CHAPTER 10

PacketCable Media Security

Revised: July 24, 2009, OL-3743-42

This chapter describes the commands and tables used in PacketCable media security provisioning. For complete information regarding PacketCable commands, provisioning, and troubleshooting, see the *Cisco BTS 10200 Softswitch PacketCable Feature Guide*.

Note In this chapter, an asterisk preceding a token name means the token is mandatory. A token without an asterisk is optional.

Ciphersuite

The Ciphersuite (ciphersuite) table contains the security parameters required for media security between multimedia terminal adapters (MTAs). The table is used when a bearer path between two MTAs needs to be encrypted. The MTAs exchange security parameters (ciphersuites) through signaling. This table allows the Cisco BTS 10200 Softswitch to specify which ciphersuites are allowed for an MTA.

Note A cipher is an algorithm that transforms data between plain text and encrypted text. A ciphersuite is a set that contains both an encryption algorithm and a message authentication algorithm.

Table Name: CIPHERSUITE

Table Containment Area: Call Agent

Command Types

Show, add, change, and delete

Examples

```
show ciphersuite id=cp1gold;
add ciphersuite id=cp1gold; proto-type=RTP; auth-algo=RTP-NULL; encrypt-algo=RTP-NULL;
priority=1;
change ciphersuite id=cp1gold; proto-type=RTP; auth-algo=RTP-NULL; encrypt-algo=RTP-NULL;
priority=10;
delete ciphersuite id=cp1gold; proto-type=RTP; auth-algo=RTP-NULL; encrypt-algo=RTP-NULL;
```

Usage Guidelines

Primary Key Token(s): id, proto-type, auth-algo, encrypt-algo

Foreign Key Token(s): id

Add Rules: PK constraints; ciphersuite-profile id must exist.

- if type is proto-type=rtp then
  - valid auth-algo values are: Rtp-null, rtp-mmh-2, rtp-mmh-4
  - valid encrypt-algo values are: rtp-null, rtp-aes, rtp-xdesx-cbc, rtp-des-cbc-pad, rtp-3des-cbc, rtp-rc4
- if type is proto-type=rtcp then
  - valid auth-algo values are: rtcp-null, rtcp-hmac-sha1-96, rtcp-hmac-md5-96
  - valid encrypt-algo values are: rtcp-null, rtcp-aes-cbc, rtcp-xdesx-cbc, rtcp-des-cbc-pad, rtcp-3des-cbc

Change Rules: Only the priority token can be changed.

Delete Rules: None.

Syntax Description

* ID	Primary key. Foreign key: Ciphersuite Profile table. Ciphersuite profile id. VARCHAR(16): 1–16 ASCII characters.
* AUTH-ALGO	Primary key. Specifies the authentication algorithm for RTP or RTCP (depending upon the value entered for proto-type). See the *PacketCable Security Specification* for more detailed information. VARCHAR(32): 1–32 ASCII characters. Permitted authentication algorithms for proto-type=RTP are: RTP-NULL RTP-MMH-2 RTP-MMH-4 Permitted authentication algorithms for proto-type=RTCP are: RTCP-NULL RTCP-HMAC-SHA1-96 RTCP-HMAC-MD5-96

* ENCRYPT-ALGO	Primary key. Specifies the encryption algorithm for RTP or RTCP (depending upon the value entered for PROTO-TYPE). See the *PacketCable Security Specification* for more detailed information. VARCHAR(32): 1–32 ASCII characters. Permitted (valid) encryption algorithms for proto-type=RTP are: RTP-NULL RTP-AES RTP-XDESX-CBC RTP-DES-CBC-PAD RTP-3DES-CBC RTP-RC4 Permitted (valid) encryption algorithms for proto-type=RTCP are: RTCP-NULL RTCP-AES-CBC RTCP-XDESX-CBC RTCP-DES-CBC-PAD RTCP-3DES-CBC **Note** Authentication and encryption algorithms are identified in the PacketCable Security Specification, PKT-SP-SEC-I06-021018.
* PRIORITY	Specifies the priority of the ciphersuite. These parameters are sent in the local connection options (LCO) in the order specified. INTEGER: 1–32 numeric digits. Priority 1 has the highest priority. Priority 32 has the lowest priority. For example, if 64/51 has a priority of 10, and 62/53 has a priority of 15, then they will go as sc-rtp:64/51; 62/53. The gateway chooses 64/51 if it is able to do so. If the gateway cannot handle a 64/51, it chooses 62/53. **Note** See the PacketCable Network-Based Call Signaling Protocol Specification, PKT-SP-EC-MGCP-I06-021127 for additional information on the sc-rtp and sc-rtcp parameters.
* PROTO-TYPE	Primary key. This token specifies whether the authentication and encryption algorithms specified are for the Real Time Protocol (RTP) or for the Real Time Control Protocol (RTCP). Encrypted packets are carried end-to-end in RTP packets. RTCP is a control protocol for RTP. VARCHAR(16): 1–16 ASCII characters. Permitted values are: RTP—Real Time Protocol. RTCP—Real Time Control Protocol.
AUTO-REFRESH	Specifies whether to display cached data on the screen. Valid only for the show command. CHAR(1): Y/N (Default = Y). Y—Queries the database for the most current data. N—Queries the database for the most current data only if the cached data is unavailable.

