Cisco BTS 10200 Softswitch System Security

Software Release 4.1, 4.2, 4.4.0/1 and 4.5

Revised: May 2, 2007 OL-5327-03

Americas 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: 408 527-0883

Text Part Number: OL-5327-03

CONTENTS

Preface

May 2, 2007 OL-5327-03

This document details the security packages applied to the Cisco BTS 10200 Softswitch. This document provides service providers and end users with a description of the security packages used on the Cisco BTS 10200 Softswitch to reduce the effectiveness of external attacks by "denial of service" or intrusion attempts.

This is an umbrella document for many general Cisco BTS 10200 Softswitch system extensions and improvements in the area of security.

Caution Altering these security packages after the delivery of the Cisco BTS 10200 Softswitch can create security issues in your network.

This document is organized as follows:

- Chapter 1, "Behaviors and Attributes"
- Chapter 2, "External Interfaces"
- Chapter 3, "Vulnerabilities in H.323 Message Processing"
- Chapter 4, "Authentication, Authorization and Accounting Support (Release 4.4)"
- Chapter 5, "Reduced Solaris Packages"

This document also provides a glossary and an index.

Modification History

Table 1 details the Cisco BTS 10200 Softswitch System Security modification history.

Table 1 System Security Modification History

Release	Modification
4.5	Added Solaris 10 section to Chapter 5. Added location and acceptability of sudo to page 1-2.
4.4	Added the following: • AAA Support—Chapter 4 • Reduced Solaris packages—Chapter 5
4.4.0/1	Added Reduced Solaris Packages section to Chapter 5.

Table 1 System Security Modification History (continued)

Release	Modification
4.2	No change.
4.1	System Security was introduced.

Scope

These security measures affect all nodes in the Cisco BTS 10200 Softswitch. They also impact the external adapter interfaces of the Element Management System (EMS) application within the Cisco BTS 10200 Softswitch including network access, user level authorization, authentication, and management.

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New* in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

CHAPTER 1

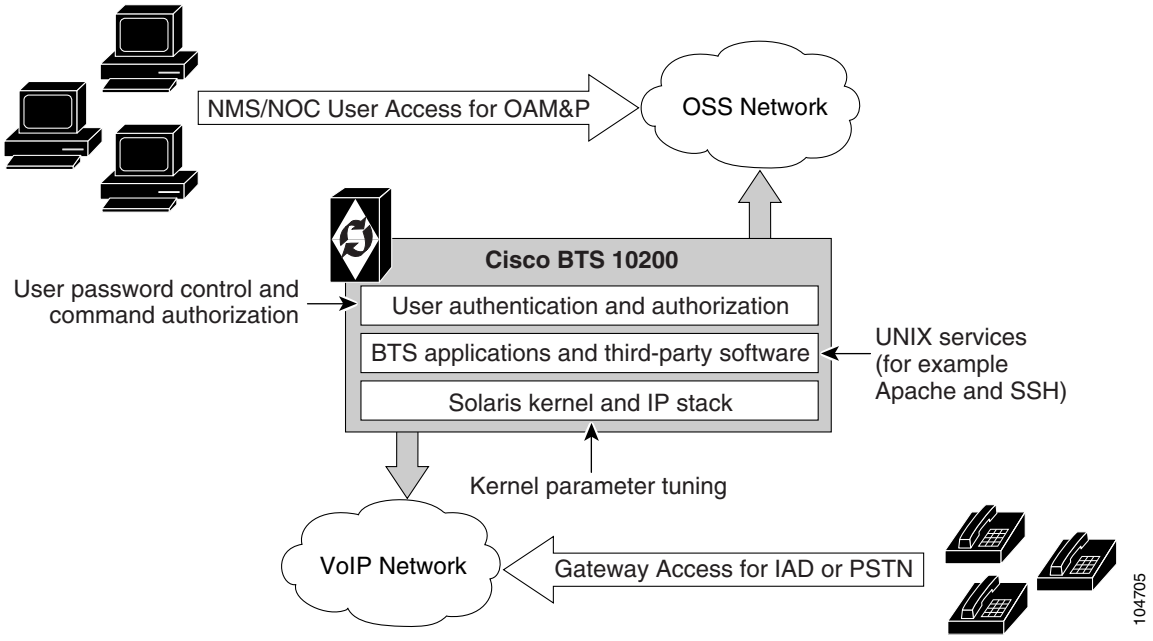
Behaviors and Attributes

May 2, 2007 OL-5327-03

This chapter details the behaviors and attributes of the various security packages in the Cisco BTS 10200 Softswitch. The sources for the items are derived from many dynamic sources. Included in these sources are security bulletins from third-party vendors to the Cisco BTS 10200 Softswitch as well as security agencies and open source organizations.

Security is an important part of the Cisco BTS 10200 Softswitch. The Cisco BTS 10200 Softswitch has interfaces to customer premise equipment (CPE) as well as northbound Operations Support System (OSS) interfaces. All of these interfaces are subject to attacks. In addition, users who are allowed onto the Cisco BTS 10200 Softswitch can also find ways to exploit applications that can lead to service-affecting situations. Therefore, many precautions are taken to ensure the solidity of the Cisco BTS 10200 Softswitch defenses while avoiding a system that is difficult to manage.

Figure 1-1 Cisco BTS 10200 Softswitch Access and Related Security



Adapter and User Security

This section describes requirements that generally involve adapter and user level of security. In the Cisco BTS 10200 Softswitch, adapters are any external, northbound interfaces of the Cisco BTS 10200 Softswitch. However, some extrapolated requirements involve adapter technology based on the current deployment:

- Support termination of a session once a provisionable inactivity timeout has occurred. An event report is issued upon each timeout expiry. The inactivity time ranges from 10 to 30 minutes.
- Restrict access as “root” to the Cisco BTS 10200 Softswitch in all cases except Cisco TAC and customer “administrator”. This is a broad statement that includes the addition of command-line interface (CLI) commands to help manage the system. In addition, UNIX services are restricted to harden the operating system (OS). The service restriction is listed in the Solaris OS Security and BTShard Package section. The process of restricting root access is an ongoing process.
- Use of "sudo" is acceptable and the formal Sun-built and packaged version is located in /opt/sfw/bin/.

Solaris OS Security and BTShard Package

This section details the security packages for the Cisco BTS 10200 Softswitch OS. These packages are automatically installed at installation. These packages are derived from both Sun Microsystems security bulletins and Cisco internal policies for safety of the OS and its applications. All services can be reactivated for the lifetime of the current kernel instance. All settings are reset on reboot of the kernel. These settings are contained in the BTShard Solaris package delivered with the Cisco BTS 10200 Softswitch.

- Remove unnecessary UNIX systems services. These services are listed below. Management of these facilities must allow for each service to be enabled or disabled on an individual basis. This service management must also be accomplished through the Cisco BTS 10200 Softswitch adapter interface.
  - FTP—FTP server is disabled and SFTP (Secure FTP) should be used. This impacts the Bulk Data Provisioning interface. It does not impact the Billing Bulk Data transfer. The FTP client code will still be available on the EMS node.
  - Telnet—This terminal protocol is disabled and SSH (Secure Shell) should be used. The telnet server and client code are still available on the EMS node.
  - Echo—This service is to be disabled. This capability has been replaced with Internet Control Message Protocol (ICMP) “ping” facilities.
  - Discard—This service is to be disabled.
  - Printer—This service is to be disabled. No printer services are supplied in the Cisco BTS 10200 product description.
  - Daytime—This service is to be disabled.
  - Chargen—This service is to be disabled.
  - SMTP—This service is to be disabled.
  - Time—This service is to be disabled.
  - Finger—This service is to be disabled. No network user facilities are required. The Cisco BTS 10200 tracks users internally and on a single BTS basis.

  - Sun RPC—This service is to be disabled. This may be enabled in a lab environment for Tooltalk usage in debugging application programs.
  - Exec—This service is to be disabled.
  - Login—This service is to be disabled.
  - Shell—This service is to be disabled. This may be required for some lab activity; however, there is no field usage for rlogin, rcp, and rsh facilities.
  - UUCP—This service is to be disabled.
  - NFS—This service is to be disabled.
  - Lockd—This service is to be disabled.
  - X11—This service is available for the near term *only*.
  - DTSCP—This service is to be disabled.
  - Font-services—This service is to be disabled.
  - HTTP—This service is to be enabled. This is used by the Cisco BTS 10200 Softswitch to offer results of report generation. This will migrate to HTTPS.

