Cisco Mobile Exchange (CMX) Solution Guide

for General Packet Radio Service (GPRS)/Universal Mobile Telecommunications System (UMTS) networks

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Text Part Number: OL-2947-01

CONTENTS

Preface

This preface describes the *Cisco Mobile Exchange (CMX) Solution Guide*, how it is organized, its intended audience, and the document conventions used in this publication.

This publication does not contain the instructions to install the Cisco 7600 family router. For information on installing the router, refer to the *Cisco 7609 Internet Router Installation Guide*.

Note For translations of the warnings in this publication, see the "Related Documentation" section on page xi.

Audience

Only trained and qualified service personnel (as defined in IEC 60950 and AS/NZS3260) should install, replace, or service the equipment described in this publication.

Organization

This publication is organized as follows:

Chapter	Title	Description
Chapter 1	"Overview of Cisco Mobile Exchange"	Presents an overview of the Cisco Mobile Exchange (CMX).
Chapter 2	"Overview of GSM, GPRS, and UMTS"	Provides an overview of GSM, GPRS, and UMTS networks.
Chapter 3	"Description of Cisco Mobile Exchange"	Describes the CMX network elements, virtual server configuration, supported services, billing configuration, and reliability configuration.
Chapter 4	"CMX Network Management"	Describes the network management applications provided by CiscoWorks for Mobile Wireless (CW4MW).
Chapter 5	"CMX Configuration Guidelines"	Provides configuration guidelines for the CMX network elements.

Chapter	Title	Description
Chapter 6	"CMX Sample Configurations"	Provides configuration examples for CMX network elements.
Appendix A	"CMX Timers and Counters"	Provides timer and counter descriptions for CMX network elements.

Conventions

This publication uses the following conventions:

Convention	Description
boldface font	Commands and keywords are in **boldface**.
italic font	Arguments for which you supply values are in *italics*.
[ ]	Elements in square brackets are optional.
{ x | y | z }	Alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
`screen` font	Terminal sessions and information the system displays are in `screen` font.
`boldface screen` font	Information you must enter is in **`boldface screen`** font.
italic screen font	Arguments for which you supply values are in *italic screen* font.
^	The symbol ^ represents the key labeled Control—for example, the key combination ^D in a screen display means hold down the Control key while you press the D key.
< >	Nonprinting characters, such as passwords are in angle brackets.

Notes use the following conventions:

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

Tips use the following conventions:

Tip Means *the following information will help you solve a problem*. The tips information might not be troubleshooting or even an action, but could be useful information, similar to a Timesaver.

Cautions use the following conventions:

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Related Documentation

For more detailed installation and configuration information, refer to the following publications:

- *Site Preparation and Safety Guide*
- *Cisco 7401ASR Installation and Configuration Guide*
- *Cisco 7401ASR Regulatory Compliance and Safety Information*
- *Regulatory Compliance and Safety Information for the Cisco 7600 Series Internet Routers*
- *Cisco 7609 Internet Router Installation Guide*
- *Cisco 7600 Series Internet Router IOS Software Configuration Guide*
- *Cisco 7600 Series Internet Router IOS Command Reference*
- *Cisco Content Services Gateway Installation and Configuration Guide*
- *Cisco Subscriber Edge Services Manager and Subscriber Policy Engine Installation and Configuration Guide*
- *IOS Server Load Balancing*
- For information about MIBs, refer to

  http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

Obtaining Documentation

These sections explain how to obtain documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at this URL:

http://www.cisco.com

Translated documentation is available at this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which is shipped with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

Ordering Documentation

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

  http://www.cisco.com/go/subscription

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. In the Cisco Documentation home page, click the **Fax** or **Email** option in the “Leave Feedback” section at the bottom of the page.

You can e-mail your comments to bug-doc@cisco.com.

You can submit your comments by mail by using the response card behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from online tools by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

If you want to obtain customized information and service, you can self-register on Cisco.com. To access Cisco.com, go to this URL:

http://www.cisco.com

Technical Assistance Center

The Cisco Technical Assistance Center (TAC) is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two levels of support are available: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Cisco TAC inquiries are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

The Cisco TAC resource that you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

Cisco TAC Web Site

You can use the Cisco TAC Web Site to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to this URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register:

http://www.cisco.com/register/

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC Web Site, you can open a case online by using the TAC Case Open tool at this URL:

http://www.cisco.com/tac/caseopen

If you have Internet access, we recommend that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. These classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled: for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). When you call the center, please have available your service agreement number and your product serial number.

CHAPTER 1

Overview of Cisco Mobile Exchange

This chapter provides an overview of the Cisco Mobile Exchange (CMX) and contains the following sections:

Introduction

Cisco Mobile Exchange (CMX) is a framework of solutions that addresses the interface between the evolving radio access network and a wide array of Internet services offered by Internet Protocol (IP) networks. The CMX framework provides flexible solutions to mobile operators, application providers, and system integrators that enable them to offer value-added data services to mobile subscribers. These services include mobile banking, web surfing, location services, and electronic payments. The challenge for mobile operators is cost-effectively managing these services, providing secure access to high revenue customers, and evolving their networks as wireless technologies advance. The Cisco Mobile Exchange provides the required flexibility to effectively meet these demands using field-proven hardware and software applications.

The key benefits of the CMX are:

- Simplified and improved user experience when accessing and using the data service (e.g., the ability to select multiple services in the same session).
- Common user experience across multiple access technologies such as General Packet Radio Service (GPRS) and Universal Mobile Telephone System (UMTS).
- Operator-customized service offering to end users.
- Enhanced corporate services including multiple virtual private network (VPN) options such as Layer 2 Tunneling Protocol (L2TP) for corporate customers.
- Flexible framework for pre- and post-paid billing at the session and content level.
- Use of Cisco's rich IOS feature set including load balancing, express routing, fast switching, VPN acceleration, and other value-added services.
- Redundancy built into the framework to ensure that the network can survive a single point of failure.

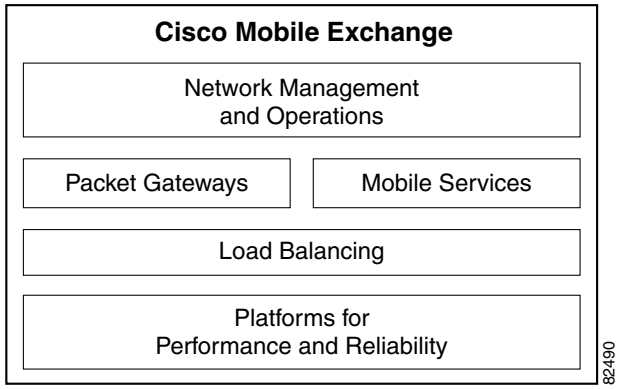
- Highly scalable architecture that allows the operator to match subscriber demand to capital investment. Operators can tailor network functions to their immediate needs while planning for future growth. An example is to provide session-level billing initially, which evolves to content billing over time.

The CMX framework incorporates the following components (Figure 1-1):

- Packet gateways
- Mobile services
- Load balancing
- Network management and operations
- Platforms

Together, these components create a flexible framework of solutions for mobile operators to generate revenues from their 2G, 2.5G, or 3G mobile packet infrastructures. They offer the flexibility of modular design and the reliability of proven platforms.

Figure 1-1 Cisco Mobile Exchange Components



Tip Go to www.cisco.com/go/mobile for more information about Cisco Mobile Exchange components.

Packet Gateways

The packet gateway is the interface between the mobile infrastructure and standard IP networks. A gateway translates between access-specific protocols of the radio access network (RAN) and the access-independent world of the Internet. Mobile operators transmit IP packets through the air using one of these standards:

- General Packet Radio Service (GPRS)/Universal Mobile Telecommunications System (UMTS) protocol through a Gateway GPRS Support Node (GGSN) packet gateway.
- Code-Division Multiple Access (CDMA) protocol through a Packet Data Serving Node (PDSN) packet gateway.

Many first-generation packet gateways do not scale to accommodate profitable numbers of users and sessions. For mobile operators seeking to upgrade their first-generation packet gateways, Cisco offers both GGSN and PDSN gateways on Cisco Internet routers and on Catalyst series switches. These gateways offer scalability features an order of magnitude beyond previous solutions.

Note Cisco Mobile Exchange provides support for GPRS networks with plans to support PDSN networks in the future.This document focuses on the CMX solution for GPRS networks. For more information on CMX support for PDSN networks, go to www.cisco.com/go/mobile.

Mobile Services

Since mobile subscribers pay for content, mobile operators need to tailor data, voice, and video services for each subscriber. Personalized services require higher-layer network intelligence that accommodates the unique requirements of mobile networking. The CMX satisfies these requirements.

Currently, Cisco Mobile Exchange offers the following mobile services:

- Service selection
- Content monitoring

Each service supplies a critical function for enabling profitable content-based services.

Service Selection

A key capability that helps service providers brand their services and lay the foundation for future growth is service selection. Service selection lets mobile operators intervene in data flows and determine particular services that subscribers can access. It enables a common look and feel to users and a uniform billing infrastructure. This capability allows a provider to both exercise discrete control over service access and enable self-provisioning to reduce operational costs, speed service availability, and recover lost revenues. For example, a mobile operator might gather substantial revenue from their messaging services. However, if a subscriber logs onto a third-party instant messaging server, the provider loses revenue for those transactions. Using service selection, the provider can provide access to alternate messaging services only if the subscriber pays a fee. Operators need the ability to support several billing structures based on particular services and market. Cisco provides this capability with its service selection technologies.

Cisco Service Selection Gateway (SSG) and Service Edge Subscriber Manager (SESM) together allow providers to control what subscribers can do based on their payments and privileges. The SSG presents a Web portal, offering service icons that the subscriber can click to access their subscribed services (see Figure 1-2 for example). It can be customized to offer a subset of the total service portfolio, display targeted advertising, or with a VPN service, appear as a corporate intranet page. The SESM enables self-provisioning, where subscribers log onto a Web page to buy services or check their service usage. Together, the SSG and SESM reduce operational expenditures and increase subscriber satisfaction through more efficient, faster service.

Figure 1-2 Example of Web Portal

Content Monitoring

Content monitoring or content billing examines packets to obtain higher-layer information such as particular URLs, domains, or file names. With this information, a mobile operator can bill for usage-based services or gather data for market research.

For example, an enterprise provides its employees with a personal digital assistant (PDA) and mobile access service. Because the provider has usage-based billing, the enterprise does not want to pay for personal activities. With content monitoring, the network can determine whether an employee is checking email (a service the enterprise pays for) or checking sports scores (a service the employee pays for). The mobile operator can split the bill between the enterprise and the employee. This helps enterprises contain network access costs. It also encourages them to sign up for new mobile services with full confidence in their usefulness to the business.

Content monitoring allows the provider to track and record subscriber usage in terms of user identity, traffic volume, content, and applications. All CMX systems can be integrated with pre-paid or post-paid billing systems for maximum business flexibility.

Load Balancing

The growing demand for TCP/IP-based application services such as e-commerce, video, and e-mail is motivating companies to increase the availability and scalability of network and server systems. Cost containment is also driving the need for intelligent server switching to scale the server complex and caching techniques to conserve WAN bandwidth.

The Cisco server load balancing (SLB) feature is an IOS feature that intelligently balances the load of user traffic across multiple TCP/IP application servers. This feature ensures continuous, high availability of content and applications with proven techniques for actively managing servers and connections in a distributed environment. By distributing user requests across a cluster of servers, SLB

optimizes responsiveness and system capacity and reduces the cost of providing large-scale Internet, database, and application services. In addition, its integrated security capability protects servers from unauthorized access.

The SLB feature offers enterprise customers and ISPs a network-based intelligent server solution. The SLB feature tracks network sessions and server load conditions in real time, directing each session to the most appropriate server and maintaining high server availability.

Network Management and Operations

Cisco is able to offer the full integration of its core network elements into an umbrella network management system, which provides the overall Operations Support System (OSS)/Base Station System (BSS) infrastructure for the mobile network.

With the introduction of new services such as GPRS and UMTS, mobile networks are becoming multi-vendor environments. For example, there could be several vendors for radio access, a vendor for the GPRS nodes, and another for the IP core. In this environment, the ability to integrate all of the network elements together under a single network management umbrella is important to both simplify provisioning and fault management and control the operations costs of the network.

Platforms for Performance and Reliability

The Cisco Mobile Exchange framework is provided on the following platforms:

- Cicso 7600 series Internet router platform
- Cisco 7400 series Internet router platform

7400 Series

The Cisco 7400 series router is an application-specific router for service providers and enterprises with applications that require a compact stackable form factor, a limited number of interfaces, a high ratio of processing per rack unit, and low power consumption.

Broadband subscriber aggregation is the primary application for the Cisco 7400 series router. The need for broadband aggregation has grown exponentially in the past several years and will continue to grow as subscribers demand more services. The stackability of this product provides the opportunity to "pay as you grow" your customer base in a modular and scalable fashion.

Service selection is another application of the Cisco 7400 series router. Combined with the Subscriber Edge Services Manager (SESM), the Service Selection Gateway (SSG) allows service providers to deploy and deliver value-added services such as videoconferencing, streaming video, business-grade Internet, shopping, and gaming services. Specifically, Cisco SSG and SESM allow service providers to offer and bill for usage-based services. They allow subscribers to dynamically select on-demand services, individually or simultaneously, and they track usage for billing based on connection time for each selected service.

7600 Series

The Cisco 7600 series Internet router delivers optical wide- and metropolitan-area network services with high-touch IP services at the network edge. Service providers and enterprises can provide services at optical speeds, offering competitive advantage and service differentiation to the service provider and high-speed connectivity and link usage efficiency to the enterprise.

The Cisco 7600 series provides a scalable system that offers the ability to bring DS0 to OC-48 WAN connectivity, 10-Mbps Ethernet to 10-Gigabit Ethernet LAN connectivity to the Internet data center, metropolitan aggregation, WAN edge aggregation, and enterprise networking applications. It supports virtual LAN (VLAN) trunking that enables multiple customers in a building or metro area to share the same access switch fabric but use separate VLANs to access the service provider's point-of-presence (POP).

The Multilayer Switch Feature Card (MSFC) in the 7600 chassis provides the performance, scalability, and intelligent services of Cisco IOS® software integrated into the Catalyst series of switches for enterprise backbone and service provider applications. The MSFC supports a full complement of routing protocols to address both enterprise and service provider requirements.

For high-availability, the MSFC also supports Hot Standby Routing Protocol (HSRP) for routing redundancy between MSFCs in the same chassis, across Catalyst switches, or between a Catalyst switch and a standalone Cisco router.

Enterprise and service provider networks require full-featured multilayer switching and services at line-rate speeds. The MSFC delivers hardware-based acceleration for Layer 2, 3, and 4 switching and services with no performance penalty. An example of this is the Cisco IOS policy routing feature. Policy routing is a flexible mechanism in which routing decisions are based on more than just the destination address. For instance, a service provider might enable policy routing to allow certain packets to be routed a different way than the typical shortest-path route.

The MSFC supports traffic statistics-collection and accounting with no impact on switching performance. This data enable enterprise customers to perform traffic engineering, monitor network performance, and provide service provider customers with resource-utilization data for billing and charge-back applications.

The CMX solution uses the policy routing feature and layer 3 static routing of the MSFC to sequentially route traffic through the multiple network elements that provide required functions. Dynamic routing using Open Shortest Path First (OSPF) protocol is used between the GGSN and the MSFC. The routing/switching platform provides layer 2 connectivity for the CMX solution through a 48-port Ethernet blade and supervisor card interfaces. The platform also supports the CMX VLAN functions to separate traffic and layer 2 switching functions.

Catalyst series switches equipped with MSFCs provide transparent Web cache redirection using Cisco Web Cache Communication Protocol (WCCP). The WCCP is a web-cache redirection protocol that localizes network traffic and provides network-intelligent load distribution across multiple network caches for maximized content availability.

Network Elements

The Cisco Mobile Exchange is a framework of solutions that integrates the following elements:

- Service Selection Gateway (SSG) and Subscriber Edge Services Manager (SESM)
- Content Services Gateway (CSG)
- Service Gateway Load Balancers
  - RADIUS Load Balancer (RLB)
  - Firewall Load Balancer (FWLB)

Service Selection Gateway and Subscriber Edge Services Manager

The Service Selection Gateway (SSG) is a switching product for service providers who offer intranet, extranet, Internet, and special content and application connections to subscribers using wireless access technologies. The SSG is an IOS feature that provides multi-service networking and enhanced user experience and billing options. It also provides subscriber authentication, service selection, and service connection capabilities to subscribers.

The SSG communicates with the authentication, authorization, and accounting (AAA) management network where Remote Authentication Dial-In User Service (RADIUS), Dynamic Host Configuration Protocol (DHCP), and Simple Network Management Protocol (SNMP) servers reside. The SSG also communicates with the service provider network, which connects to the Internet, corporate networks, and value-added services.

Together with the SSG, the Subscriber Edge Services Manager (SESM) allows a service provider to create a Web portal that presents subscribers with a menu of services, enabling them to log on to and disconnect from different services using a Web browser. This functionality improves flexibility and convenience for subscribers and enables service providers to bill subscribers for connect time and services used, rather than charging a flat rate.

The SESM operates in RADIUS mode to provide subscriber authentication, authorization, and accounting. This mode obtains subscriber and service information from a RADIUS server. When SSG is used with the SESM, the user opens an HTML browser and accesses the URL of the SESM Web server application. The SESM forwards the user login information to the SSG, which then forwards the information to the AAA server.

In a mobile operator environment, the SSG can also act as a RADIUS proxy for access requests from a downstream network access server (NAS), which shares a RADIUS secret key with the SSG. The Gateway GPRS Support Node (GGSN) can serve as the NAS.

Through the SESM, users can query the status of a session (showing services a subscriber is using), the status of the connection, the current balance for pre-paid services, and system messages from the SSG. This service can also be made free of charge by creating what is called an open garden. An open garden is a collection of websites or networks that subscribers can access as long as they have physical access to the network. Subscribers do not have to provide authentication information before accessing the websites in an open garden. In contrast, a walled garden refers to a collection of websites or networks that subscribers can access after providing minimal authentication information.

Subscribers in GPRS and UMTS networks are logged on to the network in an always-on mode. When no service is in use, the default network area is the open garden.

The user's packet data protocol (PDP) context or point-to-point (PPP) session can be held up so the user is informed before a call is ended. Treating the service connection as a separate entity from the PDP context and PPP session allows the user to be informed of what is happening to the connection.

The SSG separates the service and access technologies. This lets subscribers choose dynamically from a selection of services and lets service providers implement service- and usage-based billing strategies.

Single Access Point Name/Multiple Services

In GPRS/UMTS networks, access point names (APNs) must be provisioned in the GGSN, domain naming system (DNS) server, home location register (HLR), and mobile devices. Only a limited number of APNs are supported per mobile handset. If users want to connect to multiple APNs, they must disconnect from the active APN, then establish a connection to a different APN.

The CMX solution to this problem is provided by the Cisco SSG and SESM. The service and access configuration is simple and scalable since only one database (RADIUS server) is provisioned for new services or access. Users can have multiple services active within a single PDP context (i.e., user session) at the same time. This feature enhances the user experience. It also allows the mobile operator to generate revenue using the same radio infrastructure and offer simultaneous services, each billed by a different billing schema. The same is true for CDMA2000 networks, where users can have multiple active services within a single PPP session at the same time.

Billing Flexibility for Service Providers

The SSG allows subscribers to select particular services dynamically. The SSG then switches the subscriber traffic to the selected services. The SSG monitors user connections, service login and logout, and user activity per service. By providing per-connection accounting, the SSG lets service providers bill for connection time and services used rather than charging a flat rate.

Open Architecture

The SESM provides an architecture that complies to the Java 2 Enterprise Edition standard. The SESM can be integrated with a service provider's existing Web infrastructure. The SESM is bundled with a Java Runtime Engine (JRE) and the Jetty Web server.

Flexibility and Convenience for Subscribers

The SSG provides users with access to multiple services simultaneously. These include the Internet, gaming servers, connectivity to corporate networks, and differential service selection. Users can dynamically connect to and disconnect from any of the services available to them.

Transmission Control Protocol Redirect

The Cisco SSG allows users to authenticate their sessions without knowing the URL of the Web portal. If a user, who has not logged in, sends packets upstream to a specified group of TCP ports, the SSG sends those packets to a captive portal group (one or more servers). The Web portal handles the incoming packets by returning a login page to the user.

Captive Portal

With the ability to redirect a subscriber to a captive portal, service providers can capture a subscriber's attention with account or service messages (e.g., blocked access to service or payment request). The captive portal Web application on the SESM can also direct a subscriber to services based on interest or location.

Domain Naming System Fault Tolerance

The SSG can be configured to work with a single domain naming system (DNS) server (or two servers in a fault tolerant configuration). DNS requests are switched to the secondary server if the primary server fails to respond with a DNS reply within a set time period.

Service Access Mode

Services offered through the SSG and SESM can be configured for concurrent or sequential access. Concurrent access allows users to log in to one service while simultaneously connecting to other services. Sequential access requires that the user log out of other services before accessing a service configured for sequential access.

Single Sign-on

The SSG can be configured to allow subscribers, who have already logged on through a point-to-point client, to access the Web portal without requiring them to re-enter their user name and password. This feature is called single sign-on.

Content Services Gateway

The Cisco Content Services Gateway (CSG) is a software and hardware extension for the Cisco Catalyst platforms. The CSG provides a content-metering base that enables applications for network traffic accounting, usage-based network billing, network planning, network monitoring, outbound marketing, and activity tracking. The CSG can retrieve the following content information:

- Traffic statistics in byte counts
- The content that was transferred
- The authentication, authorization, and accounting (AAA) identity of the user
- The Transmission Control Protocol (TCP) connection termination type

For HTTP requests, for example, the URL of each request is provided. The CSG tracks the user's content transactions in real time and forwards this information to a billing agent for further processing, rating, and invoicing. The CSG measures and delivers the information required for billing based on content.

The CSG provides the following key benefits:

- Performance—The CSG handles up to 300,000 connected subscribers per line card while deciphering a finer level of content granularity for use in content-based billing.
- Content measurement—HTTP content is deciphered based on the actual object requested. By differentiating the content requests, the CSG enables billing applications to charge differently for different objects, enabling content providers to charge for the true value of the content. The content can be billed on an individual user basis, billed to the content provider, or billed to a third party for transactions such as pushed or banner advertisements.
- Enhanced user identification—In many environments, the IP address is not sufficient for properly identifying the user because it can be dynamically assigned or hidden by proxies and firewalls. In real time, the CSG associates the user ID that is captured by the AAA server to each transaction that it reports. This allows for user-based charging in a broader environment than is currently possible.

- Price/performance value for large data centers and ISPs—The CSG features a low connection cost and occupies a small footprint. It slides into a slot in Cisco Catalyst 7600 platforms and conserves valuable data-center space.
- Ease of configuration—The CSG uses the same native Cisco lOS® software interface used to configure the Cisco Catalyst 7600 platforms.

Content Measurement for Differentiated Billing

The CSG meters data traffic and generates accounting records. Unlike traditional billing models, which bill for broad classes of traffic, the CSG enables differentiated billing based on the object requested. The detailed accounting records include the user ID, session duration, and bytes uploaded and downloaded. For TCP, the information includes the content transfer size, excluding retransmissions. The connection termination type and initiator are also reported. For HTTP, the URL and hostname of the content request are provided. The billing agent uses this information to apply different rates to different services according to the operator's pricing structure.

URL Recording

The CSG records the URL (up to 512 characters) rather than just the server IP address. The various elements of a URL can have different meanings in a billing context. Domain names determine that a user has accessed a given site. However, directories, filenames, and extensions allow operators to bill for specific types of content such as video streams, MP3 files, and PDF files. Each file type can be billed differently. Individual files of the same type can also be priced differently. Some Web sites might request the user to enter a variable as part of their content selection (for example, entering a destination on an airfare Web site to generate a price). The user might select a series of variables, and the CSG would account for them. The variable is a distinct element in the billing formula. The Universal Resource Indicator (URI) substring, which is what remains beyond the domain name, filename, extension, and variable of the URL, may also be used for billing purposes to provide a premium service or other feature.

Open Interface with Multiple Billing Agents

The CSG collects the content information and sends it to a billing agent. The billing agent collects all of the information about a data session and formats it for use by the rating and billing engines. The protocols used to communicate with the billing mediation or billing devices are standard and open, enabling the billing agent to receive the CSG records.

Note The solution described in this document is based on the MIND CTI Real-Time Server (RTS) for AAA and billing mediation functions. Other partners are also available for billing and mediations.

Content Monitoring

Service providers can track the type of content being transferred across their networks. The Web sites that subscribers visit create a history of preferences, showing subscriber interests and online purchasing patterns. This information can be used by the service provider to market services that subscribers are likely to pay for. By monitoring subscriber activity on their networks, service providers can modify rating engines to generate additional revenues for high-touch services.

Configuration and Performance Summary

The following configuration limits and performance values apply to the CSG:

- 256 total virtual LANs (client and server)
- 4000 virtual servers
- 16,000 access control list items
- 1,000,000 concurrent TCP connections
- 300,000 connected subscribers
- Four gigabits-per-second (Gbps) total combined throughput per card
- 4000 connections per second for HTTP reporting; 8000 connections per second in other cases

CSG in the CMX Framework

The CSG serves two purposes in the CMX framework:

- To backup IP-layer accounting information for the SSGs
- To provide a content-based billing solution

In the first case, the CSG assumes a logical position between the packet gateway and the RLB to register IP traffic. In this position, the CSG provides reference data as a backup to the IP billing provided by the SSGs. If an SSG fails, the CSG sends secondary accounting information of all IP traffic that traversed it to the billing agent. This allows for billing records to be preserved accurately if an SSG fails.

A second CSG is logically positioned between the SSGs and the FWLB. This CSG is positioned to provide content-based billing (layers 4 though 7).

The traffic flows through the CSGs in the CMX framework are described in greater detail in "Data Traffic Flows" section on page 3-8.

Service Gateway Load Balancing

Service gateway load balancing is an integral part of the CMX framework. It is key for scalability and switch-over in the event of component failure. Service gateway load balancing is provided by the following elements:

- RADIUS Load Balancer (RLB)—Load balancing for uplink (toward network) traffic and for RADIUS messages toward the AAA servers
- Firewall Load Balancer (FWLB)—Load balancing for downlink (toward subscriber) traffic

The Cisco IOS-SLB software enables scalable deployment of Service Selection Gateways (SSGs) in a mobile wireless environment. In a GPRS/UMTS network, the RADIUS client is the Gateway GPRS Support Node (GGSN). Because a single GGSN can handle more users than a single SSG, multiple SSGs are required. The SSGs are grouped in a server farm. Each SSG acts as a RADIUS proxy server, inspecting the RADIUS messages that traverse it.

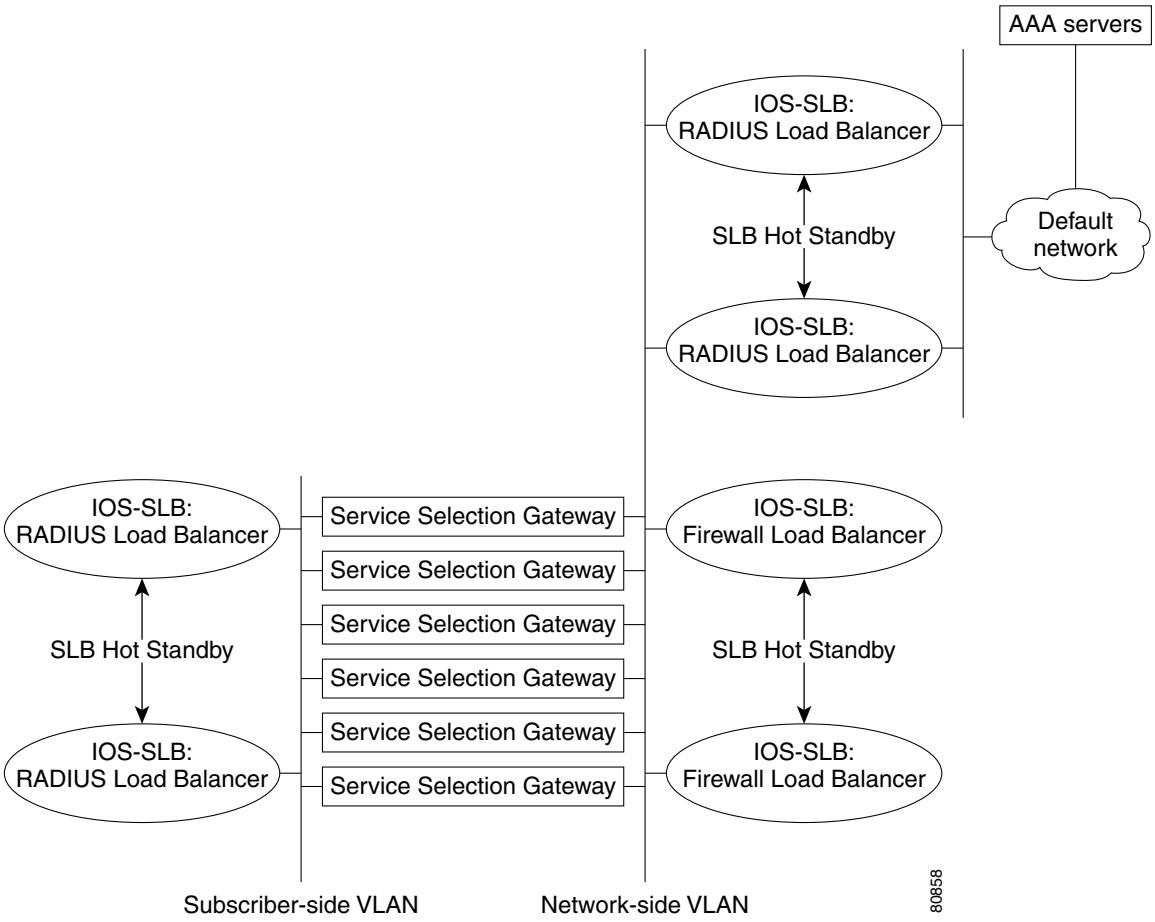
A sample service gateway load balancing configuration is shown in Figure 1-3. Load balancing for service gateways requires that the service gateways be sandwiched between the RLB and the FWLB. To protect against possible load balancer failure, redundant load balancers are deployed.

The RLB and FWLB provide load balancing and fail-over capability for a farm of SSGs. On the subscriber side, the load balancing includes management of the RADIUS message flows, as well as the data traffic. The RLB balances the load of RADIUS messages and data across multiple SSGs in the server farm.

On the network side, load balancing ensures that data traffic for sessions initiated by subscribers is returned to the same service gateway it initially traversed. In addition, the CMX can be configured to load-balance RADIUS messages toward RADIUS (AAA) servers as shown in Figure 1-3.

The RLB, FWLB, and SSG are software functions that reside on hardware platforms. The SSG function resides on the 7400 series platform. The RLB and FWLB functions reside on the 7600 series platform.

Figure 1-3 Service Gateway Load Balancing



RADIUS Load Balancing

The subscriber side requires the RLB data stream *sticky* feature provided by the IOS-SLB software. This feature examines unique data elements within the RADIUS messages while also acting as a RADIUS load balancer. It caches this information and uses it to balance subsequent connections from the subscriber. Each service gateway is configured as a real server within the SSG server farm. The server farm is configured as a virtual server with a virtual IP address. This virtual IP address is configured in the network address server (NAS) as a RADIUS server. For GPRS wireless networks, this feature

examines the content of the RADIUS messages sent to the configured RADIUS virtual IP address, extracts the framed IP attribute, and caches it. This allows the feature to *stick* all subsequent data flows from that client to the same service gateway.

The RLB detects failure of a real server within the RADIUS server farm by watching for Internet Control Message Protocol (ICMP) errors on the RADIUS flow, as well as using ping health check probes (if they are configured). When one of the entities in the server farm fails, the RLB can reassign new subscriber data flows to one of the other real servers in the server farm or in a backup server farm.

On the network side, the RLB can be configured to load-balance the flow of RADIUS messages toward the RADIUS (AAA) servers for authentication, authorization, and accounting.

Firewall Load Balancing

The network side must be able to switch return traffic to the same SSG that processed the forward flow. Using the connection-tracking feature of the FWLB, return traffic can be forwarded correctly. The FWLB tracks active connections (defined by protocol, source IP address, source port, destination IP address, and destination port) to ensure that return flows for the same connection are routed to the same service gateway that passed the forward flow.

The load balancing requirements on the two sides of the SSG farm are not symmetric. This asymmetry requires additional logic for application protocols such as file transfer protocol (FTP). By using the source/destination IP *sticky* feature, these protocols can be properly routed. The load balancer recognizes that the network-initiated connection is related to the pre-existing flow and routes the new connection through the same SSG that handled the original request for service.

Network Management

Network management of CMX elements comprises a suite of applications for managing mobile wireless service implementations based on different deployment configurations. Network management of CMX elements covers three areas:

- Transport management—Configuration, fault monitoring, performance management, and unified mediation functions
- Domain management—View of packet gateways and service domains, domain-specific resource allocation and assignment, and domain session allocation, association, and QoS control
- Service control—Interfaces to enable subscriber-based mobile services and support of OSS-ready content and billing solutions

The CiscoWorks for Mobile Wireless (CW4MW) software bundle is the element management system used to manage the CMX network elements. The CW4MW discovers the NEs under its domain to build a topology map and discover adjacent NEs. Table 1-1 lists the managment functions provided by the CW4MW.

Table 1-1 CW4MW Management Functions

Management Function	Description
Management system	CW4MW provides transport-level control and coordination of the network elements within its domain. For the CMX, the network elements include the SSG, RLB, FWLB, and CSG.
Fault Management	A network element in the CMX framework that encounters a fault condition generates SNMP traps and sends them to the management system platform. Details of the problem are based on the traps. The platform enables the operator to view the problem.

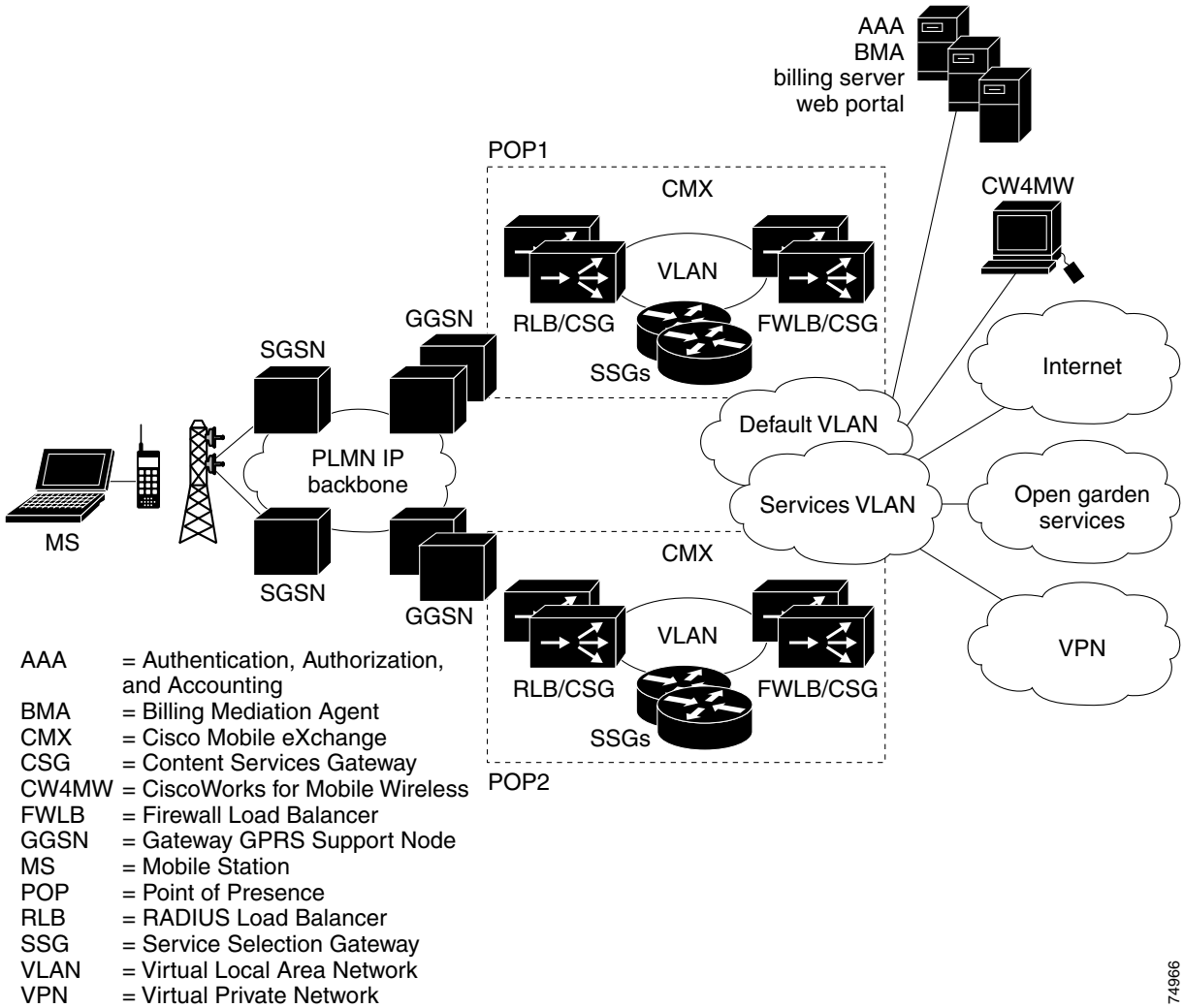
Management Function	Description
Configuration Management	The CW4MW suite provides command line interfaces to create new configurations and modify existing ones. Configurations are stored on the management platform.
Performance Management	The CW4MW suite provides capabilities to view performance data in real time. Performance data is based on the SNMP information that is polled from the device being monitored.
Security Management	The CW4MW suite provides capabilities to manage device passwords for various classes of users.

Additional information on the CW4MW is provided in "CMX Network Management" section on page 4-1.

CMX Framework Example

Figure 1-4 shows an example of the Cisco Mobile Exchange framework in a GPRS/UMTS network.

Figure 1-4 Cisco Mobile Exchange Framework



Overview of GSM, GPRS, and UMTS

The Cisco Mobile Exchange (CMX) architecture provides mobile wireless solutions for operators using General Packet Radio Service (GPRS) and Universal Mobile Telecommunication System (UMTS) access technologies. This chapter provides an overview of these technologies and their roles in the evolution from second-generation (2G) to third-generation (3G) mobile wireless networks.

- Global System for Mobile Communications (GSM)—A digital, mobile, radio standard developed for mobile, wireless, voice communications
- GPRS—An extension of GSM networks that provides mobile, wireless, data communications
- UMTS—An extension of GPRS networks that moves toward an all-IP network by delivering broadband information, including commerce and entertainment services, to mobile users via fixed, wireless, and satellite networks

This chapter includes the following sections:

Global Systems for Mobile Communications

In the early 1980s, many countries in Europe witnessed a rapid expansion of analog cellular telephone systems. However, each country developed its own system, and interoperability across borders became a limiting factor.