DISPLAY	Specifies what token information to display on the screen. Valid only for the show command. VARCHAR(1024): 1–1024 (Default = all tokens are displayed). Permitted values are any valid token that can be shown for this command. Multiple tokens can be entered by separating with a comma.
LIMIT	Specifies the number of rows to display on the screen. Valid only for the show command. INTEGER: 1–100000000 (Default = 100000000). **Note** The actual maximum number of rows displayed is currently lower than 100000000 due to software limitations.
ORDER	Specifies whether to display data on the screen in a sorted order. Valid only for the show command. VARCHAR(1024): 1–1024 (Default = all rows are displayed). Permitted values are any valid token that can be shown for this command. Multiple tokens can be entered by separating with a comma.
START-ROW	Specifies to begin displaying data on the screen at a specific row. Valid only for the show command. INTEGER: 1–100000000 (Default = 1).

Ciphersuite Profile

The Ciphersuite Profile (ciphersuite-profile) table contains the list of valid ciphersuites. A ciphersuite is a set that contains both an encryption algorithm and a message authentication algorithm.

Table Name: CIPHERSUITE-PROFILE

Table Containment Area: EMS only

Command Types

Show, add, change, and delete

Examples

```
show ciphersuite-profile id=cp1gold;
add ciphersuite-profile id=cp1gold;
change ciphersuite-profile id=cp1gold; description=This ID is used for QoS gold.
delete cipersuite-profile id=cp1gold;
```

Usage Guidelines

Primary key: id

Add Rules: Id cannot exist.

Delete Rules: Id cannot exist in any dependency tables.

Syntax Description

* ID	Primary key. ID of Ciphersuite Profile table. VARCHAR(16): 1–16 ASCII characters.
AUTO-REFRESH	Specifies whether to display cached data on the screen. Valid only for the show command. CHAR(1): Y/N (Default = Y). Y—Queries the database for the most current data. N—Queries the database for the most current data only if the cached data is unavailable.
DESCRIPTION	Described by the service provider. VARCHAR(64): 1–64 ASCII characters.
DISPLAY	Specifies what token information to display on the screen. Valid only for the show command. VARCHAR(1024): 1–1024 (Default = all tokens are displayed). Permitted values are any valid token that can be shown for this command. Multiple tokens can be entered by separating with a comma.
LIMIT	Specifies the number of rows to display on the screen. Valid only for the show command. INTEGER: 1–100000000 (Default = 100000000). **Note** The actual maximum number of rows displayed is currently lower than 100000000 due to software limitations.
ORDER	Specifies whether to display data on the screen in a sorted order. Valid only for the show command. VARCHAR(1024): 1–1024 (Default = all rows are displayed). Permitted values are any valid token that can be shown for this command. Multiple tokens can be entered by separating with a comma.
START-ROW	Specifies to begin displaying data on the screen at a specific row. Valid only for the show command. INTEGER: 1–100000000 (Default = 1).

IPSec Kerberos

The IPSec Kerberos (ipsec-kerberos) table contains the Kerberos configuration parameters used by IPSec and the associated key management application.

Table Name: IPSEC-KERBEROS

Table Containment Area: Call Agent

Command Types

Show, add, change, delete

Examples

```
show ipsec-kerberos;
add ipsec-kerberos krb-fqdn=cms-ca1.ciscolab.com; krb-realm=cisco-realm.com;
krb-srv-key=5468697320697320612061206b6579206f66203234206368612e;
srv-key-version=3;
change ipsec-kerberos; krb-fqdn=cms-ca1.ciscolab.com; krb-max-retry=25;
change ipsec-kerberos krb-fqdn=cms-ca1.ciscolab.com; srv-key-version=4;
krb-srv-key=12345678901234567890123456789012345678901234567890123456789012345678;
delete ipsec-kerberos; krb-fqdn=cms-ca1.ciscolab.com;
```

Usage Guidelines

Primary Key Token(s): krb-fqdn

Add Rules: See restrictions in the Syntax Description table. Limit 1 entry.

