

Chapter 26

Providing Admission Control with SRC-ACP on a Solaris Platform

This chapter describes how to install, configure, and manage the SRC Admission Control Plug-In (SRC-ACP) application on a Solaris platform using the SRC configuration applications that run only on Solaris platforms.

You can also use the CLI that runs on Solaris platforms and the C-series Controllers to configure SRC-ACP. See *Chapter 21, Configuring Admission Control with the SRC CLI*.

Topics in this chapter include:

- Installing SRC-ACP on page 354
- Configuring SRC-ACP on page 358
- Starting SRC-ACP on page 394
- Stopping SRC-ACP on page 394
- Monitoring and Managing SRC-ACP on page 394

For information about SRC-ACP, see *Chapter 20, Overview of Providing Admission Control with SRC-ACP*.

Installing SRC-ACP

SRC-ACP uses the SAE plug-in interface. You can install SRC-ACP on the same host as the SAE; doing so will simplify the SRC configuration. However, you may improve the performance of the SRC network by installing SRC-ACP on a separate host from the SAE.

The SRC-ACP package for Solaris platforms is located on the application library CD.

To install the SRC-ACP package:

1. On the UNIX host where you will install SRC-ACP, log in as **root**.
2. Place the application library CD in the CD drive.
3. Launch the **pkgadd** tool.

```
pkgadd -d /cdrom/cdrom0/ACP_for_SDX/UMCacp
```

The tool displays the license agreement.

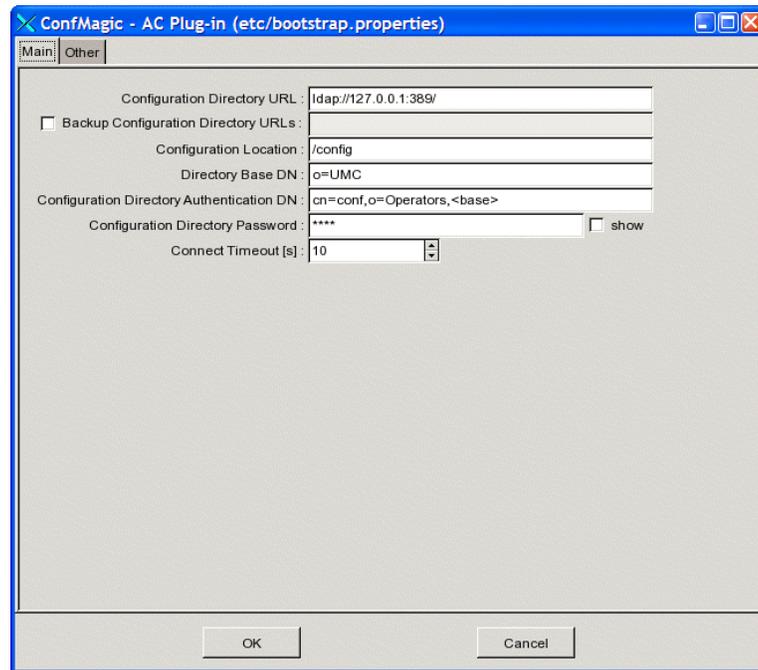
4. Press Enter to move through the agreement, and then enter **y** to accept the license agreement when prompted by the tool.
5. Follow the prompt directions to accept the installation directory for the package, to permit the use of superuser scripts required for the package, and so on.

After you have installed the SRC-ACP application on a host, you must add the SRC-ACP configuration to the directory. To do so:

1. On the SRC-ACP host, log in as **root** or as another authorized administrator.
2. Launch the local configuration tool from the ACP installation directory.

```
./opt/UMC/acp/etc/config -l&
```

The local configuration tool window appears.



3. Complete the fields in the local configuration tool window. *Local Properties for SRC-ACP* on page 355 describes the fields on the Main tab and the Other tab.
4. Click **OK**.
5. A file called *bootstrap.properties* appears in the */opt/UMC/acp/etc* folder, and the SRC-ACP configuration appears in the directory. The SRC software automatically sets some values for properties that do not appear in the local configuration tool window.

Local Properties for SRC-ACP

Use the fields in this section to configure the local properties for SRC-ACP.

