2	
MDM	MDM 15.2	refer to the MDM ordering process
QCA *		
CS 2000 SAM21 shelf controller	SAM20080	delivered with Base PCL load
CS 2000 SAM21 Manager *		
SSPFS	SPFS0080	
TMM * (optional)		
Trunks Configuration *		
Session Server	NGSS0080	
Session Server Manager		
UAS	UASA0080	

Note 1: The items marked * are components of the CS 2000 Management Components NCL (CS2M).

Note 2: The following ‘loads’ are built from the PNM08 ‘DRU’:
SESM0008 (managers), NPMM0080 (NPM), SPFS0080 (tools),
9KEM0080 (MG 9000 manager).

Component	Order code	Notes
UAS Manager *		
SAM16 Global server platform	GSS00033	
UE3K		
UE3K Manager		
USP	USP00100	
USP-Compact	USPL0100	
USP-Compact firmware	SAM20080	
USP Manager (for USP and USP-Compact)		n/a (included in USP00100 or USPL0100)
V5.2 Configuration *		
V5.2 Maintenance *		
Base PCL	SN000008	Communication Server and TDM core software; includes DRUs TOPS21, UCS21, CNA21, CCM21, PNM08, SHR21, MSH21, XPM20, SP/SPSH/MG4K21, TDMSP/TDMSPSH/SPD21, BASE/TL (CSP21)
PPL peripheral load	PLLT0021	delivered with Base PCL load
NRL commissioning tools	INST0021	delivered with Base PCL load
MUL (MS load)	MUC00021	delivered with Base PCL load
Media Gateway 7400 and MDM comprehensive package	n/a	includes PCR6.1.2 software load
Media Gateway 15000 and MDM comprehensive package	n/a	includes PCR6.1.2 software load
Media Gateway 15000	n/a	hardware identical to Media Gateways
MDM (supporting Media Gateway 15000 and 7400)	MDM 15.2	order the comprehensive package

Note 1: The items marked * are components of the CS 2000 Management Components NCL (CS2M).

Note 2: The following ‘loads’ are built from the PNM08 ‘DRU’:
SESM0008 (managers), NPMM0080 (NPM), SPFS0080 (tools),
9KEM0080 (MG 9000 manager).

Component	Order code	Notes
Centrex IP Gateway	CICM0080	
Centrex IP Client Manager EM	CICM0080	CICM7.11.184 load name
Centrex IP SoftClient	not required	CICM SoftClient available from Nortel Networks e-delivery service; customer accesses site to download client software
Note 1: The items marked * are components of the CS 2000 Management Components NCL (CS2M). ***Note 2:*** The following 'loads' are built from the PNM08 'DRU': SESM0008 (managers), NPMM0080 (NPM), SPFS0080 (tools), 9KEM0080 (MG 9000 manager).		

Client workstation software baseline

This section defines the platform requirements, operating system requirements, and Web browser requirements for 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

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
MG 9000 Manager	Desktop	PC or Sun
Note: The MG 9000 is not applicable to the PT-AAL1 solution		

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

Client Name	Invocation	Platform
MG 9000 Local Craft Interface ***Note:*** The MG 9000 Local Craft Interface is not applicable to the PT-AAL1 solution	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
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

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

Client name	Windows operating system	Solaris operating system
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
MG 9000 Manager ***Note:*** The MG 9000 Manager is not applicable to the PT-AAL1 solution	98*, 98SE*, ME*, NT, 2000, XP to Current	2.7, 2.8, 2.9 to Current
MG 9000 Local Craft Interface ***Note:*** The MG 9000 Local Craft Interface is not applicable to the PT-AAL1 solution	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
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

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
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
MG 9000 Local Craft Interface ***Note:*** the MG 9000 Local Craft Interface is not applicable to the PT-AAL1 solution	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

How to prepare an order

Use the following guidelines to prepare an order. If necessary, contact your Nortel Networks account manager for help.

- Ensure that the necessary customer responsibilities have been covered, and all the required customer-supplied hardware and software components provided (see the chapter [Customer support]).
- Complete all planning and engineering activities to determine your requirements.
- Ensure that you consider and identify any hardware and software dependencies. For example, if you order function processors and termination panels, you must also order the appropriate number and type of cables.
- Determine the date and destination address for delivery. The destination address for shipments of hardware, software, and

documentation can differ from the destination address for billing information.

- Determine your training and support needs.
- Determine any licensing requirements for software use.
- Determine and procure any additional devices needed to support the Media Gateway equipment you are ordering, for example, workstations, text interface devices and printers.
- Contact your Nortel Networks account manager to prepare a purchase order and any other required documents.

Software delivery

For most of the UA-IP Solution components, the initial deployment of software loads is on physical media for commissioning purposes. Thereafter, the solution may use electronic software delivery (where customer infrastructure permits) for upgrades and maintenance loads.

Software media for initial commissioning

For most of the UA-IP Solution components, the initial deployment of software loads is on physical media for commissioning purposes. Physical media includes digital audio tape (DAT) and CD-ROM, depending on the component.

Electronic software delivery (upgrades and maintenance loads)

Upgrades and maintenance loads can be delivered electronically, where customer infrastructure and product technology permit.

Electronic software delivery has three main parts:

- customer regulation, taxation and contractual changes
- Nortel Networks/customer electronic connectivity
- UA-IP Solution electronic connectivity

Customer regulatory, tax and contractual changes

The customer must be prepared for the regulatory, tax, and contractual changes invoked by receiving software products electronically. In some locations, electronically delivered software is exempt from sales tax. Customers operating in tax-exempt jurisdictions must be prepared to accept an invoice from Nortel Networks where certain line items have no sales tax applied. Customers assume responsibility to remit non-collected taxes if software becomes taxable. This situation can occur if an element in the Carrier VoIP Network is moved to a non-tax-exempt location.

Nortel Networks/customer electronic connectivity

Electronic connectivity to Nortel Networks is managed by Nortel Networks Partner Access Solutions (PAS). PAS is a team of Nortel Networks data network professionals who provide connectivity solutions for Nortel Networks development partners, joint ventures, licensees, and customers.

NGS operates multiple extranets worldwide, which are commonly known as the Customer Access Network (CAN). External partners connect to the CAN via dialup, leased circuits, or virtual private network connections. The CAN has analog and ISDN dialup service and shared frame relay (V.35), X.25 or E1 service. To enable electronic delivery of all possible load files in a Carrier VoIP Network solution, a connection with at least 1 Mbit/s bandwidth (1.554 Mbit/s bandwidth for North America) is required from the Nortel Networks CAN to the customer network. However, most load files can be delivered electronically via 56 kbit/s links.

For the delivery of software loads, the software must be downloaded from Nortel Networks to an external dropbox location. Some customers, however, may be provided with a software load transferred directly to their network. The network addresses of all systems to which Nortel Networks is required to deliver software must be externally accessible to Nortel Networks.

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

For the delivery of software loads, a customer contact e-mail address is required. Nortel Networks notifies this contact when loads have been delivered electronically. It is the customer’s responsibility to monitor communications from Nortel Networks notifying 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. The customer is responsible for making hard copies and/or ensuring that the users of the document receive a copy in the required format.

Solution electronic connectivity

To initiate the installation of the software loads to the network elements, the customer must first access these loads. In order to support end-to-end electronic software delivery, connectivity is required to the network elements of the UA-IP Solution.

For the installation of software loads to a gateway, the Secure File Transfer application transfers the load file from the gateways. For the CS 2000 software, the files are transferred to the CS 2000 disk device, ready for installation.

Software Optionality Control

Software Optionality Control (SOC) is a system in which certain software features which form part of the delivered load are password-protected. To use these features (known as ‘SOC options’) customers must purchase a license and are then supplied with a password. The SOC utility provides an interface for tracking and monitoring the use of SOC options.

For details of the features available, refer to *CS 2000 Software Portfolio,* NN10514-111.

Software maintainability

The UA-IP Solution uses a patch application process for delivering fixes to the CS 2000 CM load. The solution uses either a patch application process or maintenance release upgrade for delivering fixes to the remaining solution elements.

OAM&P strategy

This chapter provides an overview of the UA-IP Solution OAM&P strategy. The chapter contains the following sections:

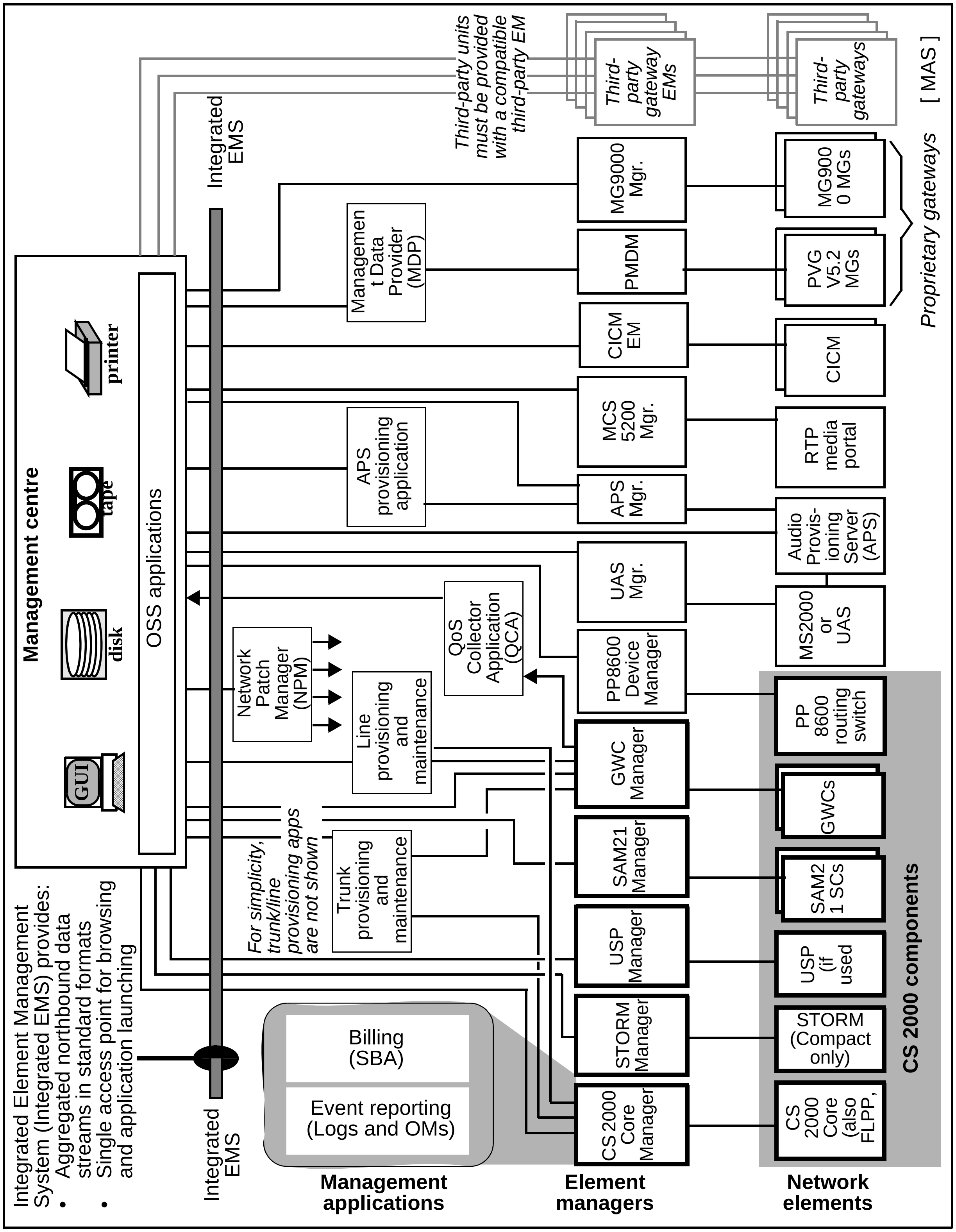
The chapter describes the OAM&P software and the third-party managers.

Overview of OAM&P

The distributed nature of the UA-IP solution presents new challenges for managing the OAM&P for the solution. The distributed elements of the network are brought together by removing many redundant software applications in the SuperNode Data Manager (SDM) platform and interworking new CVoIP applications on commercially available hardware platforms. The Integrated Element Management System (Integrated EMS) ties all the OAM&P managers and applications into a single integrated desktop environment.

The figure Logical OAM&P architecture below shows the logical OAM&P architecture.

Logical OAM&P architecture


Management centre
GUI
disk
tape
printer
OSS applications
Integrated Element Management System (Integrated EMS) provides:
• Aggregated northbound data streams in standard formats
• Single access point for browsing and application launching
Integrated EMS
Integrated EMS
For simplicity, trunk/line provisioning apps are not shown
Network Patch Manager (NPM)
Line provisioning and maintenance
Trunk provisioning and maintenance
QoS Collector Application (QCA)
APS provisioning application
Managemen t Data Provider (MDP)
Third-party units must be provided with a compatible third-party EM
Billing (SBA)
Event reporting (Logs and OMs)
Management applications
Third-party gateway EMs
MG9000 Mgr.
PMDM
CICM EM
MCS 5200 Mgr.
APS Mgr.
UAS Mgr.
PP8600 Device Manager
GWC Manager
SAM21 Manager
USP Manager
STORM Manager
CS 2000 Core Manager
Element managers
Third-party gateways
[MAS]
MG900 0 MGs
PVG V5.2 MGs
Proprietary gateways
CICM
RTP media portal
Audio Provis-ioning Server (APS)
MS2000 or UAS
PP 8600 routing switch
GWCs
SAM2 1 SCs
USP (if used
STORM (Compact only)
CS 2000 Core (also FLPP,
CS 2000 components
Network elements

Integrated EMS

Integrated EMS incorporates all the element management functionality, software and hardware, used in a CVoIP network. The Integrated EMS components provide management of the solution's functional components, services and operations. The components operate independently on the different parts of a CVoIP network and are distributed across several hardware platforms. The components include managers, and various tools and utilities.

Integrated EMS provides the following facilities:

- graphical topology and inventory relationships between the NEs and EMS modules
- aggregation of the NE/EMS fault and performance data
- an integrated network event viewing browser
- an integrated network alarm viewing browser
- alarm and event mediation from the diverse CVoIP fault interfaces and standard Integrated EMS northbound OSS event interfaces (SCC2, NTstd, custlog, SNMP)
- collected performance data reports in CSV or XML file formats along with scheduled ftp or sftp file transfer tools
- integrated audit and security log browsers
- enhanced security features, by improving the centralization of authentication and authorization, and standard interfaces to external security databases
- integrated fault streams to NML
- customer choice of OSS fault interfaces (SCC2, SYSLOG, NT STD, or SNMP)
- centralized fault viewer with filtering capability
- context-sensitive EMS launching, applications launching (for example, TMM, LMM), and NE CLUI launching
- enhanced security through a centralized administration of user accounts and passwords for PAM-enabled systems

Integrated EMS is distributed as a separate NCL (IEMS) and runs co-resident with the CS 2000 Management Components NCL (CS2M) on Sun Netra t1400 servers or the new Sun Netra 240 servers. Alternatively, it can be installed as a stand-alone configuration on a Sun Netra 240.

Managers

The managers, applications and tools which can be launched from Integrated EMS are as follows:

- Audio Provisioning Server Manager (APS Mgr)
- Batch Provisioning Tool
- Call Agent Manager (Call Agent is managed by CS 2000 Core Mgr)
- Communication Server 2000 Core Manager (CS 2000 Core Mgr)
- Communication Server 2000 GWC Manager (CS 2000 GWC Mgr)
- Communication Server 2000 Service Application Module 21 Manager (CS 2000 SAM21 Mgr)
- Device Manager (for Ethernet Routing Switch 8600)
- EMS Proxy Services (part of SSPFS)
- Line Maintenance Manager (LMM)
- MG 9000 Manager (MG 9000 Mgr)
- Media Server Manager
- Network Patch Manager (NPM; part of SSPFS)
- OSSGate Application
- PM Poller (part of SSPFS)
- Multiservice Data Manager (MDM)
- QoS Collector Application (QCA)
- STORM Client
- Succession Server Platform Foundation Software (SSPFS)
- Trunk Maintenance Manager (TMM)
- Universal Audio Server Manager (UAS Mgr)
- Universal Signaling Point Manager (USP Mgr)

> ***Note:*** The following configuration tools are part of CS 2000 Management Tools (SESM): Carrier Endpoint Configuration, Lines Configuration, Nodes Configuration, Trunks Configuration, V5.2 Configuration, V5.2 Maintenance

Distribution of element management software

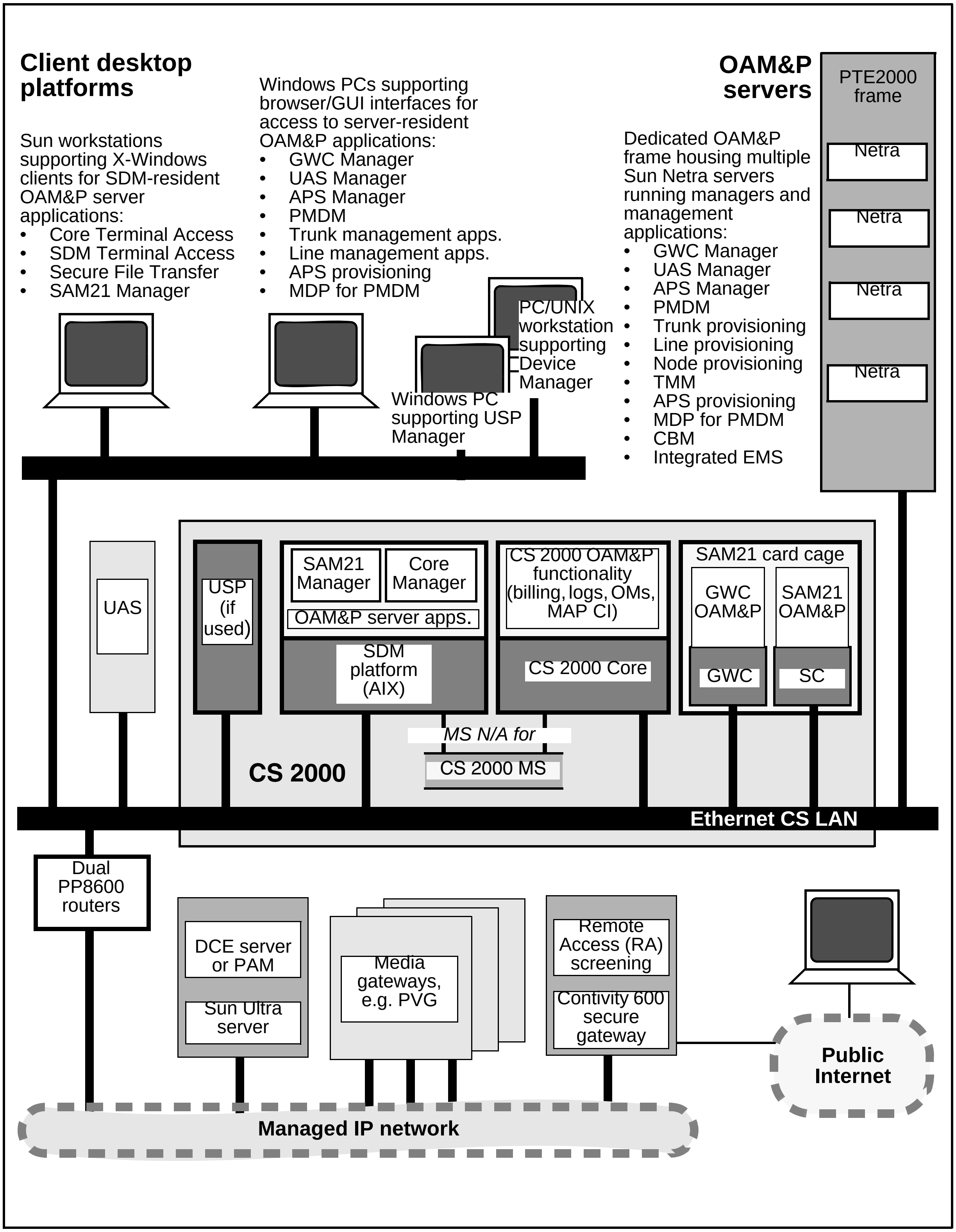
Each of the managers can itself be distributed across different hardware platforms. A part of the management software is always resident on the managed network element.

The figure Distribution of managers on page 189 shows the managers for this solution as they are distributed across:

- client workstations
- element management servers
- managed network elements

> ***Note 1:*** In a typical network, a single client workstation can be used to run the client parts of several managers.
>
> ***Note 2:*** Desktop machines, client workstations, the optional Distributed Computing Environment (DCE) server, and remote access security products (for example, the Nortel Networks recommended Contivity 600 VPN switch; see section Contivity 600 on page 223) are normally customer-supplied items.