- The following UNIX accounts are to be LOCKED but not removed from the system: lp, uucp, nuucp, nobody, listen, and any other Cisco support accounts not used in the normal course of field operation. Services managed by root are the only accounts allowed to utilize one of these identities. This is the default behavior.
- Modifications to the Solaris kernel parameters were made to close potential breeches in the OS. These types of security precautions are most often geared toward "denial of service" attacks. These types of attacks create situations that degrade the performance of a system and as a result, prohibit the critical applications from delivering the service they are designed to provide.
- The TCP protocol uses random initial sequence numbers.
- All failed login attempts are logged.
- The following users are not allowed direct FTP access to the machine: root, daemon, bin, sys, adm, nobody, and noaccess.
- A root user cannot Telnet directly to the machine. Direct root user access is granted to the console only. A user who wants to access the root account must use the **su** command from a nonprivileged account.
- The break key (<STOP> <A>) on the keyboard is disabled.
- IP_FORWARD_DIRECTED_BROADCASTS—This option determines whether to forward broadcast packets directed to a specific net or subnet, if that net or subnet is directly connected to the machine. If the system is acting as a router, this option can be exploited to generate a great deal of broadcast network traffic. Turning this option off helps prevent broadcast traffic attacks. The Solaris default value is 1 (True). For example:

  ```
  ip_forward_directed_broadcasts=0
  ```

- IP_FORWARD_SRC_ROUTED—This option determines whether to forward packets that are source routed. These packets define the path the packet should take instead of allowing network routers to define the path. The Solaris default value is 1 (True). For example:

  ```
  ip_forward_src_routed=0
  ```

- IP_IGNORE_REDIRECT—This option determines whether to ignore the ICMP packets that define new routes. If the system is acting as a router, an attacker may send redirect messages to alter routing tables as part of sophisticated attack (man-in-the-middle attack) or a simple denial of service. The Solaris default value is 0 (False). For example:

  ```
  ip_ignore_redirect=1
  ```

- IP_IRE_FLUSH_INTERVAL—This option determines the period of time at which a specific route will be kept, even if currently in use. Address Resolution Protocol (ARP) attacks may be effective with the default interval. Shortening the time interval may reduce the effectiveness of attacks. The default interval is 1200000 milliseconds (20 minutes). For example:

  ```
  ip_ire_flush_interval=60000
  ```

- IP_RESPOND_TO_ADDRESS_MASK_BROADCAST—This option determines whether to respond to ICMP netmask requests which are typically sent by diskless clients when booting. An attacker may use the netmask information for determining network topology or the broadcast address for the subnet. The default value is 0 (False). For example:

  ```
  ip_respond_to_address_mask_broadcast=0
  ```

- IP_RESPOND_TO_ECHO_BROADCAST—This option determines whether to respond to ICMP broadcast echo requests (ping). An attacker may try to create a denial of service attack on subnets by sending many broadcast echo requests to which all systems will respond. This also provides information on systems that are available on the network. The Solaris default value is 1 (True). For example:

  ```
  ip_respond_to_echo_broadcast=1
  ```

- IP_RESPOND_TO_TIMESTAMP—This option determines whether to respond to ICMP timestamp requests which some systems use to discover the time on a remote system. An attacker may use the time information to schedule an attack at a period of time when the system may run a cron job (or other time-based event) or otherwise be busy. It may also be possible predict ID or sequence numbers that are based on the time of day for spoofing services. The Solaris default value is 1 (True). For example:

  ```
  ip_respond_to_timestamp=0
  ```

- IP_RESPOND_TO_TIMESTAMP_BROADCAST—This option determines whether to respond to ICMP broadcast timestamp requests which are used to discover the time on all systems in the broadcast range. This option is dangerous for the same reasons as responding to a single timestamp request. Additionally, an attacker may try to create a denial of service attack by generating many broadcast timestamp requests. The default value is 1 (True). For example:

  ```
  ip_respond_to_timestamp_broadcast=0
  ```

- IP_SEND_REDIRECTS—This option determines whether to send ICMP redirect messages which can introduce changes into the routing table of the remote system. It should only be used on systems that act as routers. The Solaris default value is 1 (True). For example:

  ```
  ip_send_redirects=0
  ```

- IP_STRICT_DST_MULTIHOMING—This option determines whether to enable strict destination multihoming. If this is set to 1 and ip_forwarding is set to 0, then a packet sent to an interface from which it did not arrive will be dropped. This setting prevents an attacker from passing packets across a machine with multiple interfaces that is not acting a router. The default value is 0 (False). For example:

  ```
  ip_strict_dst_multihoming=1
  ```

- TCP_CONN_REQ_MAX_Q0—This option determines the size of the queue containing half-open connections. This setting provides protection from SYN flood attacks. Solaris 2.6 and 7 (and 2.5.1 with patch 103582-12 and higher) include protection from these attacks. The queue size default is adequate for most systems but should be increased for busy web servers. The default value is 1024. For example:

  ```
  tcp_conn_req_max_q0=4096
  ```

- The following startup files are removed from the level "3" runtime environment of the Cisco BTS 10200 Softswitch. These services can still be started manually if required in laboratory circumstances. They are not required for field operations.
  - S71rpc
  - S73cachefs.daemon
  - S73nfs.client
  - S74autofs
  - S80lp
  - S80spc
  - S88sendmail
  - S93cacheos.finish
  - S99dtlogin

CERT Advisories and Network Security

This section covers the network security requirements for the Cisco BTS 10200 Softswitch. These requirements are derived from CERT and Cisco Systems internal policy. These requirements cover any access to the Cisco BTS 10200 Softswitch by IP interfaces, as well as all console access. These items are addressed in the BTSossh Solaris package and the SMCapache Solaris package that are delivered with the Cisco BTS 10200 Softswitch.

- Open Secure Shell (OpenSSH) must be updated to include the following CERT advisories. These are resolved in the current OpenSSH version 3.4.p1.
  - CA-2002-24—The description of the problem from the CERT-2002-24 advisory is: "The CERT/CC has received confirmation that some copies of the source code for the OpenSSH package were modified by an intruder and contain a Trojan horse." For more information, see the full CERT advisory at http://www.cert.org/advisories/CA-2002-24.html.
  - CA-2002-18—The description of the problem from the CERT-2002-18 advisory is: "There are two related vulnerabilities in the challenge response handling code in OpenSSH versions 2.3.1p1 through 3.3. They may allow a remote intruder to execute arbitrary code as the user running sshd (often root)." The first vulnerability affects OpenSSH versions 2.9.9 through 3.3 that have the challenge response option enabled, and use SKEY or BSD_AUTH authentication. The second vulnerability affects PAM modules using interactive keyboard authentication in OpenSSH versions 2.3.1p1 through 3.3, regardless of the challenge response option setting. For more information, see the full CERT advisory at http://www.cert.org/advisories/CA-2002-18.html.
- Open Secure Socket Layer (OpenSSL) must be updated to include the following CERT advisory. This is corrected in version 0.9.8 or later. This is contained in the BTSossl Solaris package bundled with BTSossh in the Cisco BTS 10200 Softswitch.

  - CA-2002-23—The description of the problem from the CERT-2002-23 advisory is: "There are four remotely exploitable buffer overflows in OpenSSL. There are also encoding problems in the ASN.1 library used by OpenSSL. Several of these vulnerabilities can be used by a remote attacker to execute arbitrary code on the target system. All can be used to create denial of service." For more information, see the full CERT advisory at http://www.cert.org/advisories/CA-2002-23.html.
  - CERT-2003-24—The description of the problem from the CERT-2003-24 advisory is: "There is a remotely exploitable vulnerability in a general buffer management function in versions of OpenSSH prior to 3.7.1. This may allow a remote attacker to corrupt heap memory which could cause a denial-of-service condition. It may also be possible for an attacker to execute arbitrary code." For more information, see the full CERT advisory at http://www.cert.org/advisories/CA-2003-24.html.
  - CERT-2003-26—The description of the problem from the CERT-2003-26 advisory is: "There are multiple vulnerabilities in different implementations of the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols. These vulnerabilities occur primarily in Abstract Syntax Notation One (ASN.1) parsing code. The most serious vulnerabilities may allow a remote attacker to execute arbitrary code. The common impact is denial of service." For more information, see the full CERT advisory at http://www.cert.org/advisories/CA-2003-26.html.

- The Apache web server must be updated to include the following CERT advisory. This is corrected in version 2.0.39 or later. The Solaris command **pkginfo -l SMCapache** indicates the current release level of the Apache package in the Cisco BTS 10200 Softswitch.
  - CA-2002-17—The description of the problem from the CERT-2003-26 advisory is: "There is a remotely exploitable vulnerability in the way that Apache web servers (or other web servers based on their source code) handle data encoded in chunks. This vulnerability is present by default in configurations of Apache web server versions 1.2.2 and later, 1.3 through 1.3.24, and versions 2.0 through 2.0.36. The impact of this vulnerability is dependent upon the software version and the hardware platform the server is running on." For more information, see the full CERT advisory at http://www.cert.org/advisories/CA-2002-17.html.

Secure FTP (SFTP) is the default method for bulk transfer of provisioning data to the Cisco BTS 10200 Softswitch. FTP is disabled as a default. The SFTP service is provided in the BTSossh Solaris package included in the Cisco BTS 10200 Softswitch.

CHAPTER 2

External Interfaces

May 2, 2007 OL-5327-03

This chapter details the extensions provided in the Cisco BTS 10200 Softswitch software to help users manage the UNIX services and security aspects of the Cisco BTS 10200 Softswitch.

Billing Interface

No direct impact is made to the billing application on the Cisco BTS 10200 Softswitch in this release of the security services document.