In 1982, the Conference of European Post and Telecommunications (CEPT), an association of telephone and telegraph operators in Europe, established a working group to develop a new public land mobile system to span the continent. Because their working language was French, the group was called the Groupe Speciale Mobile (GSM).

The GSM group proposed the following criteria for the new mobile wireless system:

- good speech quality
- low cost for terminals and service
- international roaming
- handheld terminals
- support for introduction new services
- spectral efficiency
- compatibility with Integrated Digital Services Network (ISDN)

In 1989, the responsibility for GSM development was transferred to the European Telecommunications Standards Institute (ETSI), and phase 1 of the GSM specification was published in 1990. The first commercial service was launched in 1991.

When the official language of the GSM group changed from French to English, GSM was changed from Groupe Speciale Mobile to Global System for Mobile Communications.

In 1994, phase 2 data/fax services were launched, and in 1995, the GSM phase 2 standard was completed. The first GSM services in the United States were launched.

GSM uses a combination of both the time division multiple access (TDMA) and frequency division multiple access (FDMA) technologies. With this combination, more channels of communications are available, and all channels are digital.

The GSM service is available in four frequency bands:

- 450-MHz—Upgrade of older analog cellular systems in Scandinavia
- 900-MHz—Original band used everywhere except North America and most of South America
- 1800-MHz—New band to increase capacity and competition used everywhere except North America and most of South America
- 1900-MHz—Personal communications service band used in North America and much of South America

The higher frequency bands provide additional capacity and higher subscriber densities.

One of the unique benefits of GSM service is its capability for international roaming because of the roaming agreements established between the various GSM operators worldwide.

GSM Technology Differentiator

One of the advantages of GSM is that it offers a subscriber identity module (SIM), also known as a smart card. The smart card contains a computer chip and some non-volatile memory and is inserted into a slot in the base of the mobile handset.

The memory on the smart card holds information about the subscriber that enables a wireless network to provide subscriber services. The information includes:

- The subscriber's identity number
- The telephone number
- The original network to which the subscriber is subscribed

A smart card can be moved from one handset to another. A handset reads the information off the smart card and transmits it to the network.

GSM Network Elements

A GSM network consists of the following network components:

- Mobile station (MS)
- Base transceiver station (BTS)
- Base station controller (BSC)
- Base station subsystem (BSS)
- Mobile switching center (MSC)
- Authentication center (AuC)
- Home location register (HLR)
- Visitor location register (VLR)

Mobile Station

The mobile station (MS) is the starting point of a mobile wireless network. The MS can contain the following components:

- Mobile terminal (MT)—GSM cellular handset
- Terminal equipment (TE)—PC or personal digital assistant (PDA)

The MS can be two interconnected physical devices (MT and TE) with a point-to-point interface or a single device with both functions integrated.

Base Transceiver Station

When a subscriber uses the MS to make a call in the network, the MS transmits the call request to the base transceiver station (BTS). The BTS includes all the radio equipment (i.e., antennas, signal processing devices, and amplifiers) necessary for radio transmission within a geographical area called a cell. The BTS is responsible for establishing the link to the MS and for modulating and demodulating radio signals between the MS and the BTS.

Base Station Controller

The base station controller (BSC) is the controlling component of the radio network, and it manages the BTSs. The BSC reserves radio frequencies for communications and handles the handoff between BTSs when an MS roams from one cell to another. The BSC is responsible for paging the MS for incoming calls.

Base Station Subsystem

A GSM network is comprised of many base station subsystems (BSSs), each controlled by a BSC. The BSS performs the necessary functions for monitoring radio connections to the MS, coding and decoding voice, and rate adaptation to and from the wireless network. A BSS can contain several BTSs.

Mobile Switching Center

The mobile switching center (MSC) is a digital ISDN switch that sets up connections to other MSCs and to the BSCs. The MSCs form the wired (fixed) backbone of a GSM network and can switch calls to the public switched telecommunications network (PSTN). An MSC can connect to a large number of BSCs.

Equipment Identity Register

The equipment identity register (EIR) is a database that stores the international mobile equipment identities (IMEIs) of all the mobile stations in the network. The IMEI is an equipment identifier assigned by the manufacturer of the mobile station. The EIR provides security features such as blocking calls from handsets that have been stolen.

Home Location Register

The home location register (HLR) is the central database for all users to register to the GSM network. It stores static information about the subscribers such as the international mobile subscriber identity (IMSI), subscribed services, and a key for authenticating the subscriber. The HLR also stores dynamic subscriber information (i.e., the current location of the mobile subscriber).

Authentication Center

Associated with the HLR is the authentication center (AuC); this database contains the algorithms for authenticating subscribers and the necessary keys for encryption to safeguard the user input for authentication.

Visitor Location Register

The visitor location register (VLR) is a distributed database that temporarily stores information about the mobile stations that are active in the geographic area for which the VLR is responsible. A VLR is associated with each MSC in the network. When a new subscriber roams into a location area, the VLR is responsible for copying subscriber information from the HLR to its local database. This relationship between the VLR and HLR avoids frequent HLR database updates and long distance signaling of the user information, allowing faster access to subscriber information.

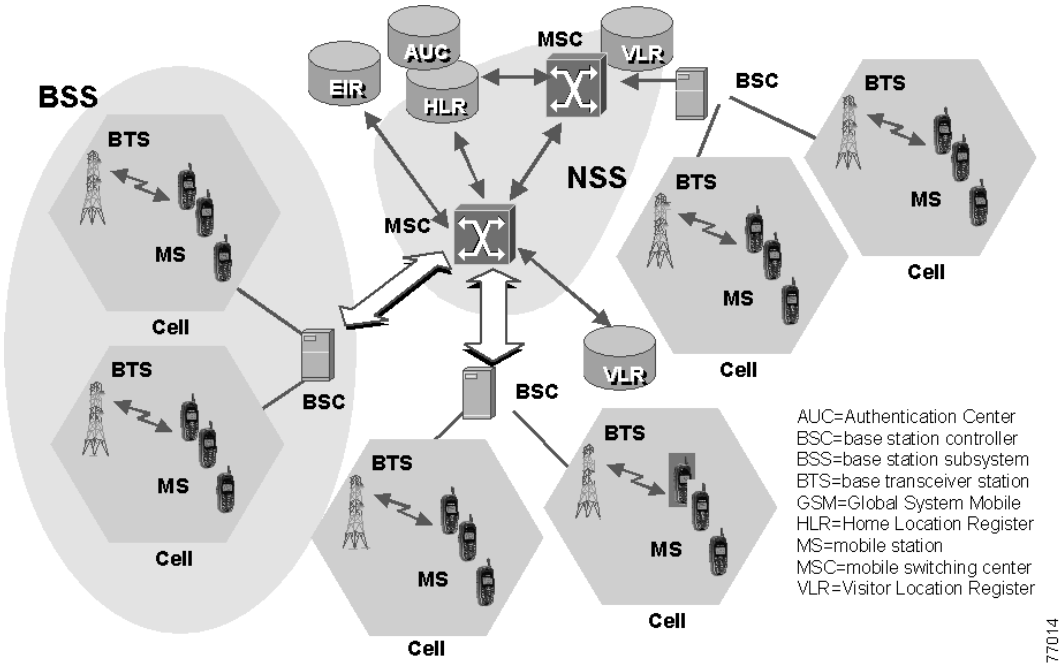
The HLR, VLR, and AuC comprise the management databases that support roaming (including international roaming) in the GSM network. These databases authenticate calls while GSM subscribers roam between the private network and the public land mobile network (PLMN). The types of information they store include subscriber identities, current location area, and subscription levels.

Network and Switching Subsystem

The network and switching subsystem (NSS) is the heart of the GSM system. It connects the wireless network to the standard wired network. It is responsible for the handoff of calls from one BSS to another and performs services such as charging, accounting, and roaming.

Figure 2-1 shows a GSM network and the network elements it contains.

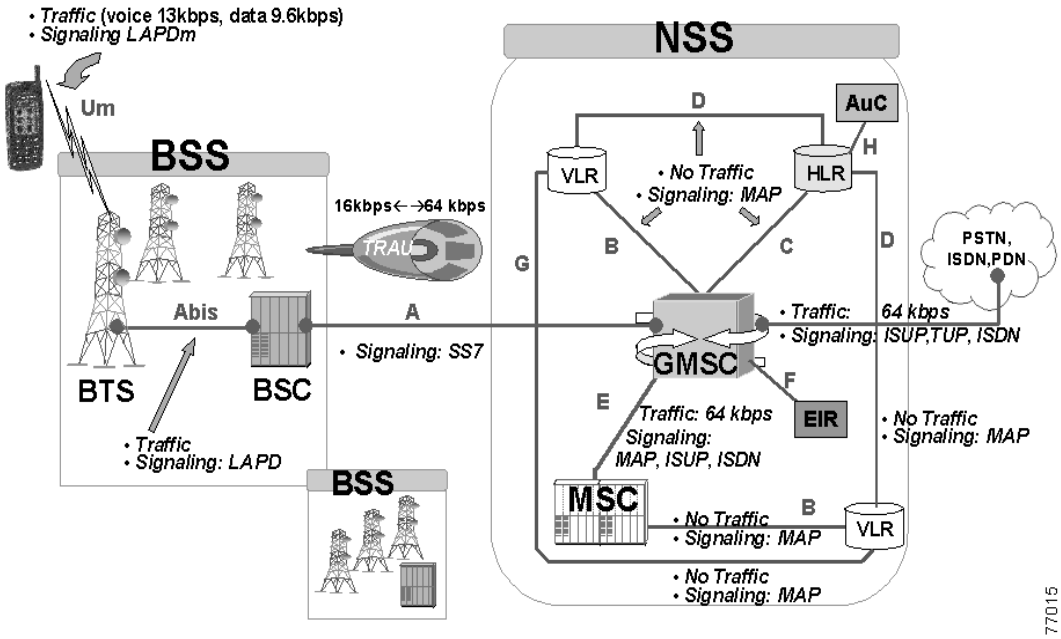
Figure 2-1 GSM Network Elements



GSM Interfaces

The GSM uses various interfaces for communication among its network elements. Figure 2-2 shows these interfaces.

Figure 2-2 GSM Interfaces



Mobile wireless communication occurs over the interfaces between the network elements in a sequential manner. In Figure 2-2, the MS transmits to the BTS, the BTS to the BSC, and the BSC to the MSC. Communications also occur over the interfaces to the management databases (HLR, VLR, AuC, and EIR). Communications might traverse multiple MSCs but ultimately must reach the gateway MSC (GMSC). The GMSC provides the gateway to the public switched telephone network (PSTN). A separate interface exists between each pair of elements, and each interface requires its own set of protocols.

In the BSS block, mobile communication occurs over the air interface to the BTS using the ISDN Link Access Procedure-D mobile (LAP-Dm). This traffic channel carries speech and data. In this example, voice operates at full-rate 13 kbps (supported by LAP-Dm), and data operates at full-rate 9.6 kbps.The BTS communicates to the BSC over the *Abis* interface using the ISDN LAP-D signaling protocol. The BSC communicates to the GMSC via the transcoder rate adapter unit (TRAU), which translates between 16 kbps on the BTS side to 64 kbps on the GMSC side. This interface uses the signaling system 7 (SS7) protocol, which defines call set-up and call services across the interface.

At the NSS, the GMSC is the central node. Link-level traffic and signaling control occurs over the interface between the GMSC and MSC and the interface to the external network (PSTN, ISDN or PDN). Different signaling protocols are used on the interfaces. Some NSS interfaces involve only control signaling protocols with no traffic. For example, no traffic is generated on the interfaces between the GMSC, HLR, and VLR. Instead, these interfaces carry only signaling using the Mobile Application Part (MAP) of the SS7 protocol. The MAP is specified in IS-41 and defines the application layer, signaling protocols, and procedures for registering mobile users and handling handoffs between cellular systems. The GMSC establishes call traffic (at 64 kbps) onto the PSTN via the ISDN user part (ISUP), which is an SS7-based protocol. The GMSC and MSC exchange traffic (over LAP-D at 64 kbps) and use SS7 (MAP and ISUP) control.

GSM Data Services

GSM networks handle both voice and data traffic requirements of the mobile communication by providing two modes of operation:

- Circuit switched (high-speed circuit switched data)
- Packet switched (GPRS)

Circuit switching provides the customer with a dedicated channel all the way to the destination. The customer has exclusive use of the circuit for the duration of the call, and is charged for the duration of the call.

With packet switching, the operator assigns one or more dedicated channels specifically for shared use. These channels are up and running 24 hours a day, and when you need to transfer data, you access a channel and transmit your data. Packet switching is more efficient than circuit switching.

The standard data rate of a GSM channel is 22.8 kbps.

General Packet Radio Service

The general packet radio system (GPRS) provides packet radio access for mobile Global System for Mobile Communications (GSM) and time-division multiple access (TDMA) users. In addition to providing new services for today's mobile user, GPRS is important as a migration step toward third-generation (3G) networks. GPRS allows network operators to implement an IP-based core architecture for data applications, which will continue to be used and expanded for 3G services for integrated voice and data applications. The GPRS specifications are written by the European Telecommunications Standard Institute (ETSI), the European counterpart of the American National Standard Institute (ANSI).

GPRS is the first step toward an end-to-end wireless infrastructure and has the following goals:

- Open architecture
- Consistent IP services
- Same infrastructure for different air interfaces
- Integrated telephony and Internet infrastructure
- Leverage industry investment in IP
- Service innovation independent of infrastructure

Benefits of GPRS

The GPRS provides the following benefits:

- Overlays on the existing GSM network to provide high-speed data service
- Always on, reducing the time spent setting up and taking down connections
- Designed to support bursty applications such as e-mail, traffic telematics, telemetry, broadcast services, and web browsing that do not require detected connection.

By implementing Cisco GPRS products and related solutions, mobile service providers can optimize their networks to deploy high quality mobile voice and data services. They can also benefit from new operating efficiencies, peer-to-peer IP-based architecture for scalability, and IP standard interfaces to billing and customer support.

GPRS Applications

GPRS enables a variety of new and unique services to the mobile wireless subscriber. These mobile services have unique characteristics that provide enhanced value to customers. These characteristics include the following:

- Mobility—The ability to maintain constant voice and data communications while on the move
- Immediacy—Allows subscribers to obtain connectivity when needed, regardless of location and without a lengthy login session
- Localization—Allows subscribers to obtain information relevant to their current location

The combination of these characteristics provides a wide spectrum of possible applications that can be offered to mobile subscribers. The core network components offered by Cisco enable seamless access to these applications, whether they reside in the service provider's network or the public Internet.

In general, applications can be separated into two high-level categories: corporate and consumer. These include:

- Communications—E-mail; fax; unified messaging; intranet/Internet access
- Value-added services—Information services; games
- E-commerce—Retail; ticket purchasing; banking; financial trading
- Location-based applications—Navigation; traffic conditions; airline/rail schedules; location finder
- Vertical applications—Freight delivery; fleet management; sales-force automation
- Advertising

Communications

Communications applications include those in which it appears to users that they are using the mobile communications network as a pipeline to access messages or information. This differs from those applications in which users believe that they are accessing a service provided or forwarded by the network operator.

Intranet Access

The first stage of enabling users to maintain contact with their offices is through access to e-mail, fax, and voice mail using unified messaging systems. Increasingly, files and data on corporate networks are becoming accessible through corporate intranets. These intranets can be protected through firewalls by enabling secure tunnels or virtual private networks (VPNs).

Internet Access

As a critical mass of users is approached, more and more applications aimed at general consumers are being placed on the Internet. The Internet is becoming an effective tool for accessing corporate data and manipulating product and service information. More recently, companies are using the Internet as an environment for conducting business through e-commerce.

Email and Fax

E-mail on mobile networks may take one of two forms. E-mail can be sent to a mobile user directly or the user can have an e-mail account maintained by the network operator or their Internet service provider (ISP). In the latter case, a notification is forwarded to the mobile terminal and includes the first few lines of the e-mail, details of the sender, the date and time, and the subject. Fax attachments can also accompany e-mails.

Unified Messaging

Unified messaging provides a single mailbox for all messages, including voice mail, faxes, e-mail, short message service (SMS), and pager messages. Unified messaging systems allow for a variety of access methods to recover messages of different types. Some use text-to-voice systems to read e-mail or send faxes over a normal phone line. Most allow the user to query the contents of the various mailboxes through data access such as the Internet. Others can be configured to alert the user on the device of their choice when messages are received.

Value Added Services

Value-added services refer to the content provided by network operators to increase the value of services to their subscribers. Two terms that are frequently used to describe delivery of data applications are *push* and *pull*, as defined below.

- *Push* describes the transmission of data at a predetermined time or under predetermined conditions. It also refers to the unsolicited supply of advertising (for example, delivery of news as it occurs or stock values when they fall below a preset value).
- *Pull* describes the request for data in real time by the user (for example, checking stock quotes or daily news headlines).

To be valuable to subscribers, this content must possess several characteristics:

- Personalized information that is tailored to the user (for example, a stock ticker that focusses on key quotes and news or an e-commerce application that knows a user's profile)
- Localized content that is based on a user's current location and includes maps, hotel finders, or restaurant reviews
- Menu screens that are intuitive and easy to navigate
- Security for e-commerce sites for the exchange of financial or other personal information

Several value-added services are outlined in the following sections.

E-commerce

E-commerce is defined as business conducted on the Internet or data service. This includes applications in which a contract is established for the purchase of goods and services and online banking applications. These applications require user authentication and secure transmission of sensitive data over the data connection.

Banking

The banking industry is interested in promoting electronic banking because electronic transactions are less costly to conduct than personal transactions in a bank. Specific banking functions that can be accomplished over a wireless connection include balance checking, money transfers between accounts, bill payment, and overdraft alert.

Financial Trading

The immediacy of transactions over the Internet and the requirement for up-to-the-minute information has made the purchasing of stocks online a popular application. By coupling push services with the ability to make secure transactions from the mobile terminal, a service that is unique to the mobile environment can be provided.

Location-Based Services and Telematics

Location-based services provide the ability to link push or pull information services with a user's location. Examples include hotel and restaurant finders, roadside assistance, and city-specific news and information. This technology also has vertical applications. These allow, for example, tracking vehicles in a fleet or managing the operations of a large workforce.

Vertical Applications

In the mobile environment, vertical applications apply to systems using mobile architectures to support the specific tasks within a company. Examples of vertical applications include:

- Sales support—Configuring stock and product information for sales staff, integrating appointment details, and placing orders remotely
- Dispatching—Communicating job details such as location and scheduling and permitting information queries to support the job
- Fleet management—Controlling a fleet of delivery or service staff and vehicle, monitoring their locations, and scheduling their work
- Parcel delivery—Tracking the locations of packages for customers and monitoring the performance of the delivery system

Advertising

Advertising services are offered as a push information service. Advertising may be offered to customers to subsidize the cost of voice or other information services. Advertising may be location sensitive. For example, a user entering a mall can receive advertisements specific to the stores in that mall.

GPRS Architecture

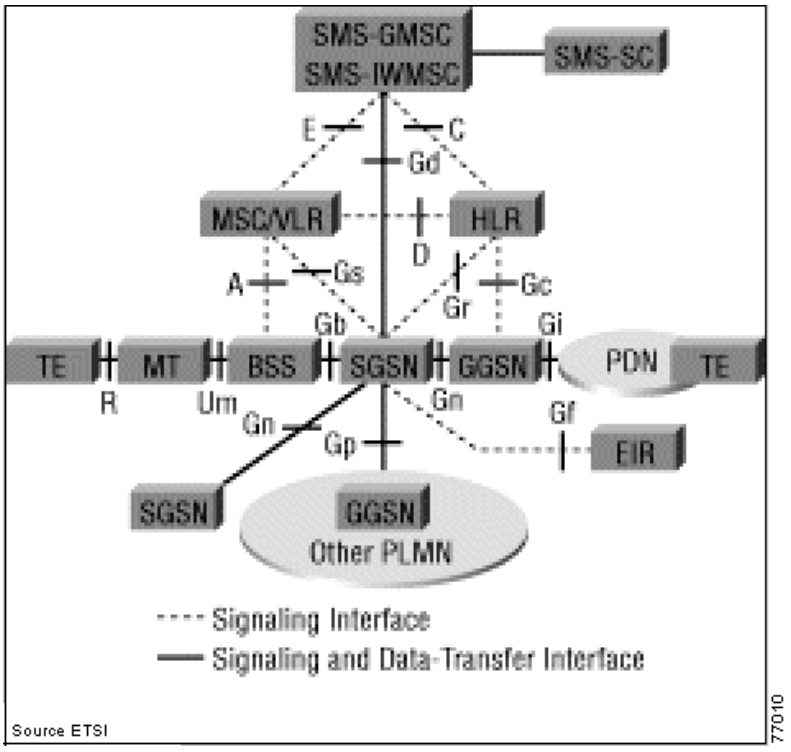
GPRS is a data network that overlays a second-generation GSM network. This data overlay network provides packet data transport at rates from 9.6 to 171 kbps. Additionally, multiple users can share the same air-interface resources simultaneously.

GPRS attempts to reuse the existing GSM network elements as much as possible, but to effectively build a packet-based mobile cellular network, some new network elements, interfaces, and protocols for handling packet traffic are required. Therefore, GPRS requires modifications to numerous network elements as summarized in Table 2-1 and shown in Figure 2-3.

Table 2-1 GPRS Network Elements

GSM Network Element	Modification or Upgrade Required for GPRS.
Terminal Equipment (TE)	New terminal equipment is required to access GPRS services. These new terminals will be backward compatible with GSM for voice calls.
BTS	A software upgrade is required in the existing base transceiver site.
BSC	The base station controller (BSC) requires a software upgrade and the installation of new hardware called the packet control unit (PCU). The PCU directs the data traffic to the GPRS network and can be a separate hardware element associated with the BSC.
GPRS Support Nodes (GSNs)	The deployment of GPRS requires the installation of new core network elements called the serving GPRS support node (SGSN) and gateway GPRS support node (GGSN).
Databases (HLR, VLR, etc.)	All the databases involved in the network will require software upgrades to handle the new call models and functions introduced by GPRS.

Figure 2-3 GPRS Reference Architecture



GPRS Subscriber Terminals

New terminals are required because existing GSM phones do not handle the enhanced air interface or packet data. A variety of terminals can exist, including a high-speed version of current phones to support high-speed data access, a new PDA device with an embedded GSM phone, and PC cards for laptop computers. These terminals are backward compatible for making voice calls using GSM.

GPRS Base Station Subsystem

Each BSC requires the installation of one or more PCUs and a software upgrade. The PCU provides a physical and logical data interface to the base station subsystem (BSS) for packet data traffic. The BTS can also require a software upgrade but typically does not require hardware enhancements.

When either voice or data traffic is originated at the subscriber terminal, it is transported over the air interface to the BTS, and from the BTS to the BSC in the same way as a standard GSM call. However, at the output of the BSC, the traffic is separated; voice is sent to the mobile switching center (MSC) per standard GSM, and data is sent to a new device called the SGSN via the PCU over a Frame Relay interface.

GPRS Support Nodes

In the core network, the existing MSCs are based on circuit-switched central-office technology and cannot handle packet traffic. Two new components, called GPRS support nodes (GSNs), are added:

- Serving GPRS support node (SGSN)
- Gateway GPRS support node (GGSN)

Serving GPRS Support Node

The SGSN delivers packets to mobile stations (MSs) within its service area. SGSNs send queries to home location registers (HLRs) to obtain profile data of GPRS subscribers. SGSNs detect new GPRS MSs in a given service area, process registration of new mobile subscribers, and keep records of their locations inside a predefined area. The SGSN performs mobility management functions such as handing off a roaming subscriber from the equipment in one cell to the equipment in another. The SGSN is connected to the base station subsystem through a Frame Relay connection to the PCU in the BSC.

Gateway GPRS Support Node

GGSNs are used as interfaces to external IP networks such as the public Internet, other mobile service providers' GPRS services, or enterprise intranets. GGSNs maintain routing information that is necessary to tunnel the protocol data units (PDUs) to the SGSNs that service particular MSs. Other functions include network and subscriber screening and address mapping. One or more GGSNs can be provided to support multiple SGSNs. More detailed descriptions of the SGSN and GGSN are provided in a later section.

GPRS Terminals

The term *terminal equipment* is generally used to refer to the variety of mobile phones and mobile stations that can be used in a GPRS environment. The equipment is defined by terminal classes and types. Cisco's gateway GPRS serving node (GGSN) and data network components interoperate with GPRS terminals that meet the GPRS standards.

Three classes of GPRS terminals are provided: Class A, Class B, or Class C.

Class A Terminals

Class A terminals support GPRS and other GSM services (such as SMS and voice) simultaneously. This support includes simultaneous attach, activation, monitor, and traffic. Class A terminals can make or receive calls on two services simultaneously. In the presence of circuit-switched services, GPRS virtual circuits are held (i.e., placed on hold) instead of being cleared.

Class B Terminals

Class B terminals can monitor GSM and GPRS channels simultaneously but can support only one of these services at a time. Therefore, a Class B terminal can support simultaneous attach, activation, and monitor, but not simultaneous traffic. As with Class A, the GPRS virtual circuits are not disconnected when circuit-switched traffic is present. Instead, they are switched to busy mode. Users can make or receive calls on either a packet or a switched call type sequentially, but not simultaneously.

Class C Terminals

Class C terminals support only sequential attach. The user must select which service to connect to. Therefore, a Class C terminal can make or receive calls from only the manually selected (or default) service. The service that is not selected is unreachable. The GPRS specifications state that support of SMS is optional for Class C terminals.

GPRS Device Types

In addition to the three terminal classes, each handset has a unique form (housing design). Some of the forms are similar to current mobile wireless devices, while others will evolve to use the enhanced data capabilities of GPRS.

The earliest available type is closely related to the current mobile phone. These are available in the standard form with a numeric keypad and a relatively small display.

PC cards are credit card-sized hardware devices that connect through a serial cable to the bottom of a mobile phone. Data cards for GPRS phones enable laptops and other devices with PC card slots to be connected to mobile GPRS-capable phones. Card phones provide functions similar to those offered by PC cards without requiring a separate phone. These devices may require an ear piece and microphone to support voice services.

Smart phones are mobile phones with built-in voice, nonvoice, and Web-browsing services. Smart phones integrate mobile computing and mobile communications into a single terminal. They come in various form factors, which may include a keyboard or an icon drive screen.

The increase in machine-to-machine communications has led to the adoption of application-specific devices. These *black-box* devices lack a display, keypad, and voice accessories of a standard phone. Communication is accomplished through a serial cable. Applications such as meter reading utilize such black-box devices.

Personal digital assistants (PDAs), such as the Palm Pilot series or Handspring Visor, and handheld communications devices are data-centric devices that are adding mobile wireless access. These devices can either connect with a GPRS-capable mobile phone via a serial cable or integrate GPRS capability. Access can be gained via a PC card or a serial cable to a GPRS-capable phone.

Data Routing

One of the main requirements in the GPRS network is the routing of data packets to and from a mobile user. The requirement can be divided into two areas: data packet routing and mobility management.

Data Packet Routing

The main functions of the GGSN involve interaction with the external data network. The GGSN updates the location directory using routing information supplied by the SGSNs about the location of an MS. It routes the external data network protocol packet encapsulated over the GPRS backbone to the SGSN currently serving the MS. It also decapsulates and forwards external data network packets to the appropriate data network and collects charging data that is forwarded to a charging gateway (CG).

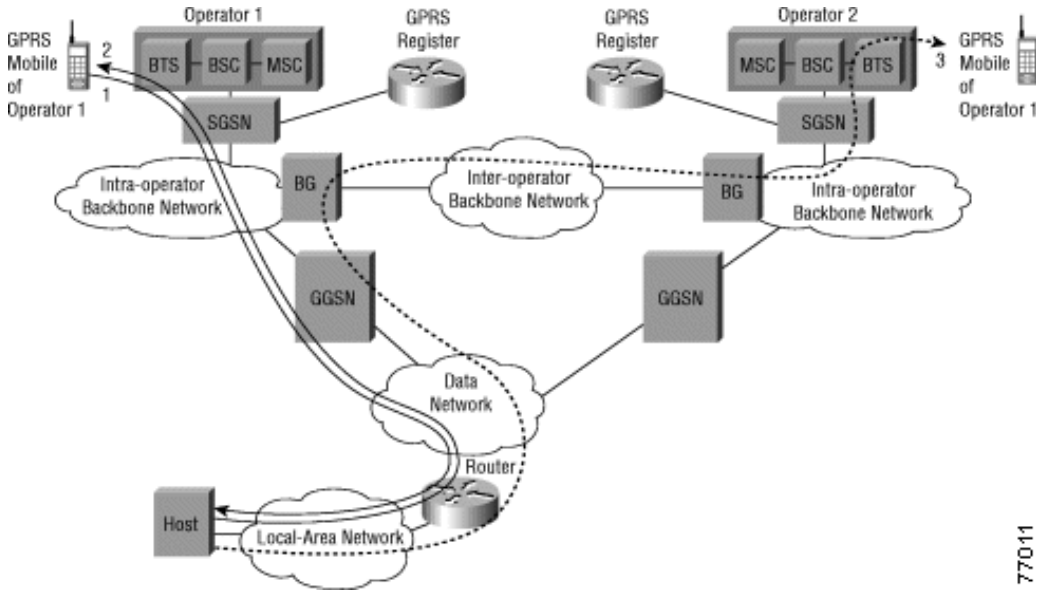
In Figure 2-4, three routing schemes are illustrated:

- Mobile-originated message (path 1)—This path begins at the GPRS mobile and ends at the Host
- Network-initiated message when the MS is in its home network (path 2)—This path begins at the Host and ends at the GPRS mobile
- Network-initiated message when the MS roams to another GPRS network (path 3)—This path is indicated by the dotted line

In these examples, the operator's GPRS network consists of multiple GSNs (with a gateway and serving functionality) and an intra-operator backbone network.

GPRS operators allow roaming through an inter-operator backbone network. The GPRS operators connect to the inter-operator network through a border gateway (BG), which can provide the necessary interworking and routing protocols (for example, border gateway protocol [BGP]). In the future, GPRS operators might implement quality of service (QoS) mechanisms over the inter-operator network to ensure service-level agreements (SLAs). The main benefits of the architecture are its flexibility, scalability, interoperability, and roaming attributes.

Figure 2-4 Routing of Data Packets between a Fixed Host and a GPRS MS



The GPRS network encapsulates all data network protocols into its own encapsulation protocol called the GPRS tunneling protocol (GTP). The GTP ensures security in the backbone network and simplifies the routing mechanism and the delivery of data over the GPRS network.

Mobility Management

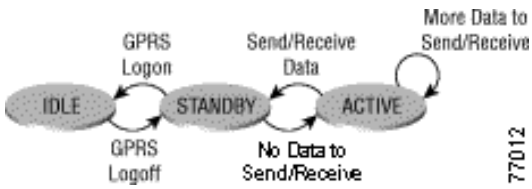
The operation of the GPRS is partly independent of the GSM network. However, some procedures share the network elements with current GSM functions to increase efficiency and to make optimum use of free GSM resources (such as unallocated time slots).

An MS has three states in the GPRS system (Figure 2-5):

- Active
- Standby
- Idle

The three-state model is unique to packet radio; GSM uses a two-state model (idle or active).

Figure 2-5 GPRS States in a Mobile Station



Active State

Data is transmitted between an MS and the GPRS network only when the MS is in the active state. In the active state, the SGSN knows the cell location of the MS.

Packet transmission to an active MS is initiated by packet paging to notify the MS of an incoming data packet. The data transmission proceeds immediately after packet paging through the channel indicated by the paging message. The purpose of the paging message is to simplify the process of receiving packets. The MS listens to only the paging messages instead of to all the data packets in the downlink channels. This reduces battery usage significantly.

When an MS has a packet to transmit, it must access the uplink channel (i.e., the channel to the packet data network where services reside). The uplink channel is shared by a number of MSs, and its use is allocated by a BSS. The MS requests use of the channel in a random access message. The BSS allocates an unused channel to the MS and sends an access grant message in reply to the random access message. The description of the channel (one or multiple time slots) is included in the access grant message. The data is transmitted on the reserved channels.

Standby State

In the standby state, only the routing area of the MS is known. (The routing area can consist of one or more cells within a GSM location area).

When the SGSN sends a packet to an MS that is in the standby state, the MS must be paged. Because the SGSN knows the routing area of the MS, a packet paging message is sent to the routing area. On receiving the packet paging message, the MS relays its cell location to the SGSN to establish the active state.

The main reason for the standby state is to reduce the load in the GPRS network caused by cell-based routing update messages and to conserve the MS battery. When an MS is in the standby state, the SGSN is informed of only routing area changes. By defining the size of the routing area, the operator can control the number of routing update messages.

Idle State

In the idle state, the MS does not have a logical GPRS context activated or any packet-switched public data network (PSPDN) addresses allocated. In this state, the MS can receive only those multicast messages that can be received by any GPRS MS. Because the GPRS network infrastructure does not know the location of the MS, it is not possible to send messages to the MS from external data networks.

Routing Updates

When an MS that is in an active or a standby state moves from one routing area to another within the service area of one SGSN, it must perform a routing update. The routing area information in the SGSN is updated, and the success of the procedure is indicated in the response message.

A cell-based routing update procedure is invoked when an active MS enters a new cell. The MS sends a short message containing the identity of the MS and its new location through GPRS channels to its current SGSN. This procedure is used only when the MS is in the active state.

The inter-SGSN routing update is the most complicated routing update. The MS changes from one SGSN area to another, and it must establish a new connection to a new SGSN. This means creating a new logical link context between the MS and the new SGSN and informing the GGSN about the new location of the MS.

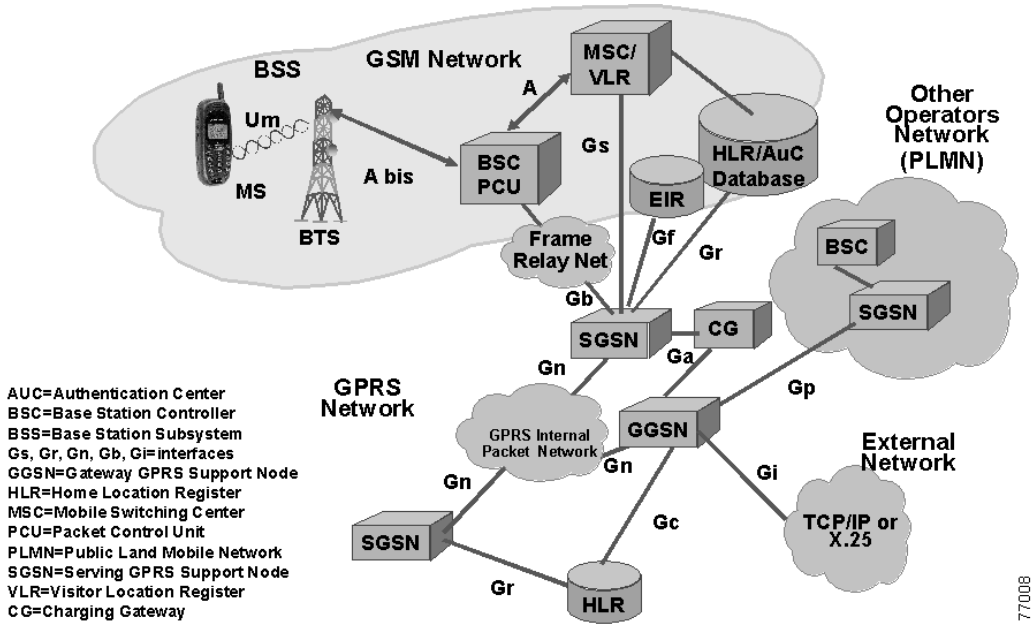
GPRS Interfaces

The GPRS architecture consists of signaling interfaces with various protocols that control and support the transmission of packets across the networks and to the mobile stations. The interfaces in a GPRS network are:

- Ga—Interface between GSN nodes (GGSN, SGSN) and charging gateway (CG)
- Gb—Interface between SGSN and BSS (PCU); normally uses Frame Relay
- Gc—Interface between GGSN and HLR
- Gi—Interface between GPRS (GGSN) and an external packet data network (PDN)
- Gn—Interface between two GSN nodes, i.e., GGSN and SGSN; this connects into the intra-network backbone, for example, an Ethernet network
- Gp—Interface between two GSN nodes in different PLMNs; this is via border gateways and is an inter-PLMN network backbone
- Gr—Interface between SGSN and HLR
- Gs—Interface between SGSN and the MSC/VLR
- Gf—Interface between SGSN and EIR

Figure 2-6 shows these interfaces.

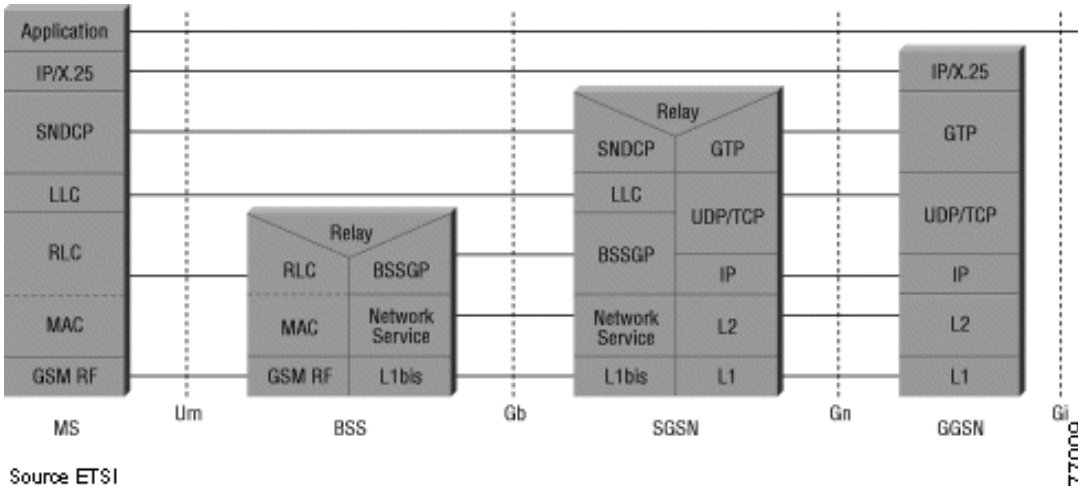
Figure 2-6 GPRS Interfaces



GPRS Protocol Stacks

Figure 2-7 shows the GPRS protocol stack and end-to-end message flows from the MS to the GGSN. The protocol between the SGSN and GGSN using the Gn interface is GTP. This is a Layer 3 tunneling protocol similar to L2TP.