Change Rules: See restrictions in the Syntax Description table.

Delete Rules: None.

Other Rules:

- If krb-srv-key is changed, srv-key-version must be changed also.
- If srv-key-version is changed, krb-srv-key must be changed also.
- For krb-srv-key and srv-key-version, each cannot exist in the IPSec Kerberos Old Service Keys table. The system updates the IPSec Kerberos table before it updates the IPSec Kerberos Old Service Keys table.

Syntax Description

* KRB-FQDN	Primary key. The Kerberos fully qualified domain name for the Call Agent. It is used to create the call management server (CMS) principal name. The krb-fqdn must be the FQDN used on the Kerberos Domain Controller (KDC) for this node. The source krb-fqdn must be a valid hostname as described in gethostbyname(3XNET). VARCHAR(256): 1–256 ASCII characters.
* KRB-REALM	The Kerberos realm, used to create the CMS principal name. VARCHAR(256): 1–256 ASCII characters.

* KRB-SRV-KEY	The Kerberos service key. When assigning a new krb-srv-key, the existing krb-srv-key is added to the IPSec Kerberos Old Service Keys table. VARCHAR(48): Length must be 48 hex characters (0–9, A–F, a–f). Input is permitted with a delimiter for readability. For example: "6854 7369 6920 2073 2061 656b 2079 666f 3220 2034 6863 2e61" is equivalent to: "6854736969202073206165 6b2079666f3220203468632e61"
* SRV-KEY-VERSION	CMS server keys. Allows the Cisco BTS 10200 Softswitch to support CMSs using different server key versions for a CMS server key. INTEGER: 1–MAXINT. **Note** MAXINT is the largest possible 4-byte integer: [2 to the power 32] –1 divided by 2.
AUTO-REFRESH	Specifies whether to display cached data on the screen. Valid only for the show command. CHAR(1): Y/N (Default = Y). Y—Queries the database for the most current data. N—Queries the database for the most current data only if the cached data is unavailable.
DISPLAY	Specifies what token information to display on the screen. Valid only for the show command. VARCHAR(1024): 1–1024 (Default = all tokens are displayed). Permitted values are any valid token that can be shown for this command. Multiple tokens can be entered by separating with a comma.
KRB-ACK-FLAG	The Kerberos Acknowledgment Flag. If enabled, an acknowledgment is requested in the AP-REPLY. CHAR(1): Y/N (Default = Y).
KRB-EXP-RETRY-TIME	The Kerberos Exponential Retry Time. Specifies the exponential backoff time, in seconds, for WAKEUP retries. SMALLINT: 1–60 (Default = 2).
KRB-MAX-OLD-SRV-KEYS	The maximum number of records to be kept in the rolling list of old Kerberos service keys. SMALLINT: 1–256 (Default = 32).
KRB-MAX-RETRY	The Kerberos maximum retries. The maximum number of times that the CMS sends a WAKEUP message without the receipt of an AP-REQ. SMALLINT: 1–100 (Default = 10).

KRB-MAX-RETRY-TIME	Kerberos Maximum Retry Time. Specifies the maximum or the total time, in seconds, that the CMS sends WAKEUP messages before it stops. SMALLINT: 1–60 (Default = 20). **Note** The krb-max-retry-time must be greater than krb-timeout and krb-exp-retry-time.
KRB-REEST-SA-ACK-FLAG	The Kerberos Reestablish Security Association (SA) Acknowledgment Flag. If enabled, the CMS reestablishes the outbound SA before the hard expiration occurs. CHAR(1): Y/N (Default = Y).
KRB-SRV-KEY-COMP-FLAG	The Kerberos Service Key Compromised Flag. If enabled, tickets using the old service key are not accepted, and a message is sent to the MTA instructing it to obtain a new ticket. If disabled, the old service key is accepted until the date-time specified in the ticket. CHAR(1): Y/N (Default = N).
KRB-TIMEOUT	The Kerberos Timeout. Specifies the amount of time, in seconds, that the CMS waits for the receipt of an AP-REQ following a WAKEUP message. SMALLINT: 1–60 (Default = 3).
LIMIT	Specifies the number of rows to display on the screen. Valid only for the show command. INTEGER: 1–100000000 (Default = 100000000). **Note** The actual maximum number of rows displayed is currently lower than 100000000 due to software limitations.
ORDER	Specifies whether to display data on the screen in a sorted order. Valid only for the show command. VARCHAR(1024): 1–1024 (Default = all rows are displayed). Permitted values are any valid token that can be shown for this command. Multiple tokens can be entered by separating with a comma.
START-ROW	Specifies to begin displaying data on the screen at a specific row. Valid only for the show command. INTEGER: 1–100000000 (Default = 1).