Operations

This section describes changes to the user interface as a result of the Cisco BTS 10200 Softswitch security services and impacts as to how the Cisco BTS 10200 Softswitch is deployed in lab situations. In addition to changes in the use of the Cisco BTS 10200 Softswitch, the indirect changes to the system (changes that cannot be directly observed) are also documented.

The most significant alteration for this release is that Secure Shell (SSH) is the default method of access to the Cisco BTS 10200 CLI/MAINT interfaces. This is changed from the Telnet interface used prior to this release. The use of SSH is documented in the *Cisco BTS 10200 Softswitch Operations, Maintenance and Troubleshooting Guide*.

Operator Interface

Additional commands have been added to manage the UNIX services in the Cisco BTS 10200 Softswitch. These commands are available from the CLI/MAINT interface. In addition, these same commands are also available from the CORBA and bulk-provisioning interface. There are no schemas and tables associated with these commands. They directly control the UNIX services. These services are only enabled for the lifetime of the current kernel instance. They are reset to the installed defaults when a kernel reboot is performed.

Table 2-1 describes the system services available using the node command.

Table 2-1 Node Command for UNIX Services

Noun	Verb	Options	Description
Node	Change	SERVICE [Required] Must be one of the following: FTP, TELNET, ECHO, DISCARD, PRINTER, DAYTIME, CHARGEN, SMTP, TIME, FINGER, SUNRPC, EXEC, LOGIN, SHELL, UUCP, NFS, LOCKD, X11, DTSCP, FONT-SERVICES, HTTP.	Defines the service to change.
Node	Change	ENABLE [Required]	A Boolean flag [Y/N] that indicates whether to turn this service on or off.
Node	Change	NODE [Required]	The node name in the Cisco BTS 10200 Softswitch where the service is managed.
Node	Show	SERVICE [Required] Must be one of the following: FTP, TELNET, ECHO, DISCARD, PRINTER, DAYTIME, CHARGEN, SMTP, TIME, FINGER, SUNRPC, EXEC, LOGIN, SHELL, UUCP, NFS, LOCKD, X11, DTSCP, FONT-SERVICES, HTTP.	Defines the service to display.
Node	Show	Node [Required]	Defines the node to display for the state of the service.

User Activity Commands

User activity commands are available to manage the users on the system. The activity timer for user sessions is not part of any schema or table. This is a system configuration token. Table 2-2 describes the Element Management System (EMS) command for idle session timeout.

Table 2-2 EMS Command for Idle Session Timeout

Noun	Verb	Options	Description
Session	Change	IDLE-SESSION [10-30]	Defines the number of minutes that a user can be idle on the CLI interface prior to being automatically logged off the Cisco BTS 10200 Softswitch.

Caution Altering user activities after the delivery of the Cisco BTS 10200 Softswitch can create security issues in your network.

Alarms

No alarms are changed or added with these security packages.

Measurements

No TMM or SNMP MIB changes are required with these security packages. Security logs and related information are accessed by alternate means for security.

Troubleshooting

There are no impacts to troubleshooting the Cisco BTS 10200 Softswitch as a result of these security packages. However, there are some issues with using SSH to access the system. All users of the system must have this software facility for access to the system. This includes any additional components to allow Windows-based PC software to access the Cisco BTS 10200 Softswitch.

Installation Issues

There are no installation issues associated with these security packages. They are automatically part of the initial installation and install as packages in the system. When the packages are removed, the system is restored to the original defaults. These are handled in the postinstall and postremove scripts in the packages.

Note These security packages are not automatically updated during normal Cisco BTS 10200 Softswitch software upgrade installations. A separate procedure is available for upgrades to these packages.

System Provisioning

Some examples of system provisioning are detailed below. To enable FTP, issue the following command at the CLI/MAINT prompt:

```
change node id=priems25; service=ftp; enable=Y
```

To display the present status of the Telnet service, which is either enabled or disabled, use the following command:

```
show node service=telnet;
```

Reply example:

```
Success: UNIX Service telnet is disabled.
```

To control the use of resources on the system consumed by user sessions, EMS CLI users use the following command:

```
change session idle-time=10;
```

CHAPTER 3

Vulnerabilities in H.323 Message Processing

May 2, 2007 OL-5327-03

During 2002 the University of Oulu Security Programming Group (OUSPG) discovered a number of implementation-specific vulnerabilities in the Simple Network Management Protocol (SNMP). Subsequent to this discovery, the National Infrastructure Security Coordination Centre (NISCC) performed and commissioned further work on identifying implementation specific vulnerabilities in related protocols that are critical to the United Kingdom Critical National Infrastructure. One of these protocols is H.225, which is part of the H.323 family and is commonly implemented as a component of multimedia applications such as Voice over IP (VoIP).

OUSPG produced a test suite for H.225 and employed it to validate their findings against a number of products from different vendors. The test results have been confirmed by testing performed by NISCC and the affected vendors contacted with the test results. These vendors' product lines cover a great deal of the existing critical information infrastructure worldwide and have therefore been addressed as a priority. However, the NISCC has subsequently contacted other vendors whose products employ H.323 and provided them with tools with which to test these implementations.

Systems impacted: Customers supporting H.323 on their solutions using the Cisco BTS 10200 Softswitch Call Agent.

Recommendation: A security fix for this vulnerability has been incorporated into the Release 4.1 Cisco BTS 10200 Softswitch. Further vendor action is not required.

CHAPTER 4

Authentication, Authorization and Accounting Support (Release 4.4)

May 2, 2007 OL-5327-03

This chapter provides the Authentication, Authorization and Accounting (AAA) extensions to the Cisco BTS 10200 Softswitch. These extensions represent modifications to the current scheme of user account management on the system. It includes support for the following two protocols; these protocols are not required to be mutually inclusive.

- Radius Protocol
- Lightweight Directory Access Protocol (LDAP)

Prior to Release 4.4, user account management for the Cisco BTS 10200 Softswitch used the standard Solaris password management facilities without the use of the Authentication Dial-In User Service Network Information Service (NIS). All accounts are stored locally and referenced locally. This security feature begins support for a complete AAA model for user account management. This model impacts several internal subsystems of the Cisco BTS 10200 Softswitch Element Management System (EMS) application. It also impacts the core login support on the other nodes of the Cisco BTS 10200 Softswitch.

Pluggable Authentication Module Support

The Cisco BTS 10200 Softswitch Release 4.4 deploys a Secure Shell (SSH) package with Pluggable Authentication Module (PAM) support. This required a new release of the BTSossh package. The package includes the PAM support required to utilize the Radius and LDAP servers.

The supporting configuration also allows for local accounts to fall through if the Radius and LDAP servers are not available. These default local accounts for the Cisco BTS 10200 Softswitch are the btsuser, btsadmin and secadmin accounts. These are the standard default accounts provided in the base product and use the native password management. These standard default accounts also replace the deprecated optiuser default login for CLI-based users.

A UNIX-based user provides access to the operating system on all nodes. The oamp user is defined for package management purposes. The account is locked and no password is available. However, to grant UNIX access to all nodes of the Cisco BTS 10200 Softswitch, a default password is provided.

When PAM support is used, SSH transfers the control of authentication to the PAM library, which then loads the modules specified in the PAM configuration file. Finally, the PAM library tells SSH whether the authentication was successful. SSH is not aware of the details of the actual authentication method employed by PAM. Only the final result is of interest.

User Security Account Management

The Cisco BTS 10200 Softswitch EMS contains an application program known as User Security Management (USM). This program determines if the account is local or off-board. Password management facilities are disabled for all accounts on the Cisco BTS 10200 Softswitch when an AAA deployment is configured. The AAA deployment transfers the responsibility for these existing facilities to the end-user AAA servers. These facilities include the following attributes:

- Password aging, warning, and expiration
- Password reset and automatic account locking
- Local account management (password and shadow files) for new accounts

CHAPTER 5

Reduced Solaris Packages

May 2, 2007 OL-5327-03

This chapter describes the reduced Solaris packages and the architecture-specific or hardware specific packages for certain Sun Microsystems configurations for the Cisco the Cisco BTS 10200 Softswitch 10200 Softswitch. The Cisco the Cisco BTS 10200 Softswitch 10200 Softswitch uses a base Solaris 8 image derived from the 02/04 release of Solaris 8 from Sun Microsystems. This core image is composed of the packages listed in Table 5-1 for Release 4.4.0/1 and Table 5-2 for Release 4.5. All of the Cisco the Cisco BTS 10200 Softswitch 10200 Softswitch application packages are included in the list for completeness.

Release 4.4.0/1

This section provides the Solaris 8 package list for Release 4.4.0/1. This is the minimum set of packages required to create a working environment for the applications. This image also includes the current Solaris patch cluster up to level 29 (108528-29).