Figure 2-7 GPRS Network Protocol Stack



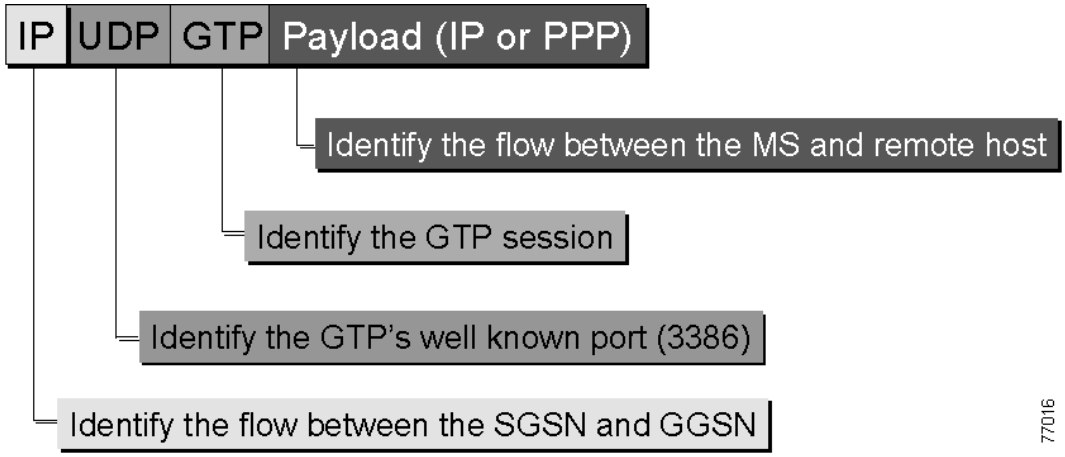
Although Figure 2-7 defines the Gn and Gi interface as IP, the underlying protocols are not specified, providing flexibility with the physical medium. The GGSN software runs on a Cisco 7206VXR hardware platform, which provides a wide range of supported physical interfaces and a high port density. The GGSN software uses a virtual template interface, which is a logical interface within the router and does not depend on the physical medium directly. A list of supported physical interfaces for the 7206VXR can be found at this URL:
http://www.cisco.com/univercd/cc/td/doc/product/core/7200vx/portadpt/index.htm.

The most common physical interface used with GPRS is Fast Ethernet. This interface provides high bandwidth, low cost, and universal connectivity to other vendor equipment. For the Gi interface, common interfaces are Serial, E1/T1 or Ethernet. Running over the physical WAN interfaces can be a wide range of protocols including Frame Relay, ISDN, and HDLC.

GPRS Tunneling Protocol

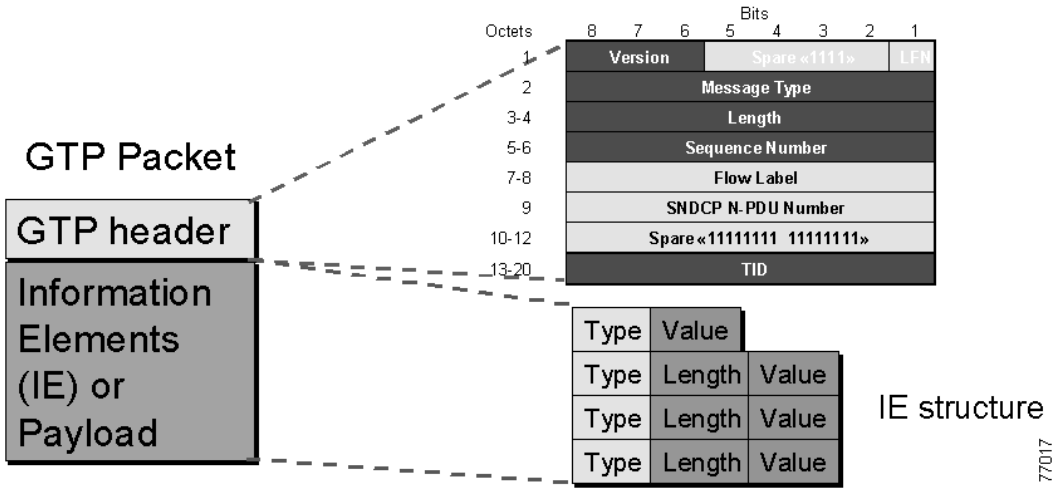
The GTP tunneling protocol is a Layer 3 tunneling protocol. The IP header identifies a session flow between the GGSN and SGSN. The UDP header identifies the GTP application protocol (Port 3386). The GTP header identifies the GTP tunnel session. The payload identifies the session flow between the mobile station and the remote host. See Figure 2-8.

Figure 2-8 GPRS Tunneling Protocol



The GTP packet structure, like any other packet, typically has a fixed-size header and other information called payload or information elements. Currently, bits 1-5 of Octet 1 and Octets 7-12 are not in use. TID is the tunnel ID that identifies a tunnel session. The length field of GTP is different from the length field of IP. In IP, the length includes the header; in GTP, length indicates only the GTP payload. See Figure 2-9.

Figure 2-9 GTP Packet Structure



GPRS Access Modes

The GPRS access modes specify whether or not the GGSN requests user authentication at the access point to a PDN (Public Data Network). The available options are:

- Transparent—No security authorization/authentication is requested by the GGSN
- Non-transparent—GGSN acts as a proxy for authenticating

The GPRS transparent and non-transparent modes relate only to PDP type IPv4.

Transparent Mode

Transparent access pertains to a GPRS PLMN that is not involved in subscriber access authorization and authentication. Access to PDN-related security procedures are *transparent* to GSNs.

In transparent access mode, the MS is given an address belonging to the operator or any other domain's addressing space. The address is given either at subscription as a static address or at PDP context activation as a dynamic address. The dynamic address is allocated from a Dynamic Host Configuration Protocol (DHCP) server in the GPRS network. Any user authentication is done within the GPRS network. No RADIUS authentication is performed; only IMSI-based authentication (from the subscriber identity module in the handset) is done.

Non-transparent Mode

Non-transparent access to an intranet/ISP means that the PLMN plays a role in the intranet/ISP authentication of the MS. Non-transparent access uses the Password Authentication Protocol (PAP) or Challenge Handshake Authentication Protocol (CHAP) message issued by the mobile terminal and piggy-backed in the GTP PDP context activation message. This message is used to build a RADIUS request toward the RADIUS server associated with the access point name (APN).

GPRS Access Point Name

The GPRS standards define a network identity called an access point name (APN). An APN identifies a PDN that is accessible from a GGSN node in a GPRS network (e.g., www.Cisco.com). To configure an APN, the operator configures three elements on the GSN node:

- Access point—Defines an APN and its associated access characteristics, including security (RADIUS), dynamic address allocation (DHCP), and DNS services
- Access point list—Defines a logical interface that is associated with the virtual template
- Access group—Defines whether access is permitted between the PDN and the MS

The Cisco GGSN is based on the routing technology, Cisco IOS. It integrates GPRS with already deployed IP services, like virtual private data networks (VPDNs) and voice over IP (VoIP).

The mobile VPN application is the first service targetted for business subscribers that mobile operators are offering when launching GPRS networks. In GPRS, the selection of the VPN can be based on the same parameters that are used in VPDN applications:

- Dialed number identification service (DNIS), i.e., the called number
- Domain, e.g., user@domain
- Mobile station IDSN (MSISDN) number, i.e, the calling number

In GPRS, only the APN is used to select the target network.The Cisco GGSN supports VPN selection based on the APN.

GPRS Processes

This section describes the following basic processes used in GPRS networks:

- Attach process—Process by which the MS *attaches* (i.e, connects) to the SGSN in a GPRS network
- Authentication process—Process by which the SGSN authenticates the mobile subscriber
- PDP activation process—Process by which a user session is established between the MS and the destination network
- Detach process—Process by which the MS *detaches* (i.e., disconnects) from the SGSN in the GPRS network
- Network-initiated PDP request for static IP address—Process by which a call from the packet data network reaches the MS using a static IP address
- Network-initiated PDP request for dynamic IP address—Process by which a call from the packet data network reaches the MS using a dynamic IP address

GPRS Attach Process

When a mobile subscriber turns on their handset, the following actions occur:

1. A handset attach request is sent to the new SGSN.
2. The new SGSN queries the old SGSN for the identity of this handset. The old SGSN responds with the identity of the handset.
3. The new SGSN requests more information from the MS. This information is used to authenticate the MS to the new SGSN.
4. The authentication process continues to the HLR. The HLR acts like a RADIUS server using a handset-level authentication based on IMSI and similar to the CHAP authentication process in PPP.
5. A check of the equipment ID with the EIR is initiated.
6. If the equipment ID is valid, the new SGSN sends a location update to the HLR indicating the change of location to a new SGSN. The HLR notifies the old SGSN to cancel the location process for this MS. The HLR sends an insert subscriber data request and other information associated with this mobile system and notifies the new SGSN that the update location has been performed.
7. The new SGSN initiates a location update request to the VLR. The VLR acts like a proxy RADIUS that queries the home HLR.
8. The new SGSN sends the Attach Accept message to the MS.
9. The MS sends the Attach Complete message to the new SGSN.
10. The new SGSN notifies the new VLR that the relocation process is complete.

Figure 2-10 and Figure 2-11 show the GPRS attach process (the numbers in the figures correspond to the numbered steps above).

Figure 2-10 GPRS Attach Request Procedure

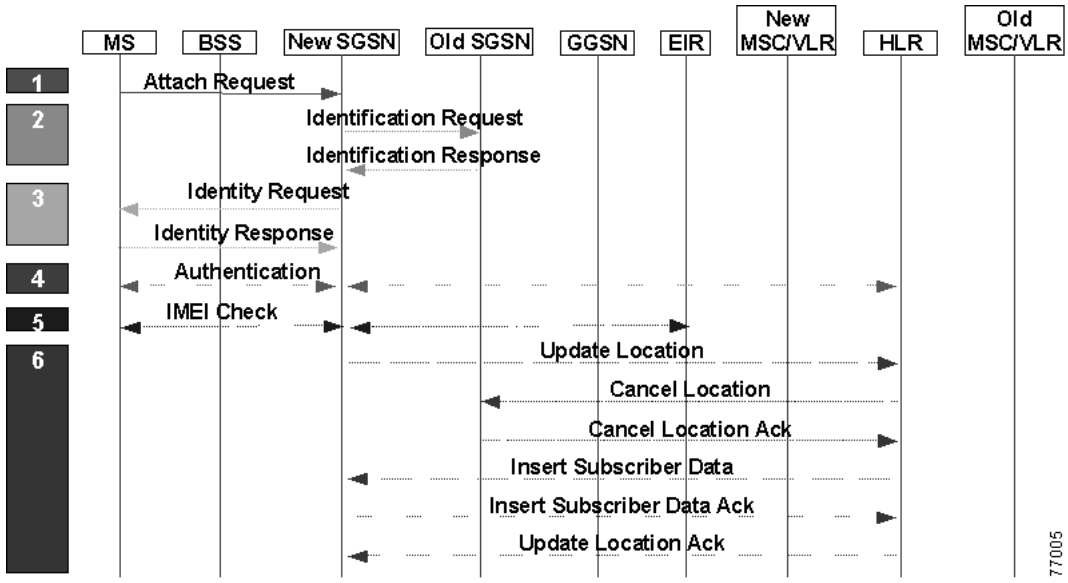
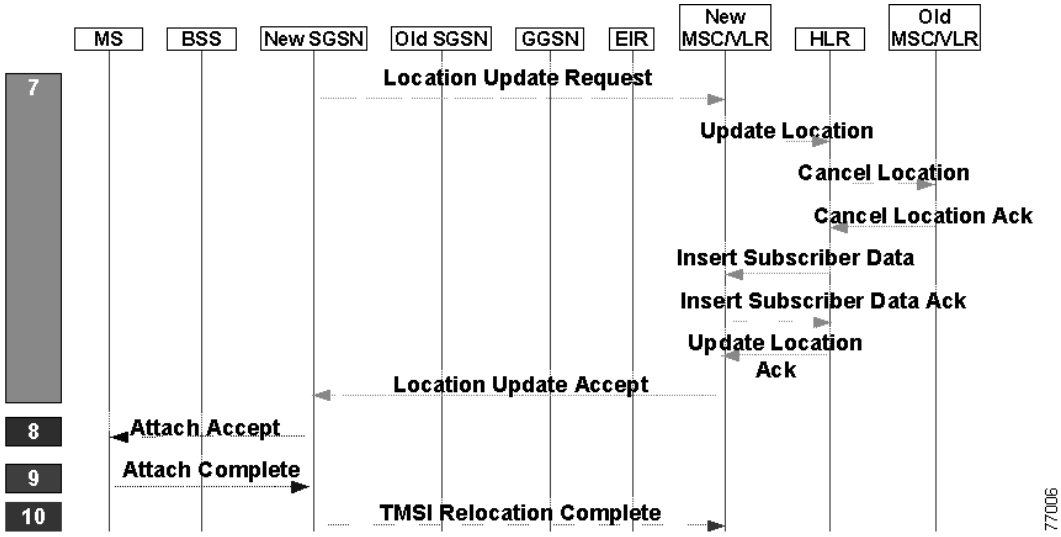


Figure 2-11 GPRS Attach Request Procedure (continued)



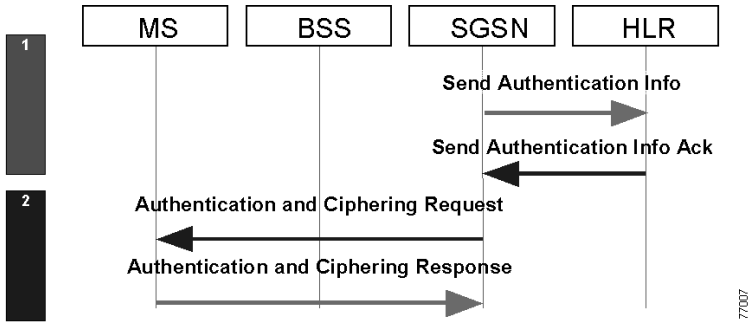
GPRS Authentication Process

The GPRS authentication process is very similar to the CHAP with a RADIUS server. The authentication process follows these steps:

1. The SGSN sends the authentication information to the HLR. The HLR sends information back to the SGSN based on the user profile that was part of the user's initial setup.
2. The SGSN sends a request for authentication and ciphering (using a random key to encrypt information) to the MS. The MS uses an algorithm to send the user ID and password to the SGSN. Simultaneously, the SGSN uses the same algorithm and compares the result. If a match occurs, the SGSN authenticates the user.

Figure 2-12 describes the GRPS authentication process that the MS uses to gain access to the network (the numbers in the figure correspond to the numbered steps above).

Figure 2-12 GPRS Authentication Procedure



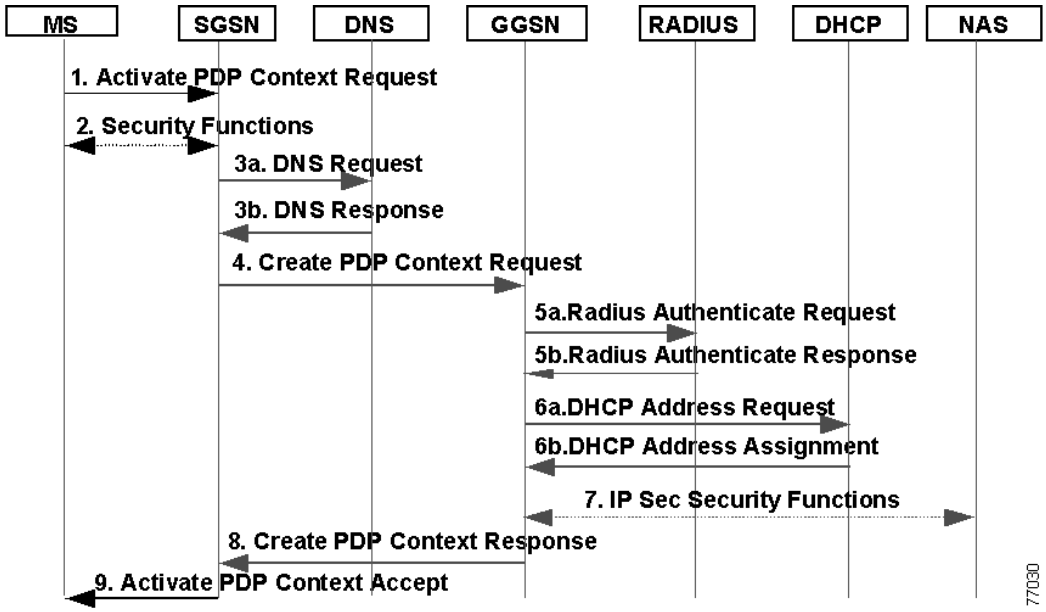
PDP Context Activation Process

The events in the PDP context activation process are described next.

1. The SGSN receives the activation request from the MS; for example, the MS requests access to the APN *Cisco.com*.
2. Security functions between the MS and SGSN occur.
3. The SGSN initiates a DNS query to learn which GGSN node has access to the *Cisco.com* APN. The DNS query is sent to the DNS server within the mobile operator's network. The DNS is configured to map to one or more GGSN nodes. Based on the APN, the mapped GGSN can access the requested network.
4. The SGSN sends a Create PDP Context Request to the GGSN. This message contains the PAP information, CHAP information, PDP request, APN, and quality of service information.
5. If operating in the non-transparent mode, the PAP and CHAP information in the PDP request packet is sent to the RADIUS server for authentication.
6. If the RADIUS server is to provide a dynamic IP address to the client, it sends a DHCP address request to the DHCP server. In transparent mode, the RADIUS server is bypassed.
7. If IPSec functionality is required, security functions occur between the GGSN and network access server (NAS).
8. The GGSN sends a Create a PDP Context Response message to the SGSN.
9. The SGSN sends an Activate PDP Context Accept message to the MS.

Figure 2-13 shows the PDP context activation procedure. The red arrows indicate the communication between the SGSN and GGSN. The numbers in the figure correspond to the numbered steps above.

Figure 2-13 PDP Context Activation Procedure



Detach Process Initiated by MS

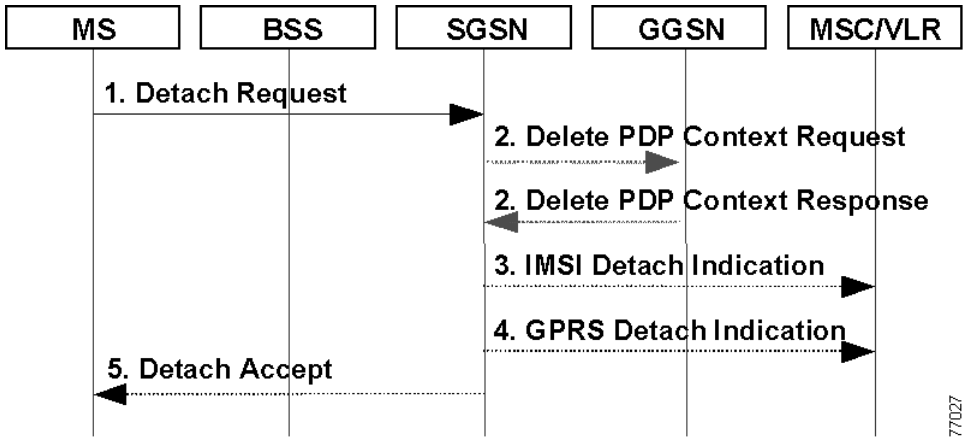
When a mobile subscriber turns off their handset, the detach process initiates. The detach process is described below.

1. The MS sends a Detach Request to the SGSN.
2. The SGSN sends a Delete PDP Context Request message to the serving GGSN.
3. The SGSN sends an IMSI Detach Indication message to the MSC/VLR indicating the MS request to disconnect.
4. The SGSN sends a GPRS Detach Indication message to the MSC/VLR.
5. The SGSN sends the Detach Accept message to the MS.

Note The GSN nodes must always respond to the detach request with a positive delete response to the MS and accept the detach request requested by the client. The positive delete response is required even if the SGSN does not have a connection pending for that client.

Figure 2-14 describes the detach process initiated by the MS. The numbers in the figure correspond to the numbered steps above.

Figure 2-14 MS Initiate Detach Procedure



Network Initiated PDP Request For A Static IP Address

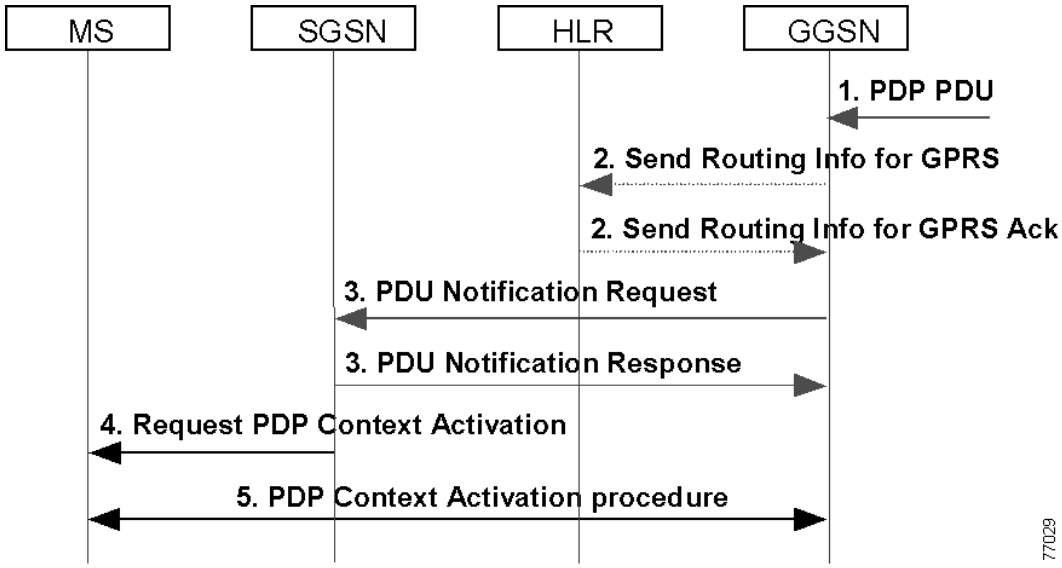
The PDP protocol data unit (PDU) initiated from the network side is not fully specified by ETSI standards. A connection request generated from the Internet/intranet site specifies only the IP address of the client in the IP packets destined for the MS. The requesting host provides no indication of the mobile device IMSI (i.e., the MAC address of the MS). In mobile communications, all communications are based on the MS MAC address called the IMSI. The IP address must be mapped to an IMSI to identify a valid GTP tunnel. Cisco's GGSN implementation provides a mapping table via command line interface (CLI) that allows the operator to key in the MS IMSI and the associated static IP address.

The following steps describe a PDP request initiated from the network side when the client has been assigned a static IP address.

1. When the GGSN receives a packet, it checks its mapping table for an established GTP tunnel for this packet.
2. When the GGSN locates the IMSI associated with this IP address, it sends a Send Routing Information message to HLR through an intermediate SGSN. The intermediate SGSN notifies the GGSN of the actual SGSN currently serving this client.
3. On locating the appropriate SGSN, the GGSN sends a PDU Notification Request message to the serving SGSN.
4. The SGSN sends a Request PDP Context Activation message to the MS and notifies it of the pending connection request.
5. If the MS agrees to accept the call, it enters the PDP Context Activation procedure with the requesting GGSN.

Figure 2-15 shows a PDP request initiated from the network side when the client has been assigned a static IP address. The numbers in the figure correspond to the numbered steps above.

Figure 2-15 Network Initiate PDP (Static IP Address)



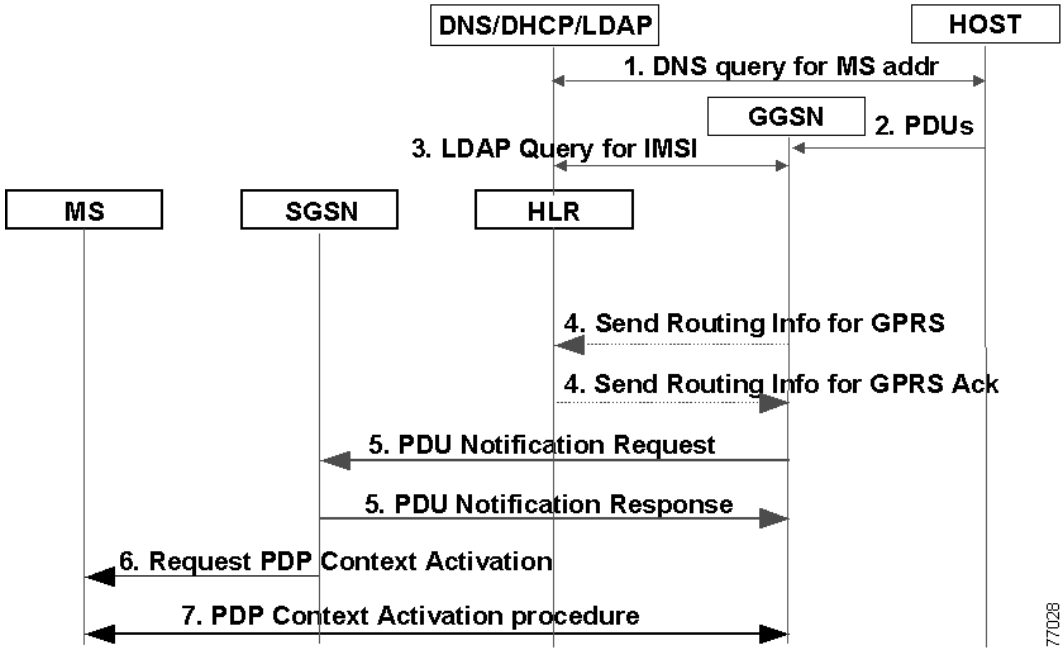
Network Initiated PDP Request For A Dynamic IP Address

The ETSI standards do not fully specify requirements for a network-generated PDP request when the client is dynamically assigned a temporary IP by a DHCP server. The following message sequence is Cisco's implementation for this scenario. This method uses Cisco's Network Registrar (CNR), which includes a DHCP, DNS, and an LDAP server.

1. The host initiates a DNS query to obtain the IP address of the MS from a DNS server. The DNS server resolves the client's name to an IP address previously assigned to the client by the DHCP server.
2. The host sends a request to the GGSN for a connection using this IP address.
3. The GGSN queries the LDAP server to obtain the MS IMSI. The LDAP server stores a record for the MS with the client IMSI, name, and IP address.
4. The GGSN sends a PDU Notification Request message to the serving SGSN.
5. The SGSN sends a Request PDP Context Activation message to the MS and notifies it of the pending connection request.
6. If the MS agrees to accept the call, it enters the PDP Context Activation procedure with the requesting GGSN.

Figure 2-16 describes a PDP request initiated from the network side when the client has been assigned a dynamic IP address. The numbers in the figure correspond to the numbered steps above.

Figure 2-16 Network Initiate PDP (Dynamic IP Address)



Universal Mobile Telecommunication System

The Universal Mobile Telecommunication System (UMTS) is a third generation (3G) mobile communications system that provides a range of broadband services to the world of wireless and mobile communications. The UMTS delivers low-cost, mobile communications at data rates of up to 2 Mbps. It preserves the global roaming capability of second generation GSM/GPRS networks and provides new enhanced capabilities. The UMTS is designed to deliver pictures, graphics, video communications, and other multimedia information, as well as voice and data, to mobile wireless subscribers.

The UMTS takes a phased approach toward an all-IP network by extending second generation (2G) GSM/GPRS networks and using Wide-band Code Division Multiple Access (CDMA) technology. Handover capability between the UMTS and GSM is supported. The GPRS is the convergence point between the 2G technologies and the packet-switched domain of the 3G UMTS.

UMTS Services

The UMTS provides support for both voice and data services. The following data rates are targets for UMTS:

- 144 kbps—Satellite and rural outdoor
- 384 kbps—Urban outdoor
- 2048 kbp—Indoor and low range outdoor

Data services provide different quality-of-service (QoS) parameters for data transfer. UMTS network services accommodate QoS classes for four types of traffic:

- Conversational class—Voice, video telephony, video gaming
- Streaming class—Multimedia, video on demand, webcast
- Interactive class—Web browsing, network gaming, database access
- Background class—E-mail, short message service (SMS), file downloading

The UMTS supports the following service categories and applications:

- Internet access—Messaging, video/music download, voice/video over IP, mobile commerce (e.g., banking, trading), travel and information services
- Intranet/extranet access—Enterprise application such as e-mail/messaging, travel assistance, mobile sales, technical services, corporate database access, fleet/warehouse management, conferencing and video telephony
- Customized information/entertainment—Information (photo/video/music download), travel assistance, distance education, mobile messaging, gaming, voice portal services
- Multimedia messaging—SMS extensions for images, video, and music; unified messaging; document transfer
- Location-based services—Yellow pages, mobile commerce, navigational service, trading

UMTS Architecture

The public land mobile network (PLMN) described in UMTS Rel. '99 incorporates three major categories of network elements:

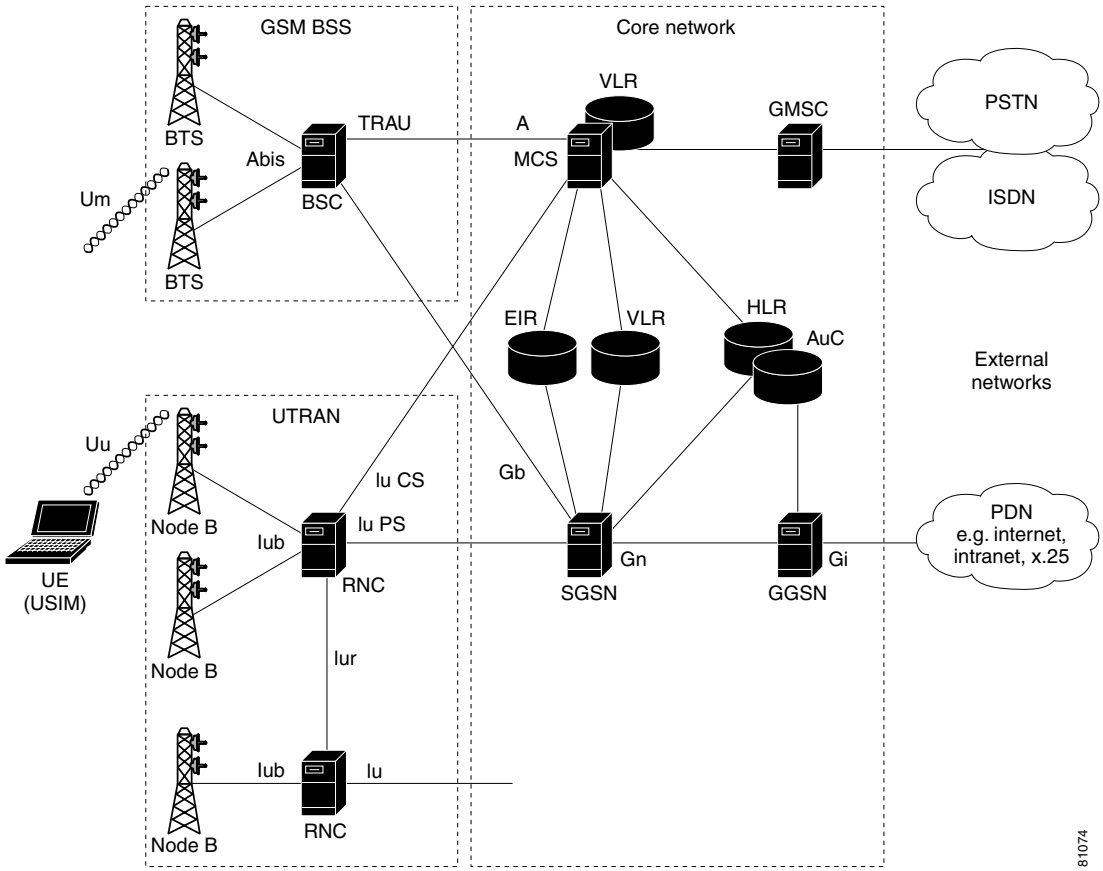
- GSM phase 1/2 core network elements—Mobile services switching center (MSC), visitor location register (VLR), home location register (HLR), authentication center (AuC), and equipment identity register (EIR)
- GPRS network elements—Serving GPRS support node (SGSN) and gateway GPRS support node (GGSN)
- UMTS-specific network elements—User equipment (UE) and UMTS terrestrial radio access network (UTRAN) elements

The UMTS core network is based on the GSM/GPRS network topology. It provides the switching, routing, transport, and database functions for user traffic. The core network contains circuit-switched elements such as the MSC, VLR, and gateway MSC (GMSC). It also contains the packet-switched elements SGSN and GGSN. The EIR, HLR, and AuC support both circuit- and packet-switched data.

The Asynchronous Transfer Mode (ATM) is the data transmission method used within the UMTS core network. ATM Adaptation Layer type 2 (AAL2) handles circuit-switched connections. Packet connection protocol AAL5 is used for data delivery.

The UMTS architecture is shown in Figure 2-17.

Figure 2-17 UMTS Architecture



General Packet Radio System

The General Packet Radio System (GPRS) facilitates the transition from phase1/2 GSM networks to 3G UMTS networks. The GPRS supplements GSM networks by enabling packet switching and allowing direct access to external packet data networks (PDNs). Data transmission rates above the 64 kbps limit of integrated services digital network (ISDN) are a requirement for the enhanced services supported by UMTS networks. The GPRS optimizes the core network for the transition to higher data rates. Therefore, the GPRS is a prerequisite for the introduction of the UMTS.

UMTS Interfaces

The UMTS defines four new open interfaces (see Figure 2-17):

- *Uu* interface—User equipment to Node B (the UMTS WCDMA air interface)
- *Iu* interface—RNC to GSM/GPRS (MSC/VLR or SGSN)
  - *Iu-CS*—Interface for circuit-switched data
  - *Iu-PS*—Interface for packet-switched data
- *Iub* interface—RNC to Node B interface
- *Iur* interface—RNC to RNC interface (no equivalent in GSM)

The *Iu*, *Iub*, and *Iur* interfaces are based on the transmission principles of aynchronous transfer mode (ATM).

UMTS Terrestrial Radio Access Network

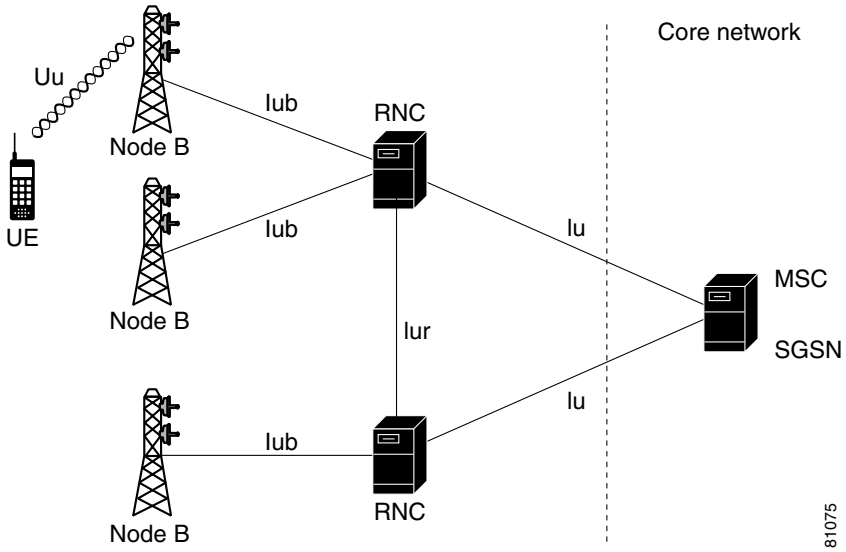
The major difference between GSM/GPRS networks and UMTS networks is in the air interface transmission. Time division multiple access (TDMA) and freqency division multiple access (FDMA) are used in GSM/GPRS networks. The air interface access method for UMTS networks is wide-band code division multiple access (WCDMA), which has two basic modes of operation: frequency division duplex (FDD) and time division duplex (TDD). This new air interface access method requires a new radio access network (RAN) called the UTMS terrestrial RAN (UTRAN). The core network requires minor modifications to accommodate the UTRAN.

Two new network elements are introduced in the UTRAN: the radio network controller (RNC) and Node B. The UTRAN contains multiple radio network systems (RNSs), and each RNS is controlled by an RNC. The RNC connects to one or more Node B elements. Each Node B can provide service to multiple cells.

The RNC in UMTS networks provides functions equivalent to the base station controller (BSC) functions in GSM/GPRS networks. Node B in UMTS networks is equivalent to the base transceiver station (BTS) in GSM/GPRS networks. In this way, the UMTS extends existing GSM and GPRS networks, protecting the investment of mobile wireless operators. It enables new services over existing interfaces such as *A*, *Gb*, and *Abis*, and new interfaces that include the UTRAN interface between Node B and the RNC (*Iub*) and the UTRAN interface between two RNCs (*Iur*).

The network elements of the UTRAN are shown in Figure 2-18.

Figure 2-18 UTRAN Architecture



Radio Network Controller

The radio network controller (RNC) performs functions that are equivalent to the base station controller (BSC) functions in GSM/GPRS networks. The RNC provides centralized control of the Node B elements in its covering area. It handles protocol exchanges between UTRAN interfaces (*Iu*, *Iur*, and *Iub*). Because the interfaces are ATM-based, the RNC performs switching of ATM cells between the interfaces. Circuit-switched and packet-switched data from the *Iu-CS* and *Iu-PS* interfaces are multiplexed together for transmission over the Iur, Iub, and Uu interfaces to and from the user equipment (UE). The RNC provides centralized operation and maintenance of the radio network system (RNS) including access to an operations support system (OSS).

The RNC uses the *Iur* interface. There is no equivalent to manage radio resources in GSM/GPRS networks. In GSM/GPRS networks, radio resource management is performed in the core network. In UMTS networks, this function is distributed to the RNC, freeing the core network for other functions. A single serving RNC manages serving control functions such as connection to the UE, congestion control, and handover procedures. The functions of the RNC include:

- Radio resource control
- Admission control
- Channel allocation
- Power control settings
- Handover control
- Macro diversity
- Ciphering
- Segmentation and reassembly
- Broadcast signalling
- Open loop power control

Node B

Node B is the radio transmission/reception unit for communication between radio cells. Each Node B unit can provide service for one or more cells. A Node B unit can be physically located with an existing GSM base transceiver station (BTS) to reduce costs of UMTS implementation. Node B connects to the user equipment (UE) over the *Uu* radio interface using wide-band code division multiple access (WCDMA). A single Node B unit can support both frequency division duplex (FDD) and time division duplex (TDD) modes. The *Iub* interface provides the connection between Node B and the RNC using asynchronous transfer mode (ATM). Node B is the ATM termination point.

The main function of Node B is conversion of data on the *Uu* radio interface. This function includes error correction and rate adaptation on the air interface. Node B monitors the quality and strength of the connection and calculates the frame error rate, transmitting this information to the RNC for processing. The functions of Node B include:

- Air interface transmission and reception
- Modulation and demodulation
- CDMA physical channel coding
- Micro diversity
- Error handling
- Closed loop power control

Node B also enables the UE to adjust its power using a technique called downlink transmission power control. Predefined values for power control are derived from RNC power control parameters.