IPSec Kerberos Old Service Keys

The IPSec Kerberos Old Service Keys (ipsec-kerberos-keys) table contains the old Kerberos Service Keys to be used by IPSec and the associated key management application. When assigning a new krb-srv-key, the existing krb-srv-key is added to this table. This is a rolling list; when the list becomes full, the oldest service key is overwritten.

Table Name: IPSEC-KERBEROS-KEYS

Table Containment Area: Call Agent

Command Types

Show and delete

Examples

```
show ipsec-kerberos-keys;
delete ipsec-kerberos-keys; krb-srv-key=5468697320697320612061206b6579206f66206234206368612e;
```

Usage Guidelines

Primary Key Token(s): krb-srv-key

Delete Rules: None.

Other Rules: Maximum number of entries is determined by the configured value of krb-max-old-srv-keys in the IPSec Kerberos table.

Syntax Description

* KRB-SRV-KEY	Mandatory for delete. Primary key. Kerberos Service Key. This key is used for Kerberos communications. The value of this field is an old Kerberos Service Key and is set when a new krb-srv-key is configured. VARCHAR(48): 1–48 ASCII characters. Array must be 48 hex characters (0–9, A–F, a–f). When a new krb-srv-key is assigned, the existing krb-srv-key is added to this table. This is a rolling list; when the list becomes full, the oldest service key is overwritten.
* SRV-KEY-VERSION	CMS server keys. Allows the Cisco BTS 10200 Softswitch to support CMSs using different server key versions. INTEGER: 1–MAXINT. **Note** MAXINT is the largest possible 4-byte integer: [2 to the power 32]–1 divided by 2.
AUTO-REFRESH	Specifies whether to display cached data on the screen. Valid only for the show command. CHAR(1): Y/N (Default = Y). Y—Queries the database for the most current data. N—Queries the database for the most current data only if the cached data is unavailable.

DISPLAY	Specifies what token information to display on the screen. Valid only for the show command. VARCHAR(1024): 1–1024 (Default = all tokens are displayed). Permitted values are any valid token that can be shown for this command. Multiple tokens can be entered by separating with a comma.
KRB-SRV-KEY-TIMESTAMP (System generated)	Not provisionable. A system-generated time stamp with the date and time that the entry was added. INTEGER.
LIMIT	Specifies the number of rows to display on the screen. Valid only for the show command. INTEGER: 1–100000000 (Default = 100000000). **Note** The actual maximum number of rows displayed is currently lower than 100000000 due to software limitations.
ORDER	Specifies whether to display data on the screen in a sorted order. Valid only for the show command. VARCHAR(1024): 1–1024 (Default = all rows are displayed). Permitted values are any valid token that can be shown for this command. Multiple tokens can be entered by separating with a comma.
START-ROW	Specifies to begin displaying data on the screen at a specific row. Valid only for the show command. INTEGER: 1–100000000 (Default = 1).

IPSec Policy

The IPSec Policy (ipsec-policy) table contains the global security policies to be used by IPSec.

Table Name: IPSEC-POLICY

Table Containment Area: Call Agent

Command Types

Show, add, and delete

Examples

```
show ipsec-policy;
add ipsec-policy id=mta01; src-fqdn=cms-ca1.ciscolab.com; dest-fqdn=mta5.ciscolab.com;
action=ipsec;
add ipsec-policy id=mta2xy; src-ipaddr=10.10.45.89; src-ipmask=255.255.255.0;
dest-ipaddr=10.10.2.44; dest-ipmask=255.255.255.0; action=permit;
delete ipsec-policy id=mta2xy;
```

Usage Guidelines

Primary Key Token(s): id

Add Rules: Both src-fqdn and src-ipaddr cannot be specified. (Release 4.2 and Release 4.4.1)

Other Rules: src-fqdn, src-ipaddr or src-port and dest-fqdn, dest-ipaddr or dest-port must be present (Release 4.4.1).