Distribution of managers



Client desktop platforms

Sun workstations supporting X-Windows clients for SDM-resident OAM&P server applications:

- Core Terminal Access
- SDM Terminal Access
- Secure File Transfer
- SAM21 Manager

Windows PCs supporting browser/GUI interfaces for access to server-resident OAM&P applications:

- GWC Manager
- UAS Manager
- APS Manager
- PMDM
- Trunk management apps.
- Line management apps.
- APS provisioning
- MDP for PMDM

PC/UNIX workstation supporting Device Manager

Windows PC supporting USP Manager

OAM&P servers

Dedicated OAM&P frame housing multiple Sun Netra servers running managers and management applications:

- GWC Manager
- UAS Manager
- APS Manager
- PMDM
- Trunk provisioning
- Line provisioning
- Node provisioning
- TMM
- APS provisioning
- MDP for PMDM
- CBM
- Integrated EMS

CS 2000 Management Tools

For information on CS 2000 Management Tools and the following managers, refer to CS 2000 Management Tools on page 200:

- Audio Provisioning Server Manager
- Batch Configuration Monitor (BCM)
- Batch provisioning tool (BPT)
- CS 2000 GWC Manager
- CS 2000 SAM21 Manager
- Line Maintenance Manager (LMM)
- Media Server Manager
- OSSGate
- Trunk Maintenance Manager (TMM)
- Universal Audio Server Manager

Manager summaries

The following sections give brief descriptions of each of the OAM&P managers (listed in alphabetical order). .

CS 2000 Manager

CS 2000 Manager is a collective term for the management applications of the CS 2000. CS 2000 Manager provides management for the CS 2000 and CS 2000-Compact, including XA-Core, Call Agent, the gateway controllers, and SAM21.

The management applications include:

- Maintenance and Administration Position (MAP) user interface
- operational measurement data delivery (OMDD)
- SuperNode billing application (SBA)
- ASCII terminal access (ATA)
- secure file transfer (SFT)
- log delivery

CS 2000 Manager has the following subcomponents:

- **CS 2000 Core Manager** - provides element management for XA-Core. The core management capabilities are provided by one of the following:
  - — Core and Billing Manager (CBM) application running on a Sun Netra 240 server (NCL CBMxx)
  - — SuperNode Data Manager (SDM) applications running on a Motorola Power PC/AIX platform (NCL CS2E)

  Note 1: The functionality of CBM on the Sun Netra 240 is not exactly equivalent to the Motorola-based product (see Core and Billing Manager on page 192).

  Note 2: It is possible to log in to the CS 2000 Core Manager (CBM or SDM) from either outside or within Integrated IEMS (see Integrated EMS on page 186).

- **Call Agent Manager** - provides element management for the CS 2000-Compact, in addition to the SDM-based CS 2000 Manager. Call Agent Manager is built into the Call Agent software load.
- **STORM Manager** - provides element management for the STORM persistent disk storage system. STORM Manager is built into the STORM software load.
- **Session Server Manager** - Provisioning and maintenance of the Session Server is accomplished using one of two Session Server web-based GUIs:
  - — CVoIP CS 2000 Session Server Manager GUI
  - — CVoIP CS 2000 Nortel Carrier-grade Linux (NCGL) Platform Manager GUI

  Both interfaces are accessed from a common web-based launch point. In general, the SIP Gateway application is provisioned and administered using the CVoIP CS 2000 Session Server Manager GUI, while the Session Server platform NCGL and operating system are managed using the CVoIP CS 2000 NCGL Platform Manager GUI.

  Fault management is generally accomplished using the CVoIP CS 2000 NCGL Platform Manager GUI. Some configuration management and performance management activities are performed using the NCGL console command line interface (CLI). All interfaces are accessible from Integrated EMS or though a proxied connection from a client workstation on the CS-LAN.

Core and Billing Manager

Core and Billing Manager (CBM) is the core management application for CS 2000 (XA-Core) and CS 2000-Compact (Call Agent), an alternative to SDM. CBM runs on one or more Sun Netra 240 servers, housed in the cabinetized OAM (COAM) configuration.

CBM provides OAM&P capabilities similar to the SDM application suite - most of the existing applications are ported to the new platform. These include high-capacity billing (AMADNS and CDR), electronic software delivery (ESD), OMs, log delivery, and GR740.

The following table shows the availability of the various applications.

CBM application availability

Existing SDM application	CBM platform support
SuperNode Billing Application	Yes
Log Delivery	Yes
OM Delivery	Yes (CBM 850, CBM 860)
Terminal Access	Yes, in non-DCE no GUI mode and SSH Security mode
Secure File Transfer	Yes, in non-DCE no GUI mode and SSH Security mode
Log Streamer	Yes (CBM 850, CBM 860)

Device Manager

Device Manager is the manager for the Ethernet Routing Switch 8600s on which the CS LAN is based. Device Manager is a real-time graphical SNMP tool. Because the software is Java-based, it can operate on a variety of operating system platforms: Windows 95/98/NT, and UNIX variants Sun Solaris, HP-UX, and IBM-AIX. If Sun Solaris is used, versions v5.6, v5.7, or v5.8 are suitable.

MG 9000 Manager

The MG 9000 Manager allows FCAPS management tasks to be performed on the MG 9000 Lines Gateway. There are two user interfaces:

- local craft interface (LCI) - The LCI is used for initial commissioning and in emergency instances when the manager is not available.

Daily operation, administration, and maintenance of the MG 9000 is performed from the MG 9000 Manager.

- MG 9000 Manager GUI - The MG 9000 Manager serves as a management system for the MG 9000 within a CVoIP Network. The MG 9000 Manager enables remote management of multiple MG 9000 network elements through a single GUI.

Multiservice Data Manager

Multiservice Data Manager (MDM) provides element management for the Media Gateway 15000 . MDM provides a base platform and a set of applications specially designed for the management of large data networks. The applications include:

- ‘Advisor’ fault management
- ‘Architect’ configuration management
- data collection management
- performance management
- security management
- multiple-vendor network management
- reporting tools
- administration tools
- general utilities

MDM must be run on the Solaris 2.8 (or later) operating system.

Customers can also install the optional Management Data Provider (MDP) with MDM (either stand-alone, or located on the same workstation as MDM). The MDP is used to spool the alarms, logs, and SCNs.

USP Manager

USP Manager provides the manager client for the USP and the USP-Compact. A Windows-based workstation runs the GUI client for OAM&P. The workstation is connected to the USP or USP-Compact via Ethernet and communicates using standard IP protocols.

Third-party managers

The following sections give brief descriptions of each of the OAM&P managers for third-party components (listed in alphabetical order). For more information on the individual managers, refer to the vendor-supplied documentation.

Fault, Configuration, Accounting, Performance, and Security management

The following sections describe how the solution's OAM&P components handle Fault, Configuration, Accounting, Performance, and Security (FCAPS) management.

Fault management

The log delivery system allows Integrated EMS to provide the following fault management functionality:

- retrieval of current alarm status for the elements
- acknowledgment or clearing of alarm conditions
- receipt of alarm raised, alarm cleared, other events from components and applications
- alarm reporting
- handling of alarm notifications and other anomalies

The Integrated EMS alarm browser provides a consolidated real-time view of the active alarms in a CS 2000 central office. The alarm browser allows the user to view the active alarms from the Nortel Networks EMS platforms, EMSs, NEs, and Management Applications in a single graphical interface. The alarm browser serves as a key tool that enables the user to monitor and debug network activities and problems. For details of the key features of the Integrated EMS alarm browser, refer to *Integrated EMS Basics*, NN10329-111.

Maintenance

Integrated EMS provides the following maintenance functionality:

- test or diagnostic recovery initiation
- graphical topology and inventory relationships between the NEs and EMS modules
- aggregation of the NE/EMS fault and performance data
- an integrated network event viewing browser
- an integrated network alarm viewing browser
- alarm and event mediation from the diverse CVoIP fault interfaces and standard Integrated EMS northbound OSS event interfaces (SCC2, NTstd, custlog, SNMP)
- collected performance data reports in CSV or XML file formats along with scheduled ftp or sftp file transfer tools

- integrated audit and security log browsers
- enhanced security features, by improving the centralization of authentication and authorization, and standard interfaces to external security databases

Configuration management

Nortel Networks delivers pre-configured CVoIP Solutions. Further configuration by the customer adds low-level functionality, for example, additional memory or ports. The CS 2000 Management Tools software provides the configuration management functionality, including:

- addition or removal of NEs through user interfaces and the CS 2000
- configuration of network connections
- distribution of configuration state changes as required throughout the subnetwork
- initiation or control of multi-NE software upgrades

Accounting management

The SuperNode Billing Application (SBA) provides operating companies with a robust, high-capacity billing/accounting platform. The SBA provides industry-standard interfaces to downstream facilities. For a list of specific features of the SBA, refer to the section SuperNode Billing Application on page 197.

Performance management

The performance management system for the CS 2000 is implemented by the Operational Measurement Data Delivery (OMDD) software. The OMDD application delivers customer selected operational measurement (OM) data in Comma Separated Values (CSV). This data can be viewed through a data browser, or any spreadsheet software. Performance management systems for other elements are available in CSV format through the respective managers.

Integrated EMS includes a performance collection subsystem. This allows the collection of performance data from the following network elements: , MS 2010, , STORM, and Ethernet Routing Switch 8600. Integrated EMS also provides an OM delivery mechanism for performance data in CSV or XML file formats to an OSS system.

Security management

A secure Integrated EMS ensures legitimate use of the network, including maintaining confidentiality, data integrity, and audit trails. Security management involves identifying network assets, threats, and vulnerabilities, and taking protective measures to prevent unauthorized use.

User administration is a prime function for Integrated EMS administrators. By default, the Integrated EMS Operations Tree contains a list of all the operations that are provided. One of the Integrated EMS administrator's security functions is to assign different operations to different users.

Users can be assigned to different groups. Authorization is then implemented by setting the scope for the operations assigned to a group. This scope defines the access restrictions for the operations in that group, and users see only the Integrated EMS information necessary for their allocated operations. For example, specifying the authorized network type for a group of users allows the users in that group to view only the nodes of the particular network on which they are authorized to perform operations.

Tool and utility strategy

This section summarizes the strategy behind the CVoIP tools and utilities.

Network configuration tools

The following tools are available to perform network configuration for the UA-IP Solution:

- CS 2000 Management Tools
- MAP

CS 2000 Management Tools

For details of individual managers, see section CS 2000 Management Tools on page 200. CS 2000 Management Tools provide the following configuration management functionality:

- determining from a single provisioning request what other entities must be provisioned or configured, and carrying out all required actions (auto-provisioning)
- determining what dependents must be reconfigured as a result of configuration or maintenance actions, and carrying out all required actions (flow-through configuration and maintenance)
- inventory retrieval or reporting for selected single or multiple elements; examples of the elements are types, versions, and instances of hardware and software, and protection status.
- additional functionality, as listed in the section Configuration management on page 195.

SWIM The Software Inventory Manager (SWIM) is for the installation of software load files and patches on the CS 2000 manager and associated workstations.

SWIM covers the following tasks:

- installation of new software
- updating existing software with a newer version
- removing existing software
- viewing a history of commands previously executed
- configuring software

Maintenance and Administration Position

The Maintenance and Administration Position (MAP) is the primary interface between the operating company personnel and the CM. System tests, data interrogation and modification, and trouble analysis functions are provided. The MAP is designed to operate as a single entity for small office applications as well as a large system interface where several units can operate concurrently. It can be used in any of the maintenance and administrative environments in the DMS switch. These include:

- General maintenance
- Network Management
- Operational Measurements
- Service Analysis
- Data Modification

Network accounting and billing management tools and utilities

The following tools and utilities are available to perform network accounting and billing management for the UA-IP Solution:

- SuperNode Billing Application
- MAP
- MDM

SuperNode Billing Application

The SuperNode Billing Application (SBA) provides network accounting and billing functionality, giving operating companies a robust billing platform which meets the increasing demand to support higher volumes of record processing. The application provides the following:

- industry-standard interfaces to downstream facilities
- a teleprocessing system which facilitates higher data transmission rates to support larger volumes of data
- near-real-time Bellcore Automatic Message Accounting (AMA) format (BAF) record delivery
- increased AMA throughput over DS512 links to the standard CS 2000 message switch, or over Ethernet connections to the CS 2000-Compact
- enhanced switch capacity which results from the off-loading of billing-related processing from the CS 2000
- formatting and storage of billing records in Automatic Message Accounting Data Networking System (AMADNS) format
- transfer of billing records to the operating company using File Transfer Protocol (FTP)
- reduced operating costs by the use of LAN/WAN facilities instead of dedicated or dial-up polling links

SBA is part of CS 2000 Core Manager (SDM or CBM).

The CS 2000 supports billing by automatically generating call records to capture information such as call start time, call duration, and calling party number. SBA periodically downloads the records to the operating company's administrative centre for processing. AMA and SMDR records are transmitted in near real time (up to 1.2 million per hour) from the SBA client on the core to the SBA server on SDM or CBM. SBA stores the records in files in AMADNS format (AMA and SMDR records) or DIRP format (AMA records only). SBA routes these billing files to the operating company's processor, using FTP to transfer the files; the customer can also use FTP to retrieve them.

The SBA main screen has the standard DMS switch MAP appearance. Access to the SDMBIL level is through the CM MAPCI and is located under the APPL banner. Functions at this level can be used to display and query the SBA status and its associated alarms. The SDM command BILLMTC opens the screen.

MAP

The MAP is used as the interface to the SBA.

MDM

MDM is a workstation-based network management system for the maintenance and monitoring of many network components from a central or a decentralized network control center. MDM has a full suite of applications and external systems interfaces to manage a number of different devices (see section Multiservice Data Manager on page 193).

Network traffic and performance management tools and utilities

The following tools are available to perform network traffic management and performance management for the UA-IP Solution:

- Integrated EMS
- MAP
- MDM

Integrated EMS

For details of individual managers, see section Managers on page 187. Integrated EMS supports traffic and performance management for the network and the network elements.

For details of performance data collection, refer to *Integrated EMS Performance Management*, NN10327-711.

MAP

The MAP is the primary interface between the operating company personnel and the CM, as described in the section Maintenance and Administration Position on page 197.

MDM

MDM is a workstation-based network management system for the maintenance and monitoring of a complete network from a central or a decentralized network control center. MDM has a full suite of applications and external systems interfaces to manage a number of different devices (see section Multiservice Data Manager on page 193), for example, identifying and analyzing traffic and performance problems.

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 Carrier Voice over IP 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)SN08 release, see What's new for the CS 2000 Management Tools on page 11.

Software

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

- CS2M on page 201 (Call Server 2000 Management)
- APS on page 202 (Audio Provisioning Server)
- SSPFS on page 202 (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 214, which includes the following components:
    - CS 2000 GWC Manager on page 224
    - Universal Audio Server Manager on page 231
    - Audio Provisioning Server Manager application on page 222
    - 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 246 (TMM)
  - Line Maintenance Manager on page 241 (LMM)
  - Batch provisioning tool on page 250 (BPT)
  - Batch Configuration Monitor on page 258 (BCM)
  - Lines Configuration (Servord+)
  - Line Test Manager (LTM)
  - ADSL flowthrough provisioning
  - OSSGate on page 277
- the SAM21 EM (CS 2000 SAM21 Manager on page 268) software package, which consists of the CS 2000 SAM21 Manager application for the SAM21 shelf controller.
- the QCA (QoS Collector application on page 274) 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 284, 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 278, the OMPUSH application on page 280, and the Network Patch Manager on page 259, 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 163or Sun Netra 240 on page 165server from Sun Microsystems.

Hardware for client workstations is provided under Client workstation requirements on page 206.

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 250 (BPT) - command line user interface (CLUI)
- Batch Configuration Monitor on page 258 (BCM) - web browser interface
- Line Maintenance Manager on page 241 (LMM) - graphical user interface (GUI)
- Trunk Maintenance Manager on page 246 (TMM) - web browser interface
- Network Patch Manager on page 259 (NPM) - GUI and CLUI (when installed and enabled on the same server as the CS 2000 Management Tools)
- CS2000 Management Tools application on page 214 (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 268 - GUI
- PM poller on page 278 - CLUI
- OMPUSH application on page 280 - CLUI

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

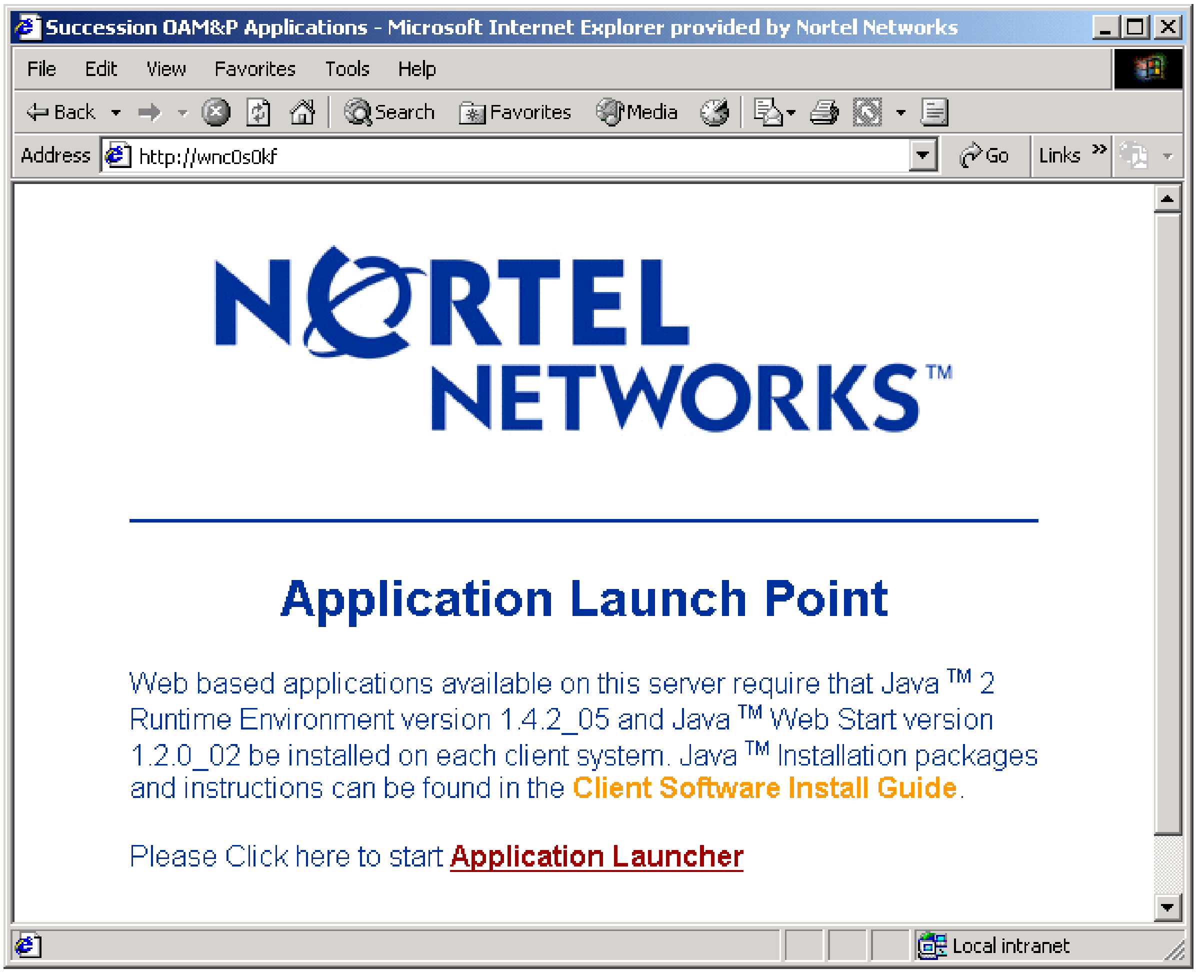
Accessing the user interfaces

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 204.

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.


Succession OAM&P Applications - Microsoft Internet Explorer provided by Nortel Networks
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://wnc0s0kf
Go Links
NORTEL NETWORKS
Local intranet

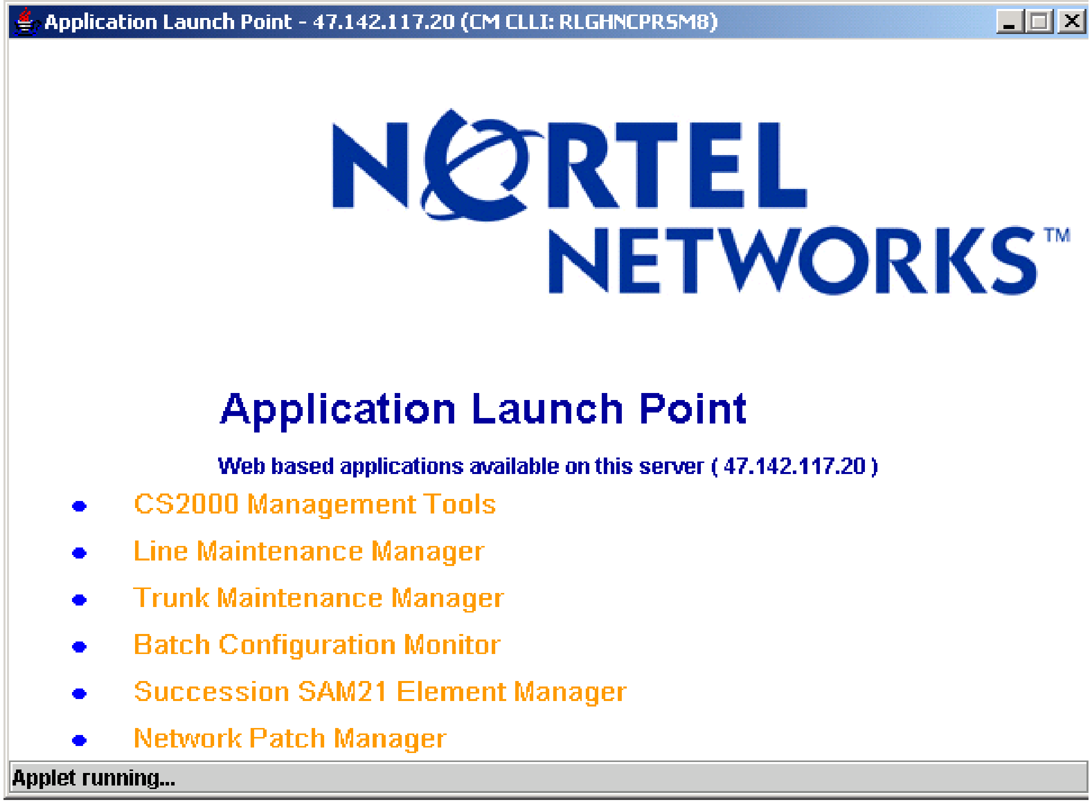
Application Launch Point

Web based applications available on this server require that Java^{TM} 2 Runtime Environment version 1.4.2_05 and Java^{TM} Web Start version 1.2.0_02 be installed on each client system. Java^{TM} Installation packages and instructions can be found in the Client Software Install Guide.