UMTS User Equipment

The UMTS user equipment (UE) is the combination of the subscriber's mobile equipment and the UMTS subscriber identity module (USIM). Similar to the SIM in GSM/GPRS networks, the USIM is a card that inserts into the mobile equipment and identifies the subscriber to the core network.

The USIM card has the same physical characteristics as the GSM/GPRS SIM card and provides the following functions:

- Supports multiple user profiles on the USIM
- Updates USIM information over the air
- Provides security functions
- Provides user authentication
- Supports inclusion of payment methods
- Supports secure downloading of new applications

The UMTS standard places no restrictions on the functions that the UE can provide. Many of the identity types for UE devices are taken directly from GSM specifications. These identity types include:

- International Mobile Subscriber Identity (IMSI)
- Temporary Mobile Subscriber Identity (TMSI)
- Packet Temporary Mobile Subscriber Identity (P-TMSI)
- Temporary Logical Link Identity (TLLI)
- Mobile station ISDN (MSISDN)
- International Mobile Station Equipment Identity (IMEI)

- International Mobile Station Equipment Identity and Software Number (IMEISV)

The UMTS UE can operate in one of three modes of operation:

- PS/CS mode—The UE is attached to both the packet-switched (PS) and circuit-switched (CS) domain, and the UE can simultaneously use PS and CS services.
- PS mode—The MS is attached to the PS domain and uses only PS services (but allows CS-like services such as voice over IP [VoIP]).
- CS mode—The MS is attached to the CS domain and uses only CS services.

CHAPTER 3

Description of Cisco Mobile Exchange

This chapter provides a detailed description of the Cisco Mobile Exchange (CMX) framework and contains the following sections:

CMX Network Elements

Cisco's CMX solution for mobile wireless networks combines multiple network elements into a single solution framework. As shown in Figure 3-1, the core of the CMX solution framework is the Cisco 7600 series switch/router. Descriptions of the CMX network elements shown in Figure 3-1 are listed in Table 3-1.

Figure 3-1 CMX Functional Components Overview

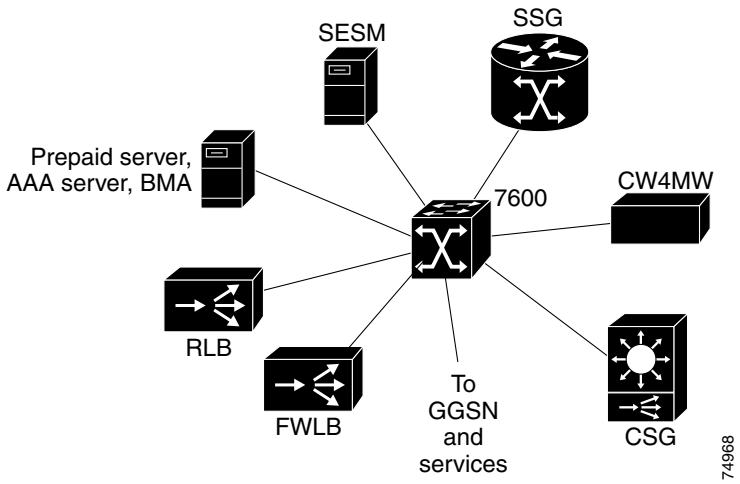


Table 3-1 CMX Network Elements

CMX Element	Description
Switch/Router (7600)	• Provides Layer 2 connectivity within CMX • Provides external interfaces from/to CMX • Performs Layer 2 switching • Performs Layer 3 routing
Service Selection Gateway (SSG)	• Acts as a RADIUS proxy and captures the authentication parameters to offer single sign-on and automatically authenticate the user through SSG • Performs TCP redirect to a captive portal • Allows multiple service selection • Performs domain naming service (DNS) redirection • Performs network address translation (NAT) • Allows connecting to multiple networks using one Protocol Data Packet (PDP) context and one access point name (APN) • Performs charging by generating RADIUS accounting records for postpaid and prepaid billing • Allows point-to-point (PPP) regeneration and Layer 2 Tunneling Protocol (L2TP) tunneling
Service Gateway Load Balancer (SGLB)	• RADIUS Load Balancer (RLB): – Load-balances RADIUS messages among multiple SSGs on subscriber side and among multiple AAA servers on network side – Load-balances user traffic among multiple SSGs • Firewall Load Balancer (FWLB): – Directs user traffic from services network to the SSGs
Content Services Gateway (CSG)	• Collects IP statistics • Generates content-based call detail records (CDRs) to a charging gateway (CG) or billing mediation agent (BMA)

Table 3-1 CMX Network Elements

CMX Element	Description
Authentication, Authorization, and Accounting (AAA) server (Cisco Access Registrar or equivalent third-party AAA server)	• Authenticates and authorizes users • Contains user service profiles for downloading to SSGs • Can allocate IP address for MS • Collects accounting records from SSGs and GGSNs • Provides front end to Prepaid Server
Prepaid server	• Provides interface to SSGs using RADIUS • Stores user prepaid balances
Billing Mediation Agent (BMA)	• Collects content-based CDRs from the CSG
Subscriber Edge Services Manager (SESM)	• Provides session authentication (via AAA server) • Provides service subscription • Provides service selection (by controlling the SSG) • Supports captive portal Web application (provided by IBM) for sessions and services
Remote Console Access (not shown in Figure 3-1)	• Provides remote access to the CMX elements
CiscoWorks for Mobile Wireless (CW4MW)	• Provides device-level management

Table 3-2 lists the CMX hardware and software components required for CMX.

Table 3-2 CMX Hardware/Software Configuration

Network Element	Platform	Software
SSG	7401-BB	IOS 12.2(8)B
RLB	7609 (MSFC)	IOS 12.1(12c)E1
FWLB	7609 (MSFC)	IOS 12.1(12c)E1
AAA server	Sun	Cisco Access Registrar or equivalent
Prepaid server	Sun	Partner (MIND CTI)
BMA	PC	Partner (MIND CTI)
SESM	Sun	SESM 3.1(3)
CW4MW	PC	CW4MW 3.0
Remote Control Access	2611	IOS 12.2T
CSG	7609	CSG 2.2(3)C2(1)/IOS 12.1(12c)E1

Note Cisco partner can provide AAA server, prepaid server, or BMA components.

Supported Features

This section describes the supported features for Cisco Mobile Exchange components.

Service Selection Gateway Features

The CMX features supported for SSG are listed in Table 3-3.

Table 3-3 SSG Supported Features

Feature	Description
SSG functions	Support for service selection and service control for GPRS users
SSG proxy service	SSG acts as a RADIUS proxy for the GGSN to authenticate user and retrieve user profile
SSG pass-through service	SSG support for pass-through service
SSG TCP redirect	SSG redirects unauthenticated users to a captive portal (SESM or other)
SSG tunnel service	SSG support for L2TP service
SSG open garden	SSG access to open garden service (no authentication required)
AAA interface	Interface to AAA server
User/password authentication	AAA support for authentication based on user name and password
Mobile station ISDN (MSISDN) authentication	AAA support for MSISDN-based authentication
Network address translation (NAT) function	Support for NAT
Three-key authentication	Support for authentication based on user name, password, and MSISDN.

Subscriber Edge Services Module Features

The CMX supports interworking between the SESM and the Web portal provider. The Web portal uses the application programming interface (API) provided by the SESM to interact with the SSGs and the AAA server.

The SESM and AAA server use the RADIUS protocol and vendor-specific attributes (VSAs) to interwork. Each of these VSAs requires the SESM to know the target SSG IP address.

High Availability Features

The CMX supports the high availability features listed in Table 3-4.

Table 3-4 High Availability Features

Feature	Description
Load balancing for SSGs	SSG load balancing provided on the access path (uplink) and subscriber traffic path (downlink). On SSG failure, incoming user sessions are redirected to available SSGs.
Redundant physical interfaces	CMX network elements support redundant physical interfaces.
Redundant load balancing functions	Load balancing functions are redundant and support a failover mechanism if load balancing fails
No single point of failure	CMX provides no single point of failure
Collection of IP statistics for backup of billing information	CSG supports backup of billing information if SSG fails
Redundant connectivity to AAA	CMX supports redundant connectivity to AAA server
Redundant connectivity to BMA	CMX supports redundant connectivity to BMA
Redundant connectivity to GGSN	CMX supports redundant connectivity to BMA

Billing Features

The CMX supports the billing features listed in Table 3-5.

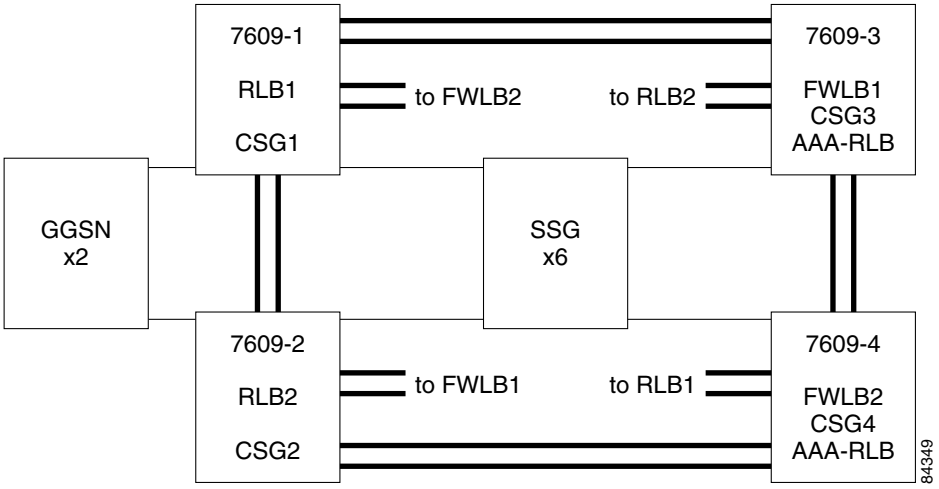
Table 3-5 Billing Features

Feature	Description
Postpaid billing	SSG generates charging records to BMA
Prepaid billing	SSG interworks with third-party prepaid billing server
Content billing	CSG provides call detail records (CDRs) based on HTTP and URLs
Hot billing	SSG and CSG generate charging records in real time to third-party billing server
Network Time Protocol (NTP) support	NTP maintains timing between all CMX entities to ensure accurate time stamps on billing records

Physical and Logical Interfaces

The CMX network elements are connected using Ethernet segments. Each element of the solution uses one or two physical fast Ethernet (FE) interfaces as shown in Figure 3-2. The interfaces run network time protocol (NTP) to maintain timing between the network elements.

Figure 3-2 CMX Physical Interfaces



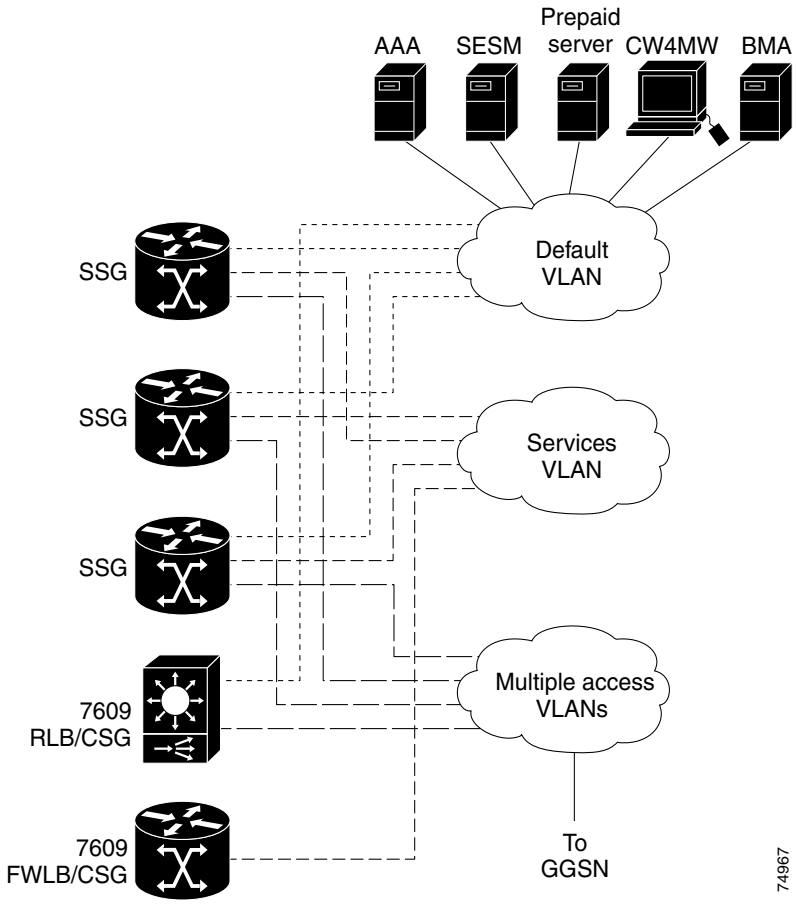
To increase efficiency and redundancy, the CMX also uses logical Ethernet interfaces. Logical Ethernet interfaces are created by configuring virtual local area networks (VLAN)s. With VLAN configuration, each physical Ethernet interface is separated into 802.1q VLAN interfaces using the 802.1q encapsulation provided by the Cisco IOS.

The CMX interconnections are organized into multiple VLANs that cover three major areas:

- Access VLANs—Multiple VLANs that interconnect the SSGs, RLB, CSG, and GGSN; pass user and RADIUS traffic between the GGSN and the SSGs; and allow the CSG to monitor user traffic and generate content-based call detail records (CDRs)
- Services VLAN—Interconnects the SSGs and FWLB for connection to the external packet data network (PDN); passes user traffic between the SSGs and services available on the PDN
- Default VLAN—Interconnects the SSGs, RLB, and CSG with the AAA server, SESM, prepaid server, CW4MW, and billing mediation agent (BMA)

The CMX VLAN organization is illustrated in Figure 3-3.

Figure 3-3 CMX VLAN Organization



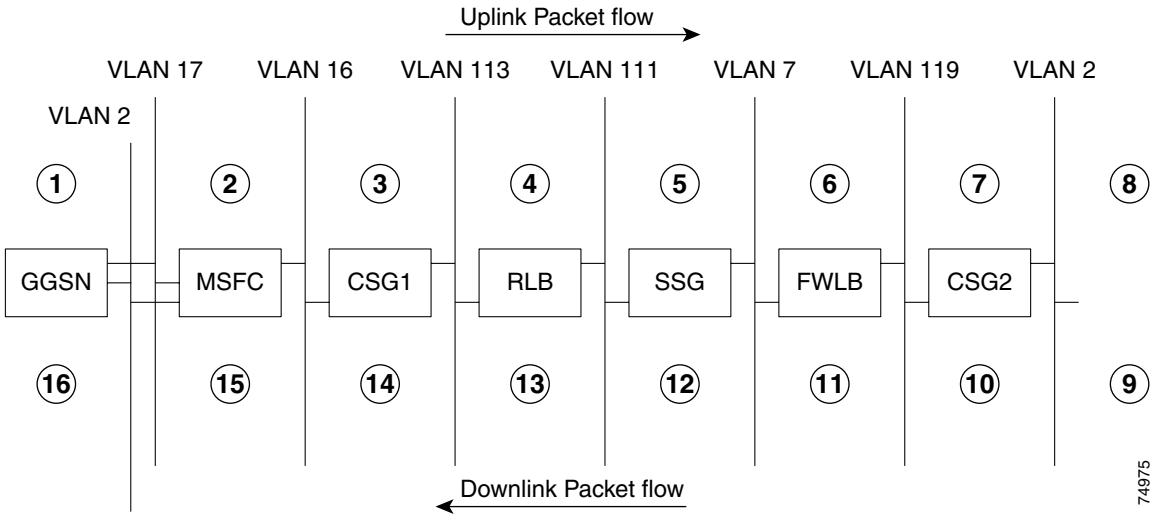
Data Traffic Flows

A basic understanding of how data traffic flows through the CMX network elements and interconnecting VLANs is beneficial to personnel who are responsible for configuring and maintaining the CMX network elements. The following sequence of events is also illustrated in Figure 3-4 (the numbers in Figure 3-4 correspond to steps below).

Note The following sequence of events describes only data traffic flows. Traffic flows for RADIUS messages are described in "Detailed RADIUS Interactions" section on page 3-19.

1. The GGSN sends user IP packets to a Multilayer Switch Feature Card (MSFC) in the RLB platform using the open shortest path first (OSPF) algorithm.
2. The MSFC uses policy routing to send the user packet to CSG1.
3. CSG1 directs all traffic on VLAN 17 to the RLB and creates accounting records for the user traffic.
4. RADIUS server load balancing (SLB) software directs the user traffic to the correct SSG.
5. The SSG performs service control and selection by sending the user packets to the selected service. The SSG can also generate RADIUS accounting records and send RADIUS authorization to the prepaid server (via the AAA server) for prepaid sessions.
6. The next hop for all service-bound packets from the SSG is the FWLB. The FWLB registers the downlink path with the correct SSG for downlink IP traffic flow.
7. The next hop is CSG2, which generates billing records for content-based billing. Encrypted AAA or tunneled traffic passes through this CSG unaltered.
8. CSG2 routes the user traffic to a next-hop router or border gateway toward the services network.
9. The downstream user traffic is received on CSG2.
10. The CSG2 generates billing records for content-based billing and sends the user packets to the FWLB.
11. The FWLB forwards the user packet to the same SSG that was used for the uplink traffic flow.
12. The SSG routes the user traffic toward the MSFC in the RLB (downstream traffic is transparent to the RLB).
13. The RLB uses policy routing to send the user traffic to CSG1.
14. CSG1 creates accounting records for the user traffic and generates content-based CDRs to send to the BMA. The user traffic is sent to the MSFC.
15. The MSFC uses the OSPF algorithm to route the user packet to the correct GGSN.
16. The GGSN receives the user packet and encapsulates it in a tunnel (using GTP) toward the mobile station.

Figure 3-4 Example of Data Traffic Flow in CMX

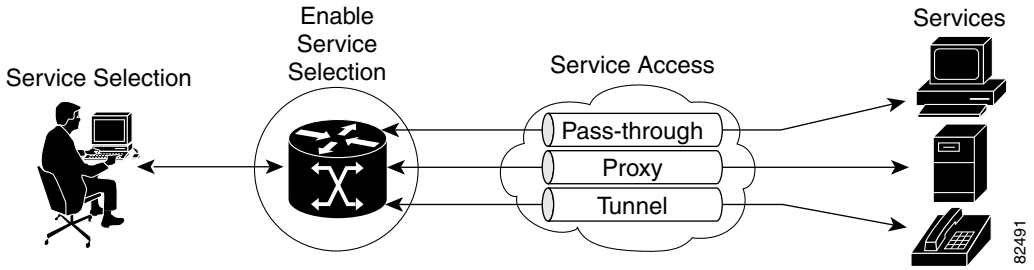


Supported Services

The CMX solution for mobile wireless networks supports the following services (Figure 3-5):

- Pass-through service—Passes subscriber through the service provider's network to the external packet data network (PDN); typically used to provide Internet access
- Proxy service—Performs AAA and support network address translation (NAT); typically used when authentication is required
- Tunnel service—Provides Layer 2 Tunneling Protocol (L2TP) via a Web portal to support virtual private networking (VPN) and other tunneling applications

Figure 3-5 CMX Supported Services



Pass-through Service

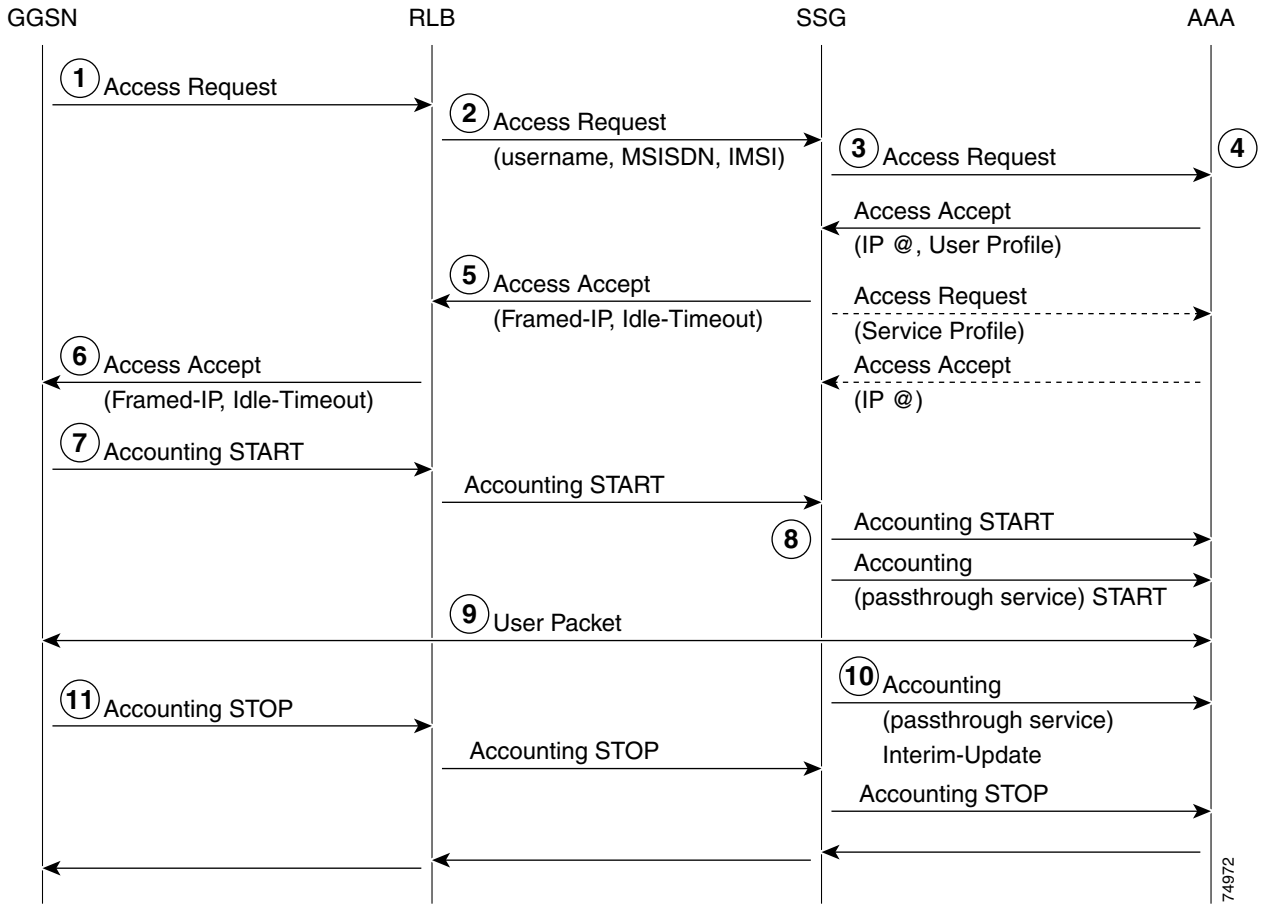
Pass-through service is typically used to provide standard Internet access to mobile wireless subscribers. This type of service allows subscribers to *pass through* the service provider's network to access the external PDN. Pass-through service can be configured to authenticate subscribers automatically based on a profile or to provide transparent (unauthenticated) service.

The events that occur to activate authenticated pass-through service are described in the steps below (steps also shown in Figure 3-6).

1. The GGSN sends an access request to the RADIUS Load Balancer (RLB) with the username, MSISDN, and IMSI of the subscriber.
2. The RLB receives the access request, selects an SSG, and forwards the request to the SSG.
3. The SSG receives the request and forwards it to the AAA server.
4. The AAA server authenticates the user and allocates an IP address for the user session. The AAA server sends the IP address and a user profile to the SSG.
5. The SSG forwards this information to the RLB, creates a host object for the user session, and queries the AAA server for the service profile to enable pass-through service.
6. The RLB retrieves the user IP address and sends it to the GGSN.
7. The GGSN sends the IP address to the mobile handset. It also sends a message to the RLB to start accounting records and forwards the message to the SSG.
8. The SSG generates a message to the AAA server to start accounting records.
9. The pass-through is enabled and the user session is active.
10. The SSG periodically sends interim update messages to the AAA server for accounting purposes.

11. The GGSN generates a message to stop RADIUS accounting records when the subscriber terminates access. The RLB clears the user IP address. The SSG sends out messages to each service the subscriber accessed and terminates the host object for the user session.

Figure 3-6 Pass-through Service Events



Transparent pass-through service allows unauthenticated subscriber traffic to be routed through the SSG in either direction. Filters can be specified to control transparent passthrough traffic. Some of the applications for this feature include:

- Integrating the SSG into an existing network, allowing users who have already authenticated with a network access server (e.g., GGSN) to bypass authentication with the SSG
- Allowing management traffic (e.g., RADIUS and Simple Network Management Protocol (SNMP)) from network access servers connected to the host network to pass through to the service provider network
- Allowing visitors or guests to access certain parts of the network

Proxy Service

When a subscriber requests access to a proxy service, the SSG proxies the Access-Request packet to the remote AAA server. On receiving an Access-Accept packet from the remote RADIUS server, the SSG logs the subscriber in. To the remote AAA server, the SSG appears as a client.

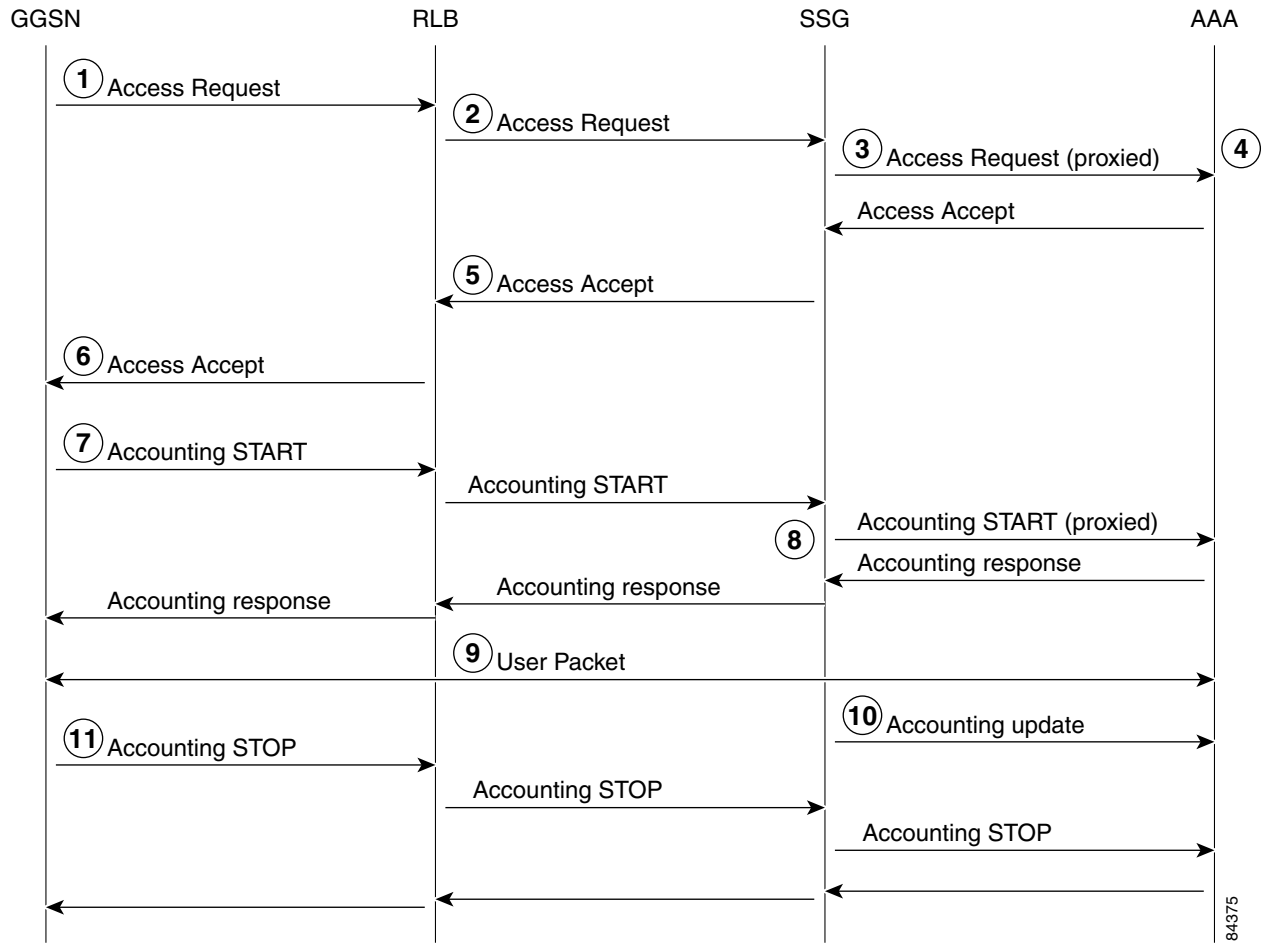
If the RADIUS server assigns an IP address to the subscriber during remote authentication, the SSG performs network address translation (NAT) between the assigned IP address and the real IP address of the subscriber. If the remote RADIUS server does not assign an IP address, NAT is not performed.

When a user selects a proxy service, there is another prompt for username and password. After authentication, the service is accessible until the user logs out from the service, logs out from the SESM, or times out.

The events that occur to enable proxy service are described in the steps below (steps also shown in Figure 3-7).

1. The GGSN sends an access request to the RADIUS Load Balancer (RLB).
2. The RLB receives the access request, selects an SSG, and forwards the request to the SSG.
3. The SSG receives the request and performs a full, transparent proxy of the request to the AAA server (to ensure propagation of all RADIUS attributes).
4. The AAA server authenticates the user and allocates an IP address for the user session. The AAA server sends the IP address and a user profile to the SSG.
5. The SSG forwards this information to the RLB and creates a host object for the user session.
6. The RLB retrieves the user IP address and sends it to the GGSN.
7. The GGSN sends the IP address to the mobile handset. It also sends a message to the RLB to start accounting records and forwards the message to the SSG.
8. The SSG proxies the message to the AAA server to start accounting records.
9. The proxy service is enabled and the user session is active.
10. The SSG periodically proxies interim update messages to the AAA server for accounting purposes.
11. The GGSN generates a message to stop RADIUS accounting records when the subscriber terminates access. The RLB clears the user IP address. The SSG sends out messages to each service the subscriber accessed and terminates the host object for the user session.

Figure 3-7 Proxy Service Events



Tunnel Service

Layer 2 Tunneling Protocol (L2TP) enables mobile wireless subscribers to access a *tunnel* to an L2TP network server (LNS) for virtual private networking (VPN) applications. The typical application for tunnel service is employee access to corporate networks from remote locations. Tunnel services are targeted to enterprises and generate high revenues for service providers.

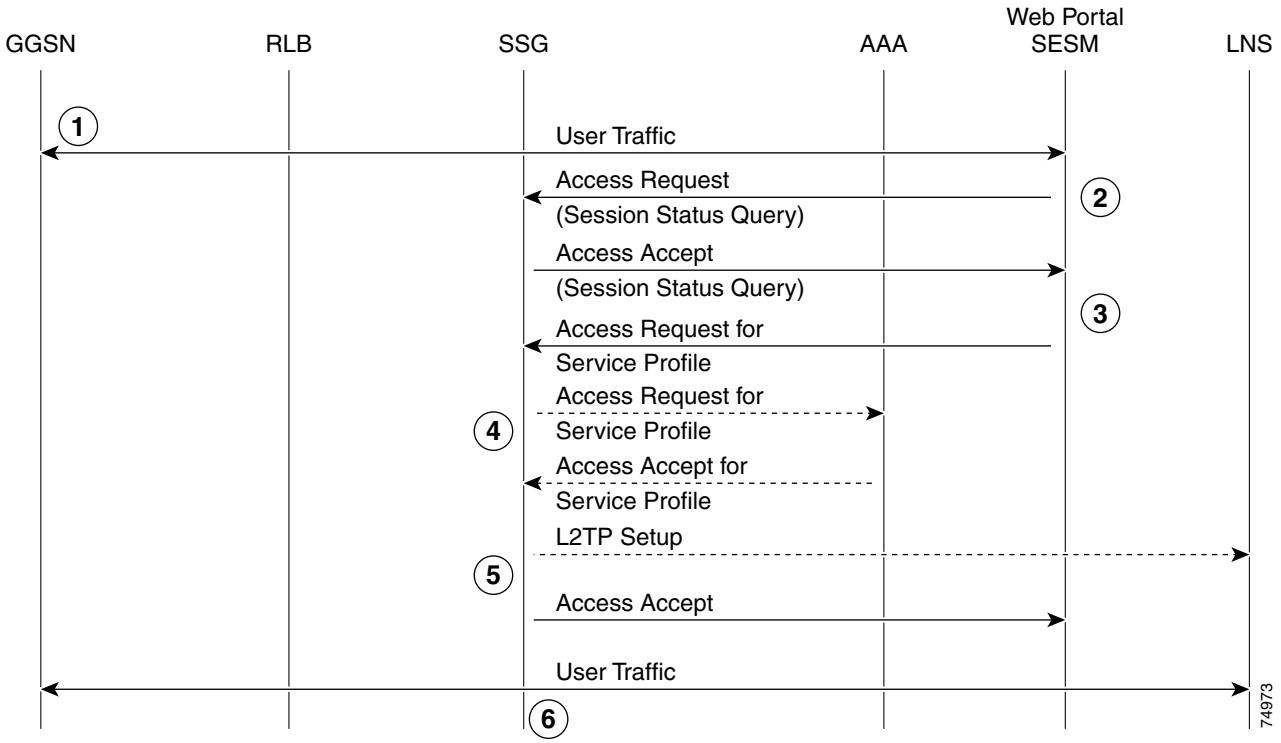
In this configuration, it is assumed that the CMX is connected to a GGSN through any IP connection.

The events that occur to enable tunnel service are described in the steps below (steps also shown in Figure 3-8).

1. The user is already connected, and a host object is created in the SSG. The user starts a user session on the provider's Web portal.
2. The Web portal (via the SESM) queries the SSG to verify that a host object exists; if no host object exists, the user is redirected (via the TCP redirect feature) to a login page.
3. The user selects the tunnel service on the Web portal; the Web portal sends an access request to the SSG to enable the creation of the tunnel service.
4. The SSG proxies the access request to the AAA server and queries the AAA server for a service profile.
5. The SSG sets up the tunnel service. The SSG can receive an IP address from the remote network server and create a network address translation (NAT) entry between the user's address domain and the address received from the network server.
6. Data traffic flows on the tunnel (see note) established between the user and the remote network server.

Note An L2TP tunnel exists between the SSG and the remote network server.

Figure 3-8 Tunnel Service Events



The Service Selection Gateway (SSG) supports the tunnel service with the following configurable features:

- Auto-logon—User is automatically authenticated and selects the tunnel service using the SESM
- TCP redirect—User is redirected to a login page (i.e., captive portal) on the SESM; when authenticated, user selects a service

Note

- **Non-transparent** access mode is used for the auto-logon feature; **transparent-mode** is used with the TCP redirect feature.
- If the GGSN supports the standard RADIUS interface (defined in GSM 09.61), the RADIUS interface is used between the GGSN and the SSG. The SSG uses the auto-logon feature to authenticate the user and select services.
- If the GGSN does not support the standard RADIUS interface, standard IP is used between the GGSN and the SSG. The subscriber uses a Web browser for authentication and selection of services. The TCP redirect feature is used in the SSG.

Auto-logon Feature

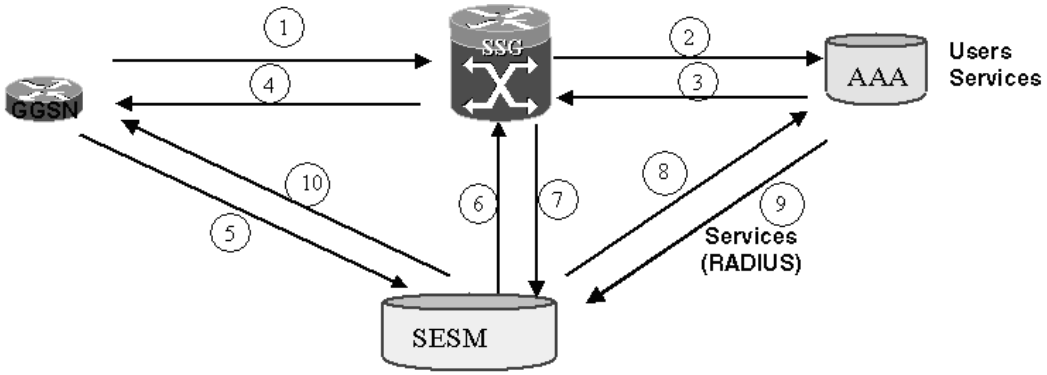
The SSG auto-logon feature allows the SSG to automatically create a host object for a user session and retrieve the user profile from the RADIUS messages sent by the GGSN. With the auto-logon feature, the SSG acts as a RADIUS proxy. The following steps describe the sequence of events that occur when the auto-logon feature is configured on the SSG.

Note Load balancing interactions are excluded from the following sequence to clarify auto-logon interactions between the GGSN, SSG, AAA server, and SESM.

1. When the GGSN receives a request for access from the mobile wireless subscriber, it sends a RADIUS access request to the SSG.
2. The SSG, configured with the auto-logon feature, forwards the request to the AAA server.
3. The AAA server authenticates the user, allocates an IP address, and sends vendor-specific attributes (VSAs) related to the user services.
4. The SSG strips off the SSG VSAs, creates a host object for the user session, and sends this information to the GGSN.
5. The PDP context is created (i.e., the user has an IP connection and can access the SESM with a Web browser). The GGSN sends a message to start accounting records for the session. The message is proxied by the SSG to the AAA server.
6. The SESM receives the HTTP request and queries the SSG.
7. The SSG responds with the username, IP address, service list, and SESM attributes.
8. The SESM uses the RADIUS interface to access a database and retrieve the user service attributes.
9. The service attributes are sent using the RADIUS interface.
10. The user home page is sent in the HTTP response to the subscriber.

Figure 3-9 illustrates these auto-logon interactions:

Figure 3-9 GGSN/SSG/AAA/SESM Interactions for Auto-logon



TCP Redirect Feature

The SSG TCP redirect feature transmits certain packets, which would otherwise be dropped, to captive portals that can handle the packets. Examples of packet redirection include the following:

- A prepaid subscriber is redirected to a Web page to recharge accounts.
- The SSG handling the user session fails and the user is redirected to a Web portal for re-authentication

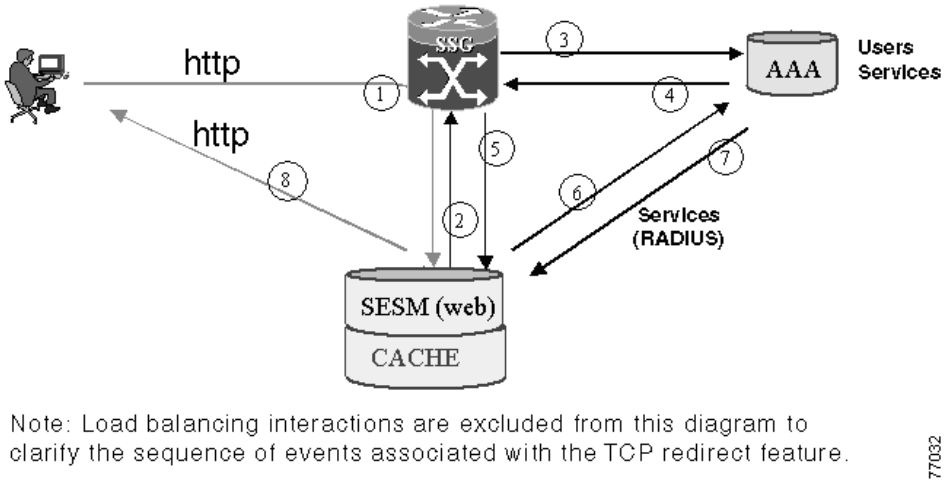
The following steps describe the sequence of events that occur when the TCP redirect feature is configured on the SSG.