Table 5-1 Solaris 8 Package List for Release 4.4.0/1

Package	Description	Type	Status
SMClsof	LSOF tool	SYSTEM	Required by the Cisco BTS 10200 Softswitch *
SUNWaccr	System Accounting (Root)	SYSTEM	
SUNWaccu	System Accounting (Usr)	SYSTEM	
SUNWadmc	System administration core libraries	SYSTEM	
SUNWadmfw	System and Network Administration Framework	SYSTEM	
SUNWadmr	System and Network Administration Root	SYSTEM	
SUNWamid	Authentication Management Infrastructure (domestic version)	SYSTEM	Required by the Cisco BTS 10200 Softswitch *

Table 5-1 Solaris 8 Package List for Release 4.4.0/1 (continued)

Package	Description	Type	Status
SUNWamidx	Authentication Management Infrastructure (64-bit domestic version)	SYSTEM	Required by the Cisco BTS 10200 Softswitch *
SUNWbash	GNU Bourne-Again shell (bash)	SYSTEM	
SUNWbtool	CCS tools bundled with SunOS	SYSTEM	
SUNWbtoox	CCS libraries bundled with SunOS (64-bit)	SYSTEM	
SUNWbzip	The bzip compression utility	SYSTEM	
SUNWcar	Core Architecture (Root)	SYSTEM	
SUNWcarx	Core Architecture (Root) (64-bit)	SYSTEM	
SUNWcrman	Encryption Kit on-line Manual Pages	SYSTEM	Required by the Cisco BTS 10200 Softswitch *
SUNWcry	Crypt Utilities	SYSTEM	Required by the Cisco BTS 10200 Softswitch
SUNWcry64	Prototype package for Crypt Library	SYSTEM	Required by the Cisco BTS 10200 Softswitch
SUNWcryr	Solaris Root Crypto	SYSTEM	Required by the Cisco BTS 10200 Softswitch
SUNWcryrx	Solaris Root Crypto (64-bit)	SYSTEM	Required by the Cisco BTS 10200 Softswitch
SUNWcsl	Core Solaris (Shared Libs)	SYSTEM	
SUNWcslx	Core Solaris libraries (64-bit)	SYSTEM	
SUNWcsr	Core Solaris (Root)	SYSTEM	
SUNWcsu	Core Solaris (Usr)	SYSTEM	
SUNWcsxu	Core Solaris (Usr) (64-bit)	SYSTEM	

Table 5-1 Solaris 8 Package List for Release 4.4.0/1 (continued)

Package	Description	Type	Status
SUNWdtcor	Solaris Desktop /usr/dt filesystem anchor	SYSTEM	
SUNWesu	Extended System Utilities	SYSTEM	
SUNWesxu	Extended System Utilities (64-bit)	SYSTEM	
SUNWfns	Federated Naming System	SYSTEM	New to the Cisco BTS 10200 Softswitch
SUNWfnsx	Federated Naming System (64-bit)	SYSTEM	New to the Cisco BTS 10200 Softswitch
SUNWftpr	FTP Server	SYSTEM	Required by the Cisco BTS 10200 Softswitch
SUNWftpu	FTP Server	SYSTEM	Required by the Cisco BTS 10200 Softswitch
SUNWgzip	The GNU Zip (gzip) compression utility	SYSTEM	
SUNWhmd	SunSwift SBus Adapter drivers	SYSTEM	
SUNWhmdx	SunSwift SBus Adapter drivers (64-bit)	SYSTEM	
SUNWi15cs	X11 ISO8859-15 Codeset Support	SYSTEM	
SUNWi1cs	X11 ISO8859-1 Codeset Support	SYSTEM	
SUNWipc	Interprocess Communications	SYSTEM	Required by the Cisco BTS 10200 Softswitch
SUNWipcx	Interprocess Communications (64-bit)	SYSTEM	Required by the Cisco BTS 10200 Softswitch
SUNWk5pk	kernel Kerberos V5 plug-in w/auth+privacy (32-bit)	SYSTEM	Required by the Cisco BTS 10200 Softswitch *

Table 5-1 Solaris 8 Package List for Release 4.4.0/1 (continued)

Package	Description	Type	Status
SUNWk5pkx	kernel Kerberos V5 plug-in w/auth+privacy (64-bit)	SYSTEM	Required by the Cisco BTS 10200 Softswitch *
SUNWk5pu	user Kerberos V5 gss mechanism w/auth+privacy (32-bit)	SYSTEM	Required by the Cisco BTS 10200 Softswitch *
SUNWk5pux	User Kerberos V5 gss mechanism w/auth+privacy (64-bit)	SYSTEM	Required by the Cisco BTS 10200 Softswitch *
SUNWkey	Keyboard configuration tables	SYSTEM	
SUNWkvm	Core Architecture (Kvm)	SYSTEM	
SUNWkvmx	Core Architecture (Kvm) (64-bit)	SYSTEM	
SUNWless	The GNU pager	SYSTEM	Required by the Cisco BTS 10200 Softswitch
SUNWlibC	Sun Workshop Compilers Bundled libC	SYSTEM	
SUNWlibCf	SunSoft WorkShop Bundled libC (cfront version)	SYSTEM	Required by the Cisco BTS 10200 Softswitch
SUNWlibms	Sun WorkShop Bundled shared libm	SYSTEM	
SUNWlmsx	Sun WorkShop Bundled 64-bit shared libm	SYSTEM	
SUNWloc	System Localization	SYSTEM	
SUNWlocx	System Localization (64-bit)	SYSTEM	
SUNWluxop	Sun Enterprise Network Array firmware and utilities	SYSTEM	
SUNWluxox	Sun Enterprise Network Array libraries (64-bit)	SYSTEM	
SUNWlxml	The XML Library	SYSTEM	Required for the Cisco BTS 10200 Softswitch *

Table 5-1 Solaris 8 Package List for Release 4.4.0/1 (continued)

Package	Description	Type	Status
SUNWmdb	Modular Debugger	SYSTEM	Required by the Cisco BTS 10200 Softswitch
SUNWmdbx	Modular Debugger (64-bit)	SYSTEM	Required by the Cisco BTS 10200 Softswitch
SUNWmdg	Solstice DiskSuite Tool	SYSTEM	Required by the Cisco BTS 10200 Softswitch
SUNWmdnr	Solstice DiskSuite Log Daemon Configuration Files	SYSTEM	Required by the Cisco BTS 10200 Softswitch
SUNWmdnu	Solstice DiskSuite Log Daemon	SYSTEM	Required by the Cisco BTS 10200 Softswitch
SUNWmdu	Solstice DiskSuite Commands	SYSTEM	Required by the Cisco BTS 10200 Softswitch
SUNWmibii	Solstice Enterprise Agents 1.0.3 SNMP daemon	SYSTEM	
SUNWnamos	Northern America OS Support	SYSTEM	
SUNWnamow	Northern America OW Support	SYSTEM	
SUNWnisu	NIS user part	SYSTEM	Required for the Cisco BTS 10200 Softswitch
SUNWpl5u	Perl 5.005_03	SYSTEM	
SUNWrmodu	Realmode modules (Usr)	SYSTEM	
SUNWsndmr	Sendmail root	SYSTEM	
SUNWsndmu	Sendmail user	SYSTEM	
SUNWsolnm	Solaris Naming Enabler	SYSTEM	

Table 5-1 Solaris 8 Package List for Release 4.4.0/1 (continued)

Package	Description	Type	Status
SUNWsprot	Solaris Bundled tools	SYSTEM	Required by the Cisco BTS 10200 Softswitch
SUNWswmt	Install and Patch Utilities	SYSTEM	
SUNWtoo	Solaris Tools	SYSTEM	Required by the Cisco BTS 10200 Softswitch
SUNWtoox	Solaris Tools (64-bit)	SYSTEM	Required by the Cisco BTS 10200 Softswitch
SUNWudf	Universal Disk Format 1.50 (Usr)	SYSTEM	
SUNWudfr	Universal Disk Format 1.50	SYSTEM	
SUNWudfrx	Universal Disk Format 1.50 (64-bit)	SYSTEM	
SUNWvts	SunVTS kernel, UI, and tests	SYSTEM	Required for the Cisco BTS 10200 Softswitch
SUNWvtsx	SunVTS kernel, UI, and tests (64-bit)	SYSTEM	Required for the Cisco BTS 10200 Softswitch
SUNWvtsmn	SunVTS kernel, UI, and test man pages	SYSTEM	Required for the Cisco BTS 10200 Softswitch
SUNWwsr2	Solaris Product Registry and Web Start runtime support	SYSTEM	
SUNWxwkey	X Windows software, PC keytables	SYSTEM	
SUNWxwmox	X Window System kernel modules (64-bit)	SYSTEM	
SUNWzip	The Info-Zip (zip) compression utility	SYSTEM	
SUNWzlib	The Zip compression library	SYSTEM	

Table 5-1 Solaris 8 Package List for Release 4.4.0/1 (continued)

Package	Description	Type	Status
SUNWzlibx	The Info-Zip compression library (64-bit)	SYSTEM	Required by the Cisco BTS 10200 Softswitch
SUNWzsh	Z-Shell (zsh)	SYSTEM	Required by the Cisco BTS 10200 Softswitch *

Release 4.5

This section provides the Solaris 10 package list for Release 4.5.

Core List of Packages

Table 5-2 lists the packages required to create a working environment for the applications. This list is derived from installing the Sun recommended Reduced Network Core list of packages. Each Finish Script that is VTG product–specific may then add and delete packages as needed by the application.