Please Click here to start Application Launcher

As indicated on the Application Launch Point page, Java^{TM} 2 Runtime Environment (JRE) version 1.4.2_05 and Java^{TM} 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.


Application Launch Point - 47.142.117.20 (CM CLLI: RLGHNCPRSM8)
NORTEL NETWORKS™

Application Launch Point

Web based applications available on this server (47.142.117.20)

- CS2000 Management Tools
- Line Maintenance Manager
- Trunk Maintenance Manager
- Batch Configuration Monitor
- Succession SAM21 Element Manager
- Network Patch Manager

Applet running...

> ***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 and NPM 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, NN10329-111.

The table titled Application to solution mapping on page 206, lists the applications that can be launched from the Application Launch Point, and indicates for each application, whether it is supported for a specific Carrier Voice over IP 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
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 compatiblity issues will be resolved using standard Nortel support processes.

Note 2: Ensure Solaris clients, using Java^{TM} 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 functionning 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 Carrier Voice over IP 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 210. Service applications provided in the main package are , Resource monitor, on page 284, 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 280, and the , Network Patch Manager, on page 259, 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

Software included with SSPFS

Vendor	Software
Apache	• Apache Web Server • Xerces Java Parser • Xalan
AppGate	• Mindterm
IBM	• DCE Client
Exolab group	• OpenORB notification • OpenORB Naming Service
Jakarta	• Tomcat • ORO • Log4J
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

Software included with SSPFS

Vendor	Software
Interhack	- rotatelog
Comprehensive Perl Archive Network	- Perl - Perl modules
DeleGate	- DeleGate
TrustICE	- Syslog client
NIST	- Expect
ILOG	- JTGO - JViews

File systems

The file system layout on SSPFS-based servers is as follows:

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 (applies to SSPFS-based servers that host the CS 2000 Management Tools, APS, and Integrated EMS)
/data/qca	QoS Collector Application (QCA) data (applies to SSPFS-based servers that host the CS 2000 Management Tools)
/data/mg9kem/logs	MG 9000 Manager logs (applies to SSPFS-based servers that host the MG 9000 Manager)

File system	Types of information stored in file system
/PROV_data	audio transaction files before they are sent to the UAS (applies to SSPFS-based servers that host the APS)
/user_audio files	audio uploaded from the user desktop prior to its import into the database (applies to SSPFS-based servers that host the APS)
/audio_files	audio data that has been imported into the database (applies to SSPFS-based servers that host the APS)

> ***Note:*** File systems "/", "/var", "/data", "/opt", and "/opt/nortel" are present on every SSPFS-based server. The other file systems vary according to the applications installed on the server.

Preset thresholds are established for file systems. When the threshold is exceeded, log SPFS 350 is generated. The preset thresholds and their severity are as follows:

- 70% - minor
- 80% - major
- 90% - critical

Backup and restore

You can back up and restore file systems and oracle data on a Succession Server Platform Foundation Software (SSPFS)-based server using a Digital Audio Tape (DAT) for Sun Netra t1400-type servers, or a CD or DVD for Sun Netra 240-type servers.

For backup and restore details and procedures, refer to the ATM/IP Security and Administration document, NN10402-600.

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

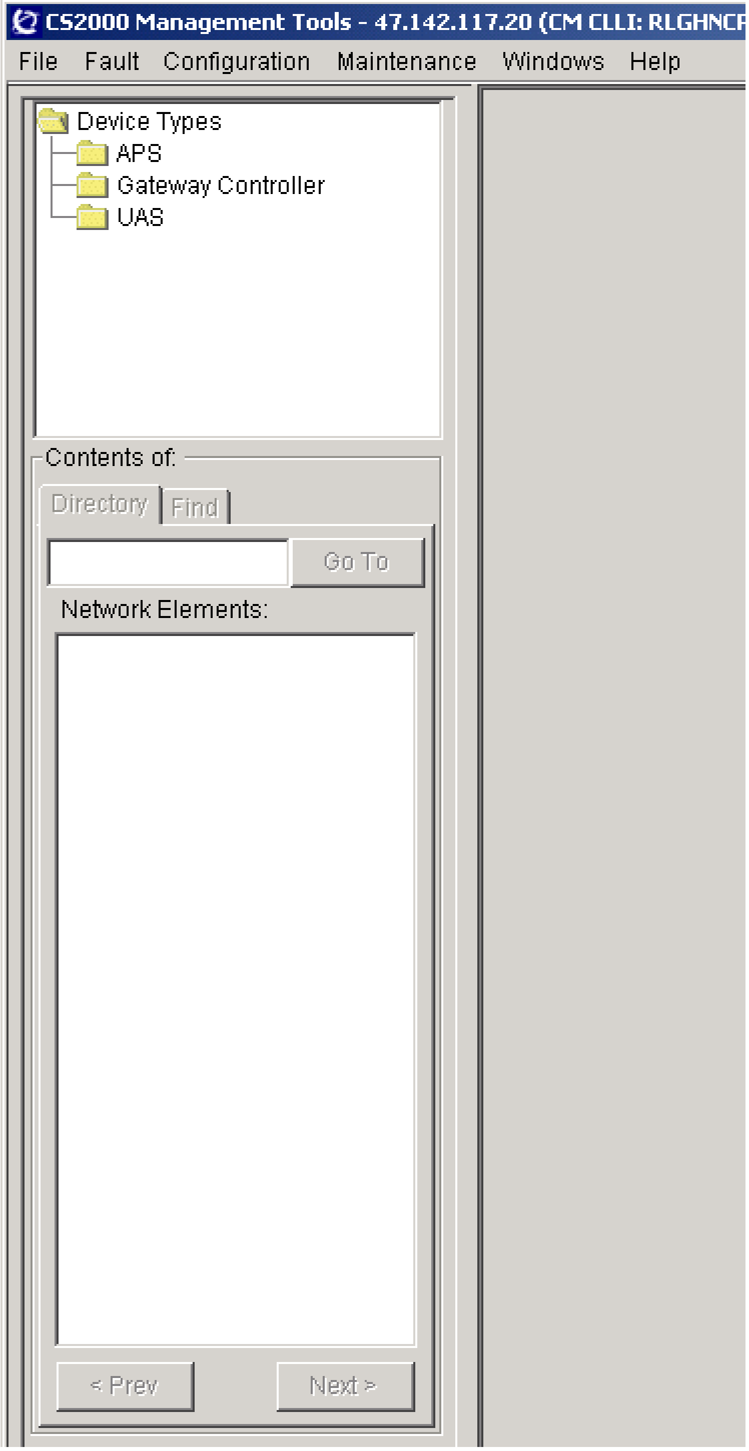
> ***Note:*** To determine if this application is supported for your solution, refer to the table titled Application to solution mapping on page 206.

User interface

The CS2000 Management Tools application GUI is accessed through the common launch page as previously described under Common launch page on page 204. 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:

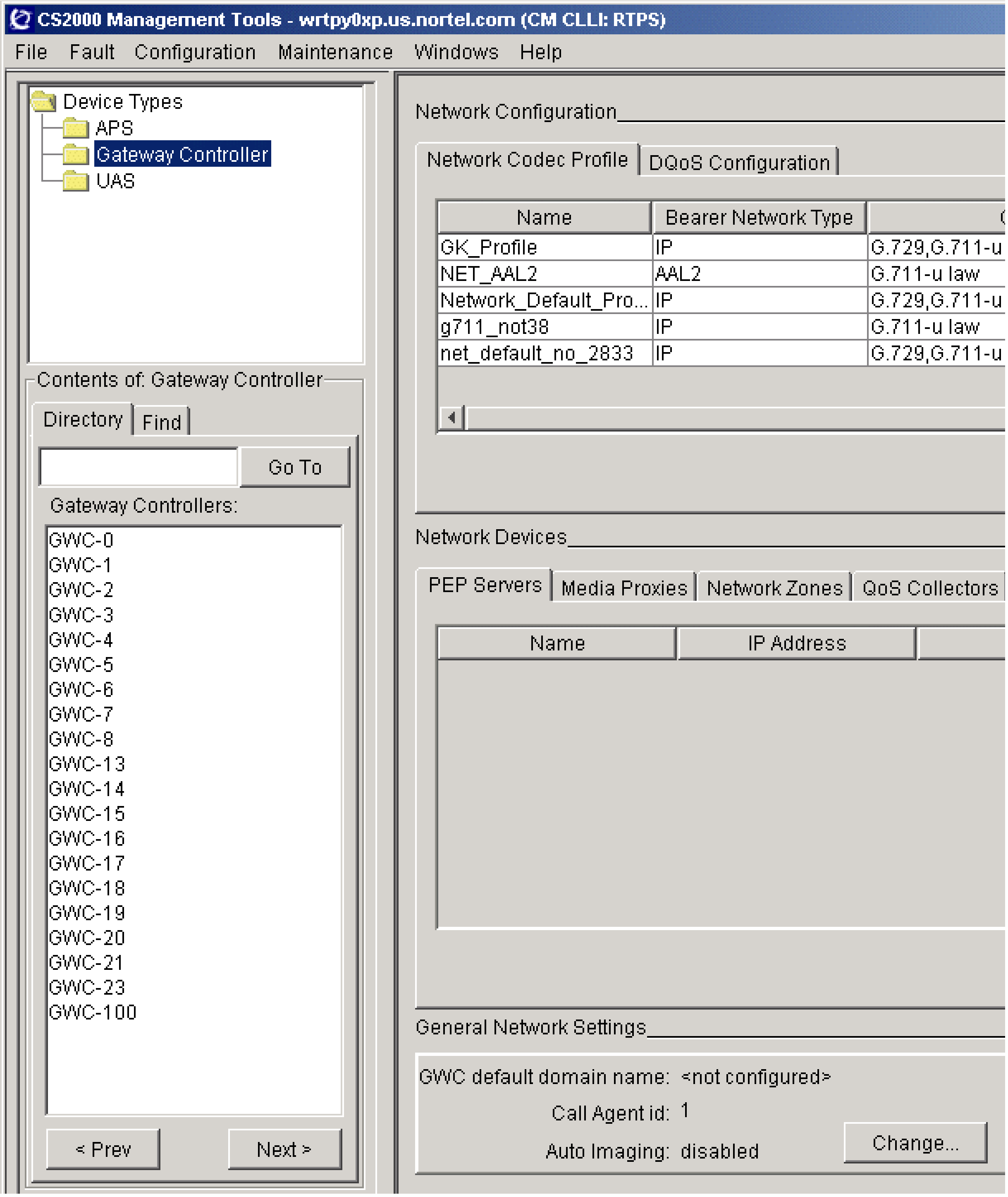
CS2000 Management Tools GUI


CS2000 Management Tools - 47.142.117.20 (CM CLLI: RLGHNCF
File Fault Configuration Maintenance Windows Help
Device Types
APS
Gateway Controller
UAS
Contents of:
Directory
Find
Go To
Network Elements:
< Prev
Next >

Selecting a device type in the Device Types folder results in the display of the provisioned network elements (for that device) in the Network

Elements pane. The Network Elements pane is located in the "Contents of" section. For example, selecting the Gateway Controller device type woud result in a display of the Gateway Controllers network elements similar to the following.

Gateway Controllers network elements



CS2000 Management Tools - wrtpy0xp.us.nortel.com (CM CLLI: RTPS)

Gateway Controllers:

GWC-0
GWC-1
GWC-2
GWC-3
GWC-4
GWC-5
GWC-6
GWC-7
GWC-8
GWC-13
GWC-14
GWC-15
GWC-16
GWC-17
GWC-18
GWC-19
GWC-20
GWC-21
GWC-23
GWC-100

Name	Bearer Network Type	(
GK_Profile	IP	G.729,G.711-u
NET_AAL2	AAL2	G.711-u law
Network_Default_Pro...	IP	G.729,G.711-u
g711_not38	IP	G.711-u law
net_default_no_2833	IP	G.729,G.711-u

GWC default domain name: <not configured>

Call Agent id: 1

Auto Imaging: disabled

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 at the bottom.

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 222, CS 2000 GWC Manager on page 224, or Universal Audio Server Manager on page 231 in this document.

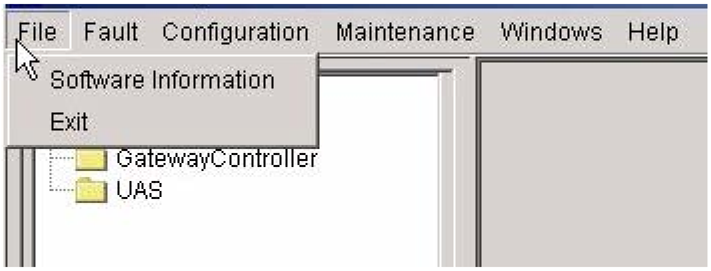
The sections that follow briefly describe the options available under each menu in the CS2000 Management Tools GUI.

> ***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.

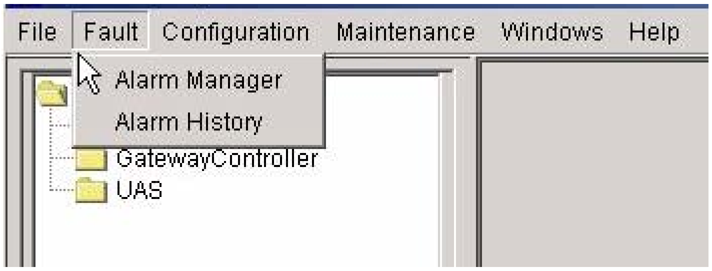
File menu



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.

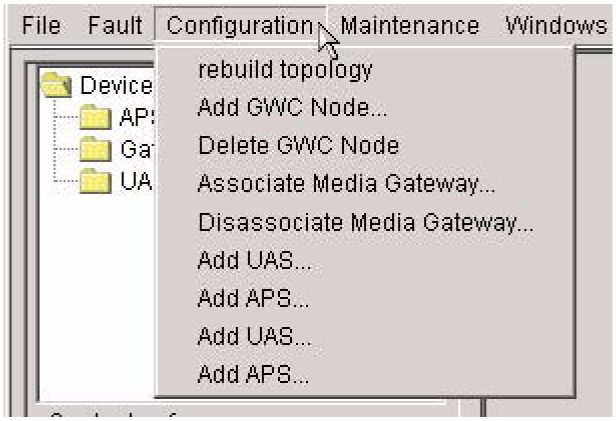
Fault menu



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

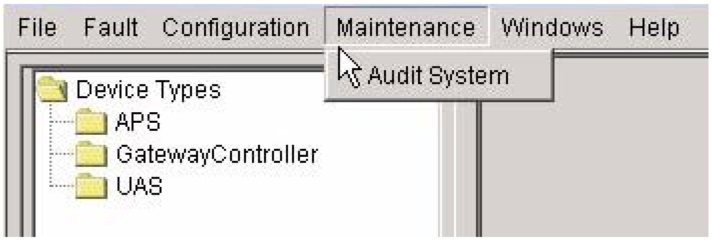


Maintenance

The Maintenance menu contains the Audit System option used to perform a line data integrity, trunk data integrity or CS2K data integrity audit. The V5.2 Data Integrity audit is available in the International version of the software, and not in the North American version shown here.

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.

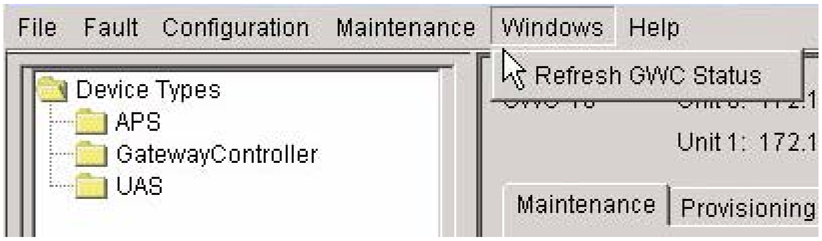
Maintenance menu



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.

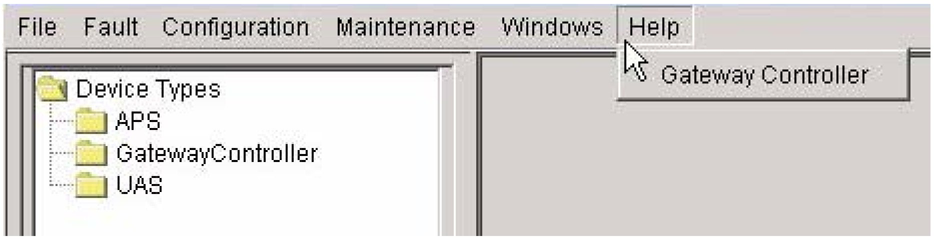
Windows menu



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 206.

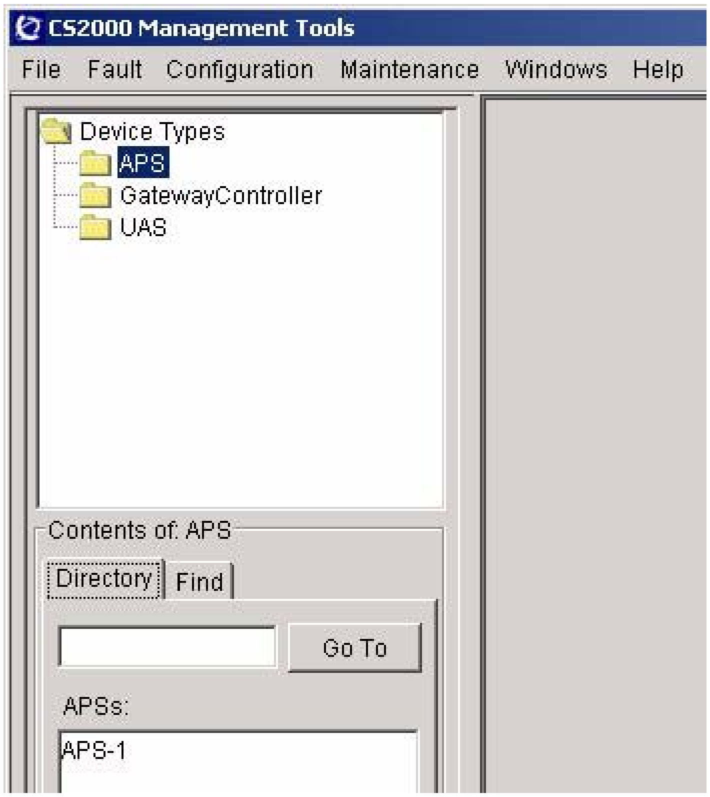
For procedures on how to provision and maintain APS NEs, refer to the UAS documentation suite.

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 204. 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

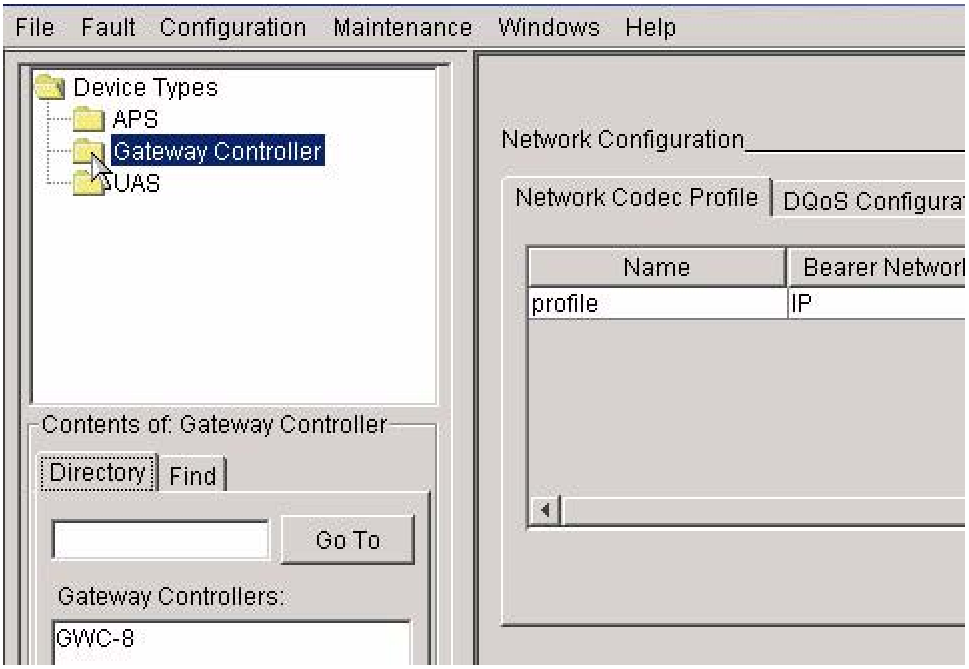
The CS 2000 GWC Manager is used to manage the GWC network elements (NEs) within a Carrier Voice over IP Network.