Note Load balancing interactions are excluded from the following sequence to clarify TCP redirect interactions between the SSG, AAA server, and SESM.

1. An IP-enabled PC accesses the SESM using a Web client. User ID and password fields are presented in HTML format.
2. The SESM translates the user ID and password received via HTML into a RADIUS authentication packet and sends it to the SSG.
3. The SSG forwards the RADIUS request to the AAA server.
4. The AAA server responds to the SSG.
5. The SSG forwards the response to the SESM and creates a host object to establish the user session.
6. The SESM requests service profiles from the AAA server.
7. The AAA server responds to the SESM request with the service profiles.
8. The SESM provides a new HTML page to the user with service selection links.

Figure 3-10 illustrates these TCP redirect interactions:

Figure 3-10 SSG/SESM/AAA Interactions for TCP Redirect Feature



The TCP redirect feature also ensures availability of user sessions in the event that a single SSG fails. The following events occur when an SSG fails:

1. The RADIUS Load Balancer (RLB) detects the failure of the SSG and load balances the user traffic to an alternate SSG.
2. The alternate SSG receives the user data but does not have a host object for the user. The SSG redirects the user traffic to the Web portal.
3. The user establishes an HTTP session with the Web portal using a browser. The user logs in, and the new SSG receives an access request from the Web portal. The user host object is created and pass-through service is established.
4. The user traffic passes through the new SSG.

Detailed RADIUS Interactions

RADIUS messages originate from one of the following network elements:

- GGSN (then proxied by the SSG)
- SSG

GGSN-initiated RADIUS Messages

The following sequence of events describes the flow of RADIUS messages that originate from the GGSN during a request for access:

1. The GGSN forwards an Access Request message to the RLB (see Figure 3-11).
2. The RLB selects an SSG from the SSG farm.
3. The selected SSG proxies the request to the AAA-RLB.
4. The AAA-RLB selects the AAA1 server.
5. The AAA1 server is in a failure mode and does not respond to the request.
6. The GGSN retransmits the request.
7. The RLB detects the retransmission and resends the request to the same SSG that was originally selected.
8. The SSG proxies the request to the AAA-RLB.
9. The AAA-RLB selects the AAA2 server and marks the AAA1 server as failed.
10. The AAA2 server returns the Access Accept message to the SSG and then back to the GGSN.

The GGSN-initiated RADIUS message flow is shown in Figure 3-11.

Figure 3-11 GGSN-initiated RADIUS Flows

The RLB uses the RADIUS request identifier to detect retransmissions and mark the AAA server as failed.

The sequence is slightly altered for an Accounting Request message. In this case, the RLB does not detect retransmissions from the GGSN. The RLB marks the SSG as failed. To avoid having the SSG marked as failed because of Accounting Request retranmissions, you can configure a probe on the RLB to periodically verify that one SSG is still operational.

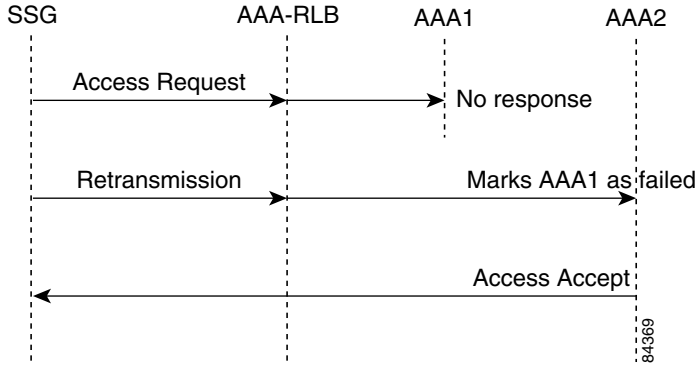
SSG-initiated RADIUS Messages

The following sequence of events describes the flow of RADIUS messages that originate from the SSG during a request for access:

1. The SSG forwards an Access Request message to the AAA-RLB (see Figure 3-12).
2. The AAA-RLB selects the AAA1 server.
3. The AAA1 server is in a failure mode and does not respond to the request.
4. The SSG retransmits the request.
5. The AAA-RLB selects the AAA2 server and marks the AAA1 server as failed.
6. The AAA2 server returns the Access Accept message to the SSG.

SSG-initiated RADIUS message flows are shown in Figure 3-12.

Figure 3-12 SSG-initiated RADIUS Message Flows



The same limitations for GGSN-initiated accounting requests apply to SSG-initiated accounting requests. You can configure a probe on the RLB to periodically verify that one AAA server is still operational.

Billing Solutions

The CMX framework enables a billing solution for mobile wireless operators that is flexible and facilates transition to next-generation networks. In legacy networks, operators charge users based on the duration of the call. In next-generation networks, the user is always on; therefore, charging based on time is not appropriate.

The CMX framework allows per-service billing based on volume (number of packets), type of content, and the applications accessed. The CMX generates the billing and accounting information, which is then used by the billing agent to bill the subscriber.

Cisco enables solutions for prepaid and postpaid billing using two components. The Service Selection Gateway (SSG) provides service volume and time accounting information. The CSG provides information based on content (Layer 4 and Layer 7).

Prepaid Billing

The two CMX components that play key roles in providing prepaid billing are the SSG and the CSG.

SSG Role

The SSG prepaid features allow the SSG to check a subscriber's available credit to determine whether to connect the subscriber to a service and how long the connection can last. The subscriber's credit is administered by the prepaid billing server as a series of quotas representing either a duration of use (in seconds) or an allowable data volume (in bytes). A quota is an allotment of available credit for a service.

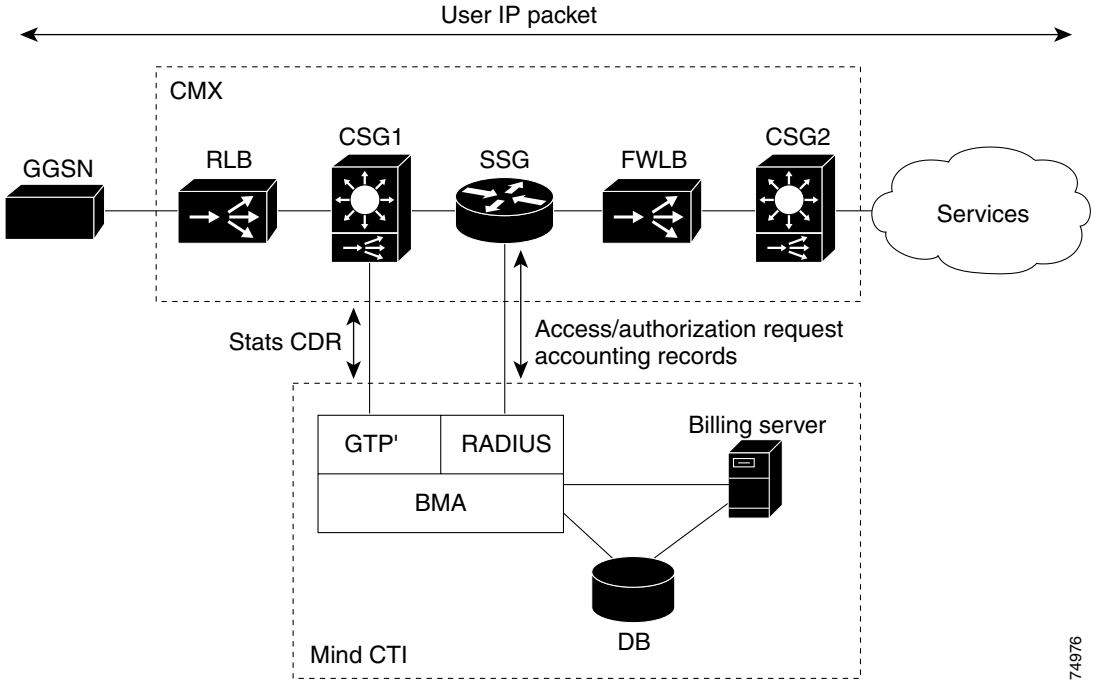
To obtain the first quota for a connection, the SSG submits an authorization request to the AAA server. The AAA server contacts the prepaid billing server, which forwards the quota values to the SSG. The SSG monitors the connection to track the quota usage. When the quota runs out, the SSG performs reauthorization. During reauthorization, the billing server can provide the SSG with an additional quota if credit is available. If no further quota is provided, the SSG logs the user off the service. The user can be redirected to a Web server to refill accounts.

A prepaid idle timeout feature allows remaining quota to be returned to the billing server if the connection remains inactive (idle) for a specified period of time. Also, if a disconnect occurs before quota depletion, the SSG returns the unused amount to the billing server.

Figure 3-13 shows the prepaid billing solution provided by the SSG (see note).

Note The configuration shown in Figure 3-13 integrates the MIND CTI Real-Time Server, which provides the AAA, rating, and billing capabilites for the overall solution.

Figure 3-13 SSG-based Prepaid Billing Solution



As shown in Figure 3-13, the SSG sends an access/authorization request to the billing mediation agent (BMA) to retrieve quotas and accounting records.

CSG Role

The CSG occupies two positions in the CMX configuration. The first CSG in the CMX configuration, represented in Figure 3-13 as CSG1, generates call detail records (CDRs) of statistics and sends them to the BMA. These CDRs are used to restore the user's balance in the event of an SSG failure. This CSG provides an important backup function for the SSG prepaid billing features.

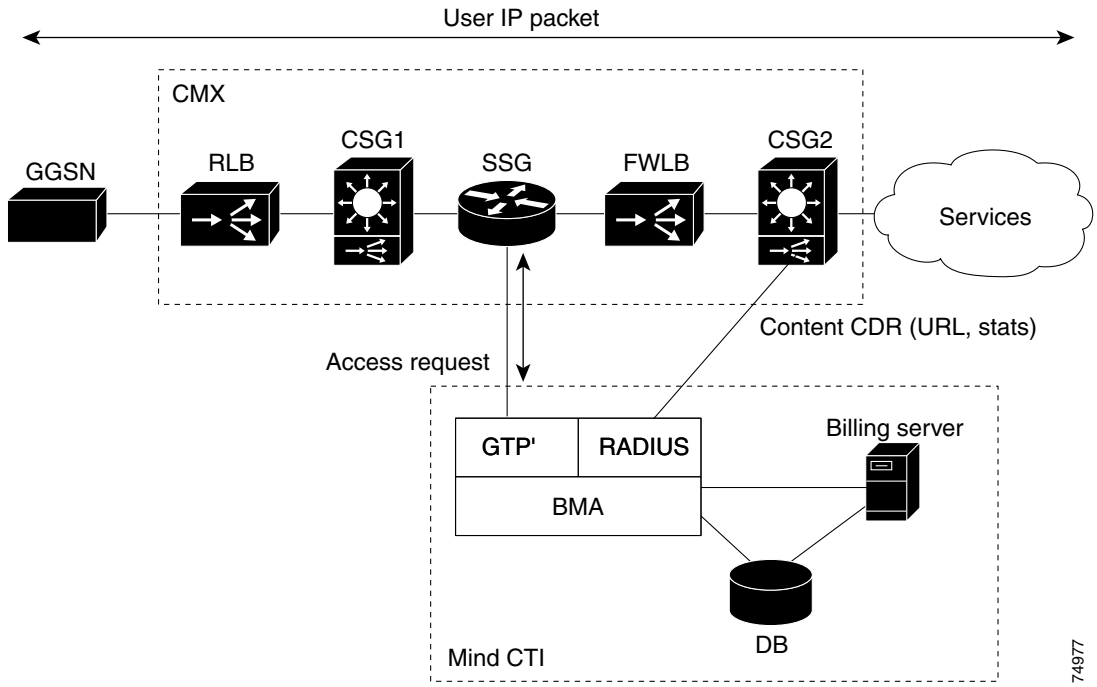
The second CSG in the CMX configuration is configured to provide content-based billing. Web pages are identified by their URLs and charged on a fixed-fare basis, also known as *per-page billing*. The subscriber incurs billing in real time as the Web page is requested.

The service provider can also configure this CSG to perform *per-event billing* from within a Web page to charge subscribers for downloading files. These events, also known as *stats*, must be structured in a keyed directory tree to distinguish them from events for which no billing occurs. Also, subscribers are billed only for files that are completely transferred (i.e., failed downloads are not billed). Files to be downloaded must reside on a dedicated server (i.e., the IP destination address of the downloading server must be different than the IP destination address of the Web server).

Per-page billing (URL-based) and per-event billing (stats) are provided by CSG2 shown in Figure 3-14. The BMA connects to a database and a billing server to verify user balances and perform rating and billing functions (see note).

Note The configuration shown in Figure 3-14 integrates the MIND CTI Real-Time Server, which provides the AAA, rating, and billing capabilites for the overall solution.

Figure 3-14 CSG-based Content Billing



Postpaid Billing

Postpaid billing based on time and volume usage is implemented by the SSG. The accounting start message sent to the AAA server initiates accounting records for the session. When the user disconnects from a service, the SSG sends an accounting stop message to the AAA server. During the user session, the SSG periodically sends interim-update messages to update the time and volume used. The RADIUS accounting records record the service volume and session duration for billing purposes.

The CSG allows service providers to bill subscribers based on service content instead of time and volume used. The CSG records user traffic based on the URL entered by the end user. Web pages that are billed can be structured as previously described (see CSG Role, page 3-22).

The CSG sends the content-based call detail records to a billing mediation agent (BMA) over a GTP' interface. The BMA uses the subscriber's IP address to retrieve the MSISDN, which is required to properly identify and charge the subscriber for the content accessed.

High Availability Solutions

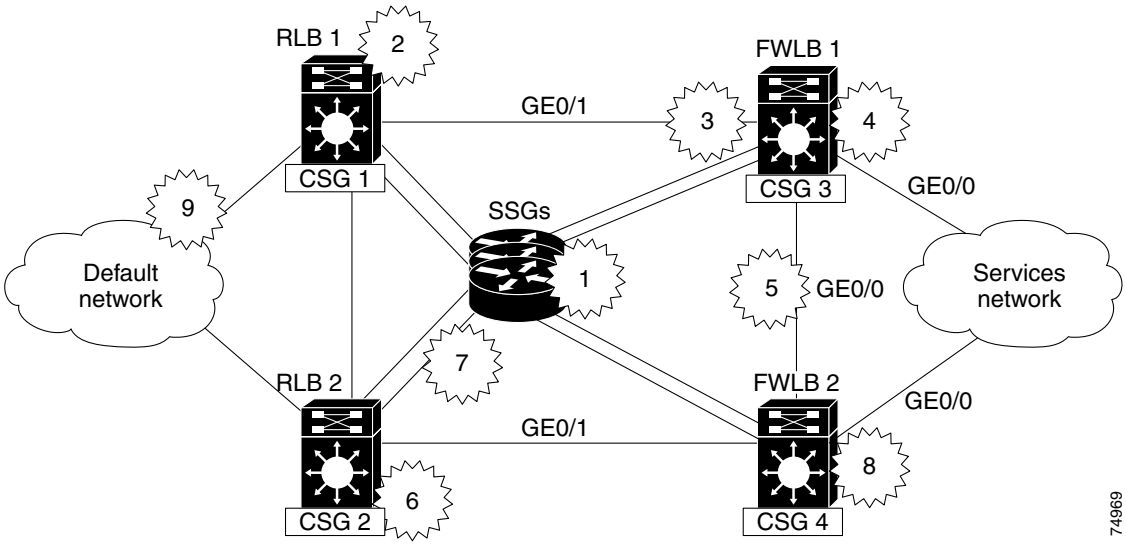
The CMX configuration handles any single point of failure by using redundant load-balancing platforms, redundant physical interfaces, and the Hot Standby Router Protocol (HSRP). Each routing element is connected to a standby element through a virtual LAN (VLAN) interface. The links between the RLB and multiple SSGs are maintained on a single VLAN using bridged virtual interfaces (BVIs) on the SSGs. This configuration uses the spanning tree protocol for quick recovery if an interface fails. This solution is based on the following:

- HSRP and CASA replication between redundant RLBs
- HSRP and CASA replication between redundant FWLBs
- Redundant Fast Ethernet (FE) interfaces to each RLB from each SSG using BVIs
- Redundant FE interfaces to the default network (AAA, BMA, SESM, prepaid server)
- Redundant trunks to the services network using Gigabit Ethernet (GE)
- Use of a fault-tolerance mechanism and aliases between the CSGs

Figure 3-15 illustrates the high-reliability solution for the CMX. The RLB1 and FWLB1 are configured to be active, and their peers, RLB2 and FWLB2, are in standby mode. If an active network element fails, the standby element becomes active. Also, both RLB1 and FWLB1 are configured to preempt their peers. For example, if RLB1 fails and RLB2 becomes active, RLB1 resumes activity when its failure condition clears.

The CSGs in the CMX framework are not configured for preemption. For example, if a failure occurs in CSG1, user traffic from the GGSN sequentially traverses RLB1, CSG2, back to RLB1, then to the SSGs. Even if the failure in CSG1 clears, user traffic continues to traverse the path through CSG2.

Figure 3-15 Failure Case Scenarios



The numbers shown in Figure 3-15 correspond to the failure scenarios listed below:

1. Failure of an SSG—When an SSG fails, user sessions supported by the SSG are lost. Incoming RADIUS requests for new user sessions are redirected to available SSGs. The RLB detects the SSG failure (using probes) and sends the user traffic to another SSG. The new SSG redirects users to the Web portal to authenticate them and restore user sessions. When the failed SSG restarts, it sends messages to the AAA server to stop accounting.

   Note The redundant CSGs in the RLB are used for backing up SSG-based prepaid billing records (if an SSG fails). The redundant CSGs in the FWLB provide content billing.

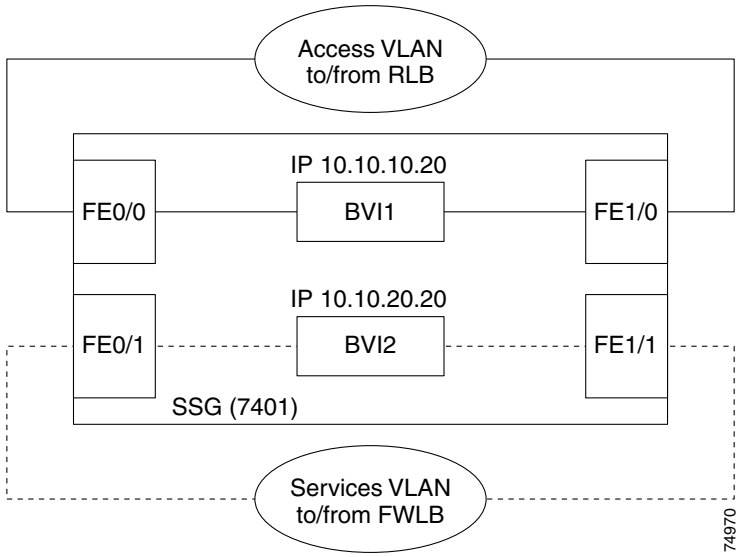
2. Failure of one RLB—HSRP runs between the two RLBs to maintain RADIUS load-balancing. When one RLB fails, the other RLB takes over the RADIUS load-balancing function.
3. Failure of the RLB-to-FWLB link—Messages are redirected via the links between the two RLBs to the peer FWLB. Spanning Tree Protocol is used to determine the alternate path.
4. Failure of an FWLB—HSRP runs between the FWLBs to maintain load-balancing of *sticky* objects between them. When one FWLB fails, the other FWLB takes over the load-balancing function.
5. Failure of the link between FWLBs—User traffic is redirected via the link between the RLBs.
6. Failure of a CSG—A fault-tolerance mechanism runs between the CSGs to maintain RLB *sticky* objects. When one CSG fails, the other CSG takes over.
7. Failure of an SSG link—The SSG supports redundant links to each RLB and FWLB. If one link fails, the other link is used.
8. Failure of the link to the services network—The FWLBs support redundant links to the services network. If one link fails, the other link is used.
9. Failure of the default network link—The RLBs support redundant links to the default network. If one link fails, the other link is used.

The configuration redundancies provided by bridged virtual interfaces (BVIs) in the SSG are illustrated in Figure 3-16. The SSG avoids any single point of failure by its connection to the two CMX VLANs. The failure of a physical interface or port adapter does not impact service.

As shown in Figure 3-16, the FE 0/0 and FE 1/0 ports are used to connect to the access VLAN, which interconnects the RLB for incoming RADIUS and user packets. The FE 0/1 and FE 1/1 ports are used to connect to the services VLAN, which interconnects the FWLB toward the services network. On each VLAN, the SSG is addressed with a single IP address; bridging is used between the interfaces and the IP addresses are configured on the BVIs.

The Spanning Tree Protocol (STP) is used to find a Layer 2 path between all the components when a physical interface fails. The RLB 1, which has the highest HSRP priority (active), is configured as the primary bridge root on the access and services VLANs. The RLB 2, which has the lowest HSRP priority (standby), is configured as the secondary bridge root on the access and services VLAN.

Figure 3-16 Example of Bridged Virtual Interfaces in SSG



CMX Network Management

This chapter contains the following sections:

Overview

CiscoWorks for Mobile Wireless (CW4MW) bundle is a suite of element management system (EMS) applications that enhance the delivery of new, mobile wireless services. Based on CiscoWorks2000, it addresses the element management requirements of mobile operators and provides fault, configuration, accounting, performance, and security (FCAPS) functionality. CiscoWorks for Mobile Wireless can facilitate mobile operators in transitioning their wireless service delivery networks from second-generation (2G) circuit-based traffic to 2.5G and third-generation (3G) IP-based services.

The CW4MW suite provides device-level management. This includes inventory, fault monitoring, statistics data view, and, from command line, configuration and image/file management.

The CW4MW suite consists of the following applications:

- Mobile Wireless Fault Mediator (MWFM)—Provides fault mediation for most of the network elements of the CMX framework
- Resource Manager Essentials (RME)—Provides image download, display of system log events, and archival/reporting of hardware, configuration, and inventory changes
- CSG Provision Manager—Provides graphical user interface (GUI) configuration of Content Services Gateways (CSGs)
- CiscoView—Provides monitoring of performance statistics and display of platform configuration attributes for most of the network elements of the CMX framework
- APN Manager—Provides a GUI to configure access point names (APNs) in a GPRS network that uses a Cisco GGSN

Mobile Wireless Fault Mediator

The Mobile Wireless Fault Mediator (MWFM) uses monitoring, automated response, and event correlation to generate alerts. The MWFM application uses a collection of agents that poll the network. This results in a stream of events. The monitoring engine removes duplicate events, allowing the MWFM to focus on more significant events.

The MWFM uses event correlation to define the corresponding occurrences that warrant a more significant event message. The MWFM also uses automated response to define how to react to the events and alerts coming from a Cisco network element.

For example, a ping fail generates an event. The MWFM then passes this event to the correlation engine, which determines if it should generate an alert. An alert (alarm) is an indication of a situation that the operator should respond to.

The graphical user interface (GUI) of the Mobile Wireless Fault Mediator (MWFM) enables you to use the CiscoWorks2000 desktop interface to view information about alerts and events processed by the MWFM server. The CiscoWorks2000 desktop is a GUI that runs in a web browser.

Four categories of faults are recognized:

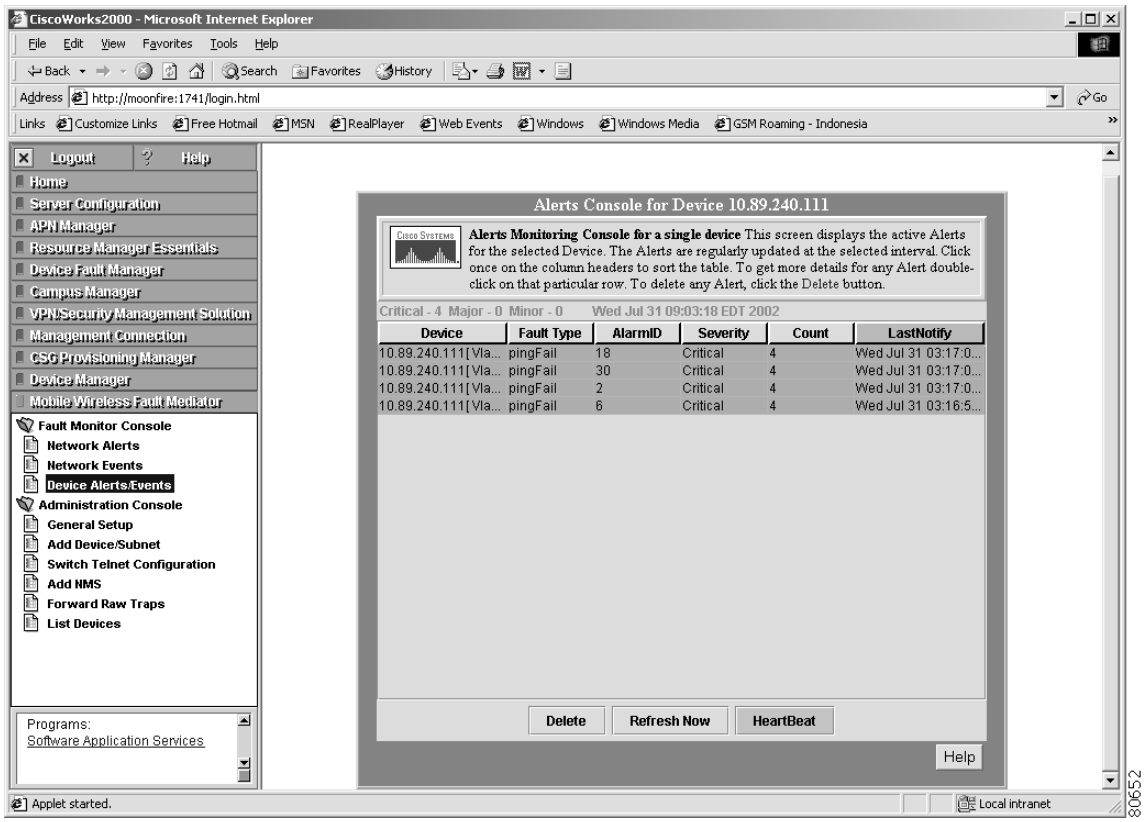
- Hardware faults
- Software faults
- Functional faults
- Loss of node capabilities

The MWFM provides fault mediation for the following CMX framework elements:

- Service Selection Gateway (SSG)
- Content Services Gateway (CSG)
- RADIUS Load Balancer (RLB)
- Firewall Load Balancer (FWLB)

Figure 4-1 shows the graphical user interface (GUI) of the MWFM.

Figure 4-1 MWFM GUI



For more information on MWFM, visit
http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2k4mw/mwfm/index.htm

Resource Manager Essentials

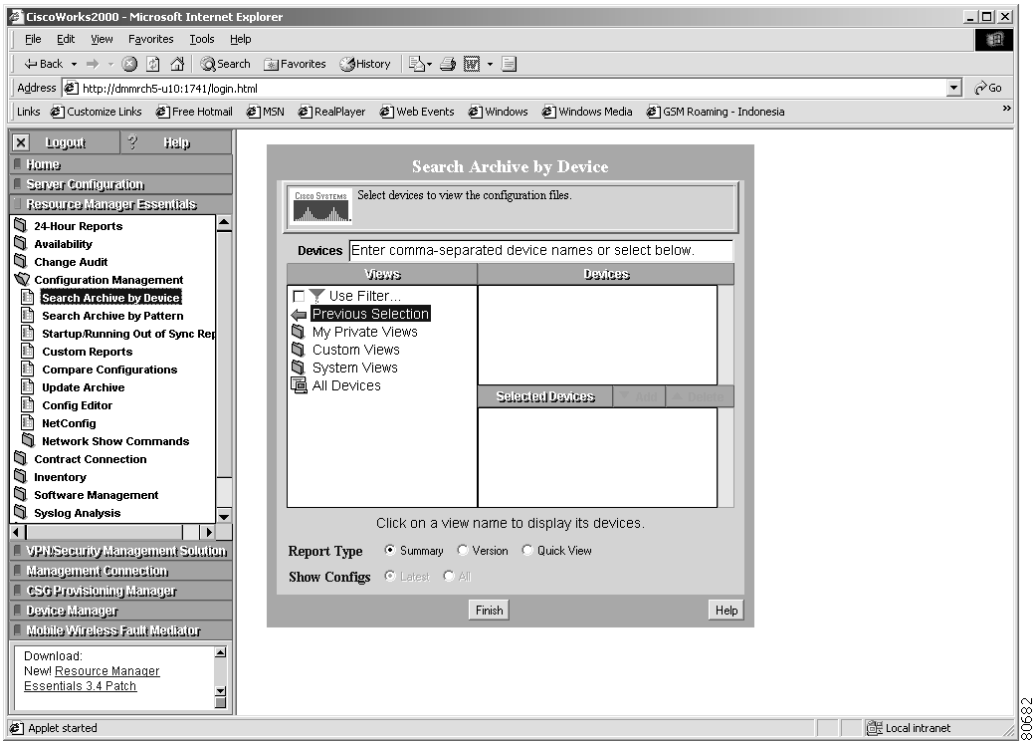
The Resource Manager Essentials (RME) suite is part of the CiscoWorks2000 family of products. It is an enterprise solution to network management. This suite of web-based, network management tools enables administrators to collect the monitoring, fault, and availability information needed to track devices critical to the network. Essentials is based on a client/server architecture that connects multiple web-based clients to a server on the network. As the number of network devices increases, additional servers or collection points can be added to manage network growth with little impact on the client browser application.

The RME provides the following applications for network-connected devices:

- Availability of devices
- Audits of network changes
- Configuration management
- Device views for reports
- Inventory control
- Software management (image upgrades and downloads)
- Syslog analysis for troubleshooting
- System configuration

Figure 4-2 shows the GUI of the RME.

Figure 4-2 RME GUI



For more information on RME, visit
http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000e/index.htm

CSG Provisioning Manager

The CSG Provision Manager (CSG Mgr) is a GUI accessible from the CiscoWorks2000 desktop that enables you to perform the following tasks:

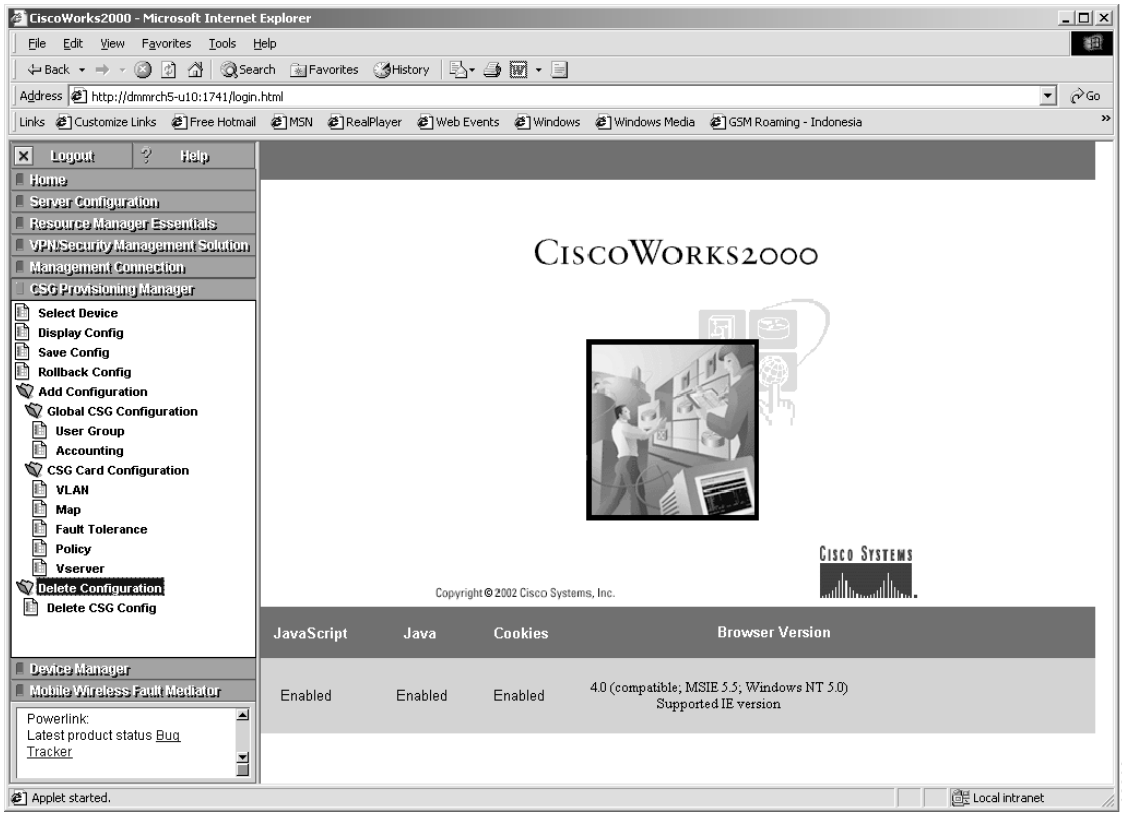
- Display the current CSG configuration
- Add a new CSG configuration or modify an existing one
- Delete a CSG configuration

Using the CSG Manager, you can configure the following on the CSG:

- User groups—Support CSG queries for user IDs and generate accounting records
- Accounting service—Enables content-based accounting
- Virtual local area networks (VLANs)—Enables client-side and server-side VLAN creation
- Fault tolerance feature—Support for redundant CSG configuration
- Policy feature—Supports filters for traffic types that are subject to the accounting service
- Virtual server information—Supports Vservers for billing records

Figure 4-1 shows the GUI of the CSG Provisioning Manager (CSG Mgr).

Figure 4-3 CSG Mgr GUI



For more information on CSG Mgr, visit
http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2k4mw/csgmgr/index.htm

CiscoView

CiscoView is a graphical, SNMP-based, device management tool that provides real-time views of networked Cisco devices. These views deliver a dynamic picture of device configuration and performance conditions with views available for multiple device sessions.

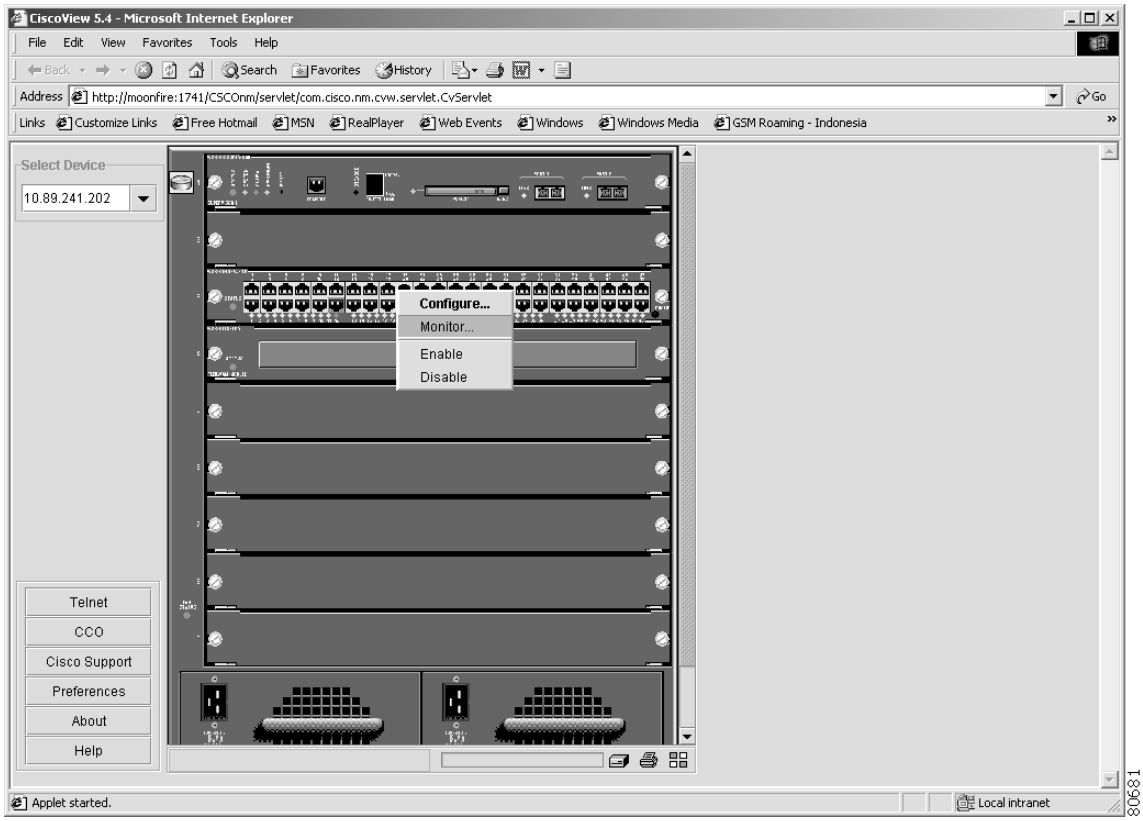
CiscoView enables you to:

- View a graphical representation of front and back device panels including component status
- Configure parameters for devices, cards, and interfaces
- Monitor real-time statistics for interfaces, resource utilization, and device performance

CiscoView provides support for the devices of the SSG, CSG, RLB, and FWLB elements of the CMX framework.

Figure 4-4 shows an example of the CiscoView GUI.