Delete Rules: None.

Syntax Description

* ID	Primary key. Policy ID. Service provider assigns, based on network configuration. Suggested format is <device-type>NN, for example, mta01, cmts01, rks01. VARCHAR(8): 1–8 ASCII characters.
* ACTION	Defines whether security is applied to outbound or inbound traffic, both, or neither. VARCHAR(6): 1–6 ASCII characters. Permitted values are: Permit—Security on inbound traffic. Apply—Security on outbound traffic. IPSec—Security on both inbound and outbound traffic. Bypass—No security.
AUTO-REFRESH	Specifies whether to display cached data on the screen. Valid only for the show command. CHAR(1): Y/N (Default = Y). Y—Queries the database for the most current data. N—Queries the database for the most current data only if the cached data is unavailable.
DEST-FQDN	Fully qualified domain name for the destination network element to which this security policy applies. The destination address value must be a valid hostname as described in gethostbyname(3XNET). You cannot specify both a dest-fqdn and a dest-ipaddr at the same time. VARCHAR(256): 1–256 ASCII characters. **Note** The 'getprotobyname' function is a UNIX system function that refers to the Internet protocols TCP, UDP, and so forth.
DEST-IPADDR	IP address for the destination network element(s) to which this security policy applies. The destination address value must be a valid hostname as described in gethostbyname(3XNET). You cannot specify both a dest-fqdn and a dest-ipaddr at the same time. VARCHAR(15): 1–15 ASCII characters. Format: IPv4 Internet decimal dot notation.
DEST-IPMASK	Valid only if dest-ipaddr is specified. The IP address mask used to establish a range of IP addresses for the destination network element(s) to which this security policy applies. VARCHAR(15): 1–15 ASCII characters. Format: IPv4 Internet decimal dot notation.

DEST-PORT	The specific port for the destination network element to which this security policy applies. SMALLINT: 1–65534.
DISPLAY	Specifies what token information to display on the screen. Valid only for the show command. VARCHAR(1024): 1–1024 (Default = all tokens are displayed). Permitted values are any valid token that can be shown for this command. Multiple tokens can be entered by separating with a comma.
LIMIT	Specifies the number of rows to display on the screen. Valid only for the show command. INTEGER: 1–100000000 (Default = 100000000). **Note** The actual maximum number of rows displayed is currently lower than 100000000 due to software limitations.
ORDER	Specifies whether to display data on the screen in a sorted order. Valid only for the show command. VARCHAR(1024): 1–1024 (Default = all rows are displayed). Permitted values are any valid token that can be shown for this command. Multiple tokens can be entered by separating with a comma.
SRC-FQDN	Fully qualified domain name for the source network element that this security policy applies to. The source fqdn must be a valid hostname as described in gethostbyname(3XNET). You cannot specify both an src-fqdn and a src-ipaddr at the same time. VARCHAR(256): 1–256 ASCII characters. **Note** The 'getprotobyname' function is a UNIX system function that refers to Internet protocols TCP, UDP, and so forth.
SRC-IPADDR	IP address for the source network element(s) that this security policy applies to. The source address value must be a valid hostname as described in gethostbyname(3XNET). You cannot specify both an src-fqdn and an src-ipaddr at the same time. VARCHAR(15): 1–15 ASCII characters. Format: IPv4 Internet decimal dot notation.
SRC-IPMASK	Valid only if src-ipaddr is specified. The IP address mask used to establish a range of IP addresses for the source network element(s) to which this security policy applies. VARCHAR(15): 1–15 ASCII characters. Format: IPv4 Internet decimal dot notation.
SRC-PORT	Specific port for the source network element that this security policy applies to. SMALLINT: 1–65534.
START-ROW	Specifies to begin displaying data on the screen at a specific row. Valid only for the show command. INTEGER: 1–100000000 (Default = 1).

ULP-NAME	IPSec SA upper-layer protocol name that the entry is matched against. Used if the SA is created only for specific protocol traffic (for example IP traffic). The value is a string as described in getprotobyname(3XNET). You cannot specify both an ulp-name and an ulp-number at the same time. VARCHAR(8): 1–8 ASCII characters. Permitted values are: IP (Default) TCP UDP The default value (IP) is adequate for most applications.
ULP-NUMBER	Upper-layer protocol that the entry is matched against. You cannot specify both an ulp-name and an ulp-number at the same time. SMALLINT: 0–255. The value is a number as described in getprotobyname(3XNET).