Table Nomenclature:

- C—denotes part of Reduced Network Core Installation Package
- D—denotes package dependency
- ?—Denotes unknown

Table 5-2 Solaris 10 Reduced Network Core List of Packages

Package	Type	Sol8	Use	Description	Notes
SUNW1394	SYSTEM	N	?	Sun IEEE1394 Framework	
SUNWaccr	SYSTEM	Y		System accounting (Root)	
SUNWaccu	SYSTEM	Y		System accounting (Usr)	
SUNWadmap	SYSTEM	Y	C	System administration applications	
SUNWadmc	SYSTEM	Y		System administration core libraries	
SUNWadmfr	SYSTEM	Y		System and Network Administration Framework Configuration	
SUNWadmfw	SYSTEM	Y		System and Network Administration Framework	
SUNWadmlib-sysid system	SYSTEM	Y		System and Network identification libraries	

Table 5-2 Solaris 10 Reduced Network Core List of Packages

Package	Type	Sol8	Use	Description	Notes
SUNWadmr	SYSTEM	Y	C	System and Network Administration Root	
SUNWaudd	SYSTEM	Y	C	Audio drivers	
SUNWbash	SYSTEM	Y		GNU Bourne-Again shell (bash)	
SUNWbind	SYSTEM	Y		BIND DNS Name server and tools	
SUNWbindr	SYSTEM	Y		BIND DNS Name server SUNWbvand tools for root	
SUNWbip	SYSTEM	Y	C	Basic IP commands (Usr)	
SUNWbtool	SYSTEM	N		CCS tools bundled with SunOS	
SUNWbzip	SYSTEM	Y	C	The bzip compression utility	
SUNWcar	SYSTEM	Y	C	Core Architecture (Root)	
SUNWcakr	SYSTEM	Y	C	Core Solaris Kernel Architecture (Root)	
SUNWced	SYSTEM	Y	C	Sun GigaSwift Ethernet Adapter driver	
SUNWcfcl	SYSTEM	N	C	Common Fibre Channel HBA API Library (Usr)	
SUNWcfclr	SYSTEM	N	C	Common Fibre Channel HBA API Library (Root)	
SUNWcfpl	SYSTEM	N	C	fp cfgadm plug-in library	
SUNWcfplr	SYSTEM	N	C	fp cfgadm plug-in library (root)	
SUNWckr	SYSTEM	Y	C	Core Solaris Kernel (Root)	
SUNWcnetr	SYSTEM	Y	C	Core Solaris Network Infrastructure (Root)	
SUNWcpc	SYSTEM	Y		CPU Performance Counter driver	
SUNWcpcu	SYSTEM	Y		CPU Performance Counter libraries and utilities	
SUNWcpp	SYSTEM	N	C	Solaris cpp	
SUNWcsd	SYSTEM	Y	C	Core Solaris devices	
SUNWcsl	SYSTEM	Y	C	Core Solaris (Shared Libs)	
SUNWcslr	SYSTEM	Y	C	Core Solaris libraries (Root)	
SUNWcsr	SYSTEM	Y	C	Core Solaris (Root)	
SUNWcstl	SYSTEM	N	?	Apptrace Utility	
SUNWcsu	SYSTEM	Y	C	Core Solaris (Usr)	
SUNWctpls	CTL	N	D	Portable layout services	(SUNWmfrun, SUNWxi18n)
SUNWdtcor	SYSTEM	Y		Solaris Desktop /usr/dt filesystem anchor	
SUNWdtdmr	SYSTEM	N		CDE daemon configuration	

Table 5-2 Solaris 10 Reduced Network Core List of Packages

Package	Type	Sol8	Use	Description	Notes
SUNWdtrc	SYSTEM	N		DTrace Clients	
SUNWdtrp	SYSTEM	N		DTrace Providers	
SUNWerid	SYSTEM	Y	C	Sun RIO 10/100 Mb Ethernet drivers	
SUNWesu	SYSTEM	Y	C	Extended System Utilities	
SUNWeuodf	SYSTEM	N	D	UTF-8 Core OPENLOOK Desktop Files (SUNWeu8df)	
SUNWeurf	SYSTEM	N	D	Global fonts	(SUNWi15rf)
SUNWfchba	SYSTEM	Y	C	Sun Fibre Channel Host Bus Adapter Library	
SUNWfchbar	SYSTEM	Y	C	Sun Fibre Channel Host Bus Adapter Library (root)	
SUNWfcip	SYSTEM	Y	C	Sun FCIP IP/ARP over FibreChannel device driver	
SUNWfcmdb	SYSTEM	Y	C	Fibre Channel adb macros and mdb modules	
SUNWfcp	SYSTEM	Y	C	Sun FCP SCSI device driver	
SUNWfcsm	SYSTEM	N	C	FCSM driver	
SUNWfctl	SYSTEM	Y	C	Sun Fibre Channel Transport layer	
SUNWfmd	SYSTEM	N	C	Fault Management Daemon and Utilities	
SUNWfss	SYSTEM	N		Fair Share Scheduler	
SUNWgcmn	SYSTEM	Y		gcmn - Common GNU package	
SUNWged	SYSTEM	Y		Sun Gigabit Ethernet Adapter driver	
SUNWgss	SYSTEM	N	?	GSSAPI V2	
SUNWgssc	SYSTEM	N	?	GSSAPI CONFIG V2	
SUNWgssdh	SYSTEM	N	?	GSS Diffie-Hellman	
SUNWgssk	SYSTEM	N	?	kernel GSSAPI V2	
SUNWgzip	SYSTEM	Y		The GNU Zip (gzip) compression utility	
SUNWhmd	SYSTEM	Y	C	SunSwift Adapter drivers	
SUNWi15rf	SYSTEM	N	D	X11 ISO8859-15 required fonts (SUNWi15cs)	
SUNWib	SYSTEM	N	C	Sun InfiniBand Framework	
SUNWidnl	SYSTEM	N	C	Internationalized Domain Name Support Library Files	
SUNWipc	SYSTEM	Y		Inter Process communications	

Table 5-2 Solaris 10 Reduced Network Core List of Packages

Package	Type	Sol8	Use	Description	Notes
SUNWifp	SYSTEM	Y		Sun Fibre Channel Arbitrated Loop device driver	
SUNWinst	SYSTEM	N	?	Install Software	
SUNWinstall-patch-utils-root	SYSTEM	Y	C	Install and Patch Utilities (root)	
SUNWipfr	SYSTEM	N	C	IP Filter utilities (Root)	
SUNWipfu	SYSTEM	N	C	IP Filter utilities (Usr)	
SUNWipoib	SYSTEM	N	C	Sun IP over InfiniBand	
SUNWiscsir	SYSTEM	Y	C	Sun iSCSI device driver (root)	
SUNWiscsiu	SYSTEM	Y	C	Sun iSCSI Management Utilities (usr)	
SUNWj5rt	SYSTEM	N	D	JDK 5.0 Runtime Env. (1.5.0_01)	(SUNWocf)
SUNWjfca	SYSTEM	N	C	JNI Fibre Channel Adapter (FCA) driver	
SUNWjfcau	SYSTEM	N	C	JNI Fibre Channel Adapter (FCA) (usr)	
SUNWjss	SYSTEM	N	C	Network Security Services for Java (JSS)	
SUNWkey	SYSTEM	Y	C	Keyboard configuration tables	
SUNWkrbr	SYSTEM	Y	C	Kerberos version 5 support (Root)	
SUNWkrbu	SYSTEM	Y	C	Kerberos version 5 support (Usr)	
SUNWkvm	SYSTEM	Y	C	Core Architecture (Kvm)	
SUNWless	SYSTEM	Y		The GNU pager (less)	
SUNWlexpt	SYSTEM	Y	C	libexpat - XML parser library	
SUNWlibC	SYSTEM	Y		Sun Workshop Compilers Bundled libC	
SUNWlibms	SYSTEM	Y	C	Math and Microtasking libraries (Usr)	
SUNWlibmsr	SYSTEM	Y	C	Math and Microtasking libraries (Root)	
SUNWlibsasl	SYSTEM	N	C	SASL v2	
SUNWlldap	SYSTEM	N	C	LDAP libraries	
SUNWloc	SYSTEM	Y	C	System Localization	
SUNWlur	APPL	N	?	Live Upgrade (root)	
SUNWluu	APPL	N	?	Live Upgrade (usr)	
SUNWluxop	SYSTEM	Y	C	Sun Enterprise Network Array firmware and utilities	
SUNWluxopr	SYSTEM	Y	C	Sun Enterprise Network Array libraries	