Figure 4-4 CiscoView GUI



For more information on CiscoView, visit http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/cw2000_d/4steditn/use_view/index.htm

APN Manager

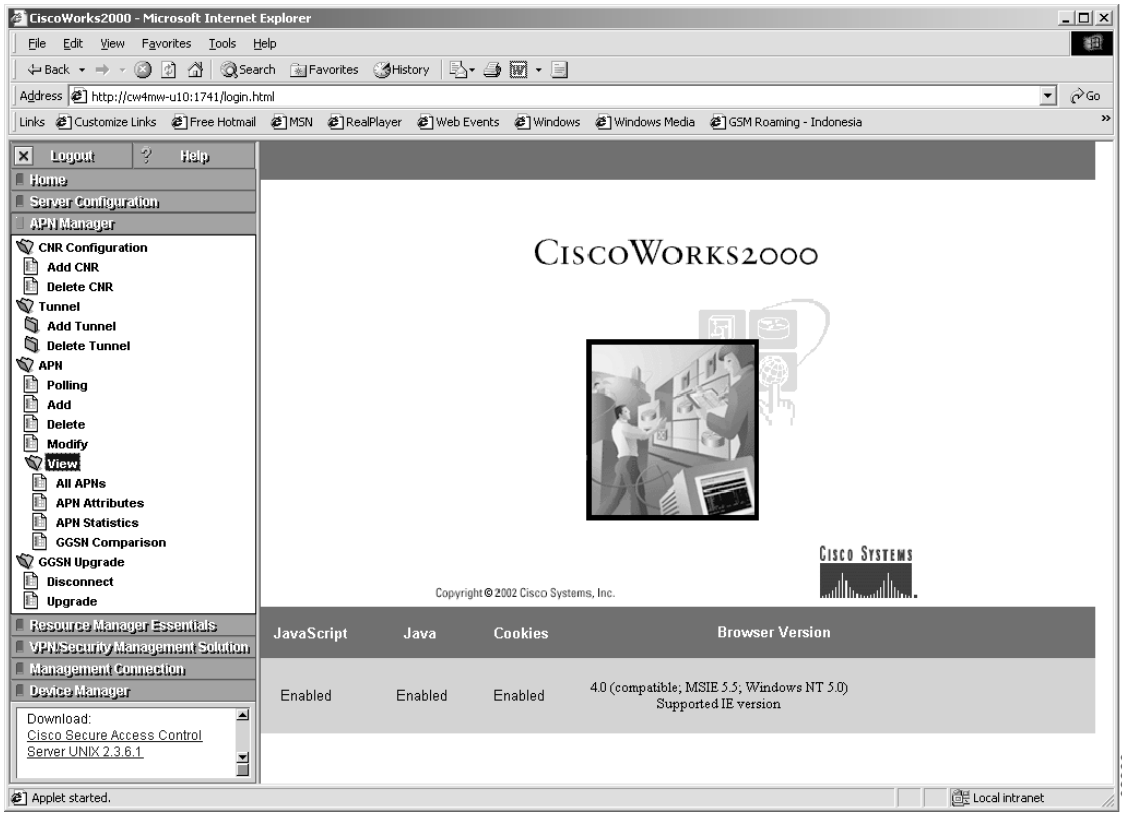
The Cisco APN Manager (APN Man) is a product you can use to manage Access Point Names (APNs) on Cisco Gateway GPRS Support Nodes (GGSNs) in a General Packet Radio Service (GPRS) network.

The APN Man GUI enables you to perform the following tasks, via the CiscoWorks2000 desktop interface:

- Create, view, modify, and delete APNs for Cisco GGSNs
- Create and delete GRE tunnels for Cisco GGSNs

Figure 4-5 shows the GUI of the APN Manager.

Figure 4-5 APN Manager GUI



Note The APN Manager is not required for network management of the CMX network elements in Release 1 of the CMX.

For more information on APN Manager, visit http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2k4mw/apnman/

CMX Configuration Guidelines

This chapter provides configuration guidelines for the Cisco Mobile Exchange (CMX).

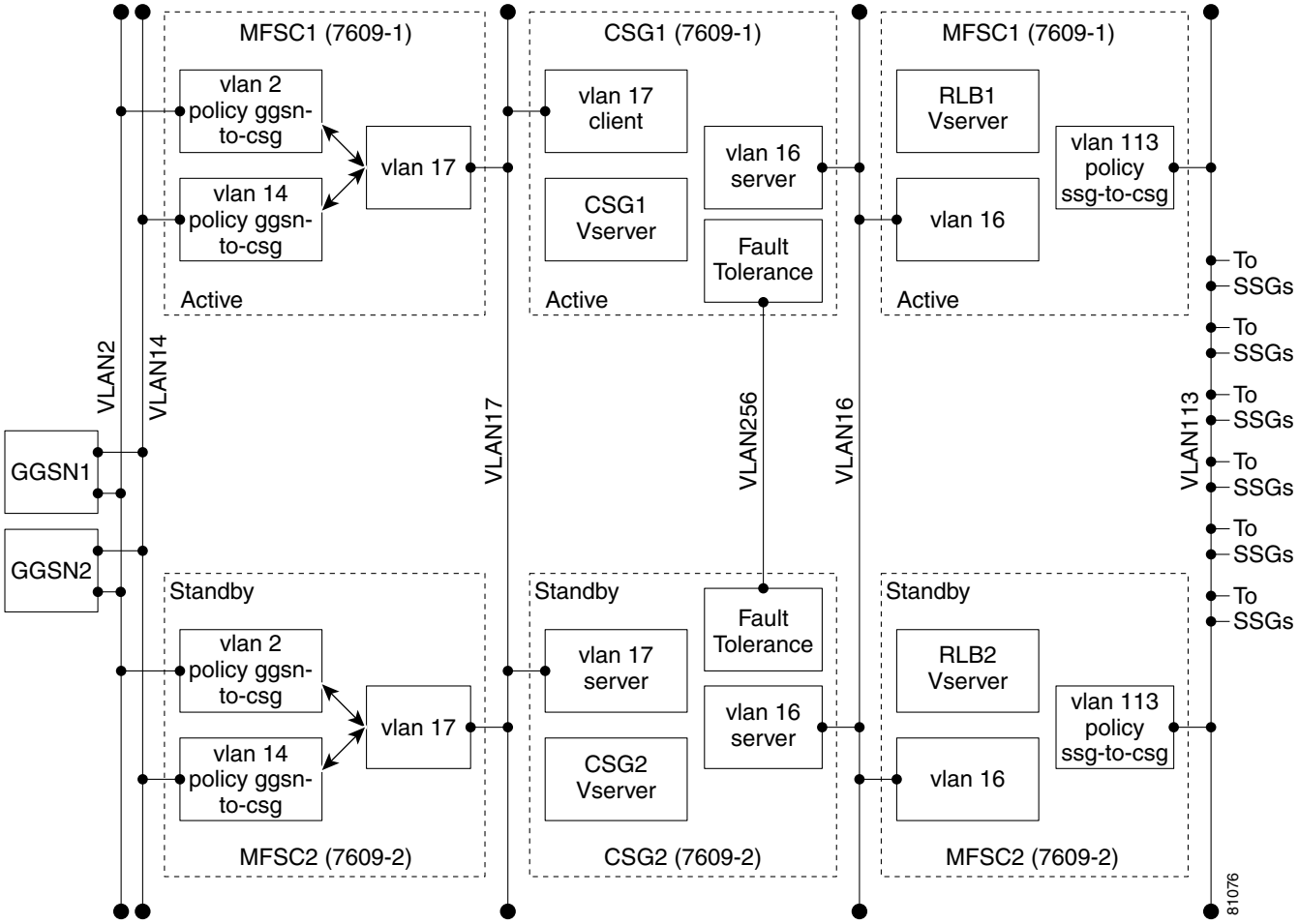
For a complete description of the CMX commands in this chapter, refer to the *Cisco IOS Mobile Wireless Command Reference*. To locate documentation of other commands that appear in this chapter, use the command reference master index or search online.

This chapter includes the following sections:

Reference Topology

The reference topology for the CMX configuration is shown in Figure 5-1 and Figure 5-2.

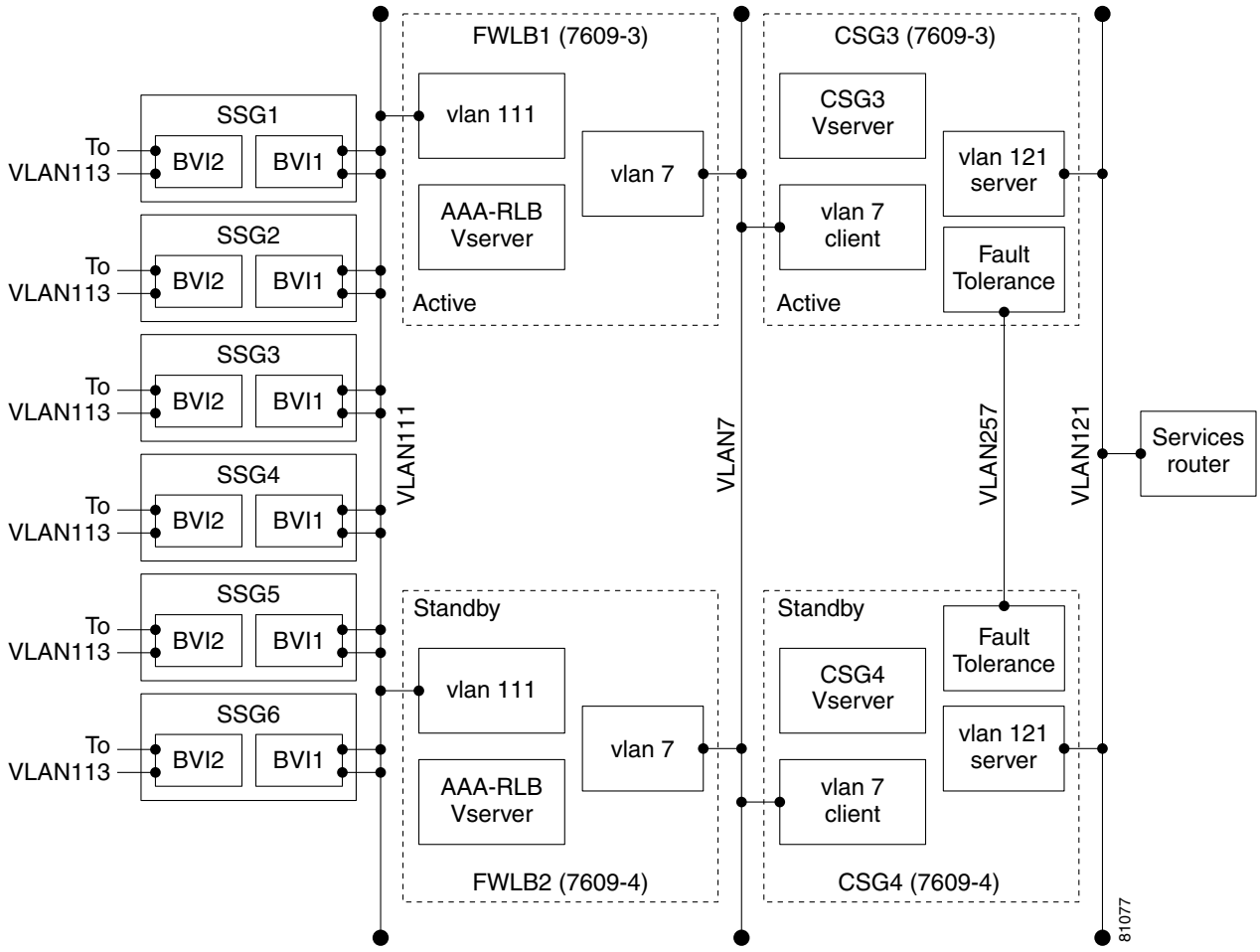
Figure 5-1 CMX Reference Topology (1 of 2)



The CMX topology is organized into several VLANs. The VLANs shown in Figure 5-1 include:

- GGSN-to-MSFC1/2 VLANs 2 and 14—Connects the GGSN to 7609-1 and 7609-2 via redundant connection, using Open Shortest Path First (OSPF) protocol to exchange routing information and detect interface failure
- MSFC1/2-to-CSG1/2 VLAN 17—Connects MSFC1/2 to CSG1/2, and interconnects MSFC1 and MSFC2 to run High Speed Router Protocol (HSRP)
- CSG1-to-CSG2 VLAN 256—Used by the fault tolerance mechanism of the CSGs
- CSG1/2-to-MSFC1/2 VLAN 16—Connects the CSG1/2 server to the MSFC1/2 (toward the RLB1/2 Vserver), and interconnects RLB1 and RLB2 for HSRP
- MSFC1/2-to-SSGs VLAN 113—Connects the MSFC1/2 running RLB1/2 to all the SSGs, and used for HSRP between MSFC1 and MSFC2

Figure 5-2 CMX Reference Topology (2 of 2)



The VLANs shown in Figure 5-2 include:

- SSGs-to-FWLB1/2 VLAN 111— Connects the SSG uplink interfaces to the FWLB1/2, and used for HSRP between FWLB1 and FWLB2
- FWLB1/2-to-CSG3/4 VLAN7—Connects the FWLB1/2 to CSG3/4, and used for HSRP between FWLB1 and FWLB2
- CSG3-to-CSG4 VLAN 257—Used by the fault tolerance mechanism of the CSGs
- CSG3/4-to-services router—Connects CSG3/4 to the services router toward the services network

VLAN Switching Blade Configuration Guidelines

This section describes how to configure the VLAN switching blade. The following tasks are presented:

Configuring VLAN Trunking Protocol

The VLAN trunking protocol (VTP) is a Layer 2 messaging protocol that maintains the VLAN configuration by managing the addition, deletion, and renaming of VLANs within a VTP domain. A VTP domain (also known as a VLAN management domain) is made up of one or more network devices that share the same VTP domain name and are interconnected with trunks. The VTP minimizes misconfigurations and configuration inconsistencies such as duplicate VLAN names, incorrect VLAN-type specifications, and security violations.

Before you create VLANs, you must decide whether to use VTP in your network. With VTP, you can make configuration changes centrally on one or more network devices and have those changes automatically communicated to all the other network devices in the network.

VTP Configuration Guidelines and Restrictions

Follow these guidelines and restrictions when implementing VTP in your network:

- All network devices in a VTP domain must run the same VTP version.
- You must configure a password on each network device in the management domain when in secure mode.

Caution If you configure VTP in secure mode, the management domain does not function properly unless you assign a management domain password to each network device in the domain.

- A VTP version 2-capable network device can operate in the same VTP domain as a network device running VTP version 1 only if VTP version 2 is disabled on the VTP version 2-capable network device (VTP version 2 is disabled by default).
- Do not enable VTP version 2 on a network device unless all of the network devices in the same VTP domain are version 2-capable. When you enable VTP version 2 on a network device, all of the version 2-capable network devices in the domain enable VTP version 2.
- In a token ring environment, you must enable VTP version 2 for token ring VLAN switching to function properly.
- Enabling or disabling VTP pruning on a VTP server enables or disables VTP pruning for the entire management domain.
- Configuring VLANs as pruning eligible or pruning ineligible on a Catalyst switch affects pruning eligibility for those VLANs on that switch only (not on all network devices in the VTP domain).

Configuring a VTP Password

To configure the VTP password parameters, use the following commands:

Command	Purpose
`Router# vtp password password_string`	Sets a password, which can be from 8 to 64 characters long, for the VTP domain
`Router# no vtp password`	Clears the password

Configuring the VTP Mode

To configure the VTP mode, use the following commands:

Command	Purpose
`Router(config)# vtp mode {client | server | transparent}`	Configures the VTP mode **Note** Use **no vtp mode** to revert to the default VTP mode (server).
`Router(config)# vtp domain domain_name`	(Optional for server mode) Defines the VTP domain name, which can be up to 32 characters long. VTP server mode requires a domain name. If the switch has a trunk connection to a VTP domain, the switch learns the domain name from the VTP server in the domain. **Note** You cannot clear the domain name.
`Router(config)# end`	Exits VLAN configuration mode
`Router# show vtp status`	Verifies the configuration

Note When VTP is disabled, you can enter VLAN configuration commands in configuration mode instead of the VLAN database mode, and the VLAN configuration is stored in the startup configuration file.

This example shows how to configure the switch as a VTP server:

```
Router# configuration terminal

Router(config)# vtp mode transparent

Setting device to VTP TRANSPARENT mode.
Router(config)# vtp domain CMX

Setting VTP domain name to CMX
Router(config)# end

Router#
```

This example shows how to verify the configuration:

```
Router# show vtp status
```

```
VTP Version                     : 2
Configuration Revision          : 247
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 24
VTP Operating Mode              : Transparent
VTP Domain Name                 : CMX
VTP Pruning Mode                : Enabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x45 0x52 0xB6 0xFD 0x63 0xC8 0x49 0x80
```

Configuring VLANs

VLANs allow you to group LAN ports to limit unicast, multicast, and broadcast traffic flooding.

Note Before you create VLANs, you must decide whether to use VLAN Trunking Protocol (VTP) to maintain global VLAN configuration information for your network. For complete information on VTP, see "Configuring VLAN Trunking Protocol" section on page 5-4.

Creating or Modifying an Ethernet VLAN

User-configured VLANs have unique IDs from 1 to 1001. Enter a VLAN command with an unused ID to create a VLAN. Enter a VLAN command for an existing VLAN to modify the VLAN. If you do not specify the VLAN type with the media keyword, the VLAN is an Ethernet VLAN.

To create a VLAN, use the following commands:

Command	Purpose
`Router# configure terminal`	Enters global configuration mode to allow you to configure the system from the terminal.
`Router(config)# vlan vlan_ID`	Adds an Ethernet VLAN. **Note** Use the **no vlan** command to delete a VLAN. You cannot delete the default VLANs for the different media types: Ethernet VLAN 1 and FDDI or Token Ring VLANs 1002 to 1005. When you delete a VLAN, any LAN ports configured as access ports assigned to that VLAN become inactive. They remain associated with the VLAN (and inactive) until you assign them to a new VLAN.
`Router(config-vlan)# end`	Updates the VLAN database and returns to privileged EXEC mode.
`Router# show vlan [id | name] vlan`	Verifies the VLAN configuration.

This example shows how to create an Ethernet VLAN in global configuration mode and verify the configuration:

```
Router# configure terminal

Router(config)# vlan 3

Router(config-vlan)# end
Router# show vlan id 3
```

```
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
3    VLAN0003                         active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
3    enet  100003     1500  -      -      -        -    -        0      0
```

Configuring a LAN Port for Layer 2 Switching

A VLAN created in a management domain is not used until you assign one or more LAN ports to it.

Note Make sure you assign LAN ports to a VLAN of the appropriate type. For CMX Release 1, you can assign Fast Ethernet and Gigabit Ethernet ports.

To assign one or more LAN ports to a VLAN, use the following commands:

Command	Purpose
`Router(config)# interface` *type slot/port*	Selects the LAN port to configure[1]
`Router(config-if)# shutdown`	(Optional) Shuts down the interface to prevent traffic flow until configuration is complete
`Router(config-if)# switchport`	Configures the LAN port for Layer 2 switching. **Note** You must enter the switchport command once without any keywords to configure the LAN port as a Layer 2 port before you can enter additional switchport commands with keywords. Use the **no switchport** command to clear Layer 2 LAN port configuration.
`Router(config-if)# no shutdown`	Activates the interface (required only if you previously shut down the interface)
`Router(config-if)# end`	Exits configuration mode
`Router# show running-config interface` [*type slot/port*]	Displays the running configuration of the interface[1]
`Router# show interfaces` [*type slot/port*] `switchport`	Displays the switch port configuration of the interface[1]
`Router# show interfaces` [*type slot/port*] `trunk`	Displays the trunk configuration of the interface[1]

1. *type* = **ethernet**, **fastethernet**, **gigabitethernet**, or **tengigabitethernet**
After you enter the switchport command, the default mode is switchport mode dynamic desirable. If the neighboring port supports trunking and is configured to allow trunking, the link becomes a Layer 2 trunk when you enter the switchport command. By default, LAN trunk ports negotiate encapsulation.

The code below represents an example of configuring a LAN port for Layer 2 switching:

```
!
interface GigabitEthernet1/1
 no ip address
 shutdown
!
interface GigabitEthernet1/2
 description trunk port to FwLB1 Gig1/2
 no ip address
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 7,111
!
interface FastEthernet4/1
 description trunk port to Lab Network
 no ip address
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 2,14
!
interface FastEthernet4/2
 description port-channel 1 trunk to RLB2 Fast4/2
 no ip address
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 2,7,14,16,17,111,113,119,256,257
 channel-group 1 mode on
!
```

Configuring the Default VLAN

To configure the default VLAN, use the following commands:

Command	Purpose
`Router(config-if)# switchport access vlan vlan_num`	(Optional) Configures the default VLAN, which is used if the interface stops trunking
`Router(config-if)# no switchport access vlan`	Reverts to the default value (VLAN 1)

The code below represents an example of configuring the default VLAN:

```
!
interface FastEthernet4/13
 description SSG4 0/0 Host Side
 no ip address
 duplex full
 speed 100
 switchport
 switchport access vlan 113
!
```

Configuring Port Channels

This feature allows multiple Fast Ethernet point-to-point links to be bundled into one logical link. You can configure the port-channel interface as you would do to any Fast Ethernet interface. After you create a port-channel interface, you assign Fast Ethernet interfaces (up to four) to it.

To configure port channel interfaces, use the following command:

Command	Purpose
`Router(config-if)# interface port-channel channel_num`	Specifies a Fast EtherChannel and enters interface configuration mode. *channel_num* is the channel number assigned to this port-channel interface. Range is 1 to 4.

The code below represents an example of configuring a port channel:

```
!
interface Port-channel1
 description trunk from RLB1 to RLB2
 no ip address
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 2,14,15,16,17,113,256
switchport mode trunk
!
```

For more information on VLAN switching blade configuration, visit:
http://www.cisco.com/en/US/products/hw/routers/ps368/products_configuration_guide_book09186a008007c883.html

RLB Configuration Guidelines

The RADIUS Load Balancer (RLB) load-balances the traffic among the SSGs using the IOS RADIUS SLB feature. The IOS SLB feature is an IOS-based solution that provides IP server load balancing. Using the IOS SLB feature, you can define a virtual server that represents a group of real servers in a cluster of network servers known as a server farm. In this environment, the clients connect to the IP address of the virtual server. When a client initiates a connection to the virtual server, the IOS SLB function chooses a real server for the connection based on a configured load-balancing algorithm.

Observe the following guidelines when configuring the redundant RLBs in the CMX framework:

- Use the correct Cisco IOS version for the RLB router (see Table 3-2 on page 3-3)
- Configure the physical and VLAN interfaces using the *Cisco 7600 Series Internet Router IOS Software Configuration Guide* at http://www.cisco.com/en/US/products/hw/routers/ps368/products_configuration_guide_book09186a008007c883.html
- Configure speed and duplex first to avoid auto-negotiation when interfaces are initialized
- Use only static routing (default routes) between the CMX elements (CSG, RLB, SSG, and FWLB)
- Use OSPF routing between the GGSN and the RLBs
- Use HSRP and CASA replication between the RLBs
- Use two fast Ethernet links to each RLB from each SSG with BVIs configured for uplink and downlink directions

The following tasks are presented in this section:

Configuring a Server Farm and Real Server

To configure an IOS SLB server farm, you will specify a server farm name and assign real servers to the server farm. Use the following commands beginning in global configuration mode:

Command	Purpose
`Router(config)# ip slb serverfarm` *serverfarm-name*	Adds a server farm definition to the IOS SLB configuration and initiates server farm configuration mode.
`Router(config-slb-sfarm)# nat` {**client** *pool* | **server**}	Configures NAT client or server address translation mode on the server farm.
`Router(config-slb-sfarm)# failaction` {**purge** | **radius reassign**}	Configures the IOS SLB behavior when a real server fails. The **radius reassign** option enables IOS SLB to automatically reassign to a new real server the RADIUS sticky objects that are destined for a failed real server.
`Router(config-slb-sfarm)# probe` *probe*	Associates a probe with the real server.

Command	Purpose
`Router(config-slb-sfarm)# real ip-addr [port]`	Identifies a real server by IP address and optional port number as a member of a server farm and enters real server configuration mode.
`Router(config-slb-real)# weight setting`	Specifies the real server's workload capacity relative to other servers in the server farm.
`Router(config-slb-real)# reassign threshold`	Specifies the threshold of consecutive unacknowledged synchronizations that, if exceeded, result in an attempted connection to a different real server.
`Router(config-slb-real)# faildetect numconns number-conns [numclients number-clients]`	Specifies the number of consecutive connection failures and, optionally, the number of unique client connection failures that constitute failure of the real server.
`Router(config-slb-real)# maxclients number-conns`	(Optional) Specifies the maximum number of entries in the IOS SLB RADIUS framed-IP sticky database that can be assigned to an individual real server.
`Router(config-slb-real)# inservice`	Enables the real server for use by IOS SLB.

The code below represents an example of configuring a server farm and a real server on the RLB:

```
!
ip slb serverfarm GPRS-SSGs
 nat server
 failaction radius reassign
 probe PROBE1
 !
 real 10.113.0.16
  weight 1
  reassign 2
  faildetect numconns 8 numclients 1
  maxclients 10000
  inservice
 !
```

Configuring a Virtual Server

To configure the virtual servers on the RLB, use the following commands beginning in global configuration mode:

Command	Purpose
`Router(config)# ip slb vserver virtual_server`	Identifies a virtual server and initiates virtual server configuration mode.
`Router(config-slb-vserver)# virtual ip-addr [netmask] {tcp | udp} [port | all | isakmp | wsp | wsp-wtp | wsp-wtls |wsp-wtp-wtls] [service service]`	Specifies the virtual server IP address, type of connection, and optional TCP or UDP port number, ISAKMP or WSP setting, and service coupling.
`Router(config-slb-vserver)# serverfarm primary-farm [backup backup-farm [sticky]]`	Associates a real server farm with a virtual server and optionally configures a backup server farm and specifies that sticky connections are to be used in the backup server farm.

Command	Purpose
`Router(config-slb-vserver)# sticky {duration [group group-id] [netmask netmask] | radius framed-ip [group group-id]}`	Specifies that connections from the same client use the same real server as long as the interval between client connections does not exceed the specified duration.
`Router(config-slb-vserver)# idle [radius {session | framed-ip}] duration`	Specifies the minimum amount of time IOS SLB maintains connection context in the absence of packet activity.
`Router(config-slb-vserver)# purge [radius {session | framed-ip}] acct on-off`	Prevents RLB from deleting information about sticky connections. **Note** The GGSN can send accouting on and off messages when powered on or shut down. On receiving these messages, the RLB would delete information about sticky connections. This command purges these GGSN messages to preserve RLB sticky connections.
`Router(config-slb-vserver)# access interface route framed-ip`	Enables framed-IP routing to inspect the ingress interface.
`Router(config-slb-vserver)# replicate casa listen-ip remote-ip port [interval] [password [0 | 7] password timeout]`	Configures a stateful backup of IOS SLB decision tables to a backup switch.
`Router(config-slb-vserver)# inservice`	Enables the virtual server for use by IOS SLB.

The code below represents an example of configuring a virtual server on the RLB:

```
!
ip slb vserver GPRS-RLB-ACCT
 virtual 10.7.7.15 udp 1646 service radius
 serverfarm GPRS-SSGs
 sticky radius framed-ip group 1
 idle radius framed-ip 3600
 purge radius framed-ip acct on-off
 access Vlan16 route framed-ip
 replicate casa 10.113.0.22 10.113.0.23 33333
 inservice standby rlb-csg
!
```

Configuring Probes

Configure probes to verify connectivity and to detect SSG failures. By default, no probes are configured in IOS SLB. To configure a probe, enter the following commands in order, beginning in global configuration mode:

Command	Purpose
`Router(config)# ip slb probe probe {dns | http | ping | tcp | wsp}`	Configures the IOS SLB probe name and changes to probe configuration submode.
`Router(config-slb-probe)# address [ip-addr]`	(Optional) Configures an IP address to which to send the probe.
`Router(config-slb-probe)# interval seconds`	(Optional) Configures the probe transmit timers.
`Router(config-slb-probe)# faildetect pings`	Specifies the number of consecutive unacknowledged pings that constitute failure of the real server or firewall.

The code below represents an example of configuring a probe on the RLB:

```
!
ip slb probe PROBE1 ping
 address 10.119.0.11
 interval 15
 faildetect 4
!
```

Enabling IOS SLB to Inspect Packets for RADIUS Framed-IP Sticky Routing

You can enable IOS SLB to inspect packets with source IP addresses that match a configured IP address and subnet mask. If the source IP address of an inspected packet matches an entry in the IOS SLB RADIUS framed-IP sticky database, IOS SLB uses that entry to route the packet; otherwise, IOS routes the packet.

To enable IOS SLB to inspect packets for routing using the RADIUS framed-IP sticky database, enter the following command in global configuration mode:

Command	Purpose
`Router(config)# ip slb route` *ip-addr netmask* `framed-ip`	Enables IOS SLB to route packets using the RADIUS framed-IP sticky database.

The code below represents an example of configuring framed-IP sticky routing on the RLB:

```
!
ip slb route 192.168.0.0 255.0.0.0 framed-ip
!
```

SSG Configuration Guidelines

Prior to configuring the SSG, the SSG image must be installed on the router and the FastEthernet port IP addresses must be configured using the **ip address** *ip-address network-mask* command. To enable the SSG, use the **ssg enable** command in the global configuration mode.

The following tasks are presented in this section:

Note For detailed information on configuring the SSG, refer to: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122b/122b_4/122b4_sg/ft_ssg.htm

Configuring Security

To configure security for SSG, use the following commands beginning in global configuration mode:

Command	Purpose
`Router(config)# aaa new-model`	Enables AAA
`Router(config)# aaa authorization config-commands`	Reestablishes the default created when the **aaa authorization commands** command was issued.
`Router(config)# aaa authorization network default group radius`	Specifies that RADIUS is the default authorization used for all network-related requests.
`Router(config)# ssg service-password` *password*	Sets the password used to authenticate the SSG with the local AAA server service profiles. This value must match the value configured for the AAA server service profiles.
`Router(config)# ssg radius-helper key` *key*	Sets the RADIUS shared secret key between SSG and SESM.
`Router(config)# ssg radius-helper [auth-port` *UDP-port-number*`] [acct-port` *UDP-port-number*`]`	Specifies the UDP default port numbers for a RADIUS authentication server (1645) and accounting server (1646).

Command	Purpose
Router(config)# **radius-server host** *{hostname | ip-address}* [**auth-port** *UDP-port-number*] [**acct-port** *UDP-port-number*]	Specifies the RADIUS server host.
Router(config)# **radius-server key** *AAAPassword*	Sets the RADIUS shared secret between the SSG and the local AAA server.

The code below represents an example of configuring security on the SSG:

```
!
aaa new-model
aaa authentication ppp default group radius
aaa authorization config-commands
aaa authorization network default group radius
aaa authorization network ssg_aaa_author_internal_list none
aaa authorization configuration default group radius
aaa accounting network default start-stop group radius
aaa accounting system default start-stop broadcast group radius
!
ssg service-password cisco
ssg radius-helper auth-port 1645 acct-port 1646
ssg radius-helper key gociscogo
!
radius-server host 172.20.51.11F auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server timeout 1
radius-server key gociscogo
!
```

Configuring the Default Network

The SESM, AAA server, CW4MW, BMA, and prepaid server reside in the default network. To assign the default network, use the following command in global configuration mode:

Command	Purpose
Router(config)# **ssg default-network** *ip-address netmask*	Sets the IP address or subnet that users are able to access without authentication. A mask provided with the IP address specifies the range of IP addresses that users can access without authentication.

The code below represents an example of configuring the default network on the SSG:

```
!
ssg default-network 10.13.0.0 255.255.255.0
!
```

Configuring the Access Network

Mobile wireless subscribers belong to the access network. To specify a downlink interface to the access network, use the following commands beginning in global configuration mode:

Command	Purpose
Router(config)# **ssg bind direction downlink {ATM** *atm-interface* | **Async** *async-interface* | **BVI** *bvi-interface* | **Dialer** *dialer-interface* | **Ethernet** *ethernet-interface* | **FastEthernet** *fastethernet-interface* | **Group-Async** *group-async-interface* | **Lex** *lex-interface* | **Loopback** *loopback-interface* | **Multilink** *multilink-interface* | **Null** *null-interface* | **Port-channel** *port-channel-interface* | **Tunnel** *tunnel-interface* | **Virtual-Access** *virtual-access-interface* | **Virtual-Template** *virtual-template-interface* | **Virtual-TokenRing** *virtual-tokenring-interface***}**	Specifies the downlink interface to the subscribers in the access network.

The code below represents an example of configuring the access network on the SSG:

```
!
ssg bind direction downlink BVI2
!
```

Configuring the Services Network

Network services, such as the pass-through service, are part of the services network. Configure one network for each service. The services networks are connected via the services VLAN. All interfaces connected to the services must be configured on the uplink interfaces. To configure the uplink interface (services network), use the following commands beginning in global configuration mode:

Command	Purpose
Router(config)# **ssg bind direction uplink {ATM** *atm-interface* | **Async** *async-interface* | **BVI** *bvi-interface* | **Dialer** *dialer-interface* | **Ethernet** *ethernet-interface* | **FastEthernet** *fastethernet-interface* | **Group-Async** *group-async-interface* | **Lex** *lex-interface* | **Loopback** *loopback-interface* | **Multilink** *multilink-interface* | **Null** *null-interface* | **Port-channel** *port-channel-interface* | **Tunnel** *tunnel-interface* | **Virtual-Access** *virtual-access-interface* | **Virtual-Template** *virtual-template-interface* | **Virtual-TokenRing** *virtual-tokenring-interface***}**	Specifies the uplink interface to the services network.

Note To verify the SSG interfaces configuration, use the **show ssg direction** command.

The code below represents an example of configuring the services network on the SSG:

```
!
ssg bind direction uplink BVI1
!
```

Enabling SSG User Profile Caching

Enabling SSG user profile caching allows the SSG to cache the user profiles of non-PPP users. User profiles of PPP and RADIUS proxy users are cached by the SSG by default. In situations in which the user profile is not available from other sources, SSG user profile caching makes the user profile available for RADIUS status queries and provides support for single sign-on functionality and failover from one SESM to another.

Note SSG user profile caching is required only when the SESM is used in RADIUS mode.

To enable SSG user-profile caching, use the following command in global configuration mode:

Command	Purpose
`Router(config)# ssg profile-cache`	Enables the caching of user profiles for non-PPP users.

Configuring the SSG to Support L2TP Service

The SSG can be configured to support L2TP service. With this configuration, when a subscriber selects a service through the SESM, the router serves as an L2TP access concentrator (LAC) and sends the PPP session through the service-specific L2TP tunnel. If the tunnel does not already exist, the LAC creates the proper tunnel to the LNS.

To configure the SSG to support L2TP, perform the following tasks:

- Configure the SSG as a LAC
- Configure RADIUS profiles for SSG support of L2TP
- Configure the LNS (LNS is not part of CMX framework)

Configuring the SSG as a LAC

To configure the SSG as a LAC, use the following command in global configuration mode:

Command	Purpose
`Router(config)# vpdn enable`	Enables L2TP functionality.

Configuring RADIUS Profiles for SSG Support of L2TP

The following vendor-specific attributes (VSAs) are used by the SSG to support L2TP:

- Cisco-AVpair VPDN
- Account-Info VPDN
- Service-Info VPDN

Cisco-AVpair VPDN Attributes

Table 5-1 lists the Cisco-AVpair attributes used in the service profile to configure VPDN.

Table 5-1 Cisco-AVpair VPDN Attributes

Attribute	Description
VPDN IP Address	Specifies the IP address of the home gateway (LNS) to receive the L2TP connections.
VPDN Tunnel ID	Specifies the name of the tunnel that must match the tunnel ID specified in the LNS VPDN group.
L2TP Tunnel Password	Specifies the secret (password) used for L2TP tunnel authentication.

Account-Info VPDN Attributes

Table 5-2 lists the Account-Info attributes used in the user profile to subscribe the user to a VPDN.

Table 5-2 Account-Info VPDN Attributes

Attribute	Description
Auto Service	(Reply attribute) Subscribes the user to a service and automatically logs the user in to the service when the user accesses the SESM. Multiple instances of this attribute can occur within a single user profile. Use one attribute for each service to which the user is subscribed.
Service Name	Specifies the name of the tunnel that must match the tunnel ID specified in the LNS VPDN group.

Service-Info VPDN Attributes

Table 5-3 lists the Service-Info attributes used in the service profile to define the L2TP service parameter.

Table 5-3 Service-Info VPDN Attributes

Attribute	Description
Type of Service	Specifies proxy, tunnel, or pass-through service. L2TP always uses tunneled service.
MTU Size	Specifies the PP maximum transmission unit (MTU) size for the SSG as a LAC. By default, the PPP MTU size is 1500 bytes.
Service Route	Specifies the networks available to the user for this service.

Configuring SSG Auto-logon Using Proxy RADIUS

To configure the SSG auto-logon using proxy RADIUS, use the following commands beginning in global configuration mode:

Command	Purpose
`Router(config)# ip cef`	Enables CEF. **Note** SSG works with CEF switching technology to provide maximum Layer 3 switching performance. Because CEF is topology-driven rather than traffic-driven, its performance is unaffected by network size or dynamics.
`Router(config)# ssg enable`	Enables SSG functionality.
`Router(config)# ssg radius-proxy`	Enables SSG RADIUS proxy and enters SSG RADIUS proxy mode.
`Router(config-radius-proxy)# server-port [auth` *auth-port*`] [acct` *acct-port*`]`	Configures the authentication and accounting ports. • **auth**—(Optional) Configures the authentication port. • *auth-port*—(Optional) Specifies the authentication port number. The default authentication port is 1645. The valid range is 0 to 65535. • **acct**—(Optional) Configures the accounting port. • *acct-port*—(Optional) Specifies the accounting port number. The default accounting port is 1646. The valid range is 0 to 65535.
`Router(config-radius-proxy)# client-address` *ip-address* `key` *secret*	Configures the client IP address and the shared key secret of a RADIUS client. • *ip-address*—IP address of a RADIUS client. • **key**—Shared secret with the RADIUS client. • *secret*—Description of the shared secret.
`Router(config-radius-proxy)# forward accounting-start-stop`	(Optional) Proxies accounting start/stop/update packets generated by any RADIUS clients to the AAA server.

The code below represents an example of configuring auto-logon using proxy RADIUS on the SSG:

```
!
ip cef
ssg enable
!
ssg radius-proxy
 server-port auth 1645 acct 1646
 client-address 5.5.5.33
  key gociscogo
 !
 client-address 10.5.5.19
  key gociscogo
 !
 forward accounting-start-stop
!
```

Enabling SSG TCP Redirect for Services

To configure the TCP redirect feature on the SSG, use the following commands beginning in global configuration mode:

Command	Purpose
`Router(config)# ip cef`	Enables CEF. **Note** SSG works with CEF switching technology to provide maximum Layer 3 switching performance. Because CEF is topology-driven rather than traffic-driven, its performance is unaffected by network size or dynamics.
`Router(config)# ssg enable`	Enables SSG functionality.
`Router(config)# ssg tcp-redirect`	Enables SSG TCP redirect.
`Router(config-ssg-redirect)# server-group` *group-name*	Defines the group of one or more servers that make up a named captive portal group and enters SSG-redirect-group configuration mode. • *group-name*—Name of the captive portal group.
`Router(config-ssg-redirect-group)# server` *ip-address port*	Adds a server to a captive portal group. • *ip-address*—IP address of the server to add to the captive portal group. • *port*—TCP port of the server to add to the captive portal group.
`Router(config-ssg-redirect)# redirect unauthenticated-user to` *group-name*	Selects a captive portal group for redirection of traffic from unauthenticated users. • *group-name*—Name of the captive portal group.
`Router(config-ssg-redirect)# port-list` *port-listname*	Defines the port list and enters SSG-redirect-port configuration mode. • *port-listname*—Defines the name of the port list.
`Router(config-ssg-redirect-port)# port` *port-number*	Adds a port to a port list. • *port-number*—Incoming destination port number. The valid range of port numbers is 1 to 65535.
`Router(config-ssg-redirect-port)# exit`	Exits SSG-redirect-port configuration mode.