This section provides a brief overview of the CS 2000 GWC Manager. For procedures on how to provision and maintain GWC NEs and associated devices 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 204. 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, diplays network configuration information in the right pane (network view). The information applies to all GWC NEs in the network.

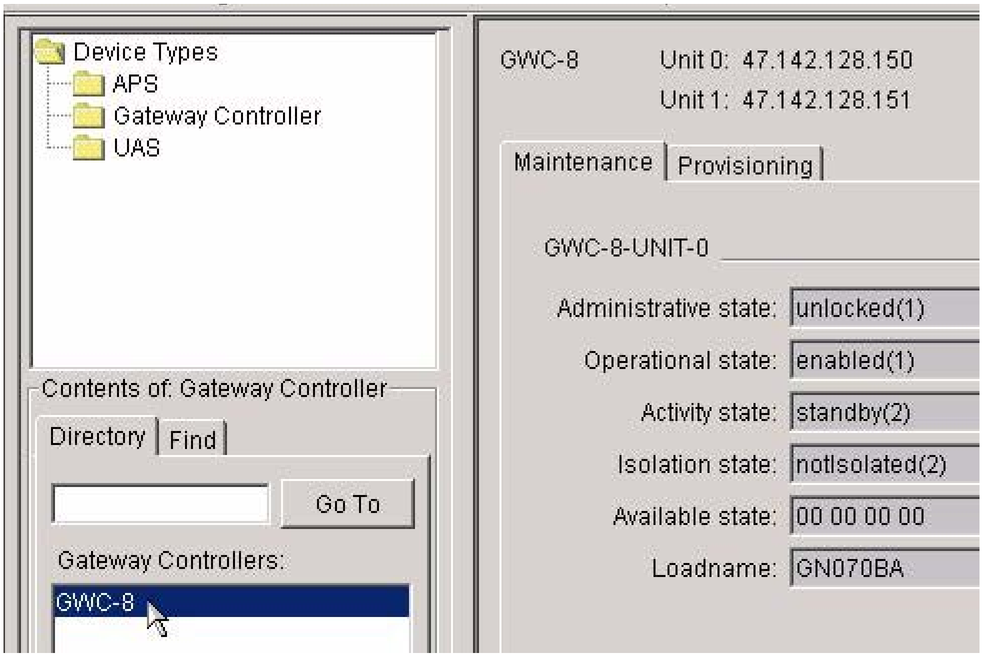


Gateway Controllers: GWC-8

Name	Bearer Networl
profile	IP

Network view

Selecting a specifc 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).



GWC-8 Unit 0: 47.142.128.150
Unit 1: 47.142.128.151

GWC-8-UNIT-0

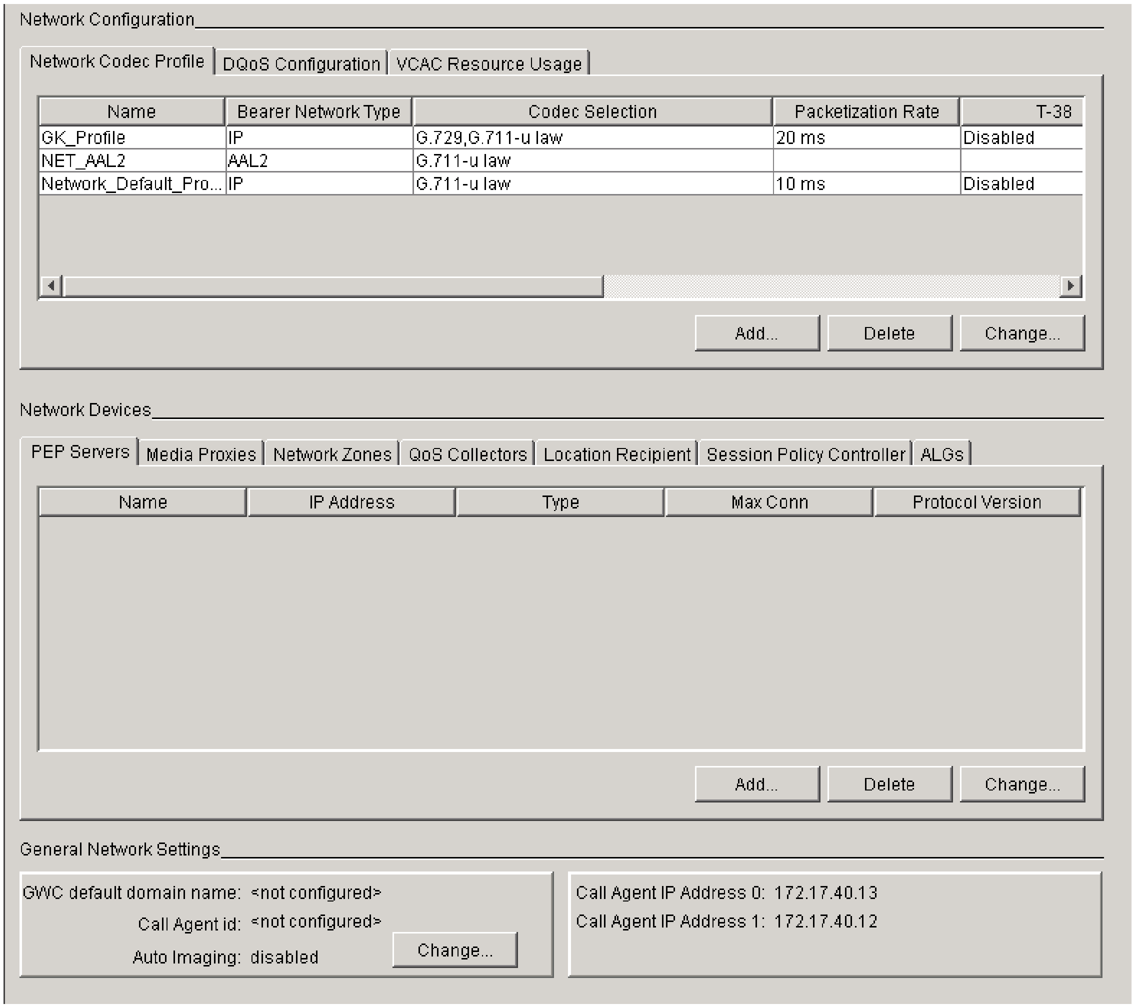
Administrative state: unlocked(1)
Operational state: enabled(1)
Activity state: standby(2)
Isolation state: notIsolated(2)
Available state: 00 00 00 00
Loadname: GN070BA

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 214

Network view

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



Name	Bearer Network Type	Codec Selection	Packetization Rate	T-38
GK_Profile	IP	G.729,G.711-u law	20 ms	Disabled
NET_AAL2	AAL2	G.711-u law		
Network_Default_Pro...	IP	G.711-u law	10 ms	Disabled

Name	IP Address	Type	Max Conn	Protocol Version

GWC default domain name: <not configured>
Call Agent id: <not configured>
Auto Imaging: disabled

Call Agent IP Address 0: 172.17.40.13
Call Agent IP Address 1: 172.17.40.12

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.
- Network Zones tab - Add or delete a Network Address Translations (NAT) device to or from the network, change the information of an existing NAT device, display the ID of a NAT device, add or delete a limited bandwidth link (LBL) device to or from the network, change the information of an existing LBL device, and provision a network zone that contains both NAT and LBL devices.
- 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 229).
- Session Policy Controller tab - Add or delete a Session Policy Controller (SPC) to or from the network, change the information of an existing SPC, and enable or disable Virtual Connection Admission Control (VCAC) in the network.
- ALGs tab - Add or delete an Application Layer Gateway (ALG) device, and change the information of an existing ALG device.

General Network Settings

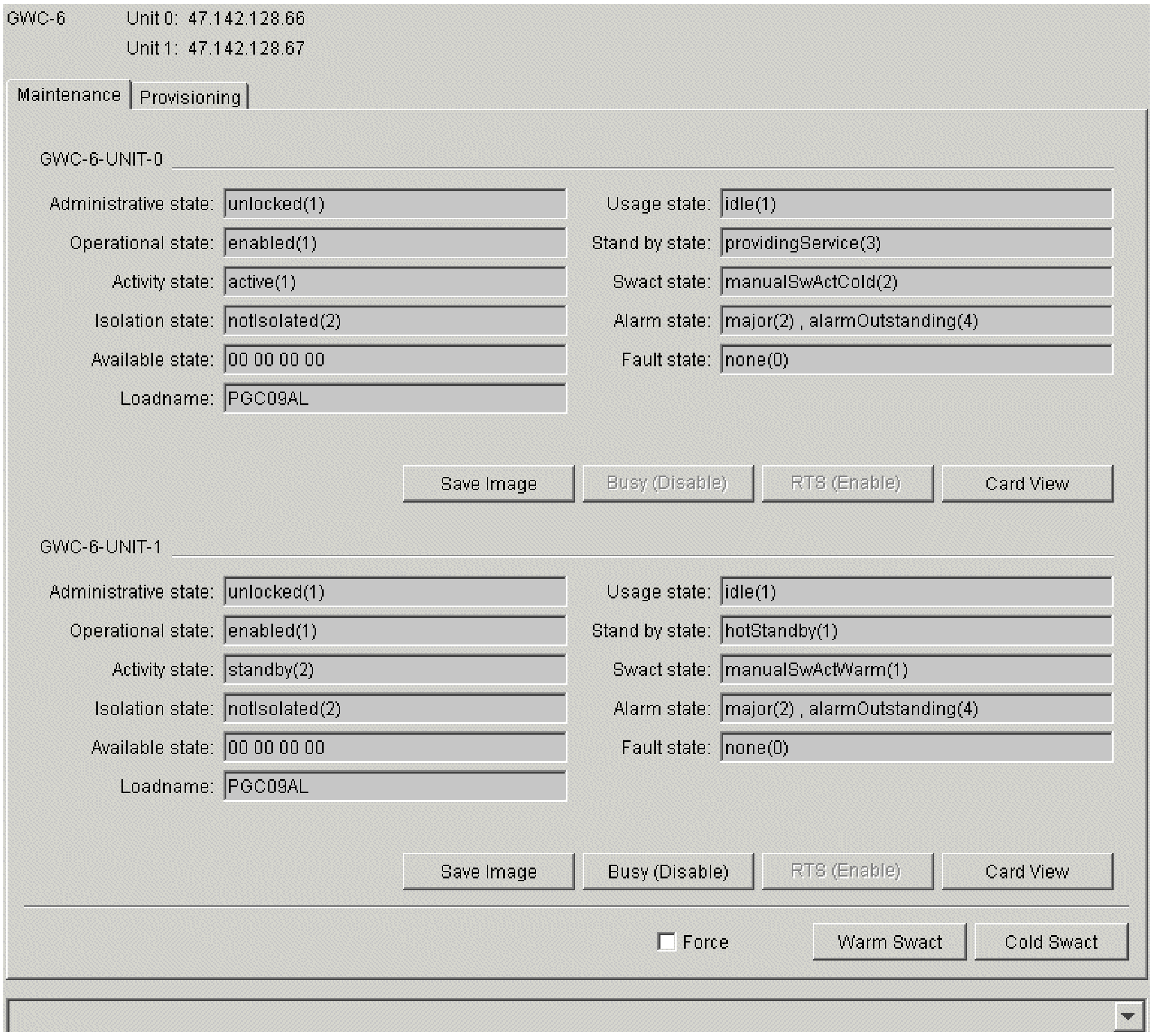
- Change button - Add, change, or delete the GWC domain name, change the call agent identifier, and enable or disable periodic auto-imaging of GWC loads. It is recommended that auto imaging be enabled in order to prevent potential losses of patching applications.
- Call Agent IP address - displays the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

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.



GWC-6 Unit 0: 47.142.128.66
Unit 1: 47.142.128.67

GWC-6-UNIT-0

Administrative state:	unlocked(1)	Usage state:	idle(1)
Operational state:	enabled(1)	Stand by state:	providingService(3)
Activity state:	active(1)	Swact state:	manualSwActCold(2)
Isolation state:	notIsolated(2)	Alarm state:	major(2) , alarmOutstanding(4)
Available state:	00 00 00 00	Fault state:	none(0)
Loadname:	PGC09AL		

GWC-6-UNIT-1

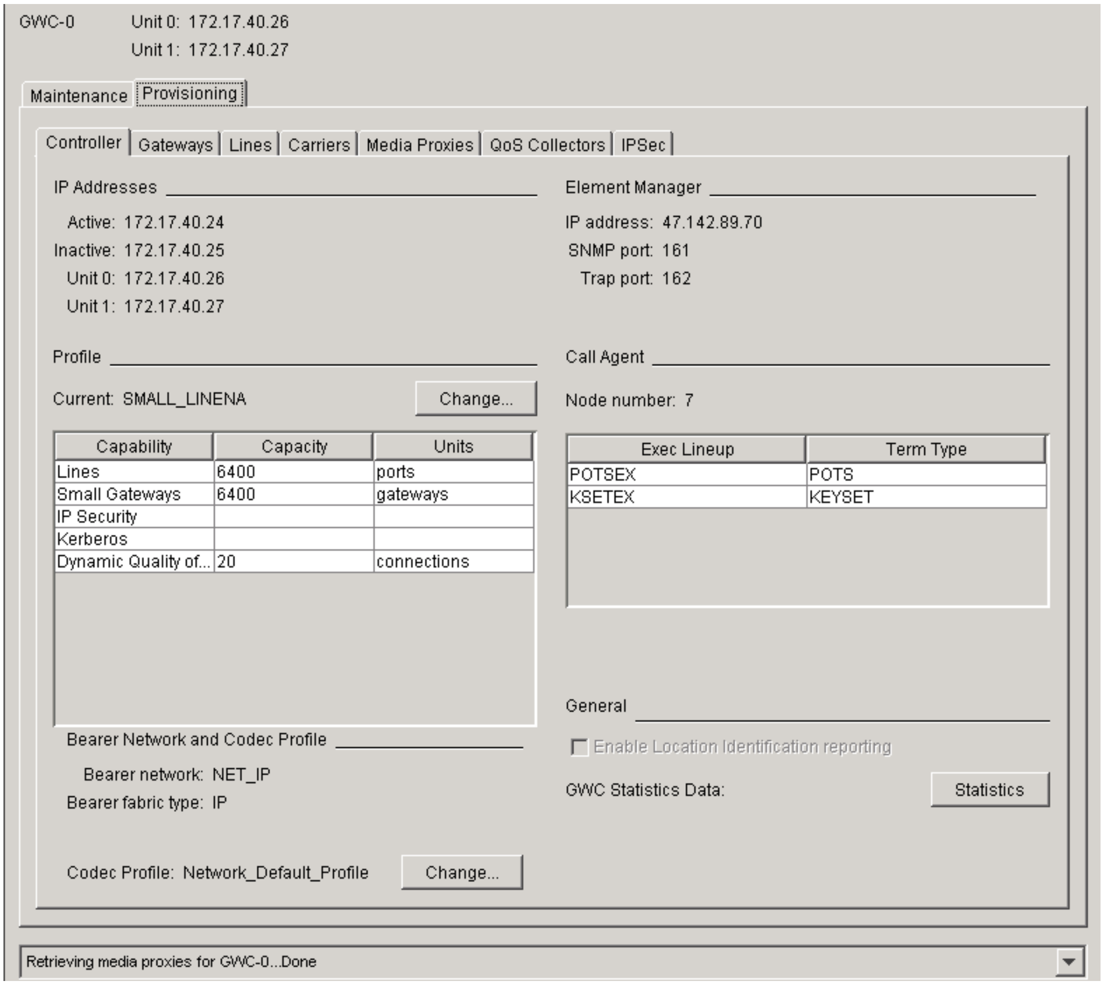
Administrative state:	unlocked(1)	Usage state:	idle(1)
Operational state:	enabled(1)	Stand by state:	hotStandby(1)
Activity state:	standby(2)	Swact state:	manualSwActWarm(1)
Isolation state:	notIsolated(2)	Alarm state:	major(2) , alarmOutstanding(4)
Available state:	00 00 00 00	Fault state:	none(0)
Loadname:	PGC09AL		

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.



GWC-0 Unit 0: 172.17.40.26
Unit 1: 172.17.40.27

Active: 172.17.40.24
Inactive: 172.17.40.25
Unit 0: 172.17.40.26
Unit 1: 172.17.40.27

IP address: 47.142.89.70
SNMP port: 161
Trap port: 162

Current: SMALL_LINENA

Node number: 7

Capability	Capacity	Units
Lines	6400	ports
Small Gateways	6400	gateways
IP Security		
Kerberos		
Dynamic Quality of...	20	connections

Exec Lineup	Term Type
POTSEX	POTS
KSETEX	KEYSET

□ Enable Location Identification reporting

GWC Statistics Data:

Bearer network: NET_IP
Bearer fabric type: IP

Codec Profile: Network_Default_Profile

Retrieving media proxies for GWC-0...Done

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, view the total number of reserved endpoints for the gateway controller, 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 226).
- 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 Carrier Voice over IP Network. With the UAS Manager application, users can view general information, perform various configuration and maintenance tasks, and view performance measurements for UAS NEs.

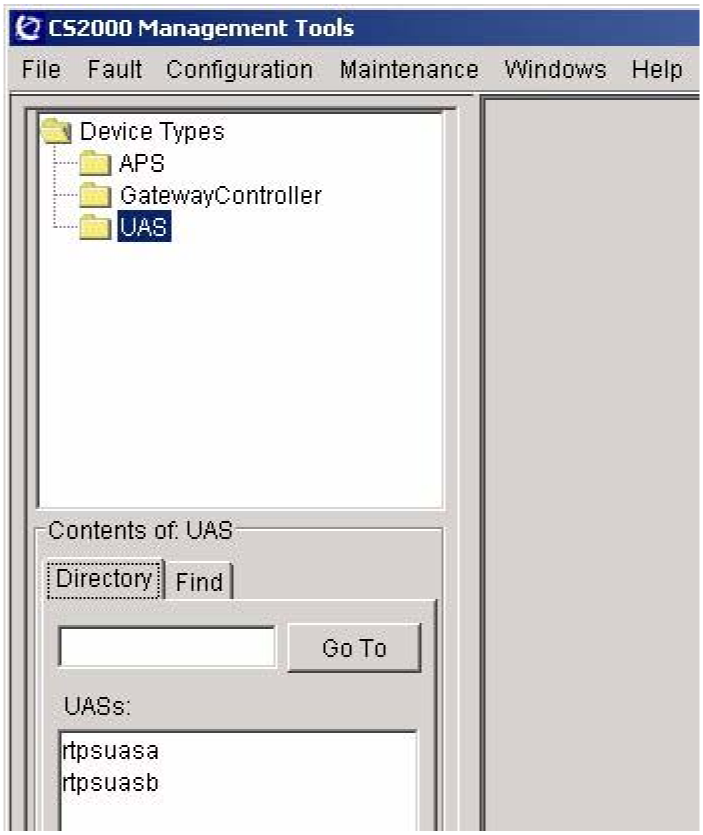
This section provides a brief overview of the UAS Manager. For procedures on how to provision and maintain UAS NEs using the UAS Manager, refer to the UAS documentation suite.

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 204. 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.

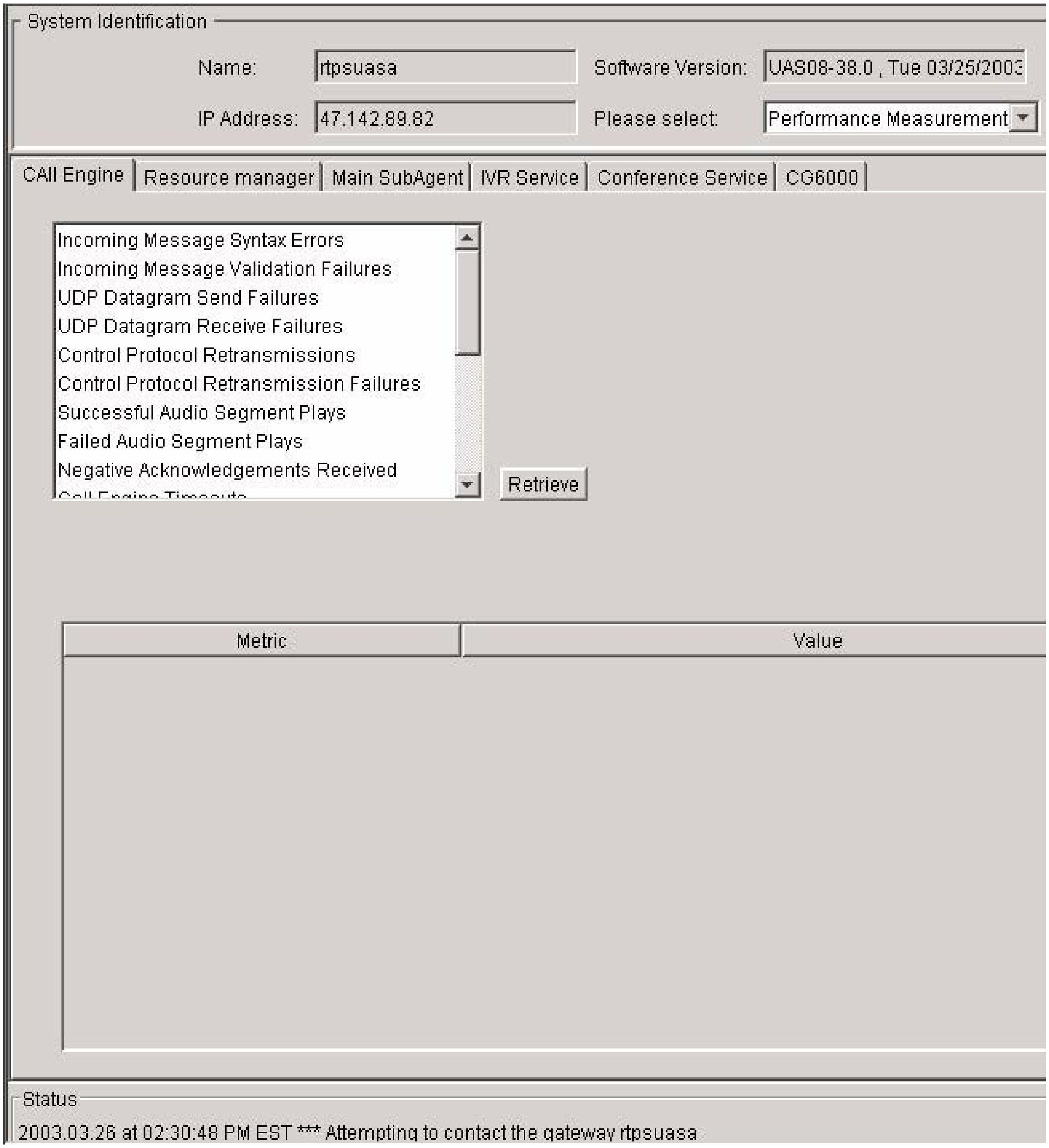
When the UAS device type is selected, a window, similar to the following is displayed:

Selecting UAS



Selecting a specifc 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



Name: rtpsuasa

Software Version: UAS08-38.0 , Tue 03/25/2003

IP Address: 47.142.89.82

Please select: Performance Measurement

Incoming Message Syntax Errors
Incoming Message Validation Failures
UDP Datagram Send Failures
UDP Datagram Receive Failures
Control Protocol Retransmissions
Control Protocol Retransmission Failures
Successful Audio Segment Plays
Failed Audio Segment Plays
Negative Acknowledgements Received
Call Engine Timeouts

2003.03.26 at 02:30:48 PM EST *** Attempting to contact the gateway rtpsuasa

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.