Configuration Directory URL

- URL of the primary directory.
- Value—URL in the format `ldap:// <host > :389`
 - <host > —IP address or name of directory host
- Example—`ldap://192.0.2.1:389/`
- Property name—`Config.java.naming.provider.url`

Backup Configuration Directory URLs

- List of redundant directories.
- Value—Space-separated list of URLs; URLs have the format `ldap:// <host > :389`
 - `<host >` —IP address or name of directory host
- Default—Unspecified
- Example—`ldap://192.0.2.1:389/ ldap://192.0.2.3:389/`
- Property name—`Config.net.juniper.smgt.des.backup_provider_urls`

Configuration Location

- Name of the object that contains the SRC-ACP configuration data.
- Value—`/ <objectName >`
- Guidelines—This object appears in `l = ACP, ou = staticConfiguration, o = Management, o = umc`. Sensible choices for this field are the name of the host or the name of a given location. If you configure SRC-ACP redundancy, use the same name in the ACP configurations on both hosts.
- Default—`/config`
- Example—`bostonConfig`
- Property name—`Config.ACP.namespace`

Directory Base DN

- DN of the root of the SRC data in the directory.
- Value—`o = <DN >`
 - `<DN >` —DN
- Guidelines—If you are storing non-SRC data in the directory, and that data changes frequently whereas the SRC data does not, you may need to adjust the default value to improve performance. For optimal performance, set the value to the DN of an entry superior to both the SRC data and the changing non-SRC data.
- Default—`o = umc`
- Example—`o = umc`
- Property name—`Config.net.juniper.smgt.des.event_baseDN`

Configuration Directory Authentication DN

- DN of the directory entry that defines the username with which the SRC component accesses the directory.
- Value—`<DN >`
- Example—`cn = nic, ou = Components, o = Operators, <base >`
- Default—`cn = conf, o = Operators, <base >`
- Property name—`Config.java.naming.security.principal`

Configuration Directory Password

- Password with which SRC-ACP accesses the directory.
- Value— < password >
- Guidelines—The password can be encoded in base64 and not visible in plain text. To use an encoded value, use the format `{BASE64} < encoded-value >`.
- Default—conf
- Example—secret
- Property name—Config.java.naming.security.credentials

Connect Timeouts (s)

- Maximum time that the directory eventing system (DES) waits for the directory to respond.
- Value—Number of seconds in the range 1-2147483647
- Default—10
- Example—5
- Property name—Config.net.juniper.smgmt.des.connect.timeout

Java Runtime Environment

- Path to the Java Runtime Environment (JRE).
- Value—Text string
- Guidelines—The SRC software requires a JRE that conforms to the Java 2 specification. The SRC software has been tested with Sun's JRE. Check the *SRC Release Notes* for information about which version of the Sun JRE is distributed with the SRC software. Other JREs should work but have not been tested with the SRC software.
- Default—`../jre/bin/java` (path for the JRE that is distributed with the SRC software and installed with the other SRC components)
- Property name—Acp.java

Java Heap Size

- Maximum amount of memory available to the JRE.
- Value—Number of megabytes in the format < integer > m
- Guidelines—Change this value if you have problems caused by lack of memory. Set the value lower than the available physical memory to avoid low performance caused by disk swapping.
- Default—64m

Configuring SRC-ACP

To use SRC-ACP in the SRC network, you must perform some configuration. For information about these configuration procedures, see:

1. Configuring the SAE for SRC-ACP on page 358
2. Configuring SRC-ACP Properties on page 361
3. (Edge and dual mode only) Configuring SRC-ACP to Manage the Edge Network on page 376
4. (Backbone and dual mode only) Configuring SRC-ACP to Manage the Backbone Network on page 382

Configuring the SAE for SRC-ACP

You must configure the SAE to recognize SRC-ACP by adding some information about SRC-ACP to the SAE properties. To do so:

1. Configure SRC-ACP as an external plug-in for the SAE.
2. Configure event publishers.
3. (Backbone and dual mode only) Optionally, configure a hosted plug-in that monitors the state of interfaces on VRs.

Configuring SRC-ACP as an External Plug-In

To configure an external plug-in for the SAE, see *SRC-PE Subscribers and Subscriptions Guide, Chapter 10, Overview of Configuring Plug-Ins for Solaris Platforms*. Use the following values for the plug-in attributes:

- Value for edge and dual modes—PA_UPSTREAM_BANDWIDTH, PA_DOWNSTREAM_BANDWIDTH, PA_SERVICE_NAME, PA_ROUTER_NAME, PA_LOGIN_NAME, PA_USER_DN, PA_PORT_ID, PA_SESSION_ID, PA_USER_IP_ADDRESS, PA_NAS_IP, PA_USER_SESSION_ID, PA_EVENT_TIME
- Value for backbone mode—PA_UPSTREAM_BANDWIDTH, PA_DOWNSTREAM_BANDWIDTH, PA_SERVICE_NAME, PA_ROUTER_NAME, PA_SESSION_ID, PA_NAS_IP, PA_EVENT_TIME

Configuring Event Publishers

You must configure the SAE to publish the following types of events to SRC-ACP:

- (Edge and dual mode only) Global user tracking
- Global service authorization
- Global service tracking

For information about configuring event publishers, see *SRC-PE Subscribers and Subscriptions Guide, Chapter 11, Configuring Accounting and Authentication Plug-Ins with the SRC CLI*. Identify the instance of SRC-ACP by the name of the host on which you configured it.