IPSec Security Administration

The IPSec Security Administration (SA) (ipsec-sa) table contains the required IPSec security associations that are not associated with IKE or Kerberos key management.

Table Name: IPSEC-SA

Table Containment Area: Call Agent

Command Types

Show, add, change, and delete

Examples

```
show ipsec-sa;
add ipsec-sa id=cmts01; auth-algo=hmac-sha-1;
auth-key=2069732061206b6579206f66203234206368612e; dest=10.10.22.33; encrypt-algo=des;
encrypt-key=4bb586a120532c07; spi=85723;
change ipsec-sa id=cmts01; encrypt-algo=3des;
encrypt-key=abcdefabcdefabcdefabcdefabcdefabcdefabcdefabcdef; soft-lifetime=3600;
hard-lifetime=7200;
delete ipsec-sa id=cmts01;
```

Usage Guidelines

Primary Key Token(s): id

Add Rules: See specific restrictions in the Syntax Description.

Change Rules: See specific restrictions in the Syntax Description.

Delete Rules: None.

Other Rules:

- The auth-key is a maximum of 40 characters.
- The size of the key configured is validated to ensure that it is 32 characters if auth-algo=hmac-md5 and 40 characters if auth-algo=hmac-sha-1.
- The size of the encrypt-key configured is validated to ensure that it is 16 characters if encrypt-algo=des and 48 characters if encrypt-algo=3des.

Syntax Description

* ID	Primary key. Service provider assigns an ID or SA identifier based on network configuration. VARCHAR(8): 1–8 ASCII characters. Suggested format is <device-type>NN, for example: mta01, cmts01, rks01.
* AUTH-ALGO	Specifies the authentication algorithm for an SA. VARCHAR(10): 1–10 ASCII characters. Permitted values are: HMAC-MD5 HMAC-SHA-1
* AUTH-KEY	Specifies the authentication key for this SA. Length varies depending on auth-algo selected. The key must be 32 characters if HMAC-MD5 is selected and 40 characters if HMAC-SHA-1 is selected. VARCHAR(40): 1–40 ASCII characters. The key is expressed as a string of hexadecimal digits (0–9, A–F, a–f).
* DEST	Specifies the destination address of the SA. The source address value must be a valid host as described in gethostbyname(3XNET). VARCHAR(15): 1–15 ASCII characters. Format: IPv4 Internet decimal dot notation. **Note** The 'getprotobyname' function is a UNIX system function that refers to the Internet protocols TCP, UDP, and so forth.
* ENCRYPT-ALGO	Specifies the encryption algorithm for an SA. VARCHAR(4): 1–4 ASCII characters. Permitted values are: DES 3DES
* ENCRYPT-KEY	Specifies the encryption key for this SA. Length varies depending on the encrypt-algo selected. The key must be 16 characters if DES is selected and 48 characters if the 3DES is selected. VARCHAR(48): 1–48 ASCII characters. The key is expressed as a string of hexadecimal digits (0–9, A–F, a–f).
* SPI	Security parameters index of the SA. INTEGER: –MAXINT to MAXINT. Permitted values are any valid integer. **Note** MAXINT is the largest possible 4-byte integer: [2 to the power 32]–1.

AUTO-REFRESH	Specifies whether to display cached data on the screen. Valid only for the show command. CHAR(1): Y/N (Default = Y). Y—Queries the database for the most current data. N—Queries the database for the most current data only if the cached data is unavailable.
DISPLAY	Specifies what token information to display on the screen. Valid only for the show command. VARCHAR(1024): 1–1024 (Default = all tokens are displayed). Permitted values are any valid token that can be shown for this command. Multiple tokens can be entered by separating with a comma.
HARD-LIFETIME	Specifies the number of seconds that this SA can exist. When the hard lifetime expires, the SA is deleted automatically by the system. INTEGER: 0–MAXINT (Default = 0). **Note** If hard-lifetime is not specified, the default value is zero, which means the SA does not expire based on how long it has been since the SA was added. MAXINT is the largest possible 4-byte integer: [2 to the power 32]–1.
LIMIT	Specifies the number of rows to display on the screen. Valid only for the show command. INTEGER: 1–100000000 (Default = 100000000). **Note** The actual maximum number of rows displayed is currently lower than 100000000 due to software limitations.
ORDER	Specifies whether to display data on the screen in a sorted order. Valid only for the show command. VARCHAR(1024): 1–1024 (Default = all rows are displayed). Permitted values are any valid token that can be shown for this command. Multiple tokens can be entered by separating with a comma.
SOFT-LIFETIME	Specifies the number of seconds that this SA can exist. When the soft lifetime expires, an SADB_EXPIRE message is transmitted by the system, and the SA is changed to DYING. INTEGER: 0–MAXINT (Default = 0). **Note** If SOFT-LIFETIME is not specified, the default value is zero, which means the SA does not expire based on how long it has been since the SA was added. MAXINT is the largest possible 4-byte integer: [2 to the power 32]–1.