Table 5-2 Solaris 10 Reduced Network Core List of Packages

Package	Type	Sol8	Use	Description	Notes
SUNWluzone	SYSTEM	N		Live Upgrade (zones support)	
SUNWlxml	SYSTEM	Y	C	The XML library	
SUNWm64cf	APPL	N	?	M64 Graphics Configuration Software	
SUNWmdb	SYSTEM	Y		Modular Debugger	
SUNWmdbdm	SYSTEM	Y		Modular Debugger Demo Source	
SUNWmdbr	SYSTEM	Y		Modular Debugger (Root)	
SUNWmdr	SYSTEM	Y	C	Solaris Volume Manager (Root)	
SUNWmdu	SYSTEM	Y		Solaris Volume Manager (Usr)	
SUNWmfrun	SYSTEM	Y		Motif RunTime kit	
SUNWmibii	SYSTEM	Y		Solstice Enterprise Agents 1.0.3 SNMP daemon	
SUNWmipr	SYSTEM	N	?	Mobile-IP (Root)	
SUNWmipu	SYSTEM	N	?	Mobile-IP (Usr)	
SUNWmkcd	SYSTEM	N	?	CD creation utilities	
SUNWnfsckr	SYSTEM	N	?	Network File System (NFS) client kernel support (Root)	
SUNWnfscr	SYSTEM	Y		Network File System (NFS) client support (Root)	
SUNWnfscu	SYSTEM	Y		Network File System (NFS) client support (Usr)	
SUNWnisu	SYSTEM	Y		Network Information System (Usr)	
SUNWnisr	SYSTEM	Y		Network Information System (Root)	
SUNWocf	SYSTEM	N	?	Open Card Framework	
SUNWocfr	SYSTEM	N	?	Configuration files for Open Card Framework	
SUNWopenssl-libraries	SYSTEM	Y	C	OpenSSL libraries (Usr)	
SUNWpd	SYSTEM	Y	C	PCI drivers	
SUNWperl584core	SYSTEM	Y	C	core Perl 5.8.4 (core)	
SUNWperl584usr	SYSTEM	Y	C	Perl 5.8.4 (non-core)	
SUNWpkgcmdsr	SYSTEM	N	C	SVr4 package commands (root)	
SUNWpkgcmdsu	SYSTEM	N	C	SVr4 packaging commands (usr)	
SUNWpool	SYSTEM	N		Resource Pools	
SUNWpoolr	SYSTEM	N		Resource Pools (Root)	
SUNWpr	SYSTEM	N	C	Netscape Portable Runtime	
SUNWproduct-registry-root	SYSTEM	N	C	Solaris Product Registry runtime support (root)	

Table 5-2 Solaris 10 Reduced Network Core List of Packages

Package	Type	Sol8	Use	Description	Notes
SUNWqfed	SYSTEM	Y	C	Sun Quad FastEthernet Adapter driver	
SUNWqlc	SYSTEM	N	C	Qlogic ISP 2200/2202 Fibre Channel device driver	
SUNWqos	SYSTEM	N	?	IP QoS (Root)	
SUNWqosu	SYSTEM	N	?	IP QoS (Usr)	
SUNWqus	SYSTEM	N		QLogic Ultra3 Scsi (Root)	
SUNWqusu	SYSTEM	N		QLogic Ultra3 Scsi (Usr)	
SUNWrcmdc	SYSTEM	N		Remote Network Client commands	
SUNWroute	SYSTEM	N	?	Network Routing daemons/commands (Usr)	
SUNWrpcib	SYSTEM	N	C	InfiniBand plugin to RPC over RDMA	
SUNWrsg	SYSTEM	N	?	RPCSEC_GSS	
SUNWrsgk	SYSTEM	N	?	kernel RPCSEC_GSS	
SUNWsacom	SYSTEM	N	?	Solstice Enterprise Agents 1.0.3 files for root file system	
SUNWsadmi	SYSTEM	N	?	Solstice Enterprise Agents 1.0.3 Desktop Management Interface	
SUNWsasnm	SYSTEM	N	?	Solstice Enterprise Agents 1.0.3 Simple Network Management Protocol	
SUNWses	SYSTEM	Y	C	SCSI Enclosure Services device driver	
SUNWsolnm	SYSTEM	Y	C	Solaris Naming Enabler	
SUNWspnego	SYSTEM	N	?	SPNEGO GSS-API mechanism	
SUNWsprot	SYSTEM	Y		Solaris bundled tools	
SUNWssad	SYSTEM	Y	C	SPARCstorage Array drivers	
SUNWsshcu	SYSTEM	Y	C	SSH common (Usr)	
SUNWsshdr	SYSTEM	Y	C	SSH server (Root)	
SUNWsshdu	SYSTEM	Y	C	SSH server (Usr)	
SUNWsshr	SYSTEM	Y	C	SSH Client and utilities (Root)	
SUNWsshu	SYSTEM	Y	C	SSH Client and utilities (Usr)	
SUNWswmt	SYSTEM	Y	C	Install and Patch utilities	
SUNWtavor	SYSTEM	N	C	Sun Tavor HCA driver	
SUNWtcsh	SYSTEM	N	?	Tenex C-shell (tcsh)	
SUNWtecla	SYSTEM	N	C	Tecla command-line editing library	
SUNWter	SYSTEM	N	?	Terminal Information	
SUNWtls	SYSTEM	N	C	Network Security Services	

Table 5-2 Solaris 10 Reduced Network Core List of Packages

Package	Type	Sol8	Use	Description	Notes
SUNWtltk	SYSTEM	N		ToolTalk runtime	
SUNWtnetc	SYSTEM	N		Telnet Command (client)	
SUNWtnetd	SYSTEM	N		Telnet daemon for user (server)	
SUNWtnetr	SYSTEM	N		Telnet daemon for root (server)	
SUNWtnfc	SYSTEM	Y		TNF Core components	
SUNWtnfd	SYSTEM	N		TNF Developer components	
SUNWtoo	SYSTEM	Y		Programming tools	
SUNWucbt	SYSTEM	N	?	Apptrace support objects for ucblib	
SUNWudaplr	SYSTEM	N	C	Sun User Direct Access Programming library (Root)	
SUNWudapltr	SYSTEM	N	C	Sun uDAPL for Tavor (Root)	
SUNWudapltu	SYSTEM	N	C	Sun uDAPL for Tavor (User)	
SUNWudaplu	SYSTEM	N	C	Sun User Direct Access Programming library (User)	
SUNWuedg	SYSTEM	N	C	USB Digi Edgeport serial driver	
SUNWugen	SYSTEM	N	C	USB Generic driver	
SUNWus	SYSTEM	N	?	UltraSPARC CPU device driver	
SUNWusb	SYSTEM	Y	C	USB device drivers	
SUNWusbs	SYSTEM	Y	C	USB generic serial module	
SUNWvld	SYSTEM	N	?	Sun Ethernet Vlan Utility Routines	
SUNWvldu	SYSTEM	N	?	Sun Ethernet Vlan Utility Headers	
SUNWwbsup	SYSTEM	N	C	WAN boot support	
SUNWwsr2	SYSTEM	Y	C	Solaris Product Registry and Web Start runtime support	
SUNWxge	SYSTEM	N	C	Xframe 10GE NIC driver	
SUNWxi18n	SYSTEM	N	D	X Window System Internationalization Common package	(SUNWplow)
SUNWxwacx	SYSTEM	N	D	AccessX client program (SUNWeuodf, SUNWeu8df)	
SUNWxwdv	SYSTEM	Y	X	Windows System Window drivers	
SUNWxwfnt	SYSTEM	N	D	X Window System platform required fonts	(SUNWxwplt, SUNWeuodf, SUNWplow)
SUNWxwice	SYSTEM	Y		X Window System Inter-Client Exchange (ICE) components	
SUNWxwplr	SYSTEM	Y		X Window System platform software configuration	

Table 5-2 Solaris 10 Reduced Network Core List of Packages

Package	Type	Sol8	Use	Description	Notes
SUNWxwplt	SYSTEM	Y		X Window System platform software	
SUNWxwrtl	SYSTEM	Y		X Window System and Graphics Runtime Library Links in /usr/lib	
SUNWzebrar	SYSTEM	N	?	zebra-GNU routing daemons (root)	
SUNWzebrau	SYSTEM	N	?	zebra-GNU routing daemons (usr)	
SUNWzip	SYSTEM	Y		The Info-Zip (zip) compression utility	
SUNWzlib	SYSTEM	Y	C	The Zip compression library	
SUNWzoner	SYSTEM	N		Solaris zones (Root)	
SUNWzoneu	SYSTEM	N		Solaris zones (Usr)	
SUNWzsh	SYSTEM	Y		Z shell (zsh)	

Finish Scripts

The SUNW packages listed in Table 5-3 are installed in the CA and EMS finish scripts for Solaris 10.

Table Nomenclature:

- C—denotes part of Reduced Network Core Installation Package
- D—denotes package dependency
- ?—Denotes unknown

Table 5-3 Solaris 10 Finish Scripts Packages

Package	Type	Sol8	Use	Description	Notes
SUNWefc	SYSTEM	N		Embedded FCode Interpreter drivers	
SUNWexplo	SYSTEM	N		Sun(TM) Explorer Data Collector	
SUNWexplu	SYSTEM	N		Sun(TM) Explorer Data Collector Config Files	
SUNWglmr	SYSTEM	N		Rasctrl environment monitoring driver for i2c (Root)	
SUNWi2cr	SYSTEM	Y		Device drivers for I2C devices (Root)	
SUNWpstl	SYSTEM	N		Platform specific apptrace support	
SUNWvts	SYSTEM	Y		SunVTS Framework	
SUNWvtsr	SYSTEM	Y		SunVTS Framework (Root)	
SUNWvtsts	SYSTEM	Y		SunVTS for tests	

Sun Microsystems Configurations

Table 5-4 lists the Solaris 8 architecture-specific or hardware specific packages for certain Sun Microsystems configurations.