Configuring the SAE to Monitor Interfaces for Congestion Points



NOTE: Configure this feature only if SRC-ACP is in backbone or dual mode.

The SAE uses a hosted internal plug-in to monitor the state of interfaces on a VR for backbone congestion points. If a subscriber tries to activate a service on an interface that is unavailable, the SAE denies the request. The plug-in also monitors the directory for new backbone congestion points. To configure an internal plug-in for the SAE, see *SRC-PE Subscribers and Subscriptions Guide, Chapter 10, Overview of Configuring Plug-Ins for Solaris Platforms* and use the properties described in *Internal Plug-In Properties for Monitoring Congestion Points* on page 359.

When this plug-in initializes, it reads all the backbone services from the directory and generates a list of the DNs (network interfaces) of the backbone congestion points. The SAE sends interface tracking events, which contain the names of the interfaces, VRs, and routers to this plug-in. For this feature to work correctly, the interface, VR, and router must appear in `o = AdmissionControl`, `o = umc` (see *Configuring Network Interfaces in the Directory* on page 382).

Internal Plug-In Properties for Monitoring Congestion Points

Use the descriptions in this section to configure an internal plug-in for the SAE.

Plug-in Class

- Class name of the plug-in.
- Value—`net.juniper.smgmt.sae.plugin.ACPIntfListener`

Plugin.acpIntfListener.host

- IP address or name of the host that supports the directory that contains backbone service definitions and network interfaces.
- Value—Plugin.acpIntfListener.host = < host > : < port >
 - < host > —IP address or name of host
 - < portNumber > —Number of the TCP port; default is 389
- Default—Plugin.acpIntfListener.host = 127.0.0.1

Plugin.acpIntfListener.bindDN

- DN of the directory entry that defines the username with which the plug-in accesses the directory.
- Value—DN
- Default—Plugin.acpIntfListener.bindDN = cn = umcadmin, < base >

Plugin.acpIntfListener.bindPW

- Password with which the plug-in accesses the directory.
- Value—Text string
- Default—Plugin.acpIntfListener.bindPW = ssp
- Example—Plugin.acpIntfListener.bindPW = secret

Plugin.acpIntfListener.baseDN

- DN at which SRC-ACP stores backbone congestion points.
- Value—DN
- Default—Plugin.acpIntfListener.baseDN = o = CongestionPoints, < base >

Plugin.acpIntfListener.acpBaseDN

- DN at which SRC-ACP stores edge congestion points.
- Value—DN
- Default—Plugin.acpIntfListener.acpBaseDN = o = AdmissionControl, < base >

Plugin.acpIntfListener.timeout

- Maximum time that the plug-in waits for the router to respond.
- Value—Number of milliseconds in the range 0–2147483647
 - 0—No timeout
 - Other values—Actual time
- Default—Plugin.acpIntfListener.timeout = 5000

Plugin.acpIntfListener.objectref = objectref

- Object reference for the ACP plug-in, as defined in the field ACP.ior in the ACP's CORBA properties (see *Configuring SRC-ACP Properties* on page 361).

Plugin.acpIntfListener.<standardJNDISuffix>**Plugin.acpIntfListener.des.net.juniper.smgt.des.<property suffix>**