SRC	Specifies the source address of the SA. The source address value must be valid host as described in gethostbyname(3XNET). VARCHAR(15): 1–15 ASCII characters. Format: IPv4 Internet decimal dot notation.
START-ROW	Specifies to begin displaying data on the screen at a specific row. Valid only for the show command. INTEGER: 1–100000000 (Default = 1).

Radius Profile

The Radius Profile (radius-profile) table is used in PacketCable networks that run a billing system based on event messages and to provide radius-based authentication for the Limited Call Duration (LCD) feature.

Table Name: RADIUS-PROFILE

Table Containment Area: Call Agent

Command Types

Show, add, change, and delete

Examples

```
show radius-profile id=rks1;
show radius-profile-unencr id=rks1;
add radius-profile id=rks1; tsap-addr=165.12.23.1:1851;
change radius-profile id=rks1; acc-req-retransmit=2; acc-rsp-timer=3;
delete radius-profile id=rks1;
```

Usage Guidelines

Primary Key Token(s): id

Unique Key Token(s): tsap-addr

Add Rules: None.

Change Rules: None.

Delete Rules: None.

Syntax Description

* ID	Primary key. Radius profile ID. ASCII string that identifies the primary or secondary record keeping server (RKS). VARCHAR(16): 1–16 ASCII characters.

* TSAP-ADDR	Unique key. TSAP address for the radius server. Unique IP address, or IP address and port number, of the primary or secondary RKS. This value must be an IP address (not a domain name), however, a domain name is allowed if server-type=prepaid. VARCHAR(64): 1–64 ASCII characters. **Note** The value of tsap-addr can be updated dynamically using the following command. No system restart is required. `change radius-profile id=[primary RKS id | secondary RKS id]; tsap-addr=[IP address:port-number];`
ACC-REQ-RETRANSMIT	Specifies the number of retransmissions of unacknowledged accounting requests. Also specifies the number of accounting request retransmissions for event message (EM) applications. This is the number of times the Cisco BTS 10200 Softswitch attempts to retransmit an EM to a target RKS. When this limit is reached, the Cisco BTS 10200 Softswitch treats the target RKS as nonresponsive and begins transmitting to another RKS. In the unlikely event that the Cisco BTS 10200 Softswitch tries, but fails, to receive acknowledgment from both RKSs, it begins storing EM files on the currently active Call Agent. INTEGER: 1–4 (Default = 3). INTEGER: 0–5 (Default = 3) (Release 4.2)
ACC-RSP-TIMER	Specifies the number of seconds that the Cisco BTS 10200 Softswitch waits for an acknowledgment of a transmission by an external radius server before retransmitting. Also specifies the time the Cisco BTS 10200 Softswitch waits for a target RKS to acknowledge receipt of a transmitted EM for EM applications. When this timer expires, the Cisco BTS 10200 Softswitch retransmits the EM. INTEGER: 1–10 (Default = 2).
AUTO-REFRESH	Specifies whether to display cached data on the screen. Valid only for the show command. CHAR(1): Y/N (Default = Y). Y—Queries the database for the most current data. N—Queries the database for the most current data only if the cached data is unavailable.
DESCRIPTION	Described by the service provider. VARCHAR(64): 1–64 ASCII characters.
DISPLAY	Specifies what token information to display on the screen. Valid only for the show command. VARCHAR(1024): 1–1024 (Default = all tokens are displayed). Permitted values are any valid token that can be shown for this command. Multiple tokens can be entered by separating with a comma.
ENCRYPTION-KEY	Specifies an optional 16-byte encryption key. VARCHAR(16): 1–16 hex characters (0–9, A–F) (Default = all zeros (0000000000000000)).