Table 5-4 Solaris Architectural- or Hardware-Specific Optional Package List

Package	Description	Type	Status
SMEvplr	SME platform links	SYSTEM	
SMEvplu	SME usr/platform links	SYSTEM	
SUNWaudd	Audio drivers	SYSTEM	
SUNWauddx	Audio drivers (64-bit)	SYSTEM	
SUNWced	Sun GigaSwift Ethernet Adapter (32-bit driver)	SYSTEM	
SUNWcedx	Sun GigaSwift Ethernet Adapter (64-bit driver)	SYSTEM	
SUNWcg6	GX (cg6) device driver	SYSTEM	
SUNWcg6x	GX (cg6) device driver (64-bit)	SYSTEM	
SUNWcsd	Core Solaris devices	SYSTEM	
SUNWdfb	Dumb Frame Buffer device drivers	SYSTEM	
SUNWensqr	Ensoniq ES1370/1371/1373 Audio device driver (32-bit) (Root)	SYSTEM	
SUNWensqx	Ensoniq ES1370/1371/1373 Audio device driver (64-bit) (Root)	SYSTEM	
SUNWeridx	Sun RIO 10/100 Mb Ethernet drivers (64-bit)	SYSTEM	
SUNWfcip	Sun FCIP IP/ARP over FibreChannel device driver	SYSTEM	
SUNWfcipx	Sun FCIP IP/ARP over FibreChannel device driver (64-bit)	SYSTEM	
SUNWfcp	Sun FCP SCSI device driver	SYSTEM	
SUNWfcpx	Sun FCP SCSI device driver (64-bit)	SYSTEM	
SUNWfctl	Sun Fibre Channel Transport layer	SYSTEM	
SUNWfctlx	Sun Fibre Channel Transport layer (64-bit)	SYSTEM	
SUNWfruid	FRU ID prtfru Command and libfru library	SYSTEM	
SUNWfruip	FRU ID Platform Data module and Access libraries	SYSTEM	
SUNWfruix	FRU ID library (64-bit)	SYSTEM	
SUNWged	Sun Gigabit Ethernet Adapter driver	SYSTEM	
SUNWglmr	rasctrl environment monitoring driver for i2c (Root) (32-bit)	SYSTEM	
SUNWglmx	rasctrl environment monitoring driver for i2c (Root) (64-bit)	SYSTEM	
SUNWi2cr	device drivers for I2C devices (Root, 32-bit)	SYSTEM	
SUNWi2cx	device drivers for I2C devices (Root, 64-bit)	SYSTEM	

Table 5-4 Solaris Architectural- or Hardware-Specific Optional Package List (continued)

Package	Description	Type	Status
SUNWidecr	IDE device drivers	SYSTEM	
SUNWidecx	IDE device drivers (Root) (64bit)	SYSTEM	
SUNWider	IDE device driver (Root)	SYSTEM	
SUNWkmp2r	PS/2 Keyboard and Mouse device drivers (Root((32-bit)	SYSTEM	
SUNWkmp2x	PS/2 Keyboard and Mouse device drivers (Root) (64-bit)	SYSTEM	
SUNWmdr	Solstice DiskSuite drivers	SYSTEM	Required by the Cisco BTS 10200 Softswitch
SUNWmdx	Solstice DiskSuite drivers(64-bit)	SYSTEM	Required by the Cisco BTS 10200 Softswitch
SUNWmdi	Sun Multipath I/O drivers	SYSTEM	
SUNWmdix	Sun Multipath I/O drivers (64-bit)	SYSTEM	
SUNWpd	PCI drivers	SYSTEM	
SUNWpdx	PCI drivers (64-bit)	SYSTEM	
SUNWpiclh	PICL Header files	SYSTEM	
SUNWpiclr	PICL Framework (Root)	SYSTEM	
SUNWpiclu	PICL libraries and Plugin modules (Usr)	SYSTEM	
SUNWpiclx	PICL libraries (64-bit)	SYSTEM	
SUNWqfed	Sun Quad FastEthernet Adapter driver	SYSTEM	
SUNWqfedx	Sun Quad FastEthernet Adapter driver (64-bit)	SYSTEM	
SUNWqlc	Qlogic ISP 2200/2202 Fiber Channel device driver	SYSTEM	
SUNWqlcx	Qlogic ISP 2200/2202 Fiber Channel device driver (64-bit)	SYSTEM	
SUNWses	SCSI Enclosure Services device driver	SYSTEM	
SUNWsesx	SCSI Enclosure Services device driver (64-bit)	SYSTEM	
SUNWsior	SuperIO 307 (plug-n-play) device drivers (Root)	SYSTEM	
SUNWsiox	SuperIO 307 (plug-n-play) device drivers (Root) (64-bit)	SYSTEM	
SUNWssad	SPARCstorage Array drivers	SYSTEM	
SUNWssadx	SPARCstorage Array drivers (64-bit)	SYSTEM	
SUNWssaop	Administration Utilities and Firmware for SPARCStorage Array	SYSTEM	
SUNWuaud	USB Audio drivers	SYSTEM	
SUNWuaudx	USB Audio drivers (64-bit)	SYSTEM	
SUNWusb	USB device drivers	SYSTEM	

Table 5-4 Solaris Architectural- or Hardware-Specific Optional Package List (continued)

Package	Description	Type	Status
SUNWusbx	USB device drivers (64-bit)	SYSTEM	
SUNWxwdv	X Windows System Window drivers	SYSTEM	
SUNWxwdvx	X Windows System Window drivers (64-bit)	SYSTEM	

GLOSSARY

May 2, 2007 OL-5327-03

A

AC automatic callback

adapter An application program that implements an external interface to allow access to the Cisco BTS 10200 Softswitch.

ADI Activation, Deactivation, and Interrogation

ADM Administration, Diagnostic, and Maintenance

AIN Advanced Intelligent Network. A telephone network architecture that adds advanced computer intelligence to the telephone system. AIN supports advanced telecommunications features such as voice recognition.

AMA Automated Message Accounting

ANI automatic number identification. The number transmitted through the network that identifies the calling party. Technically, it is a Common Channel Interoffice Signaling (CCIS) parameter referring to the number transmitted on an out-of-band basis through an SS7 signaling network identifying the calling party's telephone number. Also known as a calling party number (CPN).

ANNC announcement

Annex E Connection Over UDP—Relates to sending signaling over UDP (User Data Protocol) for quicker call establishment. UDP does not replace TCP/IP. Annex E optimizes the gatekeeper-routed call model.

Annex F Inter-Domain Communications—A domain is several zones grouped together. Inter-domain communications focuses on address resolution between domains.

ANS Announcement server

application A collection of one or more programs that provide congruent functionality to accomplish a task within the scope of the Cisco BTS 10200 Softswitch.

AR automatic recall

ASPC Analog Stored Program Control Switch

AT access tandem

ATM Asynchronous Transfer Mode

B

BAF Bellcore AMA Format

BCID billing correlation ID

BCM Basic Call Module

BDMS Bulk Data Management System. The BDMS contains the billing and performance features of the Cisco BTS 10200 Softswitch.

BE best effort

Block-DA Block Directory Assistance

Block-INTL Block International Operator Assistance

Block-TW Block Time and Weather

BLP Billing Loop Program

BLV Busy Line Verification

BTS Broadband Telephony Services

BTS 10200 Cisco Systems Broadband Telephony Softswitch 10200

C

CA Call Agent. A component of the Cisco BTS 10200 Softswitch.

CALEA Communications Assistance for Law Enforcement Act

CALLp call processing

CAS channel-associated signaling

CAS-TG channel-associated signaling trunk group

CAT customer access treatment

CBR constant bit rate

CC country code

CCC Call Content Channel

CC-NN country code—national number

CCR Continuity Check Request message

CDB call detail block

CDC call data channel

CDR call detail record

CERT	CERT and CERT Coordination Center are registered with the U.S. Patent and Trademark office as service marks of Carnagie Mellon University. Do not expand CERT into an acronym. It is appropriate to note in text that the CERT/CC was originally called the computer emergency response team.
CFB	call forward on busy
CFNA	call forward on no answer
CFU	call forwarding unconditional
CIC	Carrier Identification Code. A unique 3- or 4-digit access identification code assigned by Telcordia (formerly Bellcore). It identifies the long-distance carrier of a caller.
CIDCW	call identity with call waiting
CLH	circular line hunt
CLI	command-line interface
CLIP	calling line information presentation
CLIR	calling line information restriction
CLLI	Common Language Location Identifier code. An 11-character descriptor field assigned to a class 4/5 switch.
CM	cable modem
CMS	Call Management server
CMTS	Cable Modem Termination System
CNM	connection manager
CO	central office
COPS	Common Open Policy Service
CORBA	Common Object Request Broker Architecture
COT	continuity message
CPL	Command Privilege Level
CPOL	Cisco Patent On-line
CPSG-ID	Call Park Subscriber Group Identification
CPU	central processing unit
CRCX	MGCP create connection message type
CT	call transfer
CVR	circuit validation response

CVT Circuit Validation Test

CW call waiting

CWD call waiting deluxe

D

DA directory assistance

DA-CWI distinctive alerting/call waiting on incoming

DID direct inward dialing

DLCX MGCP delete connection message type

DN directory number

DNIS Pattern dialed number identification service

DNS domain name server

DOCSIS Data Over Cable System Interface Specification

DP detection point

DPC destination point code

DSCP Diff Service Code Point

DSPC Digital Stored Program Control Switch

DUP-Records duplicate records

E

EAEO equal access end office

EC echo cancellation

ECD Echo Control Device (normally an echo suppressor or echo canceller)

EM Event Messaging or Element Management application program in the Cisco BTS 10200 Softswitch. The application program executes on the EMS physical node.