- Standard Java Naming and Directory Interface (JNDI) and DES properties. For complete information about these properties, see *SRC-PE Getting Started Guide, Chapter 37, Distributing Directory Changes to SRC Components on a Solaris Platform*. The following list shows the properties you should include, with suggested values.
 - Plugin.acpIntfListener.securityProtocol = ldaps
 - Plugin.acpIntfListener.des.net.juniper.smgt.des.event_baseDN = o = CongestionPoints, < base >
 - Plugin.acpIntfListener.des.net.juniper.smgt.des.enable_sysman = true
 - Plugin.acpIntfListener.des.net.juniper.smgt.des.polling_interval = 30
 - Plugin.acpIntfListener.des.net.juniper.smgt.des.connect.timeout = 10
 - Plugin.acpIntfListener.des.net.juniper.smgt.des.retry_interval = 60
 - Plugin.acpIntfListener.des.net.juniper.smgt.des.connectioncheck_interval = 60
 - Plugin.acpIntfListener.des.net.juniper.smgt.des.signatureDN = < base >
 - Plugin.acpIntfListener.des.net.juniper.smgt.lib.config.polling_timeout = 10
 - Plugin.acpIntfListener.des.net.juniper.smgt.des.enable_eventing = true
 - Plugin.acpIntfListener.des.net.juniper.smgt.des.share_connection = false
 - Plugin.acpIntfListener.des.net.juniper.smgt.des.connection_manager_id = ACPIntfListener

Configuring SRC-ACP Properties

To configure SRC-ACP properties, you can use SDX Admin to modify ACP properties in *I = ACP*, *ou = staticConfiguration*, *ou = Configuration*, *o = Management*, *o = umc*.

You can also use the SRC CLI. See *Chapter 21, Configuring Admission Control with the SRC CLI*.

Configuring Logging

To configure logging, see *Configuring Logging Destinations for SRC-ACP* on page 294. For information about configuring logging, see *SRC-PE Monitoring and Troubleshooting Guide, Chapter 5, Managing SRC Log Files on a Solaris Platform*.

Configuring SRC-ACP Operation

To configure how SRC-ACP operates:

1. Access SDX Admin.
2. In the navigation pane, highlight the entry *I = ACP, ou = staticConfiguration, ou = Configuration, o = Management, o = umc*.
3. Click the Main tab in the ACP Configuration pane.
4. Edit or accept the default values for the properties that configure how SRC-ACP operates. See *SRC-ACP Operating Properties* on page 362.

SRC-ACP Operating Properties

In SDX Admin, you can modify the following SRC-ACP operating properties in the content pane for an SRC-ACP configuration.

ACP.backup.dir

- Folder that stores backup information about subscribers, services, and congestion points.
- Value—Absolute path or a path relative to *opt/UMC/acp*
- Default—backup

ACP.mode

- Regions of the network that SRC-ACP manages.
- Value
 - Edge—SRC-ACP operates in the edge region of network only.
 - Backbone—SRC-ACP operates in the backbone region of the network only.
 - Dual—SRC-ACP operates in both the edge and backbone regions of network.
- Default—Dual

ACP.backup.cacheSize

- Number of plug-in events from the SAE that SRC-ACP can store in its cache. Specifying a large number increases the efficiency of SRC-ACP, and minimizes the use of CPU resources; however, the amount of memory available for the cache will depend on the host's resources.
- Value—Integer in the range 0–4294967295
- Default—10000

ACP.overloadControl

- Specifies how SRC-ACP deals with situations where the components exceed the allocated bandwidth because the service was activated after the authorization was granted.
- Value—Integer in the range -1–4294967295
 - -1—SRC-ACP ignores overload
 - Integer greater than or equal to 0 – bandwidth (in bps) by which the maximum may be exceeded
- Default—0

ACP.INTFAutoCompletion

- Specifies whether SRC-ACP uses the information acquired from the router to determine the congestion points (see *Deriving Edge Congestion Points* on page 275).
- Value
 - Yes—Information used
 - No—Information not used
- Default—No

ACP.BackgroundBandwidthTuningFactors

- Specifies factors that compensate for actual use of bandwidth, as opposed to allocated bandwidth.
- Value—List of tuning factors, separated by commas; each tuning factor is a floating number in the range 0–1
- Default—None
- Example—0.8, 0.9

UserBandwidthExceed.message

- Error message that SRC-ACP sends when the subscriber exceeds the allocated bandwidth.
- Value—Text string
- Default—User bandwidth exceeded

networkBandwidthExceed.message

- Error message that SRC-ACP sends when traffic flow exceeds the allocated bandwidth on an interface between the subscriber and the router.
- Value—Text string
- Default—Network bandwidth exceeded

ACP.backupDb.reorganizationSize

- Value by which the sum of the sizes of the files that contain ACP data can increment before SRC-ACP reorganizes the files. Reorganizing the files reduces their size.
- Value—Text string in the format < number > m or < number > g
 - < number > m—Size of database in megabytes
 - < number > g—Size of database in gigabytes
- Default—100m
- Example—1g
- Guidelines—Choose a value that is significantly lower than the capacity of the machine's hard disk.