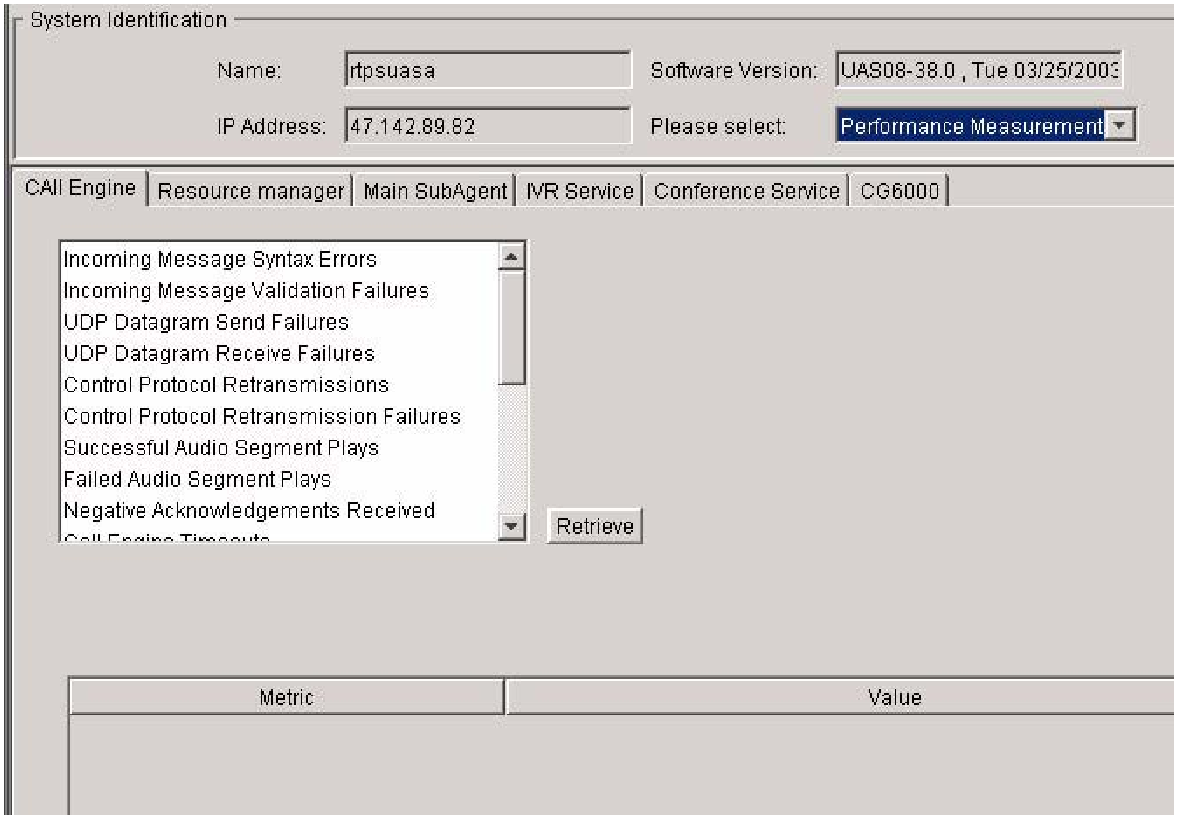
Managing UAS NEs is done through the Performance Measurement, Configuration, Maintenance, and SNMP Configuration options of the UAS Manager, and some menu options in the CS2000 Management Tools application GUI as previously mentioned in CS2000 Management Tools application on page 214.

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



System Identification

Name: rtpsuasa

Software Version: UAS08-38.0 , Tue 03/25/2003

IP Address: 47.142.89.82

Please select: Performance Measurement

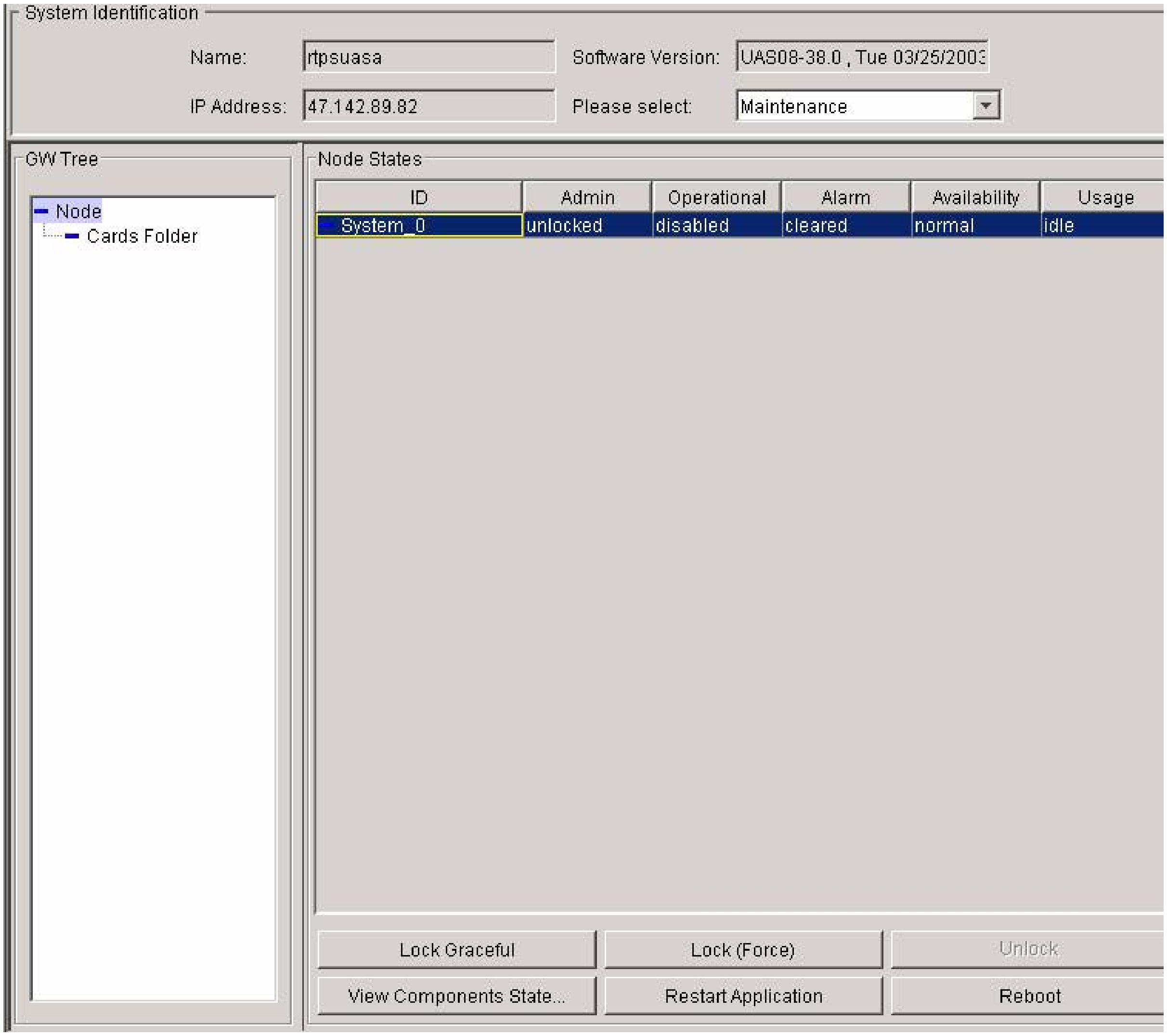
CAll Engine
Resource manager
Main SubAgent
IVR Service
Conference Service
CG6000
Incoming Message Syntax Errors
Incoming Message Validation Failures
UDP Datagram Send Failures
UDP Datagram Receive Failures
Control Protocol Retransmissions
Control Protocol Retransmission Failures
Successful Audio Segment Plays
Failed Audio Segment Plays
Negative Acknowledgements Received
Call Engine Timeouts
Retrieve
Metric
Value

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)



Name: rtpsuasa

Software Version: UAS08-38.0 , Tue 03/25/2003

IP Address: 47.142.89.82

Please select: Maintenance

ID	Admin	Operational	Alarm	Availability	Usage
System_0	unlocked	disabled	cleared	normal	idle

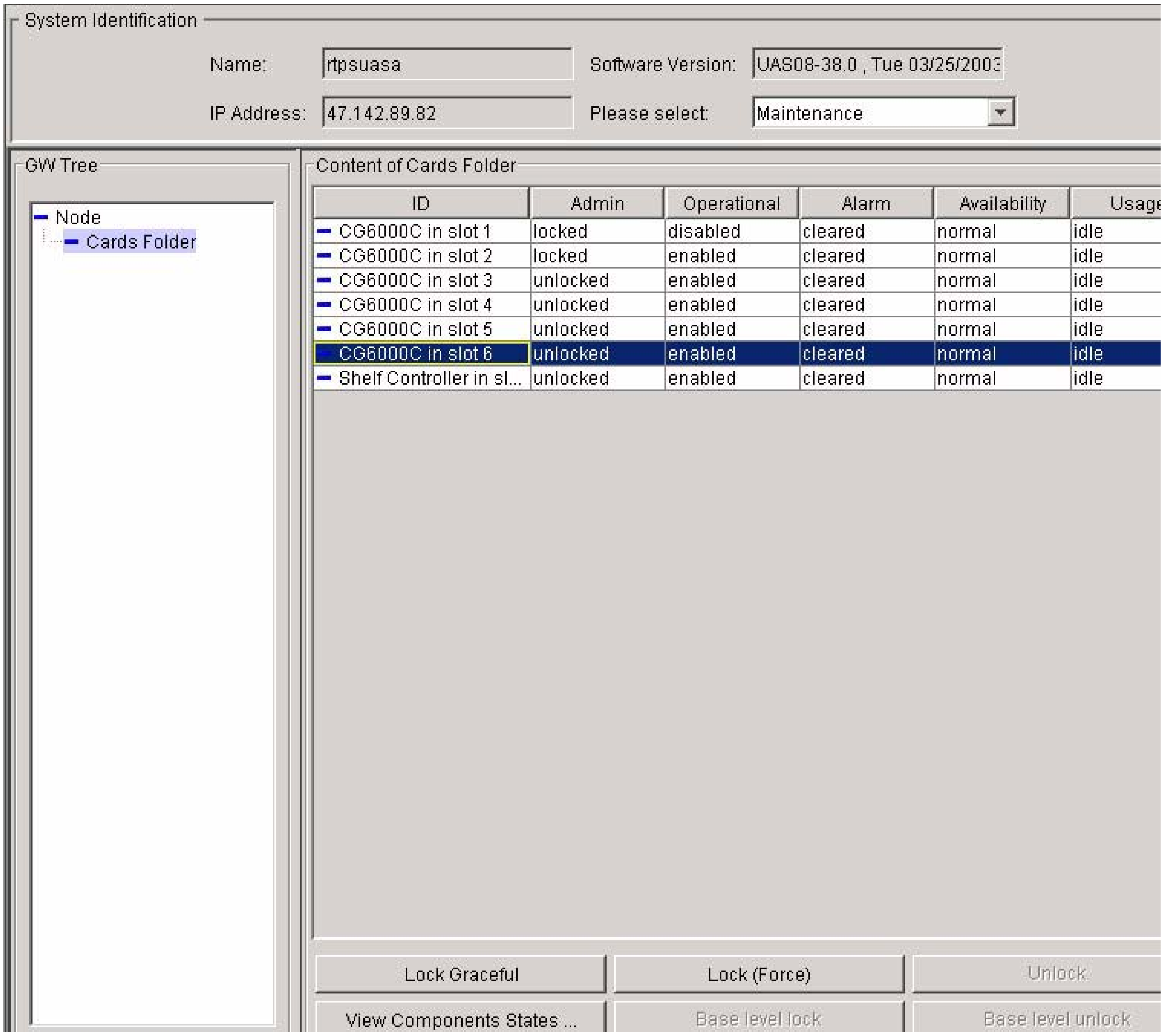
From this window, you can perform any one of the following activities: reboot the UAS, restart the UA

- 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)



System Identification

Name: rtpsuasa

Software Version: UAS08-38.0 , Tue 03/25/2003

IP Address: 47.142.89.82

Please select: Maintenance

Content of Cards Folder

ID	Admin	Operational	Alarm	Availability	Usage
CG6000C in slot 1	locked	disabled	cleared	normal	idle
CG6000C in slot 2	locked	enabled	cleared	normal	idle
CG6000C in slot 3	unlocked	enabled	cleared	normal	idle
CG6000C in slot 4	unlocked	enabled	cleared	normal	idle
CG6000C in slot 5	unlocked	enabled	cleared	normal	idle
CG6000C in slot 6	unlocked	enabled	cleared	normal	idle
Shelf Controller in sl...	unlocked	enabled	cleared	normal	idle

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

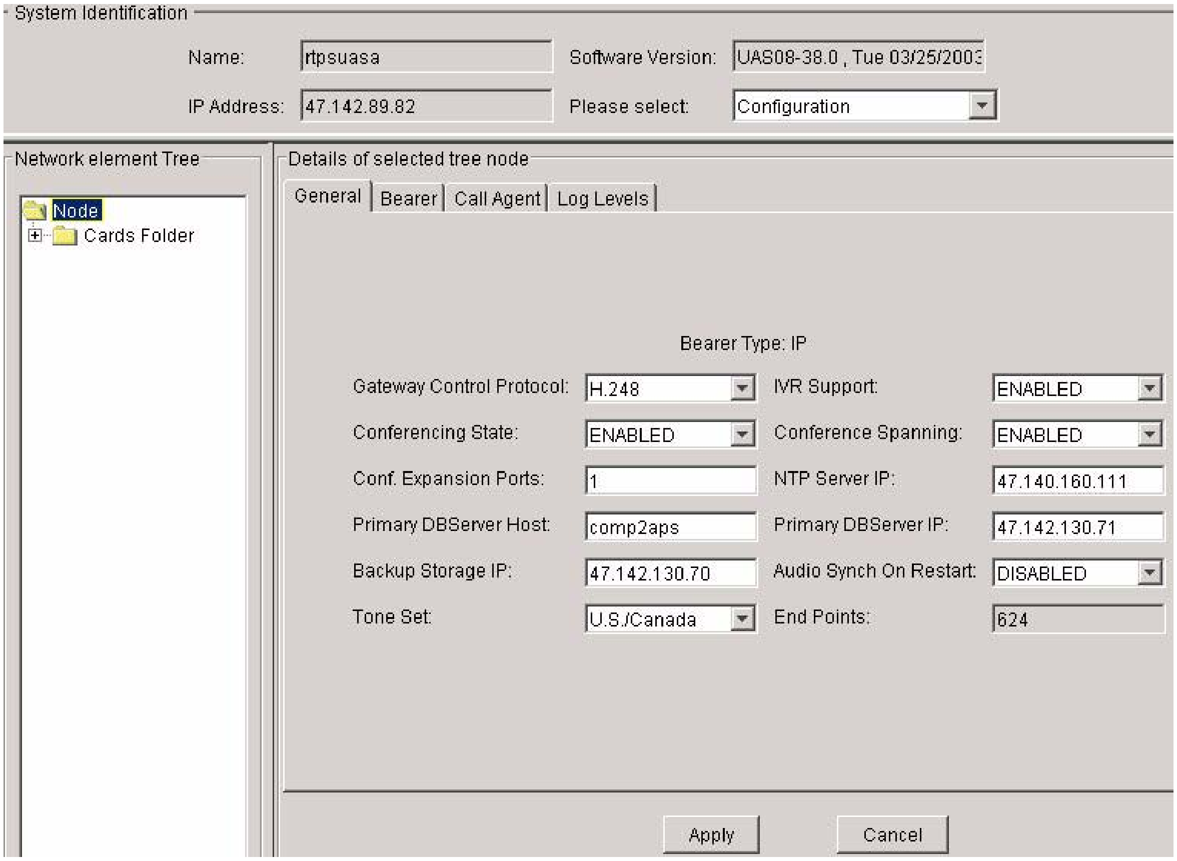
- Lock Graceful button - lock a card but not completety shut it down (used to perform some administrative tasks on the card)
- Lock (Force) button - lock a card (overriding any pending operations)
- Unlock button - unlock a card
- View Component States... button - view component states associated with 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)



System Identification

Name: rtpsuasa

Software Version: UAS08-38.0 , Tue 03/25/2003

IP Address: 47.142.89.82

Please select: Configuration

Bearer Type: IP

Gateway Control Protocol: H.248

IVR Support: ENABLED

Conferencing State: ENABLED

Conference Spanning: ENABLED

Conf. Expansion Ports: 1

NTP Server IP: 47.140.160.111

Primary DBServer Host: comp2aps

Primary DBServer IP: 47.142.130.71

Backup Storage IP: 47.142.130.70

Audio Synch On Restart: DISABLED

Tone Set: U.S./Canada

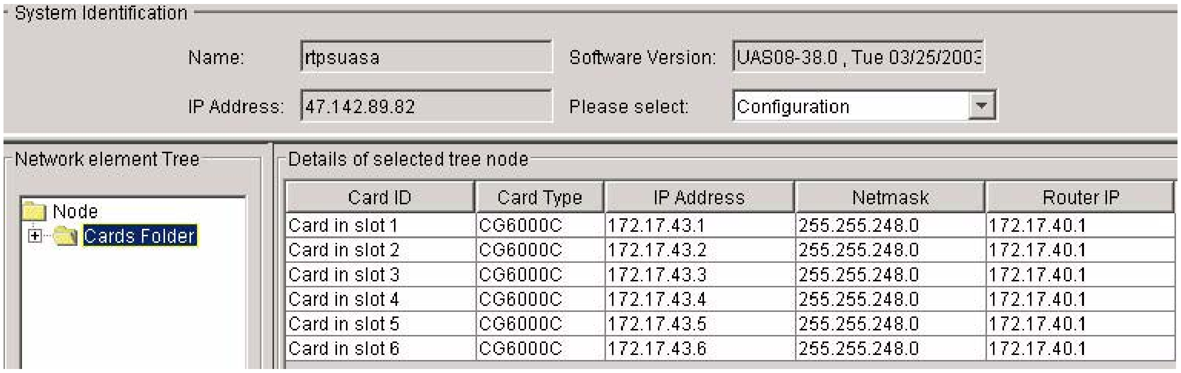
End Points: 624

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)