EMA Event Message Adapter

EMG Emergency (911) call

EMS Element Management System of the Cisco BTS 10200 Softswitch. This refers to the physical node the EMS resides on.

EMTA Embedded Media Terminal Adapter

EO end office

ESA Electronic Surveillance Adapter

EXT extension

F

FCLI functional command-line interface

FCP Feature Control Protocol

FEID financial entity ID

FGD Feature Group D

FIM feature interaction manager

FName feature name

FQDN fully qualified domain name

FS Feature Server

FTP File Transfer Protocol

G

G guaranteed

GC gate controller

GK gatekeeper—A device that does E.164 to IP address resolution, bandwidth management and load balancing.

GTD generic transport descriptor—ASCII-based encoding scheme used to pass signaling information end-to-end.

GW gateway

H

H.225 The call signaling protocol of H.323. H.225 uses messages similar to messages defined in Q.931 ITU-T Recommendation.

H.245 The resource exchange protocol of H.323. H.245 is used to help the two peers determine the master-slave relationship, the exchange of capabilities, and the opening or closing of logical channels.

H.323 ITU-T recommendation adopted by the VoIP Forum as the call signaling protocol over LAN.

H3A The H.323 signaling adaptor subsystem of the Cisco BTS 10200 Softswitch.

HFC hybrid fiber coaxial

HMN hardware monitor

HPTime higher packetization time

I

IAD Integrated Access Devices

IETF Internet Engineering Task Force

INS In-Service

interLATA Calls that cross LATA boundaries.

INTL international

intraLATA Calls that occur within a single LATA.

IP Internet Protocol

ISDN Integrated Services Digital Network

ITP intraLATA toll presubscription

ITU-T International Telecommunication Union - Telecommunication Sector

IVR interactive voice response

IXC Interexchange Carrier

J

JIP jurisdiction information parameter

L

LATA local access transport area

LEC local exchange carrier

LNP local number portability

LPTime lower packetization time

LRN local routing number

LSA local service area

M

MAX-Digits maximum number of digits

MDCX MGCP modify connection message type

MG/MGW media gateway

MGA media gateway adapter

MGC MGCP media gateway controller

MGCP Media Gateway Control Protocol, used by the Cisco BTS 10200 Softswitch for controlling the bearer path on Media Gateway

MGW media gateway. The main functionality of MGW is to packetize voice PCM stream from IMT in to RTP stream and vice-versa. The Call Agent controls MGWs using MGCP commands.

MIN-Digits minimum number of digits

MLHG multiline hunt group

MSN Microsoft Network

MTA media terminal adapter

MWI-On message waiting indicator on

N

NANP North American Numbering Plan

NAS network access server

NCA no circuit available

NCS Network Based Call Signaling

NFAS nonfacility-associated signaling

NMS network management system

NOD nature of dial

Noun The name of a table in the Cisco BTS 10200 Softswitch database

NPA Numbering Plan Area (area code)

NTE Named telephony event. An event such as DTMF digits that must be encoded and transported in an RTP packet. RFC 2833 specifies the format of the RTP NTE payload.

NTF no trouble found

NTP Network Time Protocol

NXX office code or prefix with a first digit of 2 to 9

O

O- originating, such as CMS and MGC

OAMP operations, administration, maintenance, and provisioning

OCB outgoing call barring

OCB_ACT OCB activation

OCLLI CLLI of the originating trunk group

OCN original called number information element

OLD-DN old subscriber directory number

OLI originating line information

OOB out of band

OOS out of service

OPER-Status operational status

ORB Object Request Broker

OSI open switch interval

OSS Operations Support Systems

OSSS operator services signaling system

P

P1 Priority 1

P2 Priority 2

P3 Priority 3

P4 Priority 4

PBX private branch exchange

PCM pulse code modulation

PCS personal communications service

PDP Policy Decision Point

PEP Policy Enforcement Point

PIC preferred interlata carrier or point in call

POP point of presence

POTS plain old telephone service

PRD Product Requirement Document

PSIRT Product Security Incident Response Team

PSTN public switched telephone network

PVC permanent virtual circuit

Q

QoS quality of service

R

RAC Resource Availability Confirmation message

RACF remote activation of call forwarding

RADIUS Remote Authentication Dial In User Service

RAI Resource Availability Indication RAS message

RAS Registration, Admission, and Status Protocol. RAS is defined in the H.225 ITU-T Recommendation. RAS is used to communicate between gateways, endpoints, and gatekeeper. RAS is also used to communicate between two gatekeepers.

Registration: A function of the gateway to the gatekeeper to inform the gatekeeper about information pertinent to the gateway. The information is: E.164 number assigned to the POTS port of the gateway, H.323 Alias, and technology prefix.

Admission: A function of the gateway to request the gatekeeper for E.164 number to IP address translation.

Status: A function of the gateway to inform the gatekeeper about an active call.

RBOC Regional Bell Operating Company

RCF Registration Confirmation message

RDN Redirecting Number Information Element

RGW residential gateway

RIP Request In Progress message

RKS Record Keeping Server; Record Keeping System

ROH receiver off hook

ROTL Remote Office Test Line

RRJ Registration Reject message

RRQ Registration Request message

RSVP Resource Reservation Protocol. An IETF protocol for providing integrated services and reserving resources in an IP-based internet.

RTP Real-Time Transport Protocol—A protocol for transporting multimedia over IP; see RFC 1889, *RTP: A Transport Protocol for Real-Time Applications*.

S

S7A SS7 ISUP signaling Adapter

SCP Service Control Point

SDP Session Description Protocol. A protocol for defining information needed to establish multimedia transport over IP. SDP transmits information such as session announcement, session invitation, transport addresses, and media types. For example, in a SIP call, SDP messages indicates if NTE is used, which events to send using NTE, and the NTE payload type value. See RFC 2327, *SDP: Session Description Protocol*.

Send-ATP Send Access Transport Parameter

Send-CIP Send Carrier Information Parameter

Send-CN Send Charge Number

Send-CPN Send Calling Party Number

Send-CSP Send Carrier Selection Parameter

Send-GAP Send Generic Address Parameter

Send-GN Send Generic Name

Send-OCN Send Original Called Number

SG4.0 Signaling Gateway 4.0 Release

SIM service interaction module

SIP Session Initiation Protocol. A protocol for transporting multimedia that is independent of the underlying packet control layer, such as the User Datagram Protocol (UDP), and is based on client/server architecture. See RFC 2543, *SIP: Session Initiation Protocol*.

SIP Session Initiation Protocol

SK service key

SMG Session Manager

SNMP Simple Network Management Protocol

SPCS Stored Program Control switching System / Softswitch

SPVC soft permanent virtual circuit

SQL Structured Query Language

SS7 Signaling System Number 7

SSF Service Switching Function

SSH Secure Shell

SSL Secure Socket Layer

SVC switched virtual circuit

T

T-	Terminating, such as CMS and MGC
Table	A database entity containing customer provisioned data
TAC	Technical Assistance Center
TCCLI	CLLI of the terminating Trunk Group
TDP	trigger detection point
Technology Prefix	A number used in the gateway and gatekeeper RAS communication to indicate to the gatekeeper the type of service this gateway is capable of handling. Examples of the type of service are voicemail, fax server, and so forth.
TG	trunk group
TGCP	Trunking Gateway Control Protocol
TGW	trunking gateway (SS7/PSTN)
TID	trigger ID
TNS	Transit Network Selection
TOD	time of day
TOS	type of service
translated DN	translated directory number
TS	Tandem Switch
TSAP	Transport Service Access Point
T-Stamp	time stamp
TType	Trigger Type
TUT	trunk under test
TW	time and weather

U

UCD	Uniform Call Distribution
Update-ANI	Update Automatic Number Identification
UPL	user privilege level

V

VBR	variable bit rate
VMA	voicemail access

VoIP Voice over IP. The ability to carry normal telephony-style voice over an IP-based Internet with POTS-like functionality, reliability, and voice quality. VoIP is a blanket term which generally refers to Cisco's standards-based (for example, H.323) approach to IP voice traffic.

VoP voice over packet

X

XML eXtensible Markup Language

INDEX

N

O

P

R

S

T

U

V