IKE-CS	Specifies a list of ciphersuites supported by IKE, in priority order. This list is used to negotiate the encryption-authentication algorithm pair used by IKE. The list can contain only those ciphersuites using the authentication algorithms HMAC-MD5 and HMAC-SHA and the encryption algorithm ESP-3DES. VARCHAR(64): 1–64 ASCII characters. Permitted values are: 3DES-MD5, 3DES-SHA1 (Default list) 3DES-SHA1, 3DES-MD5 3DES-MD5 3DES-SHA1
IKE-GROUP	Internet Key Exchange (IKE) group. Specifies the available groups in which the Diffie-Helman exchange can occur. INTEGER: Valid values are 1 or 2 (Default = 2).
IKE-KEY	The IKE preshared key. This value is used for security on the interface between the Cisco BTS 10200 Softswitch and the RKS. VARCHAR(256): 1–256 ASCII characters. (Release 4.5) The system encrypts the value of the ike-key token and stores the encrypted value as ike-key-encr. See the ike-key-encr token for additional details.
IKE-KEY-ENCR (System generated) (Release 4.5)	The IKE preshared key in encrypted form. The system encrypts the value of the ike-key token and stores the encrypted value as ike-key-encr. It is then decrypted and displayed only when accessed by a privileged user. VARCHAR(256): 1–256 ASCII characters. To show the ike-key-encr token in encrypted form, use the following command: `show radius-profile;` To show the ike-key token in unencrypted form, use the following command: **`show radius-profile-unencr;`**
IKE-SA-LIFETIME	Sets the IKE SA expiration, in seconds. This is the hard expiration. INTEGER: 0–MAXINT (Default = 86400). **Note** MAXINT is the largest possible 4-byte integer, that is, [2 to the power 32]–1.

IPSEC-SA-ESP-CS	The IPSec SA ESP ciphersuite list in priority order. Used to negotiate an encryption-authentication algorithm pair used by IPSec. The list can contain only those ciphersuites using the authentication algorithms HMAC-MD5 and HMAC-SHA and the encryption algorithms ESP-3DES and ESP-NULL. VARCHAR(64): 1–64 ASCII characters. 3DES-MD5, 3DES-SHA1, NULL-MD5, NULL-SHA1 (Default list) **Note** This list can be modified to be a subset of this initial list using the CLI and can be reordered to specify a new priority selection. For example: - 3DES-MD5, 3DES-SHA1, NULL-SHA1, NULL-MD5 - 3DES-SHA1, NULL-MD5, NULL-SHA1 - 3DES-MD5, NULL-MD5 - NULL-SHA1 and additional values
IPSEC-SA-GRACE-PERIOD	The IPSec SA key expiration grace period, in seconds. This is used to calculate the soft expiration. INTEGER: 0–MAXINT (Default = 21600). **Note** The ipsec-sa-grace-period must be less than or equal to 25% of the provisioned value for ipsec-sa-lifetime. If not specified when provisioning a new ipsec-sa-lifetime, the ipsec-sa-grace-period defaults to 25% of the ipsec-sa-lifetime.
IPSEC-SA-LIFETIME	The IPSec SA expiration in seconds. This is the hard expiration. INTEGER: 0–MAXINT (Default = 86400). **Note** MAXINT is defined as the largest possible 4-byte integer, that is, [2 to the power 32]–1.
IPSEC-ULP-NAME	IPSec SA upper-layer protocol name. Used if the SA is created only for specific protocol traffic (for example, IP traffic). The value is a string as described in getprotobyname(3XNET). VARCHAR(8): 1–8 ASCII characters. Permitted values are: IP (Default) TCP UDP **Note** The default value (IP) is adequate for most applications.
LIMIT	Specifies the number of rows to display on the screen. Valid only for the show command. INTEGER: 1–100000000 (Default = 100000000). **Note** The actual maximum number of rows displayed is currently lower than 100000000 due to software limitations.
ORDER	Specifies whether to display data on the screen in a sorted order. Valid only for the show command. VARCHAR(1024): 1–1024 (Default = all rows are displayed). Permitted values are any valid token that can be shown for this command. Multiple tokens can be entered by separating with a comma.

SERVER-TYPE (Release 4.5)	Specifies whether the Radius server is for limited call duration features. VARCHAR(8): 1–8 ASCII characters (Default = OTHER). Permitted values are: PREPAID OTHER
START-ROW	Specifies to begin displaying data on the screen at a specific row. Valid only for the show command. INTEGER: 1–100000000 (Default = 1).