System Identification

Name: rtpsuasa

Software Version: UAS08-38.0 , Tue 03/25/2003

IP Address: 47.142.89.82

Please select: Configuration

Network element Tree

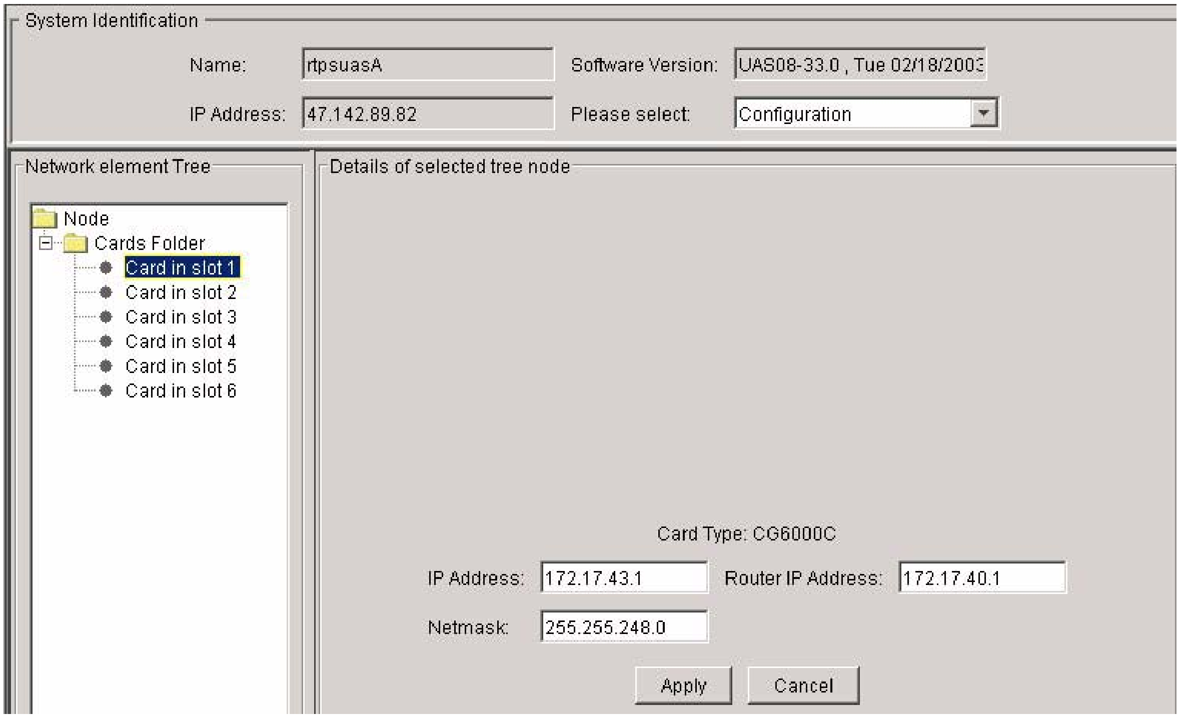
Details of selected tree node

Card ID	Card Type	IP Address	Netmask	Router IP
Card in slot 1	CG6000C	172.17.43.1	255.255.248.0	172.17.40.1
Card in slot 2	CG6000C	172.17.43.2	255.255.248.0	172.17.40.1
Card in slot 3	CG6000C	172.17.43.3	255.255.248.0	172.17.40.1
Card in slot 4	CG6000C	172.17.43.4	255.255.248.0	172.17.40.1
Card in slot 5	CG6000C	172.17.43.5	255.255.248.0	172.17.40.1
Card in slot 6	CG6000C	172.17.43.6	255.255.248.0	172.17.40.1

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)



System Identification

Name: rtpsuasA

Software Version: UAS08-33.0 , Tue 02/18/2003

IP Address: 47.142.89.82

Please select: Configuration

Network element Tree

Details of selected tree node

Card Type: CG6000C

IP Address: 172.17.43.1

Router IP Address: 172.17.40.1

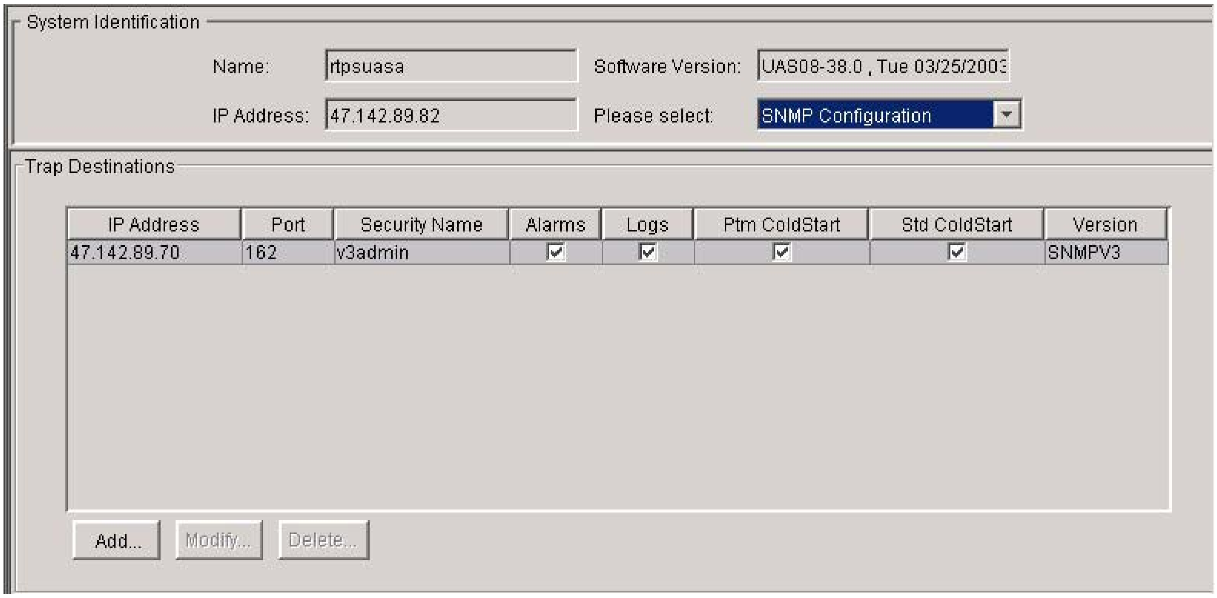
Netmask: 255.255.248.0

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



System Identification

Name: rtpsuasa

Software Version: UAS08-38.0 , Tue 03/25/2003

IP Address: 47.142.89.82

Please select: SNMP Configuration

Trap Destinations

IP Address	Port	Security Name	Alarms	Logs	Ptm ColdStart	Std ColdStart	Version
47.142.89.70	162	v3admin	☑	☑	☑	☑	SNMPV3

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 206.
>
> ***Note 2:*** The LMM does not currently support hunt groups.

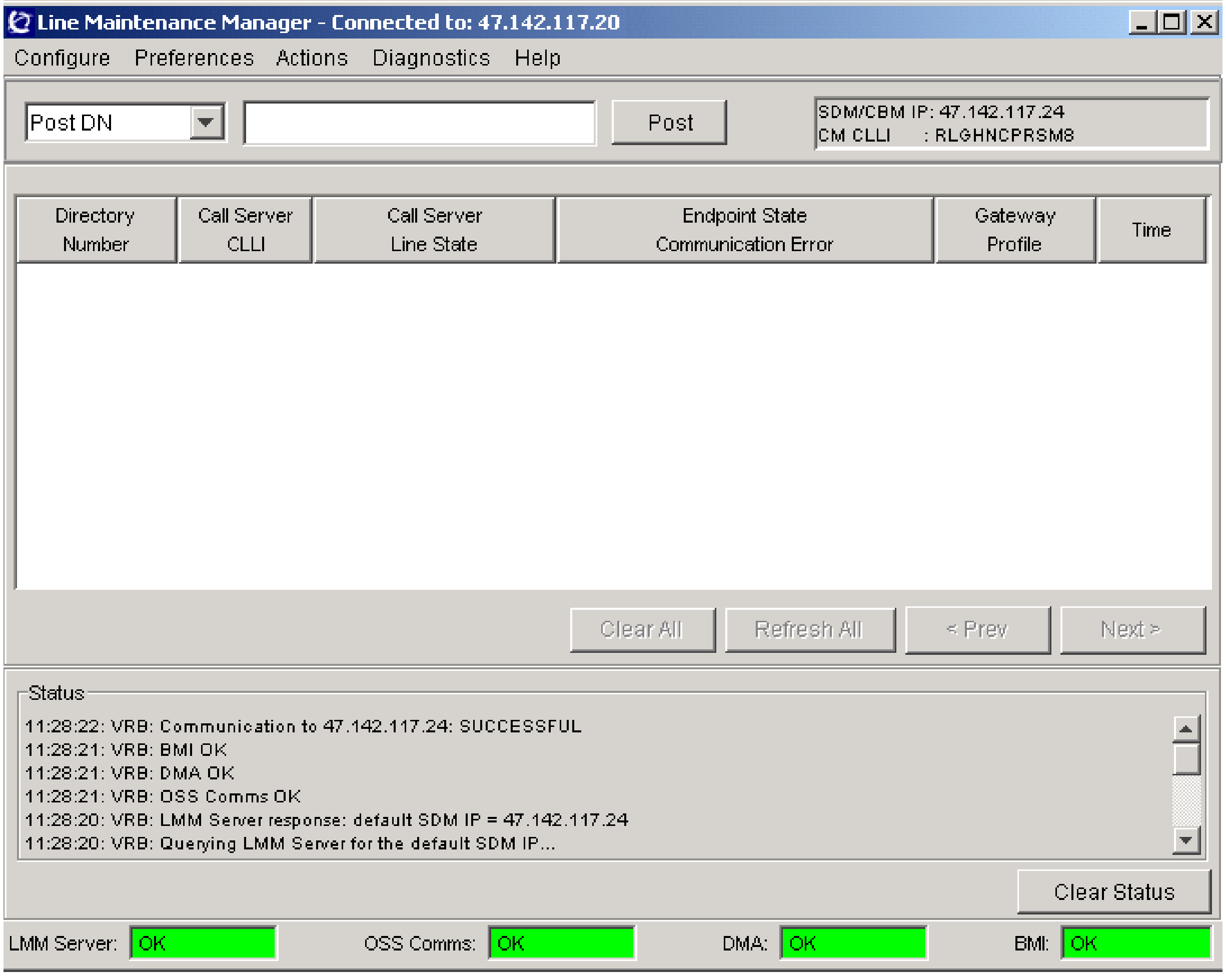
This section provides a brief overview of the LMM. For procedures on how to perform line maintenance activities using the LMM, refer to the Fault document.

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 204. 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



SDM/CBM IP: 47.142.117.24
CM CLLI : RLGHNCPRSM8

```
11:28:22: VRB: Communication to 47.142.117.24: SUCCESSFUL
11:28:21: VRB: BMI OK
11:28:21: VRB: DMA OK
11:28:21: VRB: OSS Comms OK
11:28:20: VRB: LMM Server response: default SDM IP = 47.142.117.24
11:28:20: VRB: Querying LMM Server for the default SDM IP...
```

LMM Server: OK OSS Comms: OK DMA: OK BMI: OK

The main panel displays the following information:

- **SDM/CBM IP address and CM CLLI** - The IP address of the core manager (SDM/CBM) and associated 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:

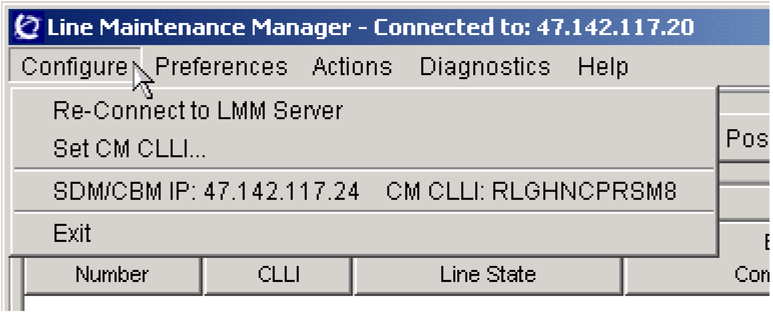
- **Post** - Post the lines according the selection in the pull down menu. Selecting Post DN, displays a line by its directory number (DN). Selecting Post by Gateway, displays the lines associated with the specific gateway.
- **Clear All** - Remove all posted lines from the display.
- **Refresh All** - 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 when the connection times out, set or re-set the CLLI of the Communication Server 2000 by setting the IP address of the core manager (SDM/CBM), which automatically retrieves the associated CM CLLI, and exit the LMM GUI

Configure menu

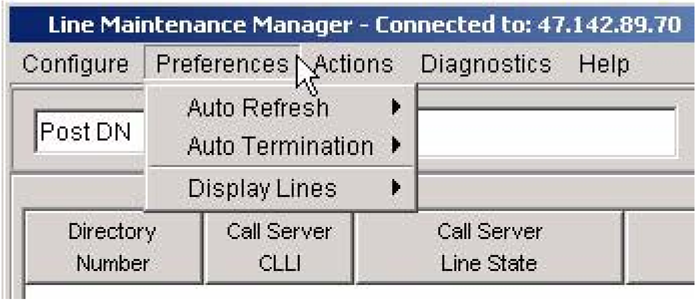

Line Maintenance Manager - Connected to: 47.142.117.20

SDM/CBM IP: 47.142.117.24 CM CLLI: RLGHNCPRSM8

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, and disable Auto refresh, cancel pending CPD requests, and display a fixed number of lines

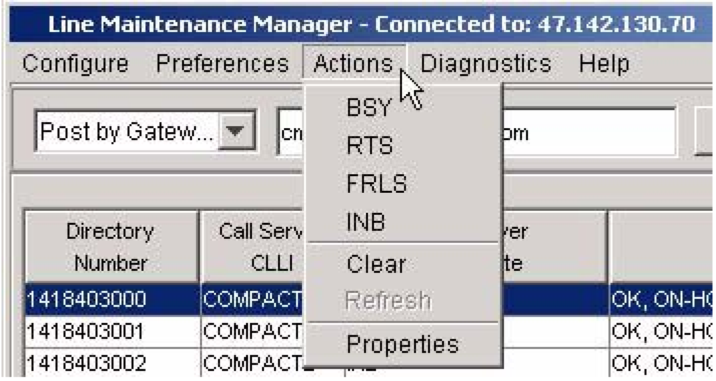
Preferences menu



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.

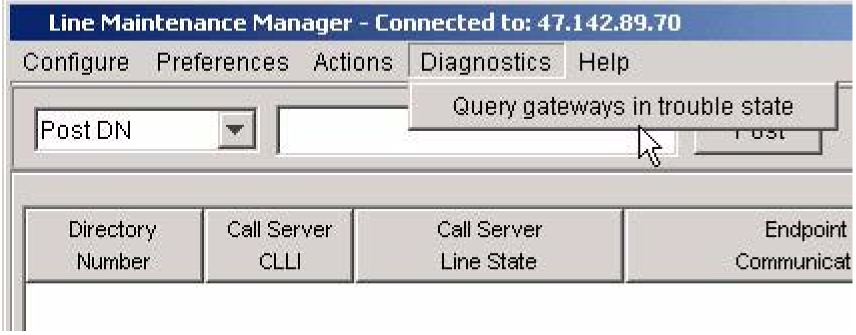
Actions menu


Line Maintenance Manager - Connected to: 47.142.130.70
Configure
Preferences
Actions
Diagnostics
Help
BSY
RTS
FRLS
INB
Clear
Refresh
Properties
Post by Gatew...
cn
om
Directory Number
Call Serv CLLI
ver te
1418403000 COMPACT OK, ON-HO
1418403001 COMPACT OK, ON-HO
1418403002 COMPACT OK, ON-HO

Diagnostics

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

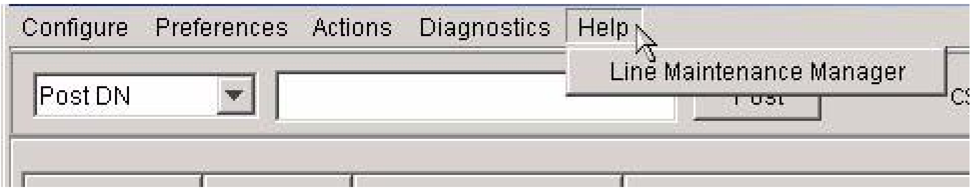
Diagnostics menu



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 206.

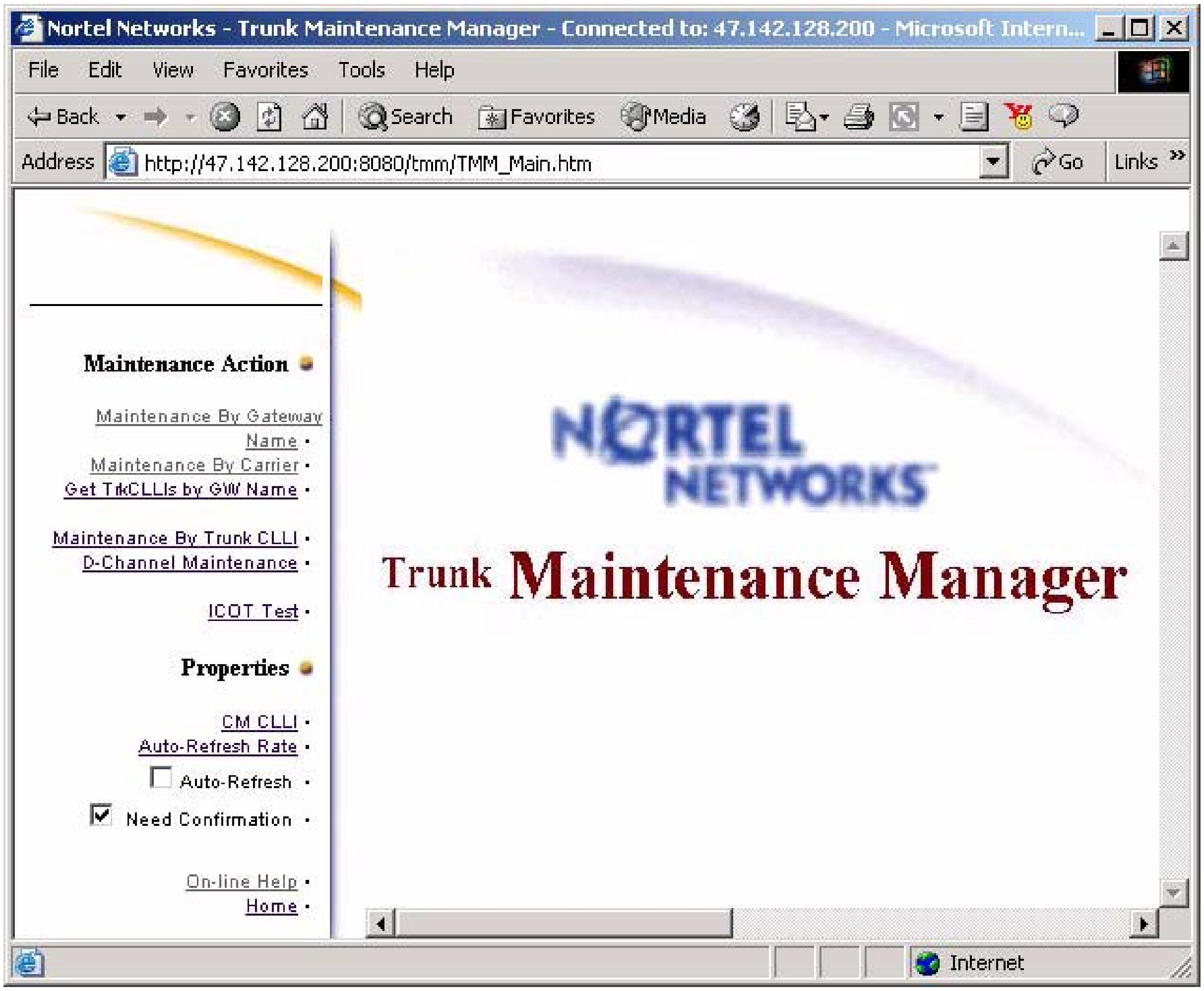
This section provides a brief overview of the TMM. For procedures on how to perform trunk maintenance activities using the TMM, refer to the ATM/IP Solution-level Fault Management document, NN10408-900.

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 204. 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



□ Auto-Refresh

☑ Need Confirmation

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 group 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 trunk member selected by CLLI name.

- **CM CLLI** - Set or re-set the CLLI of the Communication Server 2000 by setting the IP address of the core manager (SDM/CBM), which automatically retrieves the associated 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 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

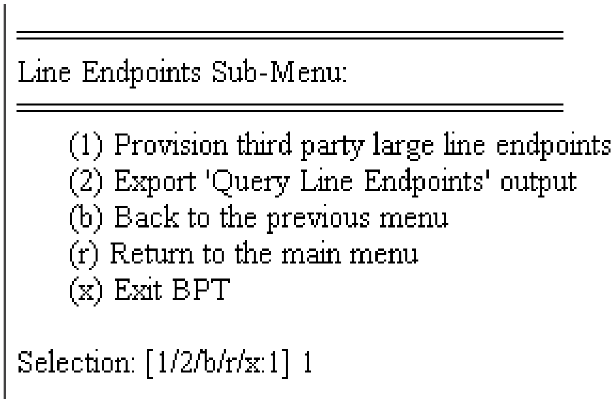
The Execute Batch File option allows you to execute batch provisioning commands. When you select this option, the Provisionining Input Entry Menu, similar to the following, is displayed.