Command	Purpose

`Router(config-ssg-redirect)# redirect port port-number to group-name`
or
`Router(config-ssg-redirect)# redirect port-list port-listname to group-name`
	Configures a TCP port or named TCP port list for SSG TCP redirection.
	• **port**—Specifies a TCP port to mark for SSG TCP redirection.
	• **port-list**—Specifies the named TCP port list to mark for SSG TCP redirection.
	• *port-number*—Specifies the incoming destination port number of the TCP port to mark for SSG TCP redirection.
	• *group-name*—Defines the name of the captive portal group to redirect packets that are marked for a destination port or named TCP port list.
	• *port-listname*—Specifies the name of the named TCP port list.

`Router(config-ssg-redirect)# redirect captivate initial default group group-name duration seconds`	Selects the default captive portal group for initial captivation of users upon initialization. • *group-name*—Name of the captive portal group. • *seconds*—The duration in seconds of the initial captivation. The valid range is 1 to 65,536 seconds.
`Router(config-ssg-redirect)# redirect captivate advertising default group group-name duration seconds frequency frequency`	Selects the default captive portal group for captivation of advertisements for users. • *group-name*—Name of the captive portal group. • *seconds*—The duration in seconds of the advertising captivation. The valid range is 1 to 65,536 seconds. • *frequency*—The frequency in seconds at which TCP packets are redirected to the captive portal group. The valid range is 1 to 65536 seconds.
`Router(config-ssg-redirect)# network-list network-listname`	Defines the network list and enters SSG-redirect-network configuration mode. • *network-listname*—Defines the name of the network list.
`Router(config-ssg-redirect-network)# network ip-address netmask`	Adds the specified IP address to the named network list. • *ip-address*—The IP address to add to a named network list.
`Router(config-ssg-redirect-network)# exit`	Exits SSG-redirect-network configuration mode.

Command	Purpose
`Router(config-ssg-redirect)# redirect unauthorized-service [destination network-list network-listname] to group-name`	Creates a list of destination IP networks that can be redirected by the named captive portal group. • (Optional) **destination network-list**—Checks incoming packets from authenticated hosts to networks that they are not authorized to access to determine if they need redirection. • (Optional) *network-listname*—Name of the list of destination IP networks. • *group-name*—Name of the captive portal group. **Note** If you do not specify a destination IP network by configuring the optional **destination network-list** keywords, the captive portal group specified in the *group-name* attribute is used as the default group for unauthorized service redirection when the IP address of the unauthorized packet does not fall into any network list associated with the captive portal group.
`Router(config-ssg-redirect)# redirect smtp group group-name [all | user]`	Selects a captive portal group for redirection of SMTP traffic. • group-name—Name of the captive portal group. • (Optional) all—All SMTP packets are forwarded. • (Optional) user—SMTP packets from users that have SMTP forwarding permission are forwarded. **Note** If you do not configure the optional **all** or **user** keywords, the default is **all**.

The code below represents an example of enabling TCP redirect on the SSG:

```
!
ssg tcp-redirect
 server-group RedirectServer
  server 10.13.0.13 8090
 !
 redirect unauthenticated-user to RedirectServer
!
```

Configuring the RADIUS Attributes for SSG TCP Redirect

Configure the RADIUS attributes in the user profiles on the AAA server. The user profile is downloaded from the AAA server as part of user authentication.

Table 5-4 lists vendor-specific attributes needed in the user profile to perform SSG TCP redirection.

Table 5-4 RADIUS Attributes for TCP Redirect

Feature Attribute ID	VendorID	SubAttrID	SubAttrName	SubAttrDataType	Account-Info Feature Code
26	9	250	Account-Info	String	R

Additional features allowed include the following:

- **"S"**—User has SMTP forwarding capability.
- **"I***group*;*duration*[;*service*]"—User has initial captivation capability. This attribute also indicates the duration of the captivation in seconds. If you specify the optional *service* field, initial captivation starts only when the user activates the named service.
- **"A***group*;*duration*;*frequency*[;*service*]"—User has advertisement captivation capability. Specifies the captive portal group to use and the duration and approximate frequency of the captivation in seconds. If you add the optional *service* field, advertisement captivation starts only when the user activates the named service active.

Configuring SSG Prepaid Billing

To configure SSG to provide the prepaid billing server with session ID and time-stamp information, use the following commands in global configuration mode:

Command	Purpose
`Router(config)# radius-server attribute 44 include-in-access-req`	Sends RADIUS attribute 44 (accounting session ID) in access request packets before performing user authentication (including requests for preauthentication).
`Router(config)#radius-server attribute 55 include-in-acct-req`	Sends RADIUS attribute 55 (event timestamp) in accounting packets.

Configuring Local Service Profiles

You can configure local service profiles in addition to the service profiles on the remote RADIUS server.

To configure a local service profile, use the following commands beginning in global configuration mode:

Command	Purpose
`Router(config)# local-profile profilename`	Configures a local RADIUS service profile. Enters profile configuration mode.
`Router(config-prof)# attribute radius-attribute-id [vendor-id] [cisco-vsa-type] attribute-value`	Configures an attribute in a local RADIUS service profile. **Note** Only attributes that can appear in RADIUS Access-Accept packets can be configured using the attribute command.

Configuring an Open Garden

A Web portal presents subscribers with a menu of services that they can access using a Web browser. An open garden is a part of the Web portal that is free of charge to subscribers who have not been authenticated. Examples of free services in the open garden include checking the status of the user connection and obtaining the current balance for prepaid services.

To configure an open garden, use the following commands beginning in global configuration mode:

Command	Purpose
`Router(config)# local-profile profilename`	Creates a local service profile and enters profile configuration mode.
`Router(config-prof)# attribute 26 9 251 "Rip-address;subnet-mask"` **Note** Repeat this step as necessary.	(Service Route attribute) Specifies the network available to the service. You can add multiple networks to an open garden service.
`Router(config-prof)# attribute 26 9 251 "Dip-address"`	(DNS server address attribute) Specifies the DNS server for the service. **Note** Enter this command twice to specify two DNS servers for DNS fault tolerance. SSG sends DNS requests to the first DNS server in its list. If the first server does not respond to the requests, SSG sends the requests to the second DNS server.
`Router(config-prof)# attribute 26 9 251 "Odomain-name"` **Note** Repeat step as necessary.	(Domain name attribute) Specifies the domain name that gets DNS resolution from the DNS server specified in Step 3. You can add multiple domain names to an open garden service.
`Router(config-prof)# exit`	Returns to global configuration mode.

Command	Purpose
`Router(config)# ssg open-garden profile-name`	Designates the service as an open garden service.
`Router(config)# ssg bind service service {ip-address | ATM atm-interface | Async async-interface | BVI bvi-interface | Dialer dialer-interface | Ethernet ethernet-interface | FastEthernet fastethernet-interface | Group-Async group-async-interface | Lex lex-interface | Loopback loopback-interface | Multilink multilink-interface | Null null-interface | Port-channel port-channel-interface | Tunnel tunnel-interface | Virtual-Access virtual-access-interface | Virtual-Template virtual-template-interface | Virtual-TokenRing virtual-tokenring-interface}`	Specifies the interface for a service. **Note** This step is required only if the open garden is routed through a next-hop gateway. Routes to the open garden network must be added to the routing table.

The code below represents an example of configuring an open garden network on the SSG:

```
!
ssg bind service opengarden1 10.111.0.15
ssg bind service ssg-gprs-passthru-service1 10.111.0.15
ssg bind service ssg-cisco-passthrough-service1 10.111.0.15
ssg bind service ssg-gprs-walled-service1 10.111.0.15
ssg open-garden opengarden1
!
local-profile opengarden1
  attribute 26 9 251 "R10.115.0.0;255.0.0.0"
!
```

SESM Configuration Guidelines

Prior to installing and configuring SESM, Solaris must be installed and configured with an IP address. To install and configure SESM, the following steps must be completed:

Step 1 Install the SESM.

Step 2 Configure the SESM with the SSG addresses (see note).

Note A typical SESM deployment consists of multiple SSGs. An SESM web application must know which SSG is handling each subscriber request. Each request arriving at an SESM web application contains a source IP address (also known as a client IP address). The SESM uses this client IP address to determine which SSG should handle each request. You must configure the associations between a subscriber request and its SSG.

Step 3 Configure captive portal, single sign-on, and port mapping.

Note For detailed information on configuring the SESM, visit http://www.cisco.com/univercd/cc/td/doc/solution/sesm/sesm_313/index.htm

FWLB Configuration Guidelines

The Firewall Load Balancer (FWLB) implements load balancing among the Service Selection Gateways (SSGs) similar to the load balancing in the RADIUS Load Balancer (RLB). See "RLB Configuration Guidelines" section on page 5-10. The FWLB uses the IOS server load balancing (SLB) feature to balance traffic flows to the SSGs. The SLB feature is used in the FWLB to ensure that traffic flows to the same SSG in the downlink direction that was used in the uplink direction.

To configure the FWLB for the CMX, use the following commands:

Command	Purpose
`Router(config)# ip slb probe name ping`	Places the user in ping probe configuration submode; the *name* string identifies the probe instance; maximum 15 characters long
`Router(config-slb-probe)# address ip-address`	In ping probe submode, *ip-address* is the destination intended to respond to the ping **Note** If this probe is associated with a server farm, and the address is not specified, the address is inherited from the server farm real servers. If this probe is associated with a firewall farm, the address must be specified.
`Router(config-slb-probe)# interval seconds`	(Optional) Configures the probe transmit timers
`Router(config)# ip slb firewallfarm name`	Places the user in firewall configuration submode
`Router(config-slb-sfarm)# probe name`	(Optional) Associates a probe with the real server

Command	Purpose
`Router(config-slb-sfarm)# real ip-address`	Identifies a real server by IP address as a member of a server farm and enters real firewall configuration submode
`Router(config-slb-real)# faildetect number`	Configures the number of consecutive unanswered pings before failing the real server
`Router(config-slb-real)# maxconns { udp | tcp number }`	(Optional) Specifies the maximum number of active connections allowed on the real server at one time
`Router(config-slb-real)# inservice`	Enables the real server for use by IOS SLB
sticky *duration*	(Optional) Specifies that connections from the same client use the same real server as long as the interval between client connections does not exceed the specified duration
idle *duration*	(Optional) Specifies the minimum amount of time IOS SLB maintains connection context in the absence of packet activity

The code below represents an example of configuring the default VLAN:

```
!
ip slb probe PING-PROBE1 ping
 address 10.111.0.16
 interval 600
!
!
ip slb firewallfarm FIRE
 inservice standby fwlb-ssg
 !
 real 10.111.0.16
  probe PING-PROBE1
  inservice
 !
!
 real 10.111.0.26
  probe PING-PROBE4
  inservice
 protocol tcp
  sticky 60 destination
 protocol datagram
  sticky 60 destination
 replicate casa 10.111.0.17 10.111.0.18 22222
```

CSG Configuration Guidelines

The CMX framework uses the Content Services Gateway (CSG) in two locations to provide two distinct functions. In the uplink direction, it assumes a position *before* the RADIUS Load Balancer (RLB) and the Service Selection Gateways (SSGs). This CSG provides reference data as a backup to the IP billing in the SSG (in case the SSG fails). A second CSG is positioned *after* the SSGs and the Firewall Load Balancer (FWLB) in the uplink direction. This CSG is positioned to provide content-based billing. Each of these CSGs has a redundant standby. In the reference topology shown in Figure 5-1 on page 5-2, CSG pair 1 and 2 provide the billing backup for the SSGs. The CSG pair 3 and 4 provide the content billing function (shown in Figure 5-2 on page 5-3).

The configuration guidelines for the Content Services Gateway (CSG) include the following categories:

- User groups
- Accounting policies
- Client/server connectivity
- CSG location and interface association
- Client-side VLAN
- Server-side VLAN
- Server farms
- Policies
- Filters
- Billing traffic (virtual servers)
- Fault tolerant group

For complete configuration details, use the guidelines provided in the *Content Services Gateway Installation and Configuration Guide*. This guide is available at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/mwg/csg/icfg221/bsconfig.htm

Configuring User Groups

To configure the CSG to record and generate accounting records, you must specify the user group(s) for which you want to generate accounting records. You also specify the user database that the CSG queries for user IDs.

To configure user groups on the CSG, and to specify the user database and RADIUS endpoint, use the following commands:

Command	Purpose
`Router# ip csg user-group group-name`	Creates a group of end users that you want to generate accounting records for.
`Router(config-csg-group)# database ip address port number`	Specifies the location of the user database, including its IP address and port number.
`Router(config-csg-group)# radius key secret`	Specifies and configures the CSG to be the RADIUS endpoint for accounting records and provides the key.
`Router(config-csg-group)# radius acct-port port`	Specifies the port number for the RADIUS accounting endpoint.

This example shows how to configure a CSG user group, database, and RADIUS endpoint:

```
ip csg user-group U1
 database 10.10.10.10 6666
 radius key secret
 radius acct-port 7777
```

Configuring and Activating Accounting Policies

To configure the CSG to record and generate accounting records, you need to define content-based client accounting as a service. This includes specifying the user group(s) you want to generate accounting records for, as well as the Billing Mediation Agent (BMA) to send accounting records to.

To configure the accounting policies on the CSG, use the following commands:

Command	Purpose
`Router# ip csg accounting name`	Defines content-based client accounting as a policy.
`Router(config-csg-acct)# user-group name`	Associates a user group with a specific accounting service.
`Router(config-csg-acct)# agent ip_address port number priority`	Specifies the primary or backup billing mediation agent to send accounting records to (including IP address, port numbe, and priority).
`Router(config-csg-acct)# inservice`	Activates the accounting service on a CSG.
`Router(config)# module ContentSwitcingModule number`	Specifies the CSG location on the router/switch.
`Router(config-module-csm)# csg accounting name`	Activates the accounting policy on the CSG.

This example shows how to define the CSG accounting policy:

```
!
ip csg accounting GGSN-BMA
 user-group MN-ID
 agent 172.18.41.70 3333 1
 agent 172.18.41.70 4444 2
 inservice
!
module ContentSwitchingModule 3
 csg accounting GGSN-BMA
```

Configuring Client-side VLAN

To configure client-side VLANs, use the following commands:

Caution You cannot use VLAN 1 as a client-side or server-side VLAN for the CSG.

Command	Purpose
`Router(config-module-csm)# vlan vlanid client`	Configures the client-side VLANs and enters the client VLAN mode[1].
`Router(config-slb-vlan-client)# ip ip-address netmask`	Configures an IP address to the CSG. This address is used by probes and ARP requests on this particular VLAN[2].
`Router(config-slb-vlan-client)# route ip-address netmask gateway gw-ip-address`	Configures a static route to reach the real clients if they are more than one Layer 3 hop away from the CSG.

1. Enter the **exit** command to leave a mode or submode. Enter the **end** command to return to the menu's top level.
2. The **no** form of this command restores the defaults.

This example shows how to configure the CSG for client-side VLANs:

```
!
 vlan 17 client
  ip address 10.17.17.29 255.255.255.0
  route 192.168.0.0 255.0.0.0 gateway 10.17.17.15
!
```

Configuring Server-side VLAN

To configure server-side VLANs, use the following commands:

Command	Purpose
`Router(config-module-csm)# vlan vlanid server`	Configures the server-side VLANs and enters the server VLAN mode[1].
`Router(config-slb-vlan-server)# ip ip-address netmask`	Configures an IP address for the server VLAN[2].
`Router(config-slb-vlan-server)# route ip-address netmask gateway gw-ip-address`	Configures a static route to reach the real servers if they are more than one Layer 3 hop away from the CSG.

1. Enter the **exit** command to leave a mode or submode. Enter the **end** command to return to the menu's top level.
2. The **no** form of this command restores the defaults.

This example shows how to configure the CSG for server-side VLANs:

```
!
 vlan 16 server
  ip address 10.16.16.29 255.255.255.0
  route 0.0.0.0 0.0.0.0 gateway 10.16.16.15
!
```

Configuring Server Farms

A server farm or server pool is a collection of servers that contain the same content. You specify the server farm name when you configure the server farm and when you bind the server farm to a virtual server.

To use the CSG billing feature, you must specify a server farm and associate it with any policies that you create. The server farm associated with a policy receives all the requests that match that policy.

To configure server farms on the CSG, use the following commands:

Command	Purpose
`Router(config-module-csm)# serverfarm` *serverfarm-name*	Creates and names a server farm and enters the server farm configuration mode[1] [2].
`Router(config-slb-sfarm)# predictor` *forward*	Configures the load-balancing prediction algorithm[2]. **Note** Be sure to specify **forward**.
`Router(config-slb-real)# inservice`	Enables the server farm.

1. Enter the **exit** command to leave a mode or submode. Enter the **end** command to return to the menu's top level.
2. The **no** form of this command restores the defaults.

This example shows how to configure a server farm for the CSG. This serverfarm, named RLB, uses the predictor forward algorithm, and has no NAT or client servers.

```
!
 serverfarm RLB
  no nat server
  no nat client
  predictor forward
!
```

Note Configure the CSG server farm without a real server. Configure no NAT server, no NAT client, and set the predictor forward.

Configuring Policies and Filters

Policies are access rules that traffic must match for a server farm. Policies allow the CSG to apply filters to certain types of traffic subject to the accounting service.

Note You must associate a server farm with a policy. A policy that does not have an associated server farm cannot forward traffic. The server farm associated with a policy receives all the requests that match that policy.

When the CSG is able to match policies, it selects the policy that appears first in the policy list. Policies are located in the policy list in the sequence in which they were bound to the virtual server. You can reorder the policies in the list by removing policies and reentering them in the correct order.

To configure accounting records policies and filters, use the following commands:

Command	Purpose
`Router(config-module-csm)# policy policy-name`	Creates the policy and enters the policy submode to configure the policy attributes[1].
`Router(config-slb-policy)# url-map name`	Specifies a URL map for the policy.
`Router(config-slb-policy)# serverfarm name`	Specifies a server farm for the policy.
`Router(config-slb-policy)# csg filter service name type <http | other> string ASCII string`	Specifies which type of accounting records should be generated, as well as the string to include in the accounting records.

1. Enter the **exit** command to leave a mode or submode. Enter the **end** command to return to the menu's top level.

The following example illustrates how to configure policies and filters on the CSG:

```
!
 map WALLED-GARDEN url
  match protocol http url *cisco*
  match protocol http url *billing*
!
 policy HTTP
  url-map WALLED-GARDEN
  serverfarm RLB
  csg filter EVENT-BMA type http string CSG3-HTTP
!
```

Tip A policy will not work unless the **csg filter** *name* parameter matches the the **ip csg accounting** *name* parameter. See "Configuring and Activating Accounting Policies" section on page 5-29.

Configuring Billing Traffic (Virtual Servers)

Virtual servers (Vservers) represent groups of real servers and are associated with real server farms through policies. The CSG uses Vservers to specify destinations for billing records.

Configuring virtual servers requires that you set the attributes of the virtual server specifying the default server farm (default policy) and that you associate other server farms through a list of policies. The default server farm (default policy) is used if a request does not match any CSG filter policy or if there are no policies associated with the virtual server.

Before you can associate a server farm with the virtual server, you must configure the server farm. Policies are processed in the order in which they are entered in the virtual server configuration.

Note Although all IP protocols have a protocol number, the CSG allows you to specify TCP or UDP by name instead of requiring you to enter their numbers.

To configure virtual servers, use the following commands:

Command	Purpose
`Router(config-module-csm)# vserver virtserver-name`	Identifies the virtual server and enters the virtual server configuration mode[1, 2].
`Router(config-slb-vserver)# virtual ip-address [ip-mask] protocol port-number [service ftp]` **Note** Billing is not enabled for **service ftp**	Sets the IP address for the virtual server optional port number or name and the connection coupling and type[2]. The *protocol* value is **tcp**, **udp**, **any** (no port-number is required), or a *number* value (no port-number is required).
`Router(config-slb-vserver)# serverfarm serverfarm-name` **Note** Supports predictor forward only.	Associates the default server farm with the virtual server[2 3]. Only one server farm is allowed. If the server farm is not specified, all the requests not matching any other policies will be discarded.
`Router(config-slb-vserver)# replicate csrp {sticky | connection}`	Configures CSRP replication for connection redundancy on the CSGs.
`Router(config-slb-vserver)# persistent rebalance`	Enables HTTP 1.1 persistence for connections in the virtual server. When a client connection fails during a transaction, the connection is *rebalanced* (using the load-balancing policy) to a new server in the server farm.
`Router(config-slb-vserver)# slb-policy policy name`	(Optional) Associates a filter policy with a virtual server[2].
`Router(config-slb-vserver)# inservice`	Enables the virtual server for use by the CSM[2].

1. Enter the **exit** command to leave a mode or submode. Enter the **end** command to return to the menu's top level.
2. The **no** form of this command restores the defaults.
3. These parameters refer to the default policy.

This example shows how to configure virtual servers on the CSG:

```
!
 vserver LNSINT
  virtual 10.103.0.0 255.0.0.0 any
  serverfarm RLB
  replicate csrp connection
  persistent rebalance
  slb-policy IP
  inservice
!
```

Configuring Fault Tolerant Group

This section describes a fault-tolerant configuration. In this configuration, two separate Catalyst 7600 devices each contain a CSG.

The client-side and server-side VLANs provide the fault-tolerant (redundant) connection paths between the CSG and routers on the client side and the servers on the server side. In a redundant configuration, two CSGs perform active and standby roles. Each CSG contains the same IP address, virtual server, and server farm. From the client-side and server-side networks, each CSG is configured identically. The network sees the fault-tolerant configuration as a single CSG.

Note When you configure multiple fault-tolerant CSG pairs, do not configure multiple CSG pairs to use the same FT VLAN. Use a different FT VLAN for each fault-tolerant CSG pair.

To configure a CSG for fault tolerance, use the following commands:

Command	Purpose
`Router(config-module-csm)# ft group` *ft-group-number* **vlan** *vlanid*	Assigns a VLAN to a fault tolerant group.
`Router(config-module-csm)# priority` *level*	Assigns a priority level to the CSG in a fault-tolerant pair of CSGs. The CSG with the highest priority level is the primary CSG.
`Router(config-module-csm)# heartbeat-time` *time*	Specifies number of seconds between heartbeat transmissions.
`Router(config-module-csm)# failover` *value*	Specifies number of seconds (default of 3) the CSG waits before assuming the mate CSG is not operational.
`Router(config-module-csm)# show module csm` *csm-number* **ft**	Displays statistics and counters for the CSG fault-tolerant pair.

This example shows how to configure fault tolerance on the CSG:

```
!
 ft group 1 vlan 256
  priority 20
!
 ft group 2 vlan 257
  priority 20
!
```

Refer to the *Content Services Gateway Installation and Configuration Guide* for a detailed description of fault tolerant configurations. This guide is available at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/mwg/csg/icfg221/bsconfig.htm

CHAPTER 6

CMX Sample Configurations

This chapter provides sample configurations for the Cisco Mobile Exchange (CMX).

Note Samples show configurations for the RADIUS Load Balancer (RLB), Service Selection Gateway (SSG), and Firewall Load Balancer (FWLB). Configurations for the Content Service Gateway (CSG) are embedded in the samples for RLB and FWLB. The AAA-RLB configures is contained in the FWLB sample. The samples listed in this section do not reflect the complete topology for the CMX framework and its redundant configuration.

For a complete description of the CMX commands in this chapter, refer to the *Cisco IOS Mobile Wireless Command Reference*. To locate documentation of other commands that appear in this chapter, use the command reference master index or search online.

This chapter includes the following sections:

RADIUS Load Balancer Sample Configuration

```
rlb-7600-1#sh run
Building configuration...

Current configuration : 15127 bytes
!
! Last configuration change at 08:02:50 EDT Thu Aug 8 2002
!
version 12.1
!
service timestamps debug datetime localtime show-timezone     ! Configures time stamps
service timestamps log datetime localtime show-timezone       ! for debug and log messages
no service password-encryption
!
hostname rlb-7600-1
!
boot system flash sup-bootflash:c6sup22-psv-mz.sticky
enable password lab
!
username cisco password 0 lab
clock timezone EST -5
clock summer-time EDT recurring
clock calendar-valid
vtp domain CMX
vtp mode transparent
ip subnet-zero
!
! CSG configuration begins here...
ip csg user-group MN-ID
!
ip csg accounting GGSN-BMA
 user-group MN-ID
 agent 10.18.56.40 4444 1
 agent 10.18.56.40 3333 2
 inservice
!
ip slb route 192.168.0.0 255.0.0.0 framed-ip   ! Enables IOS SLB to inspect packets for
                                               ! RADIUS framed IP sticky routing
!
ip slb probe PROBE1 ping     ! Configures probe to verify connectivity and detect failures
 faildetect 150
!
ip slb serverfarm GPRS-SSGs  ! Configures server farms for the SSG cluster
 nat server
 failaction radius reassign
 probe PROBE1
 !
 real 10.113.0.16                    !Configures real server in SSG server farm
  weight 1
  reassign 2
  faildetect numconns 8 numclients 1
  maxclients 10000
  inservice
 !
 real 10.113.0.24                    !Configures real server in SSG server farm
  weight 1
  reassign 2
  faildetect numconns 8 numclients 1
  maxclients 10000
  inservice
 !
 real 10.113.0.25                   ! Configures real server in SSG server farm
```

```
  weight 1
  reassign 2
  faildetect numconns 8 numclients 1
  maxclients 10000
  inservice
 !
 real 10.113.0.26                    ! Configures real server in SSG server farm
  weight 1
  reassign 2
  faildetect numconns 8 numclients 1
  maxclients 10000
  inservice
!
ip slb vserver GPRS-RLB-ACCT          ! Configures virtual server for the SSG server farm
 virtual 10.7.7.15 udp 1646 service radius
 serverfarm GPRS-SSGs
 sticky radius framed-ip group 1
 idle radius framed-ip 3600
 purge radius framed-ip acct on-off   ! Prevents RLB from deleting information about
                                      ! sticky connections caused by messages from GGSN
 access Vlan16 route framed-ip
 replicate casa 10.16.16.22 10.16.16.23 33333
 inservice standby rlb-csg
!
ip slb vserver GPRS-RLB-AR
 virtual 10.7.7.15 udp 1645 service radius
 serverfarm GPRS-SSGs
 sticky radius framed-ip group 1        ! Group 1 places the virtual server in the
                                        ! specified sticky group for coupling of
                                        ! services. In essence, the 'group' keyword and
                                        ! group-id argument tie multiple virtual servers
                                        ! together. Valid values range from 0 to 255.
 idle radius framed-ip 3600       ! Specifies the number of seconds the RLB keeps an entry
 purge radius framed-ip acct on-off
 access Vlan16 route framed-ip
 replicate casa 10.16.16.22 10.16.16.23 22222
 inservice standby rlb-csg
!
no spanning-tree vlan 16-17
spanning-tree vlan 113,256 priority 8192
spanning-tree vlan 2,14,113,256 forward-time 5
module ContentSwitchingModule 3
 csg accounting GGSN-BMA
 vlan 17 client
  ip address 10.17.17.29 255.255.255.0
  route 192.168.0.0 255.0.0.0 gateway 10.17.17.15
!
 vlan 16 server
  ip address 10.16.16.29 255.255.255.0
  route 0.0.0.0 0.0.0.0 gateway 10.16.16.15
!
 serverfarm RLB
  no nat server
  no nat client
  predictor forward
!
 policy IP
  serverfarm RLB
  csg filter GGSN-BMA string CSG1-IP
!
 vserver FORWARD-CLIENT
  virtual 0.0.0.0 0.0.0.0 any
  vlan 16
  serverfarm RLB
```

```
  replicate csrp connection
  persistent rebalance
  slb-policy IP
  inservice
!
 vserver FORWARD-SERVER
  virtual 0.0.0.0 0.0.0.0 any
  vlan 17
  serverfarm RLB
  replicate csrp connection
  persistent rebalance
  slb-policy IP
  inservice
!
 ft group 1 vlan 256
  priority 20
!
redundancy
 mode rpr-plus
 main-cpu
  auto-sync running-config
  auto-sync standard
error-detection swbus-timeout-duration 10
error-detection swbus-stall-duration 3
!
!
vlan 2,14,15,16,17,113,256
!
!
interface Port-channel1
 description trunk from RLB1 to RLB2
 no ip address
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 2,14,15,16,17,113,256
switchport mode trunk
!
interface Port-channel2
 description trunk from RLB1 to FWLB1
 no ip address
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 15
 switchport mode trunk
!
interface Port-channel3
 description trunk from RLB1 to FWLB2
 no ip address
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 15
 switchport mode trunk
!
interface GigabitEthernet1/2
 description trunk port to FWLB1 Gig1/2
 no ip address
 shutdown
!
interface FastEthernet4/1
 description trunk port to GGSN
 no ip address
 duplex full       ! On all Ethernet interfaces, set speed and duplex upfront to avoid any
                   ! auto negotiation when interface is brought up
 speed 100
```

```
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 2,14
 switchport mode trunk
!
interface FastEthernet4/2
 description port-channel 1 trunk to RLB2 Fast4/2
 no ip address
 duplex full
 speed 100
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 2,14,15,16,17,113,256
switchport mode trunk
 channel-group 1 mode on
!
interface FastEthernet4/3
 description port-channel 1 trunk to RLB2 Fast4/3
 no ip address
 duplex full
 speed 100
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 2,14,15,16,17,113,256
switchport mode trunk
 channel-group 1 mode on
!
interface FastEthernet4/5
 description port-channel 2 to FWLB1
 no ip address
 duplex full
 speed 100
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 15
 switchport mode trunk
 channel-group 2 mode on
!
interface FastEthernet4/6
 description port-channel 2 to FWLB1
 no ip address
 duplex full
 speed 100
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 15
 switchport mode trunk
 channel-group 2 mode on
!
interface FastEthernet4/9
 description port-channel 3 to FWLB2
 no ip address
 duplex full
 speed 100
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 15
 switchport mode trunk
 channel-group 3 mode on
!
interface FastEthernet4/10
 description port-channel 3 to FWLB2
 no ip address
 duplex full
```

```
 speed 100
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 15
 switchport mode trunk
 channel-group 3 mode on
!
interface FastEthernet4/13
 description SSG4 0/0 Host Side
 no ip address
 duplex full
 speed 100
 switchport
 switchport access vlan 113
!
interface FastEthernet4/14
 description SSG3 0/0 Host Side
 no ip address
 duplex full
 speed 100
 switchport
 switchport access vlan 113
!
interface FastEthernet4/16
 description SSG6 0/0 Host Side
 no ip address
 duplex full
 speed 100
 switchport
 switchport access vlan 113
!
interface FastEthernet4/17
 description SSG5 0/0 Host Side
 no ip address
 duplex full
 speed 100
 switchport
 switchport access vlan 113
!
interface Vlan2
 description VLAN 2 from RLBs to GGSNs
 ip address 10.2.2.22 255.255.255.0
 no ip redirects
 ip ospf hello-interval 2
 ip policy route-map ggsn-to-csg
!
interface Vlan14
 description VLAN 14 from RLBs to GGSNs
 ip address 10.14.14.22 255.255.255.0
 no ip redirects
 ip ospf hello-interval 2
 ip policy route-map ggsn-to-csg
!
interface Vlan15
 description Management VLAN 15
 ip address 10.15.15.10 255.255.255.0   ! Configure 10.15.15.11 on RLB2 router
 ip access-group 103 out                ! denies user data traffic over management VLAN 15
 no ip redirects
 standby delay minimum 0 reload 0
 standby 15 ip 10.15.15.15        ! HSRP IP address, group 15 must be same on RLB2 VLAN 15
 standby 15 priority 110 !  Sets priority for choosing active router; highest number
                         !  represents highest priority; set lower priority on RLB2.
 standby 15 preempt      !  Set so that when local router has higher priority than active
                         !  router, it assumes control as active router.
```

```
!
interface Vlan16
 description RLB1 VLAN 16
 ip address 10.16.16.22 255.255.255.0
 no ip redirects
 standby delay minimum 0 reload 0
 standby 16 ip 10.16.16.15            ! HSRP IP address, group 16 must be the same on RLB2
 standby 16 priority 110              ! Configure priority 100 on RLB2 router
 standby 16 preempt delay sync 5      ! Used to allow enough time for the RLB to exchange
                                      ! sticky DB information.
 standby 16 authentication rlb-csg    ! Configure same group and authentication on RLB2
 standby 16 name rlb-csg
!
interface Vlan17
 ip address 10.17.17.22 255.255.255.0
 no ip redirects
 standby delay minimum 0 reload 0
 standby 17 ip 10.17.17.15        ! HSRP IP address, group 17 must be same on RLB2 VLAN 17
 standby 17 priority 110          ! Configure lower priority on RLB2 router
 standby 17 preempt
 standby 17 authentication msfc-csg       ! Configure same on RLB2 router
!
interface Vlan113
 description VLAN 113 to SSGs BVI2
 ip address 10.113.0.22 255.255.255.0
 no ip redirects
 ip policy route-map ssg-to-csg
 standby delay minimum 0 reload 0
 standby 113 ip 10.113.0.15
 standby 113 priority 110
 standby 113 preempt
 standby 113 authentication RLB-bvi
 standby 113 name rlb-ssg
!
interface Vlan256
 description VLAN 256 from CSG1 to CSG2
 no ip address
!
router ospf 100
 router-id 10.2.2.22
 log-adjacency-changes
 redistribute connected metric 20 subnets    ! Specifies metric for OSPF to force traffic
                                             ! to go to RLB1; if RLB1 fails, traffic is
                                             ! routed to RLB2.
 redistribute static metric 20 subnets
 network 10.2.2.0 0.0.0.255 area 0
 network 10.14.14.0 0.0.0.255 area 0
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.15.15.15    ! non-user traffic to HSRP address on VLAN 15 FWLB
no ip http server
!
access-list 103 permit icmp any host 10.17.17.30
route-map ssg-to-csg permit 20
 match ip address 102
 set ip next-hop 10.16.16.30            ! CSG server 16 alias address
!
route-map ggsn-to-csg permit 20
 match ip address 101
 set ip next-hop 10.17.17.30            ! CSG client 17 alias address
!
snmp-server community public RO
snmp-server community private RW
snmp-server enable traps
```

```
snmp-server host 13.0.0.1 public        ! 13.0.0.1 address of network management server
!
line con 0
 exec-timeout 0 0
line vty 0
 exec-timeout 0 0
 login
line vty 1 4
 exec-timeout 0 0
 password lab
 login
!
!
monitor session 1 source interface Po1
monitor session 1 destination interface Fa4/48
end
```

Service Selection Gateway Sample Configuration

```
ssg5-7400#
ssg5-7400#sh run
Building configuration...

Current configuration : 4099 bytes
!
version 12.2
no parser cache
no service pad
service timestamps debug datetime localtime show-timezone
service timestamps log datetime localtime show-timezone
no service password-encryption
!
hostname ssg5-7400
!
logging buffered 1234567 debugging
aaa new-model        ! enables authentication, authorization, and accounting (AAA)
!
aaa authentication ppp default group radius        ! specifies AAA for PPP interfaces
! aaa authorization commands restrict user access to a network:
aaa authorization config-commands
aaa authorization network default group radius
aaa authorization network ssg_aaa_author_internal_list none
aaa authorization configuration default group radius
! aaa accounting commands enable AAA accounting for billing or security when using RADIUS:
aaa accounting network default start-stop group radius
aaa accounting system default start-stop broadcast group radius
aaa session-id common
enable password lab
!
username cisco password 0 cisco
clock timezone EST -5
clock summer-time EDT recurring
ip subnet-zero
!
!
ip ftp source-interface BVI1
ip ftp username pdsn-test
ip ftp password pdsnteam
!
ip cef
vpdn enable
vpdn authen-before-forward
!
! Baseline SSG Configuration:
ssg enable
ssg profile-cache
ssg pass-through
ssg pass-through filter 1 uplink
ssg pass-through filter 2 downlink
ssg default-network 10.13.0.0 255.255.255.0
ssg service-password cisco
ssg radius-helper auth-port 1645 acct-port 1646
ssg radius-helper key gociscogo
ssg port-map enable
ssg port-map destination range 8080 to 8100 ip 10.13.0.13
ssg port-map source ip 10.111.0.25
ssg bind service opengarden1 10.111.0.15
ssg bind service ssg-gprs-passthru-service1 10.111.0.15
ssg bind service ssg-cisco-passthrough-service1 10.111.0.15
ssg bind service ssg-gprs-walled-service1 10.111.0.15
```

```
ssg bind direction uplink BVI1
ssg bind direction downlink BVI2
ssg open-garden opengarden1
!
ssg radius-proxy
 server-port auth 1645 acct 1646
 client-address 5.5.5.33
  key gociscogo
 !
 client-address 10.5.5.19
  key gociscogo
 !
 forward accounting-start-stop
!
ssg tcp-redirect        ! TCP redirect configuration
 server-group RedirectServer
  server 10.13.0.13 8090
 !
 redirect unauthenticated-user to RedirectServer
!
local-profile opengarden1        ! local profile configuration
  attribute 26 9 251 "R10.115.0.0;255.0.0.0"
!
bridge irb        ! routes a protocol between routed interfaces and bridge groups
!
! Layer 2/Layer 3 interface configuration:
interface GigabitEthernet0/0
 no ip address
 keepalive 5
 duplex full
 speed 100
 media-type rj45
 bridge-group 2
!
interface GigabitEthernet0/1
 no ip address
 keepalive 5
 duplex full
 speed 100
 media-type rj45
 bridge-group 2
!
interface FastEthernet1/0
 no ip address
 keepalive 5
 duplex full
 speed 100
 bridge-group 1
!
interface FastEthernet1/1
 no ip address
 keepalive 5
 duplex full
 speed 100
 bridge-group 1
!
! To create a bridged virtual interface to other routed interfaces:
interface BVI1
 mac-address 0009.1153.1111
 ip address 10.111.0.25 255.255.255.0
!
interface BVI2
 mac-address 0009.1153.1113
 ip address 10.113.0.25 255.255.255.0
```

```
 ip nat inside
ip default-gateway 10.18.56.1        ! defines default gateway when IP routing is disabled
ip classless
ip route 0.0.0.0 0.0.0.0 10.111.0.15
ip route 10.2.2.0 255.255.255.0 10.113.0.15
ip route 10.5.5.19 255.255.255.255 10.113.0.15
ip route 5.5.5.33 255.255.255.255 10.113.0.15
ip route 10.7.7.15 255.255.255.255 10.113.0.15
ip route 10.77.208.0 255.255.255.0 10.111.0.15
ip route 10.89.240.0 255.255.254.0 10.111.0.15
ip route 10.11.11.0 255.255.255.0 10.111.0.15
ip route 10.14.14.0 255.255.255.0 10.113.0.15
ip route 10.101.0.0 255.0.0.0 10.111.0.15
ip route 172.19.0.0 255.0.0.0 10.111.0.15
ip route 192.168.0.0 255.0.0.0 10.113.0.15
no ip http server
ip pim bidir-enable
!
!
access-list 1 permit 10.113.0.23
access-list 1 permit 10.113.0.22
access-list 1 permit 10.115.0.12
!
snmp-server community public RO
snmp-server community private RW
!
! SSG RADIUS server configuration:
radius-server host 172.20.51.11 auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server timeout 1
radius-server key gociscogo
! Layer 2/3 bridge interface configuration:
bridge 1 protocol ieee
bridge 1 route ip
bridge 2 protocol ieee
bridge 2 route ip
call rsvp-sync
!
!
mgcp profile default
!
dial-peer cor custom
!
!
!
!
gatekeeper
 shutdown
!
```