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


     (1) Lines
     (2) ADSL
     (3) Line Endpoints
     (4) 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
- Line Endpoints
- 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

Line Endpoints

The Line Endpoints sub-menu of the Provisioning Input Entry Menu allows you to provision third party large line endpoints, and to export "Query Line Endpoints" output. When you select the Line Endpoints option, the Line Endpoints Sub-Menu, similar to the following, is displayed.



```
=====================================================
Line Endpoints Sub-Menu:
=====================================================
      (1) Provision third party large line endpoints
      (2) Export 'Query Line Endpoints' output
      (b) Back to the previous menu
      (r) Return to the main menu
      (x) Exit BPT

Selection: [1/2/b/r/x:1] 1
```

- Provision third party large line endpoints - allows you to provision third party large line endpoints
- Export "Query Line Endpoints" output - allows you to export the "Query Line Endpoints" file to the directory of your choice
- Back to the previous menu - takes you to the parent menu "Provisioning Entry Input Menu"
- Return to the main menu - brings you back to the Main menu
- Exit BPT- exits the Batch Provisioning Tool CLUI

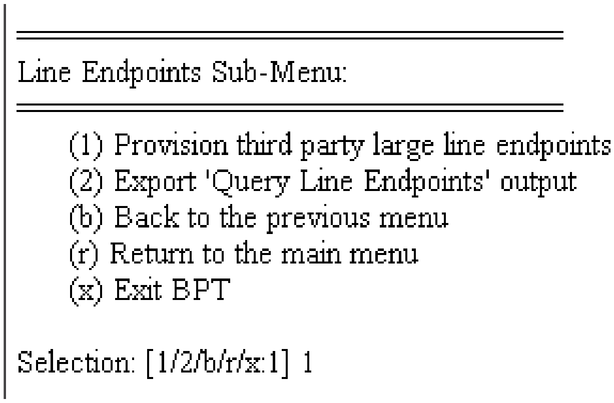
Display Output

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) Line Endpoints
     (4) 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
- Line Endpoints - allows you to view the output files that are currently Line Endpoints 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

Line Endpoints
The Line Endpoints sub-menu of the Display Output Menu allows you display the Line Endpoints output . When you select the Line Endpoints option, the Line Endpoints Sub-Menu, similar to the following, is displayed.



```
================================
Line Endpoints Sub-Menu:
================================
    (1) Provision third party large line endpoints
    (2) Export 'Query Line Endpoints' output
    (b) Back to the previous menu
    (r) Return to the main menu
    (x) Exit BPT

Selection: [1/2/b/r/x:1] 1
```

- Provision third party large line endpoints - allows you to provision third party large line endpoints
- Export “Query Line Endpoints” output - allows you to export the “Query Line Endpoints” file to the directory of your choice
- Back to the previous menu - takes you to the parent menu “Provisioning Entry Input Menu”
- Return to the main menu - brings you back to the Main menu
- Exit BPT- exits the Batch Provisioning Tool CLUI

Display Logs

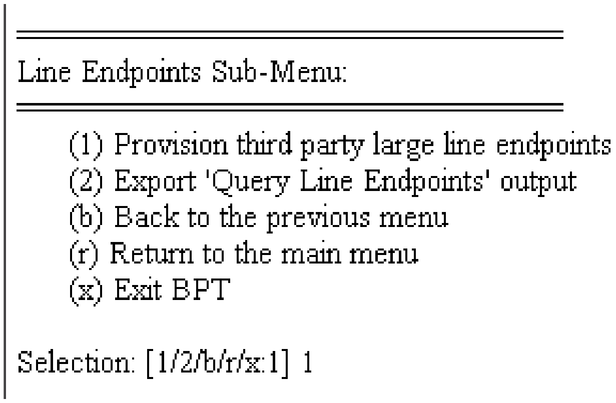
The Display Logs option allows you to view the log files associated with each batch provisioning process. When you select this option, the Display Log File Menu, similar to the following, is displayed.

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


     (1) Lines
     (2) ADSL
     (3) Line Endpoints
     (4) 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
- Line Endpoints - allows you to view the log files that are currently in the logs directory for Line Endpoints
- 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

Line Endpoints

The Line Endpoints sub-menu of the Display Log File Menu allows you display the Line Endpoints log file . When you select the Line Endpoints option, the Line Endpoints Sub-Menu, similar to the following, is displayed.



```
================================================
Line Endpoints Sub-Menu:
================================================
    (1) Provision third party large line endpoints
    (2) Export 'Query Line Endpoints' output
    (b) Back to the previous menu
    (r) Return to the main menu
    (x) Exit BPT

Selection: [1/2/b/r/x:1] 1
```

- Provision third party large line endpoints - allows you to provision third party large line endpoints
- Export “Query Line Endpoints” output - allows you to export the “Query Line Endpoints” file to the directory of your choice
- Back to the previous menu - takes you to the parent menu “Provisioning Entry Input Menu”
- 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) Line Endpoints
     (4) 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
- Line Endpoints - allows you to Line Enpoints output files or Line Endpoints 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

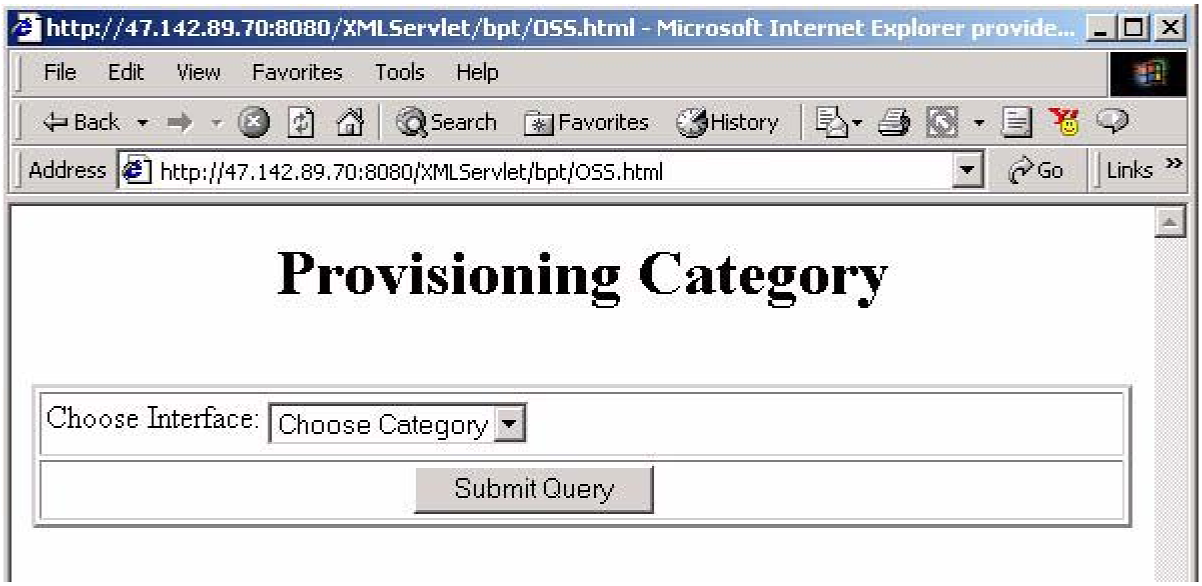
Overview

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 206.

The Batch Configuration Monitor is accessed through the common launch page as previously described under Common launch page on page 204. 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.


http://47.142.89.70:8080/XMLServlet/bpt/OSS.html - Microsoft Internet Explorer provide...
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://47.142.89.70:8080/XMLServlet/bpt/OSS.html
Go Links
Provisioning Category
Choose Interface: Choose Category
Submit Query

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
- Core Element Manager (CEM)
- 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 recommeded) 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

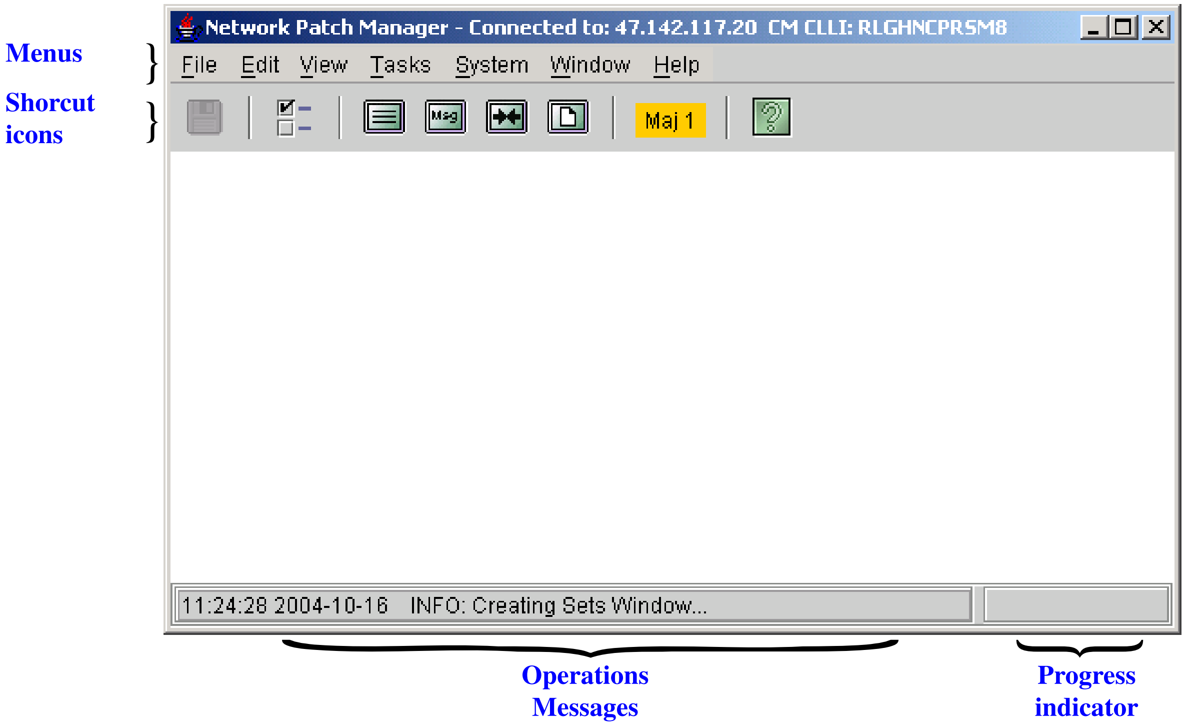
Users who need to perform patching activities using the NPM GUI or CLUI, need to belong to user group “emsadm”. If required, refer to procedure “Setting up local user accounts on an SSPFS-based server” in *ATM/IP Security and Administration*, NN10402-600, if you are locally managing user accounts. If you are centrally managing user accounts through the Integrated Element Management System (IEMS), refer to procedure “Configuring user settings” in *Integrated EMS Security and Administration*, NN10336-611.

NPM GUI

The NPM GUI is a Java^{TM} 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 204.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



Network Patch Manager - Connected to: 47.142.117.20 CM CLLI: RLGHNCPRSM8

11:24:28 2004-10-16 INFO: Creating Sets Window...

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. The IP address of the NPM server and the office CLLI are displayed at the top of the window. Operations messages are displayed at the bottom left of the window, and a progress indicator, which shows the progress of patch requests, is provided at the bottom right of the window.

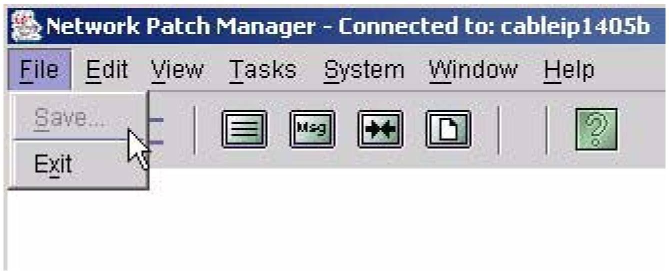
The sections that follow, briefly describe the options available under each menu. More details are provided in the online help for the Network Patch Manager (see Help on page 266).

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

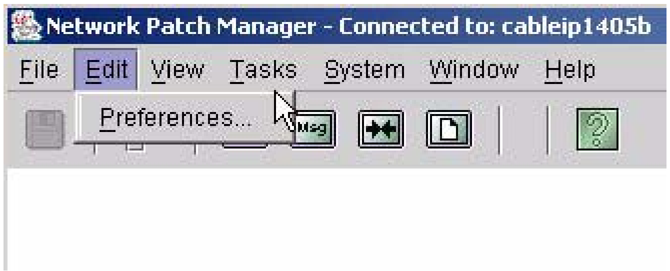
File menu



Edit

The Edit menu contains the **Preferences** option used to set the user preferences (enable or disable the display of patching activity results, and enable or disable debug message), and set the patch file retrieval preferences (PFRS drop box information).

Edit menu

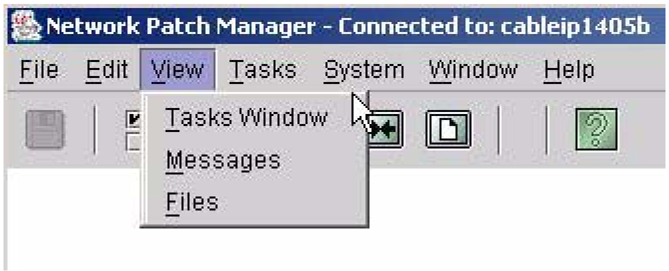


View

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

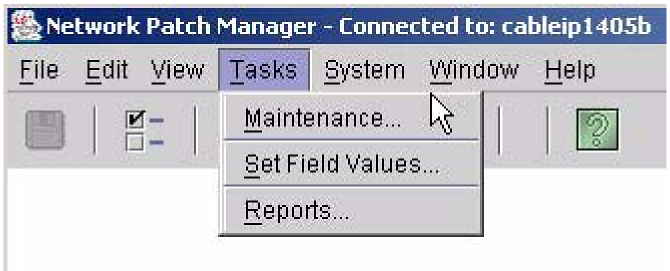


Tasks

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

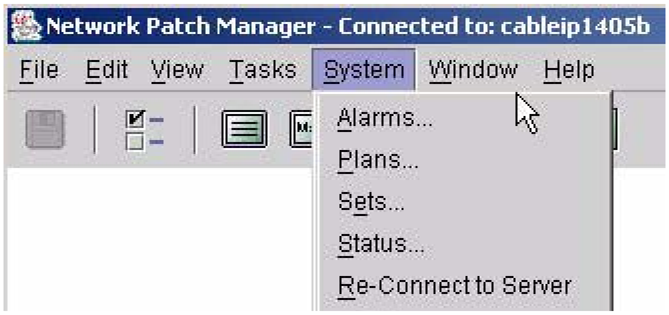


System

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

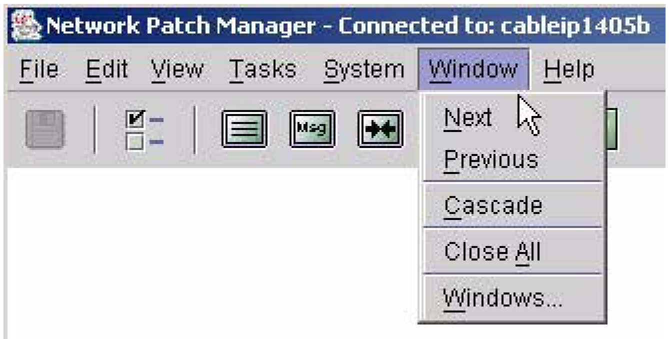


Window

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

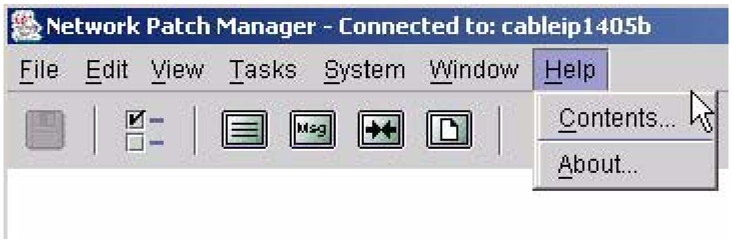


Help

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 Carrier Voice over IP 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 Carrier Voice over IP 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 Carrier Voice over IP 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 206.

User interface

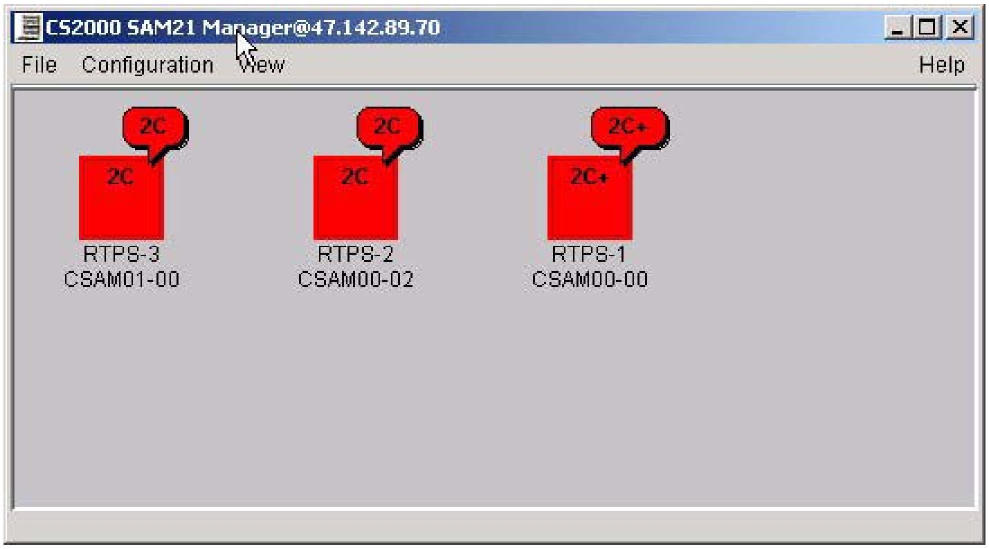
The user interface for the CS 2000 SAM21 Manager application is a web-based GUI (graphical user interface), which is accessed through the common launch page as previously described under Common launch page on page 204. To access the CS 2000 SAM21 Manager GUI, refer to procedure “Launching the CS 2000 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

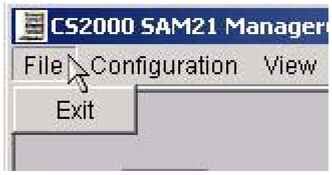
The subnet view, similar to the following, is displayed when the CS 2000 SAM21 Manager GUI is launched.

CS 2000 SAM21 Manager subnet view



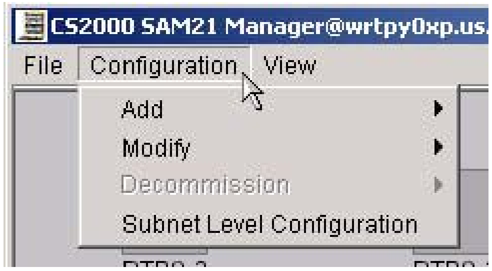
File menu

The File menu provides the options to Exit the CS 2000 SAM21 Manager.



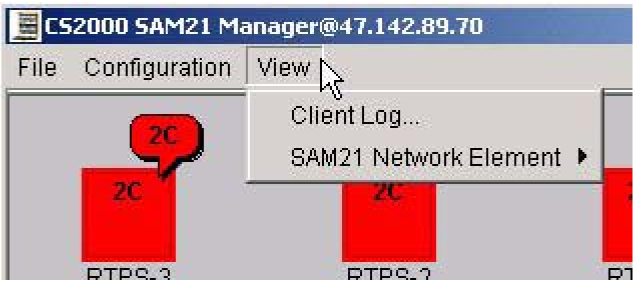
Configuration menu

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

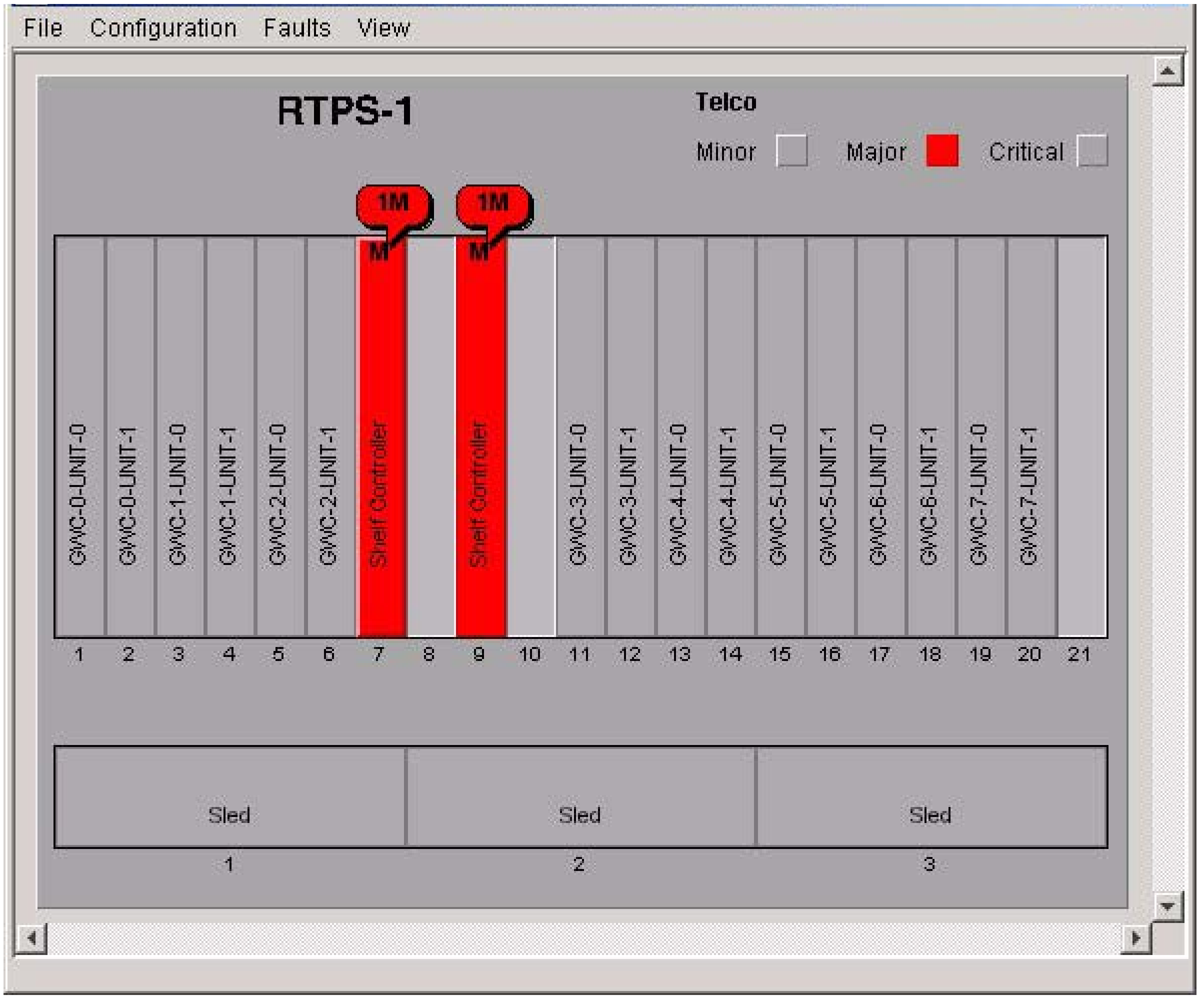
The View menu provides the options to view the client log and display the shelf view of a SAM21 network element.



> ***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

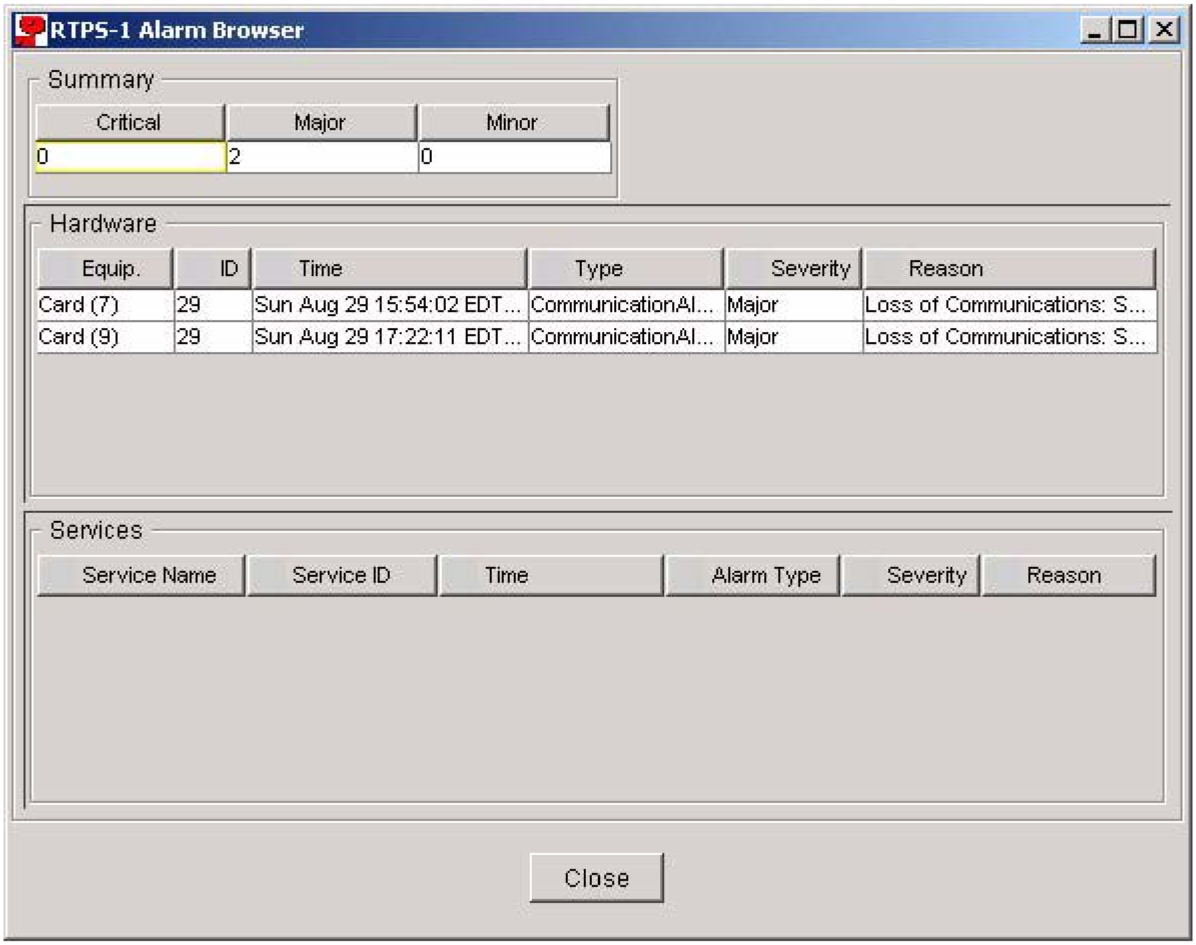
The File menu provides the option to close the shelf view.

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.



RTPS-1 Alarm Browser

Summary

Critical	Major	Minor
0	2	0

Hardware

Equip.	ID	Time	Type	Severity	Reason
Card (7)	29	Sun Aug 29 15:54:02 EDT...	CommunicationAl...	Major	Loss of Communications: S...
Card (9)	29	Sun Aug 29 17:22:11 EDT...	CommunicationAl...	Major	Loss of Communications: S...

Services

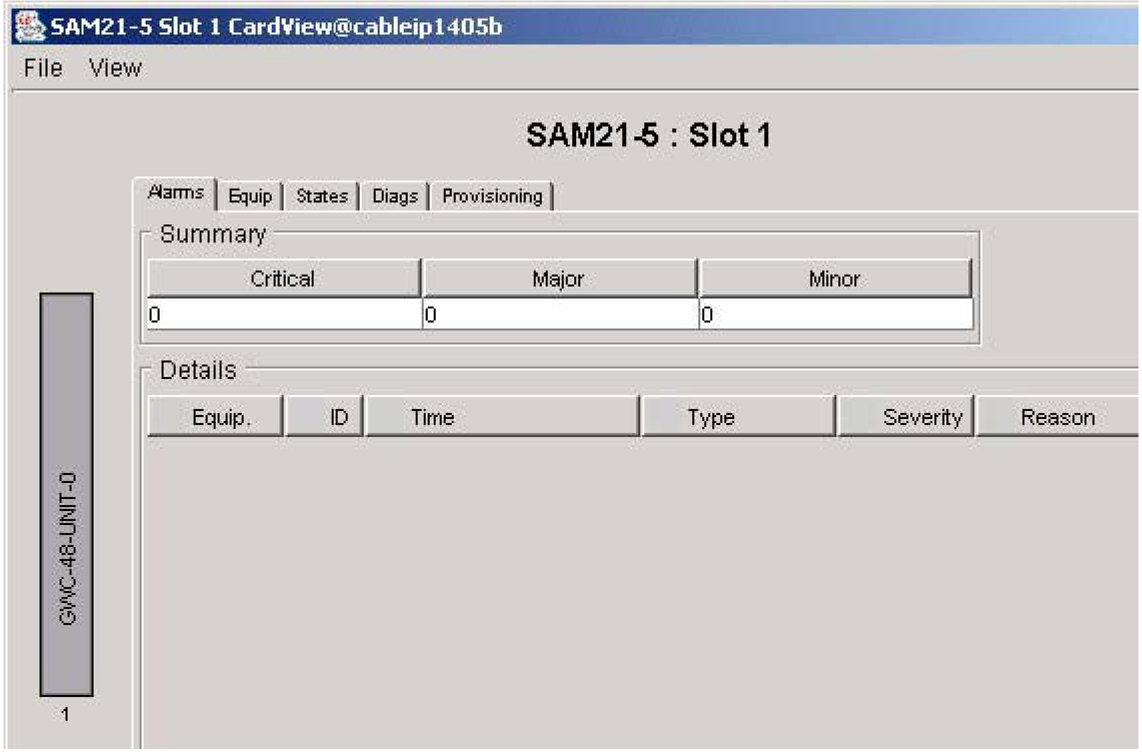
Service Name	Service ID	Time	Alarm Type	Severity	Reason

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.



Summary

Critical	Major	Minor
0	0	0

Details

Equip.	ID	Time	Type	Severity	Reason

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 276.

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 Carrier Voice over IP Network Upgrades document, NN10440-450.

  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 Carrier Voice over IP 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 a file system on an SSPFS-based server” in the ATM/IP Solution-level Security and Administration document, NN10402-600.

OSSGate

Overview

OSSGate is an application that provides a machine interface for provisioning components within Carrier Voice over IP solutions. 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 Carrier voice over IP 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 tranfer 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 280.
- OMPUSH session configuration tool on page 281.

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 281.

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 282.

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 Carrier Voice over IP 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.

Customer support

This chapter describes how the responsibilities for setting up and running a Carrier VoIP Network are divided between Nortel Networks and the customer. The chapter contains the following sections:

Product and customer support

Nortel Networks provides product support using standard Customer Service Center (CSC) and Global Product Support (GPS) policies and procedures. For issues that cannot be resolved, contact the Nortel Networks CSC and a representative will open a Customer Service Report (CSR). If the regional representative cannot resolve the problem, the CSC refers the matter to the next level of support.

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 strategy

A Carrier VoIP Software Release consists of the Communication Server Product Computing load (PCL), based on the XA-Core processor, and the Nortel Networks brand Network Element software loads that are required for the UA-IP solution. The software release carries one-year support policy. For Third Party Network Element software sold by Nortel Networks in conjunction with a Carrier VoIP Software Release, the Third Party software support policy will be in effect.

Ordering and support overview

A Carrier VoIP 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 a retired (unsupported) software release in existing networks and will not deploy a retired release to an initial (new) Carrier VoIP installation or an extension. Therefore, each individual Carrier VoIP 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 contact, and will be limited to support which does not require patching or other design effort.

Software upgrade path overview

Generally, Carrier VoIP Software releases will reach FVS status about every six months. Thus, at the end of the six months after FVS of a Carrier VoIP Software Release, another new release will be available for ordering and loading. The network provider can choose either to deploy this next Carrier VoIP 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 Carrier VoIP Software Release and Support Policy must be made through Product/Service Update and/or Product/Service Information publications. For more information about Nortel Networks software development cycles and software administrative policy, please contact your Nortel Networks representative.

Optional support packages overview

The Table Standard software support policy lists the Network Elements that require optional support packages for software support. Some of these optional support packages will require the Network Element to be upgraded to the latest software release when the standard software support expires.

Standard software support policy

Network element	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 workarounds).
Nortel Networks Ethernet Routing Switch 8600/Device Manager	Software Support is available for the last published software release and one release back (including their associated patches, fixes and workarounds).
Media Gateway 15000 / Media Gateway 7400	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.
Nortel Networks 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 Network Elements, 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

Website information

Nortel Networks website, 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.

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 a 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

The documentation for the UA-IP Solution (which includes solution, product, and supporting documentation) is delivered via CD ROM.

Nortel Networks website, 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 your 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 UA-IP solution. These services will be offered in addition to the engineering, installation, and commissioning services that are part of the base product.

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 UA-IP solution product 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 and realization
- business contingency and disaster recovery planning
- program and project management
- translations for Communication Server 2000 (CS 2000) Media Gateway 15000 and for the Media Gateway 7400
- packet configuration
- LAN design and setup and manager setup
- Integrated EMS 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 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

This 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 & 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-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.

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

Customer responsibilities

Windows client requirements for (I)SN08 Remote Access

The following items are required:

- Windows 2000/NT with minimum 256 Mbyte RAM
- Exceed 6.2
- Contivity Extranet Access Client 4_15.06
- JRE 1.3.1_02 (automatically downloaded from SESM access)
- Netscape 4.6 or higher (excluding 6.2.1 and higher; Netscape 4.7 is ideal for SESM access)
- Internet Explorer 5.5 or higher (excluding 6.0 and higher)
- Telnet (Hummingbird is recommended)
- FTP (Hummingbird is recommended)

Hardware and software requirements

This section describes hardware and software components that must be supplied by the customer.

Ethernet LAN

A 10Base-T Ethernet local area network (LAN) with connectivity to the corporate wide area network (WAN) is required for OAM&P connectivity between the Integrated Element Management System (Integrated

EMS), operations, administration, and maintenance (OA&M) systems, Communication Server 2000 (CS 2000), Services Application Module 21 (SAM21), Universal Audio Server (UAS), and the Media Gateway 15000; optionally connected via an transport network) of the UA-IP Solution. The customer is responsible for supplying this Ethernet LAN.

LAN/WAN requirements for Carrier VoIP Network

In the UA-IP Solution, the Media Gateway 15000 communicates with Integrated EMS over the CS LAN/WAN for the purposes of:

- initial commissioning
- milestone and maintenance software upgrades
- normal OAM&P activity

> ***Note:*** The customer is not responsible for supplying the CS LAN.

Customer requirements The operating company's LAN/WAN must meet the following requirements:

1. The LAN/WAN must have sufficient capacity for the addition of Nortel Networks MDM and the number of Media Gateway 15000s in the customer's configuration.
2. The LAN/WAN must extend to all geographically dispersed gateways of a Carrier VoIP Network.

   > ***Note:*** The Media Gateway 15000s may be optionally connected via in-band connectivity over an transport backbone.

3. The first router which is directly or indirectly (via hub/switch) connected to a dispersed Media Gateway 15000 must support the BootP protocol and be activated for BootP forwarding.
4. As far as possible, all routers in the communication path between the network manager and the Media Gateway 15000s should be implemented to support data precedence and Type of Service (TOS) functions as provided by the TOS byte in the IP header.
5. The LAN/WAN must support the following protocols:
   - BootP
   - simple network management protocol (SNMP)
   - trivial file transfer protocol (TFTP)
   - secure file transfer (SFT)

Operations support system connectivity

The customer must provide Ethernet connectivity from Integrated EMS to the corporate WAN to support the operations support system (OSS) interfaces. This requirement also applies if Nortel Networks provides an integrated network manager (INM) OSS, or if the customer provides an embedded OSS.

DCE cell hardware and software

Distributed Computing Environment (DCE) was decoupled from Carrier VoIP in (I)SN05 and is now an optional application. Customers wishing to continue using DCE must provide all workstations, personal computers, and related software required for integration with Integrated EMS.

Customers may choose to use DCE as part of an evolution plan for their OSSs. This should be implemented in coordination with ASG Technologies /Passwerks or other security solution provider. In (I)SN05 and later releases, DCE is an option only for XA-Core and SDM access (ETA and ATA). All other OAM&P interfaces, including the default/standard solution for XA-Core and SDM, use Unix, PAM and Passwerks for security.

Fiber transmission equipment

The customer must provide all fiber transmission equipment between the Communication Server and the end offices. The UA-IP Solution does not include the customer end-to-end fiber transmission facilities, unless Nortel Networks is specifically contracted to install these facilities as part of the contract. The fiber transmission facilities must be installed and tested prior to the installation start date of the Carrier VoIP Network.

Electronic Software Delivery requirements

Information on Electronic Software Delivery (ESD) patches is included in the Upgrade module of this solution (NN10440-450). Carrier VoIP solution ESD requirements include:

- Software delivery

  Software delivery for Media Gateway 15000, Media Gateway 7400, and Nortel Networks MDM software loads is done using the BaaN 165 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 software delivery electronically, the software order codes that make up the Carrier VoIP solution load are retrieved from a software vault. The appropriate formatting (pre-mastering) is applied and the load is stored on a Nortel Networks ESD server.

After customers retrieve the load from the Nortel Networks ESD 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. Customers are expected to have the optional Distributed Computing Environment (DCE) application or an alternative security product for security and authentication on the WAN to which the CS 2000 Core Manager is connected.

ESD methods

There are two main ways to use ESD:

- ‘Pull’ method

  Customers using the ‘pull’ method are notified and provided with the details and the directory structure of the load on the Nortel Networks ESD server. Customers can then connect to the Nortel Networks ESD server to pull the load.

- ‘Push’ method

  For customers requiring the ‘push’ method, Nortel Networks sends the loads to the CS 2000 Core Manager, a repository server or drop box. The drop box can be either customer-provided within the customer’s network, or Nortel-provided within Nortel Networks’ network. The Nortel Networks account team and Software Delivery work with the customer to choose the best option based on the customer’s needs and security requirements. Any repository set up in the customer’s network must be externally accessible to Nortel Networks. A customer e-mail address is required for subsequent notification of software load delivery.

Both ESD methods transmit the software load in a compressed form. The load is decompressed after receipt at the destination.

Transmission and download times

The available data connection bandwidth proportionately affects the load transmission time. The link from the Nortel Networks ESD server to the customer’s LAN/WAN must have a minimum throughput of 1.544 Mbit/s. As an example of the transmission time, if the available connectivity is at the minimum value of 1.544 Mbit/s (a T1 connection), the transmission time for a 2 Gbyte load is approximately 3 hours.

For satisfactory download performance, it is recommended that the customer’s LAN/WAN has a minimum throughput of 300 kbyte/s 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, the download time to move a complete Carrier VoIP load from the customer's server to the CS 2000 Core Manager is approximately 1.5 hours.

The table Link types and download times below gives the approximate download times over various dedicated connection links. Customers must consider what download time is acceptable to their operations in order to determine the throughput requirements for their network.

Link types and download times

Type of data link	Data rate	Download time
28 kbit/s modem	28.8 kbit/s	10+ hours
56 kbit/s modem, ISDN, EIU, X25, DataPac	56-64 kbit/s	5+ hours
T1	1.5 Mbit/s	10+ minutes
10 base-T Ethernet	10 Mbit/s	80 seconds
OC-3	84 x T1 (155 Mbit/s)	6 seconds

The peak demand for network resource for ESD occurs when a milestone software upgrade is scheduled. A lesser demand occurs when an NCL or an MNCL is transmitted by ESD. An NCL upgrade occurs about twice a year, and an MNCL upgrade about once a month.

Security requirements

For the Media Gateway 15000, Media Gateway 7400, and Nortel Networks MDM software loads, Nortel Networks uses a secure-access delivery system. Customer login IDs and passwords are managed as part of the POL suite.

For DMS software loads (where access from the Nortel Networks ESD server to the customer's LAN/WAN is over a switched circuit) security is provided by user identification and password. When logging in from the Nortel Networks ESD server to the customer's LAN/WAN, the security algorithm (for example, Secure ID) required by the customer is used. The optional DCE application or an alternative security product is used in the customer's network for security and user authentication.

Emergency remote access

Under emergency conditions, Nortel Networks support staff require remote access to the customer's OSS network. This access can be provided by dial-up lines or terminal servers. Nortel Networks recommends the Contivity 600 VPN switch for this purpose. The Contivity 600 product and service is available for purchase from Nortel Networks as an add-on option. Two options are available: 56-bit encryption and 128-bit encryption.

ESD summary

In summary, the ESD requirements are as follows:

- The customer's network engineer must work with the Nortel Networks ESD engineer to discuss and agree the technical details.
- The link from the Nortel Networks ESD server to the customer's LAN/WAN must have a minimum throughput of 1.544 Mbit/s.
- The customer's LAN/WAN must have a minimum throughput of 300 kbyte/s to download Carrier VoIP solution loads to the customer's CS 2000 Core Manager in a reasonable time period.
- The customer's server must have a minimum storage space of 36 Gbytes.
- If DCE is used for security, the CS 2000 Core Manager and the LAN/WAN server must be integrated into the customer's DCE cell.

Network provisioning information

Customers must provide all the necessary IP address information to configure /commission the Carrier VoIP Network elements for Ethernet and network access. Customers must provide the IP addressing requirements for each of the Carrier VoIP Network elements during the customer information (CI) meeting prior to the start of the Carrier VoIP Network installation.

System capacity testing

Nortel Networks does not perform system capacity testing on customer premises. System capacity tests are performed in Nortel Networks labs. Documentation and/or customer involvement can be arranged as required, to ensure that customers are confident that Nortel Networks can meet its committed requirements.

Pre-installation meeting

The Nortel Networks Project Manager and installation representatives must schedule a pre-installation meeting with the customer. This is to ensure that all customer requirements regarding IP address information, Ethernet LAN/WAN, transmission/transport facilities, workstations, ESD links, third-party equipment, and site readiness, have been reviewed with the customer for readiness status. During the meeting, the Project Manager must inform the customer that all customer-provided facilities and equipment must be present and serviceable prior to the installation start dates.

Points of demarcation

The following sections describe the points of demarcation.

Physical

Customers must provide physical installation points of demarcation during the CI meeting. This includes all points of connectivity between all Carrier VoIP Network elements (such as the CS 2000 and Media Gateway 15000s) and the customer-provided demarcation equipment. Nortel Networks does not terminate connections directly on third-party switching equipment or third-party end offices. Customers must provide an interim point of demarcation.

All demarcation facilities/equipment (such as fiber management system (FMS), patch panel, third-party switch ports, router/switch/hub ports, RJ45 plugs in wall) are customer-provided and must be installed and available prior to the start of the Carrier VoIP Network installation.

Testing

Nortel Networks tests the UA-IP Solution to ensure proper installation, and end-to-end connectivity. Nortel Networks' responsibility and liability ends at the customer transmission/transport point(s) of demarcation.

Customers are responsible for testing the following systems, and for ensuring that:

- all corporate LAN/WAN network facilities necessary to support OAM&P, OSS, and ESD requirements are functional and meet the technical specifications required to ensure sufficient bandwidth for the UA-IP Solution data communications
- all fiber transmission/transport facilities between all points of demarcation are functional and meet the technical specifications required to carry UA-IP Solution traffic and in-band OAM&P data
- all third-party switches (if used) within the corporate network are functional and meet the technical specifications required to transmit UA-IP Solution traffic and in-band OAM&P data

Installation of the UA-IP Solution does not include communication server capacity/assessment testing or customer translations.