Firewall Load Balancer Sample Configuration

```
fwlb-7600-1#
fwlb-7600-1#sh run
Building configuration...

Current configuration : 13839 bytes
!
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname fwlb-7600-1
!
diagnostic level complete
ip subnet-zero
!
ip csg user-group MN-ID
!
ip csg accounting EVENT-BMA
 user-group MN-ID
 agent 10.18.56.40 3333 1
 agent 10.18.56.40 4444 2
 inservice
!
ip slb probe PING-PROBE1 ping
 address 10.111.0.16           ! Configures probe for SSG 3
 interval 600
!
ip slb probe PING-PROBE2 ping
 address 10.111.0.24           ! Configures probe for SSG 4
 interval 600
!
ip slb probe PING-PROBE3 ping
 address 10.111.0.25           ! Configures probe for SSG 5
 interval 600
!
ip slb probe PING-PROBE4 ping
 address 10.111.0.26           ! Configures probe for SSG 6
 interval 600
!
ip slb probe PROBE-AAA ping
 interval 15
!
ip slb serverfarm AAA       ! Configures the AAA server farm
 nat server
 probe PROBE-AAA
 !
 real 10.18.41.70           ! Configures the real AAA server address
  weight 1
  faildetect numconns 8 numclients 1
  inservice
 !
 real 10.18.61.17           ! Configures the redundant real AAA server address
  weight 1
  faildetect numconns 8 numclients 1
  inservice
!
ip slb firewallfarm FIRE         ! Configures the firewall server farm
 inservice standby fwlb-ssg      ! See the standby 111 name fwlb-ssg on interface VLAN 111
 !
 real 10.111.0.16                ! IP address of SSG 3
```

```
  probe PING-PROBE1
  inservice
 !
 real 10.111.0.24                ! IP ddress of SSG 4
  probe PING-PROBE2
  inservice
 !
 real 10.111.0.25                ! IP ddress of SSG 5
  probe PING-PROBE3
  inservice
 !
 real 10.111.0.26                ! IP ddress of SSG 6
  probe PING-PROBE4
  inservice
 protocol tcp                    ! Configures TCP protocol and sticky connections
  sticky 500 destination
 protocol datagram               ! Configures datagram protocol and sticky connections
  sticky 500 destination
 replicate casa 10.111.0.17 10.111.0.18 22222
!
ip slb vserver AAA-RLB         ! Configures virtual server for load-balancing AAA messages
 virtual 10.120.0.15 udp 0 service radius    ! SSGs point to this address and port
 serverfarm AAA
 inservice standby fwlb-ssg
!
! Configures Spanning Tree Protocol for FWLB1 VLANs
spanning-tree vlan 7,111,121,257 priority 8192     Configure priority on FWLB2 to 16384
spanning-tree vlan 111 forward-time 7
spanning-tree vlan 121 forward-time 7
!
module ContentSwitchingModule 3
 csg accounting EVENT-BMA
vlan 7 client
  ip address 107.0.0.32 255.0.0.0
  route 192.168.0.0 255.0.0.0 gateway 10.107.0.15
  route 10.111.0.0 255.0.0.0 gateway 10.107.0.15
  route 10.113.0.0 255.0.0.0 gateway 10.107.0.15
  route 10.0.0.0 255.0.0.0 gateway 10.107.0.15
  route 10.122.0.0 255.0.0.0 gateway 10.107.0.15
  route 10.120.0.15 255.255.255.255 gateway 10.107.0.15
!
 vlan 121 server
  ip address 10.121.0.32 255.0.0.0
  route 0.0.0.0 0.0.0.0 gateway 10.121.0.11
!
 map WALLED-GARDEN url
  match protocol http url *cisco*
  match protocol http url *billing*
!
 serverfarm RLB
  no nat server
  no nat client
  predictor forward
!
 policy HTTP
  url-map WALLED-GARDEN
  serverfarm RLB
  csg filter EVENT-BMA type http string CSG3-HTTP
!
 policy IP
  serverfarm RLB
  csg filter EVENT-BMA string CSG3-IP
!
 vserver 115OPENGARDEN
```

```
  virtual 10.115.0.0 255.0.0.0 any
  serverfarm RLB
  replicate csrp connection
  persistent rebalance
  inservice
!
 vserver 117WALLEDGARDEN
  virtual 10.117.0.0 255.0.0.0 any
  serverfarm RLB
  replicate csrp connection
  persistent rebalance
  inservice
!
 ft group 2 vlan 257
  priority 20
!
!
redundancy
 mode rpr-plus
 main-cpu
  auto-sync running-config
  auto-sync standard
error-detection swbus-timeout-duration 10
error-detection swbus-stall-duration 3
!
!
! Configuration of physical interfaces follows...
interface Port-channel1
 description trunk from FWLB1 to FWLB2
 no ip address
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 7,111,257
 switchport mode trunk
!
interface Port-channel2
 description trunk from FWLB1 to RLB1
 no ip address
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 15
 switchport mode trunk
!
interface Port-channel3
 description trunk from FWLB1 to RLB2
 no ip address
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 15
 switchport mode trunk
!
interface FastEthernet4/1
 description port-channel 1 trunk to FWLB2 Fast4/1
 no ip address
 duplex full
 speed 100
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 7,111,257
 switchport mode trunk
 channel-group 1 mode on
!
interface FastEthernet4/2
 description port-channel 1 trunk to FWLB2 Fast4/2
```

```
 no ip address
 duplex full
 speed 100
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 7,111,257
 switchport mode trunk
 channel-group 1 mode on
!
interface FastEthernet4/5
 description port-channel 2 trunk to RLB1 Fast4/5
 no ip address
 duplex full
 speed 100
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 15
 switchport mode trunk
 channel-group 2 mode on
!
interface FastEthernet4/6
 description port-channel 2 trunk to RLB1 Fast4/6
 no ip address
 duplex full
 speed 100
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 15
 switchport mode trunk
 channel-group 2 mode on
!
interface FastEthernet4/9
 description port-channel 3 trunk to RLB2 Fast4/9
 no ip address
 duplex full
 speed 100
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 15
 switchport mode trunk
 channel-group 3 mode on
!
interface FastEthernet4/10
 description port-channel 3 trunk to RLB2 Fast4/10
 no ip address
 duplex full
 speed 100
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 15
 switchport mode trunk
 channel-group 3 mode on
!
interface FastEthernet4/14
 description SSG3 Service Side
 no ip address
 duplex full
 speed 100
 switchport
 switchport access vlan 111
!
interface FastEthernet4/16
 description SSG6 1/0 Service Side
 no ip address
```

```
 duplex full
 speed 100
 switchport
 switchport access vlan 111
!
interface FastEthernet4/17
 description SSG5 1/0 Service Side
 no ip address
 duplex full
 speed 100
 switchport
 switchport access vlan 111
!
interface FastEthernet4/48
 description trunk port to core router (services)
 no ip address
 duplex full
 speed 100
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 121
 switchport mode trunk
!
interface Vlan7
 ip address 10.107.0.17 255.255.255.0
 no ip redirects
 arp timeout 15
 standby 7 ip 10.107.0.15
 standby 7 priority 110
 standby 7 preempt delay minimum 25
 standby 7 authentication FwLB-WCC
 standby 7 track Vlan111
!
interface Vlan15
 description Management VLAN 15
 ip address 10.15.15.20 255.255.255.0   ! Configure 10.15.15.21 on FWLB2 router
 no ip redirects
 standby delay minimum 0 reload 0
 standby 5 ip 10.15.15.25       ! HSRP IP address, group 5 must be same on FWLB2 VLAN 15
 standby 5 priority 110  !  Sets priority for choosing active router; highest number
                         !  represents highest priority; set lower priority on FWLB2.
 standby 5 preempt       !  Set so that when local router has higher priority than active
                         !  router, it assumes control as active router.
!
interface Vlan111
 description VLAN 111 to SSGs BVI1
 ip address 10.111.0.17 255.255.255.0
 no ip redirects
 standby 111 ip 10.111.0.15
 standby 111 priority 110
 standby 111 preempt delay sync 20
 standby 111 authentication Fwlb-bvi
 standby 111 name fwlb-ssg
!
interface Vlan121
 no ip address
!
ip default-gateway 10.18.56.1
ip classless
ip route 10.13.0.0 255.0.0.0 10.107.0.30         ! Directs user traffic to CSG for billing
ip route 10.113.0.0 255.0.0.0 10.111.0.25
ip route 10.122.0.16 255.255.255.255 10.111.0.16
ip route 10.122.0.25 255.255.255.255 10.111.0.25
ip route 10.122.0.26 255.255.255.255 10.111.0.26
```

```
ip route 192.168.0.0 255.0.0.0 10.111.0.24
no ip http server
!
access-list 1 permit 192.168.0.2
snmp-server community public RO
snmp-server community private RW
snmp-server enable traps snmp-server host 172.18.56.40 public
!
line con 0
 exec-timeout 0 0
line vty 0 4
 login
!
end
```

CMX Timers and Counters

This appendix provides descriptions of CMX timers and counters for the CMX configuration shown in Figure 5-1 and Figure 5-2 on page 5-3:

The following rules should be used regarding timers:

- The sum of all GGSN RADIUS retransmissions must be less than the RLB idle session timer.
- The following timers should have the same value:
  - RLB idle framed-sticky timer
  - SSG idle timer
  - GGSN PDP idle timer
  - SESM idle timer
- The timer to re-allocate the same IP address on AAA should be greater than the idle timers for RLB, SSG, and GGSN
- FWLB timer for flows entries must be synchronized with TCP
- Round-trip for Access Request message (from GGSN to AAA through the SSG) should be much less than GTP T3-timer on SGSN
- OSPF timers on GGSN and MSFC (RLB) should be optimized for interface failover

Note Set speed and duplex values on all Ethernet interfaces before configuring timers and counters to avoid auto-negotiation when the interfaces are brought up.

This section provides descriptions of the following CMX timers and counters:

- 7609-1 (RLB1) Timers and Counters—Table A-1 on page A-2
- 7609-2 (RLB2) Timers and Counters—Table A-2 on page A-4
- SSG Timers and Counters—Table A-3 on page A-6
- 7609-3 (FWLB1) Timers and Counters—Table A-4 on page A-7
- 7609-4 (FWLB2) Timers and Counters—Table A-5 on page A-8
- CSG Timers and Counters—Table A-6 on page A-9

Table A-1 7609-1 (RLB1) Timers and Counters

Timer/Counter	Description	Range	Recommended
RLB: **idle radius request** *seconds*	Specifies the number of seconds the RLB keeps an entry for a particular RADIUS request if there is no activity	10-65535	30 (default)
RLB: **idle radius framed-ip** *seconds*	Specifies the number of seconds the RLB keeps an entry for a particular IP address if there is no acitivity	0-65535	3600
STP: **spanning-tree vlan** *rlb-ssg-vlan* **forward-time** *seconds*	Sets the spanning tree protocol (STP) forward delay time	4-30	7
STP: **spanning-tree vlan** *rlb-ssg-vlan* **hello-time** *seconds*	Sets the duration between the generation of configuration messages by the root switch	1-10	Default (2)
STP: **spanning-tree vlan** *rlb-ssg-vlan* **max-age** *seconds*	Sets the maximum number of seconds the information in a BPDU is valid	6-40	Default (20)
HSRP: **standby** *group-number* **preempt delay sync** *delay*	Specifies the maximum synchronization period in delay seconds; used to allow enough time for the RLB to exchange sticky database information; if the synchronization comes before the delay, the RLB preempts and becomes active	0-65535	5
HSRP: **standby delay minimum** *min-delay* **reload** *reload-delay*	Delays HSRP group initialization for a period after an interface-up event; reload delay applies to the first interface-up event after the router has reloaded; minimum delay applies to all subsequent interface-up events	0-3600	0 (minimum) 0 (reload)
HSRP: **standby** *group-number* **timers** *hellotime holdtime*	Specifies, in milliseconds, the hello and hold timers for HSRP	0-655535	3 (Default, hello) 10 (Default, hold)
OSPF: **ip ospf retransmit-interval** *seconds*	Specifies the time between link-state advertisement retransmissions for adjacent devices belonging to the interface	1-65535	Default (5)
OSPF: **ip ospf transmit delay** *seconds*	Sets the estimated time to transmit a link state update packet on the interface	1-65535	Default (1)
OSPF: **ip ospf hello-interval** *seconds*	Specifies the number of seconds between the hello packets that the Cicso IOS software sends on an OSPF interface	1-65535	2
OSPF: **ip ospf dead-interval** *seconds*	Specifies the number of seconds that a device must wait before it declares a neighbor OSPF router to be down because it has not received a hello packet	—	Default (4 times the value of **hello-interval**)
HSRP: **standby** *vlan* **priority** *counter*	Specifies value that prioritizes a potential Hot Standby router. The value 1 denotes the lowest priority and 255 denotes the highest priority. The router in the HSRP group with the highest priority value becomes the active router.	1-255	110

Timer/Counter	Description	Range	Recommended
RLB: **slb serverfarm faildetect numconns** *counter1* **numclients** *counter2*	Specifies the number of consecutive connection failures and, optionally, the number of unique client connection failures, that constitute failure of the real server. When RADIUS requests for a different MS exceed the value of*counter1*, the SSG is declared failed.	1-8	8 (numconns) 1 (numclients)
RLB: **slb real reassign** *counter*	Specifies threshold before RLB reassigns another SSG; after one RADIUS request retransmission from GGSN, RLB reassigns another SSG	1-8	2
OSPF: **redistribute connected metric** *m* **subnets**	Specifies the metric for OSPF to force the traffic to go to RLB1; if RLB1 fails, traffic is routed to RLB2	—	20
STP: **spanning-tree vlan** *ssg-downlink-vlan, csg-vlan* **priority** *priority-level*	Configures STP on a per-VLAN basis and specifies the STP priority level	—	8192

Table A-2 7609-2 (RLB2) Timers and Counters

Timer/Counter	Description	Range	Recommended
RLB: **idle radius request** *seconds*	Specifies the number of seconds the RLB keeps an entry for a particular RADIUS request if there is no activity	10-65535	30 (default)
RLB: **idle radius framed-ip** *seconds*	Specifies the number of seconds the RLB keeps an entry for a particular IP address if there is no acitivity	0-65535	36000 (10 hours)
STP: **spanning-tree vlan** *rlb-ssg-vlan* **forward-time** *seconds*	Sets the spanning tree protocol (STP) forward delay time	4-30	7
STP: **spanning-tree vlan** *rlb-ssg-vlan* **hello-time** *seconds*	Sets the duration between the generation of configuration messages by the root switch	1-10	Default (2)
STP: **spanning-tree vlan** *rlb-ssg-vlan* **max-age** *seconds*	Sets the maximum number of seconds the information in a BPDU is valid	6-40	Default (20)
HSRP: **standby delay minimum** *min-delay* **reload** *reload-delay*	Delays HSRP group initialization for a period after an interface-up event; reload delay applies to the first interface-up event after the router has reloaded; minimum delay applies to all subsequent interface-up events	0-3600	0 (minimum) 0 (reload)
HSRP: **standby** *group-number* **timers** *hellotime holdtime*	Specifies, in milliseconds, the hello and hold timers for HSRP	0-655535	3 (Default, hello) 10 (Default, hold)
OSPF: **ip ospf retransmit-interval** *seconds*	Specifies the time between link-state advertisement retransmissions for adjacent devices belonging to the interface	1-65535	Default (5)
OSPF: **ip ospf transmit delay** *seconds*	Sets the estimated time to transmit a link state update packet on the interface	1-65535	Default (1)
OSPF: **ip ospf hello-interval** *seconds*	Specifies the number of seconds between the hello packets that the Cicso IOS software sends on an OSPF interface	1-65535	2
HSRP: **standby** *vlan* **priority** *counter*	Specifies value that prioritizes a potential Hot Standby router. The value 1 denotes the lowest priority and 255 denotes the highest priority. The router in the HSRP group with the highest priority value becomes the active router.	1-255	100
RLB: **slb serverfarm faildetect numconns** *counter1* **numclients** *counter2*	Specifies the number of consecutive connection failures and, optionally, the number of unique client connection failures, that constitute failure of the real server. When RADIUS requests for a different MS exceed the value of*counter1*, the SSG is declared failed.	1-8	8 (numconns) 1 (numclients)
RLB: **slb real reassign** *counter*	Specifies threshold before RLB reassigns another SSG; after one RADIUS request retransmission from GGSN, RLB reassigns another SSG	1-8	2

Timer/Counter	Description	Range	Recommended
OSPF: **redistribute connected metric** *m* **subnets**	Specifies the metric for OSPF to force the traffic to go to RLB1; if RLB1 fails, traffic is routed to RLB2	—	30
STP: **spanning-tree vlan** *ssg-downlink-vlan*, *csg-vlan* **priority** *priority-level*	Configures STP on a per-VLAN basis and specifies the STP priority level	—	16384

Table A-3 SSG Timers and Counters

Timer/Counter	Description	Range	Recommended
RADIUS: **radius-server timeout** *seconds*	Specifies the number of seconds a router waits for a reply to a RADIUS request before retransmitting the request	1-1000 (seconds)	Default (3)
BVI: **bridge** *bridge-group* **hello-time** *seconds*	Specifies the interval between hello bridge protocol data units (BPDUs)	1-10	Default (1)
BVI: **bridge** *bridge-group* **max-age** *seconds*	Changes the amount of time a bridge waits for BPDUs from the root bridge	10-200	Default (15)
SSG: **ssg accounting interval** *timer*	Specifites interval in minutes between RADIUS interim update	1-655535	Default (10)
STP: **spanning-tree vlan** *rlb-ssg-vlan* **forward-time** *seconds*	Sets the spanning tree protocol (STP) forward delay time	4-30	7
STP: **spanning-tree vlan** *rlb-ssg-vlan* **hello-time** *seconds*	Sets the duration between the generation of configuration messages by the root switch	1-10	Default (2)
STP: **spanning-tree vlan** *rlb-ssg-vlan* **max-age** *seconds*	Sets the maximum number of seconds the information in a BPDU is valid	6-40	Default (20)
RADIUS: **radius-server retransmit** *counter*	Specifies the number of times the SSG transmits each RADIUS request to the server before giving up **Note** SSG does not retransmit the RADIUS messages proxied from GGSN	1-1000	2
BVI: **bridge 1 priority number** *counter*	Specifies the priority of the bridge for STP	0-64000	Default (32768)
BVI: **bridge 2 priority number** *counter*	Specifies the priority of the bridge for STP	0-64000	Default (32768)

Table A-4 7609-3 (FWLB1) Timers and Counters

Timer/Counter	Description	Range	Recommended
STP: **spanning-tree vlan** *ssg-fwlb-vlan* **forward-time** *delay*	Sets the STP forward delay time	4-30	7
STP: **spanning-tree vlan** *ssg-fwlb-vlan* **hello-time** *seconds*	Sets duration in seconds between the generation of configuration messages by the root switch	1-10	Default (2)
STP: **spanning-tree vlan** *ssg-fwlb-vlan* **max-age** *seconds*	Sets maximum number of seconds the information in a BPDU is valid	6-40	Default (20)
FWLB: **protocol tcp idle** *seconds*	Specifies the minimum amount of time in seconds the FWLB maintains connection information in the absence of packet activity	10-65535	60
FWLB: **protocol datagram idle** *seconds*	Specifies the minimum amount of time in seconds the FWLB maintains connection information in the absence of packet activity	10-65535	30
FWLB: **protocol tcp sticky** *seconds*	Assigns all connections from a client to the same SSG for the specified number of seconds; sticky object remains the specified number of seconds after the TCP connection is closed	10-65535	60
FWLB: **protocol datagram sticky** *timer*	Assigns all connections from a client to the same SSG for the the specified number of seconds	10-65535	60
FWLB: **ip slb probe PING-PROBE ping interval** *seconds*	Specifies interval in seconds between pings for the FWLB probe **Note** Ping probes are not needed in the CMX environment but must be configured in the FWLB to operate.		600
HSRP: **standby** *fwlb-ssg-vlan* **preempt delay sync** *seconds*	Specifies the maximum synchronization period in delay seconds; used to allow enough time for the FWLB to exchange sticky database information. If the synchronization comes before the delay, the FWLB preempts and becomes active.	0-65535	5
HSRP: **standby** *fwlb-ssg-vlan* **timers** *hellotime holdtime*	Specifies in milliseconds the hello and hold timers for HSRP	0-655535	3 (Default, hello) 10 (Default, hold)
RLB: **idle radius request** *seconds*	Specifies the number of seconds the RLB keeps an entry for a particular RADIUS request if there is no activity	00-65535	30 (Default)
HSRP: **standby** *vlan* **priority** *counter*	Specifies the HSRP priority		110 (FWLB1)
RLB: **slb real reassign** *counter*	Specifies threshold before RLB reassigns another AAA; after one RADIUS request retransmission from GGSN, RLB reassigns another AAA	1-8	2
STP: **spanning-tree vlan** *ssg-uplink-vlan, csg-vlan* **priority** *priority-level*	Configures STP on a per-VLAN basis and specifies the STP priority level	—	8192

Table A-5 7609-4 (FWLB2) Timers and Counters

Timer/Counter	Description	Range	Recommended
STP: **spanning-tree vlan** *ssg-fwlb-vlan* **forward-time** *delay*	Sets the STP forward delay time	4-30	7
STP: **spanning-tree vlan** *ssg-fwlb-vlan* **hello-time** *seconds*	Sets duration in seconds between the generation of configuration messages by the root switch	1-10	Default (2)
STP: **spanning-tree vlan** *ssg-fwlb-vlan* **max-age** *seconds*	Sets maximum number of seconds the information in a BPDU is valid	6-40	Default (20)
FWLB: **protocol tcp idle** *seconds*	Specifies the minimum amount of time in seconds the FWLB maintains connection information in the absence of packet activity	10-65535	60
FWLB: **protocol datagram idle** *seconds*	Specifies the minimum amount of time in seconds the FWLB maintains connection information in the absence of packet activity	10-65535	30
FWLB: **protocol tcp sticky** *seconds*	Assigns all connections from a client to the same SSG for the specified number of seconds; sticky object remains the specified number of seconds after the TCP connection is closed	10-65535	60
FWLB: **protocol datagram sticky** *timer*	Assigns all connections from a client to the same SSG for the the specified number of seconds	10-65535	60
FWLB: **ip slb probe PING-PROBE ping interval** *seconds*	Specifies interval in seconds between pings for the FWLB probe **Note** Ping probes are not needed in the CMX environment but must be configured in the FWLB to operate.		600
HSRP: **standby delay minimum** *min-delay* **reload** *reload-delay*	Delays HSRP group initialization for a period after an interface-up event; reload delay applies to the first interface-up event after the router has reloaded; minimum delay applies to all subsequent interface-up events	0-3600	30
HSRP: **standby** *rlb-ssg-vlan* **timers** *hellotime holdtime*	Specifies in milliseconds the hello and hold timers for HSRP	0-655535	3 (Default, hello) 10 (Default, hold)
RLB: **idle radius request** *seconds*	Specifies the number of seconds the RLB keeps an entry for a particular RADIUS request if there is no activity	10-65535	30 (Default)
HSRP: **standby** *vlan* **priority** *counter*	Specifies the HSRP priority		100
RLB: **slb real reassign** *counter*	Specifies threshold before RLB reassigns another AAA; after one RADIUS request retransmission from GGSN, RLB reassigns another AAA	1-8	2
STP: **spanning-tree vlan** *ssg-uplink-vlan, csg-vlan* **priority** *priority-level*	Configures STP on a per-VLAN basis and specifies the STP priority level	—	16384

Table A-6 CSG Timers and Counters

Timer/Counter	Description	Range	Recommended
FAILOVER: **ft failover** *seconds*	Sets the time for a standby CSG to wait before becoming an active CSG	1-65535	3 (Default)
FAILOVER: **ft heartbeat-time** *seconds*	Sets time interval between heartbeat transmissions in seconds	1-65535	1 (Default)
VSERVER: **idle** *seconds*	Sets time in seconds the CSG maintains connection information in the absence of packet activity; also indicates how long the CSG waits before sending the STATS CDR when there is no packet activity for a server; can be different between CSG 1/2 (used for backup of SSG) and CSG 3/4 (used for hot billing)	4-65535	4
FAILOVER: **ft group** *group-number* **vlan** *vlan-number* **priority** *counter*	Sets the priority for fault-tolerance	—	20 (CSG1/3) 10 (CGS2/4)

A

AAA Authentication, Authorization, and Accounting. A RADIUS-compliant server that authenticates and authorizes users and stores user service profiles. The AAA can allocate IP addresses for MSs and collect accounting records from SSGs.

Access Point Name See APN.

APN Access Point Name. Identifies a packet data network configured on a GGSN.

Authentication, Authorization, & Accounting See AAA.

B

Base Station Controller See BSC.

Base Station Subsystem See BSS.

Base Transceiver Station See BTS.

BGP Border Gateway Protocol. A gateway protocol that routers use to exchange various levels of information.

Border Gateway Protocol See BGP.

Bridged Virtual Interface See BVI.

BSC Base Station Controller. Equipment that manages radio resources in a GSM network (e.g., BTSs).

BSS Base Station Subsystem. A subsystem in a GSM network that refers to the combined functions of the BTS and BSC.

BTS Base Transceiver Station. The equipment in a GSM network that is used to transmit radio frequencies over the air waves.

BVI Bridged Virtual Interface. A virtual interface that provides a bridge between two physical interfaces on the SSG.

C

Call Detail Record See CDR.

Captive Portal A Web site that the owner positions as an entrance to other Internet sites. Typically, it offers free E-mail, search engines, instant messaging, personalized web pages, and web hosting. Captive portals are big revenue generators for content providers.

CASA Cisco Applications and Services Architecture. A protocol designed to allow network appliances to selectively control the flow of IP packets through participating forwarding agents (routers and switches).

CDMA Code Division Multiple Access. An access technology that combines each phone call with a code that only one cellular phone extracts from the air.

CDR Call Detail Record. A record providing details of a call.

Challenge Handshake Authentication Protocol See CHAP.

CHAP Challenge Handshake Authentication Protocol. An authentication method used when connecting to an ISP that uses a three-way handshake process and encrypted passwords.

Cisco Applications and Services Architecture See CASA.

Cisco Mobile Exchange See CMX.

CLI Command Line Interface. An interface that uses commands entered on a command line to configure and maintain network elements.

CMX Cisco Mobile Exchange. A network architecture based on Cisco's 6500/7600 switch/router that bridges the gap between the radio access networks and external packet data networks.

Code Division Multiple Access See CDMA.

Command Line Interface See CLI.

Content Services Gateway See CSG.

CSG Content Services Gateway. A Cisco high-speed processing module that provides content billing capability.

D

DHCP Dynamic Host Configuration Protocol. A TCP/IP protocol that enables PCs/workstations to use IP addresses from central servers for a predefined length of time; used by GGSN to assign an IP address to a mobile session.

DNS Domain Naming System. Mechanism for translating host computer names to IP addresses so users are not required to remember the IP address but a name instead.

Domain Naming System See DNS.

Dynamic Host Configuration Protocol See DHCP.

E

EIR Equipment Identity Record. Database used to validate equipment used in mobile telephone service with security features to block calls from stolen mobile stations.

Equipment Identity Record See EIR.

F

FDMA Frequency Division Multiple Access. Method that allocates a discreet amount of frequency to each user to permit many simultaneous conversations.

Frequency Division Multiple Access See FDMA.

G

Ga GPRS interface to a charging gateway or billing mediation agent using GTP.

Gateway GPRS Support Node See GGSN.

Gateway Mobile Switching Center See GMSC.

General Packet Radio Service See GPRS.

Generic Routing Encapsulation See GRE.

Gi GPRS interface that functions as a reference point between a GPRS network and an external PDN using IP.

GGSN Gateway GPRS Support Node. A wireless gateway in a GPRS network that allows mobile cell phone users to access the packet data network.

Global System for Mobile Communications See GSM.

GMSC Gateway MSC. An MSC that functions as a gateway to route an MS call to the MSC containing the called party HLR.

Gn GPRS interface between GSNs in a GPRS network that uses GTP as its protocol.

Gp GPRS interface between two GPRS networks that are interconnected using border gateways.

GPRS General Packet Radio Service. The data service for GSM networks.

GPRS Support Node See GSN.

GPRS Tunneling Protocol See GTP

GRE Generic Routing Encapsulation. Method of encapsulating one data packet inside another and used by tunnel servers to tunnel through the Internet to provide a secure VPN.

GSM Global System for Mobile Communications. Digital cellular telephone standard.

GSN GPRS Support Node. Generic term that refers to SGSNs and GGSNs in a GPRS network.

GTP GPRS Tunneling Protocol. A layer 3 tunneling protocol used between the SGSN and GGSN.

GTP′ An extension of GTP that reuses the GTP header and adds some new messages to provide a charging protocol between GSNs and a billing mediation agent.

H

HLR Home Location Register. Permanent SS7 database used in cellular networks to identify the subscriber, identify features or services subscribed, and track the current location of the mobile subscriber.

Home Location Register See HLR.

Hot Standby Router Protocol See HSRP.

HSRP Hot Standby Router Protocol. Cisco routing protocol for fault-tolerant IP routing that enables a set of routers to work together to present the appearance of a single virtual router to the hosts on a LAN; used in environments where critical applications are running and fault-tolerant networks have been designed.

I

ICMP Internet Control Message Protocol. A network-layer protocol that provides message packets to report errors and other information related to IP packet processing.

IMEI International Mobile Equipment Identity. Equipment ID that identifies a mobile station and is stored in the EIR.

IMSI International Mobile Subscriber Identity. 50-bit field that identifies a mobile subscriber's home country and carrier in a GSM network and is stored in the Subscriber Identity Module (SIM).

International Mobile Equipment Identity See IMEI.

International Mobile Subscriber Identity See IMSI.

Internet Control Message Protocol See ICMP.

Internetwork Operating System See IOS.

IOS Internetwork Operating System. Cisco’s operating system for routers.

ISDN User Part See ISUP.

ISUP ISDN User Part. The call control part of the SS7 protocol that is used to set up, coordinate, and take down trunk calls on an SS7 network.

L

L2TP Layer 2 Tunneling Protocol. Standard tunneling protocol for VPNs to provide secure node-to-node communications.

L2TP Access Concentrator See LAC.

L2TP Network Server See LNS.

LAC L2TP Access Concentrator. The access endpoint of an L2TP tunnel that is a peer to the L2TP network server (LNS).

LAPD Link Access Protocol on the D channel. Link level protocol for ISDN connections.

Layer 2 Tunneling Protocol See L2TP.

Link Access Protocol - D See LAPD.

LNS L2TP Network Server. The network endpoint of an L2TP tunnel that is a peer to the L2TP access concentrator (LAC).

M

MAP Mobile Application Part. Part of the SS7 protocol dealing with registration of roamers and intersystem hand-off procedures; uses TCAP over an SS7 network.

MD5 Message Digest 5. Algorithm that takes an input message of arbitrary length and outputs a 128-bit fingerprint that is used to compress large files in a secure manner before encrypting them with a private key under a public-key algorithm.

Message Digest 5 See MD5.

Mobile Application Part See MAP.

Mobile Station See MS.

Mobile Station ISDN Number See MSISDN.

Mobile Switching Center See MSC.

Mobile Terminal See MT.

MS Mobile station. Handset in a mobile wireless network.

MSC Mobile Switching Center. Switching center in a mobile wireless network.

MSFC Multilayer Switched Feature Card. The card in the Cisco 7600 series switch/router that provides the server load balancing function.

MSISDN Mobile Station ISDN. The telephone number of a mobile station.

Multilayer Switched Feature Card See MSFC.

MT Mobile Terminal. GSM/GPRS handset.

N

NAS Network Access Server. Server that aggregates mobile traffic from the radio access network and provides an interface to the Cisco Mobile Exchange; the GGSN in a GPRS network.

NAT Network Address Translation. Internet standard that enables a LAN to use one set of IP addresses for internal traffic and a second set of addresses for external traffic.

Network Access Server See NAS.

Network Address Translation See NAT.

Network and Switching Subsystem See NSS.

Network Time Protocol See NTP.

Node B Physical unit for radio transmission/reception with cells in the UTRAN.

Non-transparent mode Proxy mode that modifies a client request for access to provide additional services.

NSS Network and Switching Subsystem. The part of the GSM network that manages calls and connects to other networks through the GMSC.

NTP Network Time Protocol. Timing protocol that maintains a common time among Internet hosts in a network.

O

OMC Operations and Maintenance Center. Computer hardware and software that monitors and manages one part of a GSM/GPRS network (e.g., OMC-R manages the radio interface and OMC-G manages the GGSN interface).

Operations and Maintenance Center See OMC.

OSPF Open Shortest Path First. Link-state algorithm that is used to calculate routes based on the number of routers, transmission speed, delays, and route cost.

Open Shortest Path First See OSPF.

P

Packet Control Unit See PCU.

Packet Data Network See PDN.

Packet Data Protocol See PDP.

Packet Data Serving Node See PDSN.

Packet Data Unit See PDU.

PAP Password Authentication Protocol. Authentication method in which one router connects to another and sends a plain text login and password; see also CHAP.

Password Authentication Protocol See PAP.

PAT Port Address Translation. Feature that lets you number a LAN with inside local addresses and filter them through one globally routing IP address; also called NAT.

PCU Packet Control Unit. Unit in the base station controller that directs data traffic to the GPRS network.

PDA Personal Digital Assistant. Electronic device that performs functions such as personal database, calculator, and personal communicator.

PDN Packet Data Network. Generic term for a packet data network.

PDP Packet Data Protocol. GPRS term for a range of protocols (e.g., IP and PPP) that support the transfer of packet data over a 3G wireless cellular network.

PDP context The subscriber data stored in the HLR and MT that provides the context to establish a user session to a packet data network.

PDSN Packet Data Serving Node. Provides the primary wireless mobile data access to Internet and intranets using the CDMA2000 Radio Access Network environment.

PDU Protocol Data Unit. Generic term for a packet.

Personal Digital Assistant See PDA.

PLMN Public Land Mobile Network. Communications network for mobile telephones.

Port Address Translation See PAT.

PSTN Public Switched Telephone Network. Local and long distance telephone communication system in the public domain.

Public Land Mobile Network See PLMN.

Public Switched Telephone Network See PSTN.

R

Radio Network Controller See RNC.

Radio Network System See RNS.

RCA Remote Console Access. Cisco product that provides remote console access to CMX network elements.

Remote Authentication Dial-in User Service See RADIUS.

Remote Console Access See RCA.

Resource Manager Essentials See RME.

RADIUS Remote Authentication Dial-in User Service. Authentication and accounting system used by many ISPs for user ID/password authentication.

RADIUS Load Balancer See RLB.

RLB RADIUS Load Balancer. Cisco software and hardware that load-balances user traffic in the uplink direction and RADIUS messages among multiple Service Selection Gateways (SSGs).

RME Resource Manager Essentials. Part of the Cisco network management system that includes image download, display of system log events, and inventory changes.

RNC Radio Network Controller. Network element that controls one or more Node B transceiver stations in the UTRAN.

RNS Radio Network System. Network system controlled by an RNC.

S

Server Load Balancing See SLB.

Service Selection Dashboard See SSD.

Service Selection Gateway See SSG.

Serving GPRS Support Node See SGSN.

SESM Subscriber Edge Services Module. Cisco product that provides session authentication and service selection through a captive portal.

Simple Network Management Protocol See SNMP.

SLB Server Load Balancing. Cisco feature that balances the user traffic across multiple TCP/IP-based servers.

SNMP Simple Network Management Protocol. Common method by which network management applications can query a management agent using a supported management information base.

SGSN Serving GPRS Support Node. GPRS node that handles data to and from the MS, maintains MS location information, and communicates between the MS and the GGSN.

SSG Service Selection Gateway. Cisco product that acts as RADIUS proxy and enables service selection flexibility without the requirement to change APNs in a GPRS network.

SSD Service Selection Dashboard. Java-based application that presents users with a menu of services that they can log in and out of and enables service providers to bill based on time and services used rather than a flat rate.

Subscriber Edge Services Module See SESM.

Serving GPRS Support Node See SGSN.

T

TDMA Time Division Multiple Access. Technology that allocates a discrete amount of frequency bandwidth to each user to separate multiple conversation transmissions over a finite frequency spectrum.

Time Division Multiple Access See TDMA.

Transparent access Proxy mode that makes no modifications to a client request for access

U

UDP User Datagram Protocol. Layer 4 IP protocol that provides for exchange of datagrams without acknowledgements or guaranteed delivery and used to transport GTP packets between the GGSN and SGSN.

UE User Equipment. End user equipment in a UMTS network (equivalent to MS).

UMTS Universal Mobile Telecommunications System. Third generation wireless standard for supporting data transfer rates of 144 kbs (vehicular), 384 kbs (pedestrian), or up to 2 Mbs in buildings.

UMTS Terrestrial Radio Access Network See UTRAN.

Universal Mobile Telecommunications System See UMTS.

User Datagram Protocol See UDP.

User Equipment See UE.

USIM UMTS SIM. Subscriber identity module used in UMTS user equipment.

UTRAN UMTS Terrestrial RAN. Radio access network for UMTS networks.

V

Vendor Specific Attribute See VSA.

Virtual LAN See VLAN.

Virtual Private Network See VPN.

Visitor Location Register See VLR.

VLAN Virtual Local Area Network. LAN in which users on different physical LAN segments have priority access privileges across the LAN backbone, making them appear to be on the same physical LAN; the CMX uses three VLANs: access VLANs (user traffic and RADIUS traffic between GGSN and SSGs), services VLAN (user traffic toward SSGs), and default VLAN (SESM, AAA, CW4FM interconnections).

VLR Visitor Location Register. Local database maintained by cellular provider in whose territory the mobile subscriber is roaming.

VPN Virtual Private Network. Software-defined network running over a shared private network and offering the appearance (and same functionality) of a dedicated private network.

VSA Vendor Specific Attribute. An attribute that defines the operation of an SSG and is included in the Access-Accept message for user authentication; there are multiple types of VSAs.

Numerics

A

B

C

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V

W