ACP.indexedDB.keys

- Values to look for in the configuration data. Specifying index keys can improve performance by filtering the data.
- Value—List of attributes, separated by commas; an attribute is one of the following text strings
 - accountingId—Value of directory attribute accountingUserId.
 - dhcpPacket—Content of the DHCP discover request.
 - hostname— Name of the host on which the SAE is installed.
 - ifIndex—SNMP index of the interface. This attribute is not supported on JUNOS routing platforms.
 - ifRadiusClass—RADIUS class attribute on the JUNOS interface. This attribute is not supported on JUNOS routing platforms.
 - ifSessionId—Identifier for RADIUS accounting on the JUNOS interface. This attribute is not supported on JUNOS routing platforms.
 - interfaceAlias—Alias of the interface; that is, the IP description in the interface configuration.
 - interfaceDescr—SNMP description of the interface.
 - interfaceName—Name of the interface.
 - loginName—Subscriber's login name.
 - nasInetAddress—IP address of the router; using a byte array instead of an integer.
 - nasPort—NAS port used by the router to identify the interface to RADIUS.
 - portId—Identifier of VLAN or virtual circuit. For a virtual circuit, use the format < VPI > / < VCI > . This attribute is not supported on JUNOS routing platforms.
 - < VPI > —Virtual path identifier
 - < VCI > —Virtual connection identifier
 - primaryUserName—PPP login name or the public DHCP username. This attribute is not supported on JUNOS routing platforms.

- routerName—Name of the virtual router in the format < virtualRouter > @ < router > .
 - < virtualRouter > —Virtual router name
 - < router > —Router name
- routerType—Type of router driver.
- userInetAddress—IP address of the subscriber; using a byte array instead of an integer.
- userMacAddress—MAC address of the DHCP subscriber. This attribute is not supported on JUNOS routing platforms.
- userRadiusClass—RADIUS class attribute of the subscriber session for a service. This attribute can occur multiple times and can be returned by an authorization plug-in.
- userType—Type of subscriber.
- Default—interfaceName, routerName

ACP.interfaceTracking.filters

- Interface tracking event to be ignored by SRC-ACP. Filtering the interface tracking events can improve performance and can reduce the amount of memory required for keeping the congestion points updated.
- Value—Filter strings in the format of a list of < attribute > = < value > pairs; that can be contained within query operations
 - < attribute > —Name of an attribute for an interface tracking event. See value for the field ACP.indexedDB.keys on page 364.
 - < value > —Filtering string of the following types:
 - *—Any value
 - Explicit string—Any value matching the specified string (not case-sensitive)
 - String containing an asterisk—Any value containing the specified string (not case-sensitive)
 - To perform query operations on filter strings, you can use the following values in your filter strings:
 - ()—Match no objects.
 - (*)—Match all objects.
 - (& < filter > < filter > ...)—Performs logical AND operation on filter strings; true if all filter strings match.
 - (| < filter > < filter > ...)—Performs logical OR operation on filter strings; true if at least one filter string matches.
 - (! < filter >)—Performs logical NOT operation on filter string; true if the filter string does not match.
- Default—*
- Example—(& (interfaceName = fastEthernet3/0) (routerName = default@erx))

Configuring CORBA Interfaces

To configure CORBA interfaces for SRC-ACP:

1. Access SDX Admin.
2. In the navigation pane, highlight the entry *I = ACP, ou = staticConfiguration, ou = Configuration, o = Management, o = umc*.
3. Click the Main tab in the ACP Configuration pane.
4. Edit or accept the default values for the properties that configure CORBA interfaces for SRC-ACP. See *CORBA Interfaces Properties* on page 366.

CORBA Interfaces Properties

In SDX Admin, you can modify the following SRC-ACP properties in the content pane for an SRC-ACP configuration.

ACP.ior

- Exports the object reference for SRC-ACP through either a local file or a Common Object Services (COS) naming service.
- Values—One of the following references
 - file:// < path > —Exports object reference through a local file
 - < path > —Absolute path to local file
 - corbaname:: < cosNameServer > # < KEY > —Exports object reference through COS naming services
 - < cosNameServer > —IP address or Domain Name System (DNS) name of COS naming server
 - < KEY > —Object reference of SRC-ACP
 - corbaname:rir# < KEY > —Exports object reference through COS naming service; resolve-initial-references (rir) function finds DNS name of COS naming server
- Default—file:///var/acp/acp.ior

ACP.syncRateAdapter.ior

- Object reference for the ACP external interface.
- Value—See value for the field ACP.ior on page 366.
- Default—file:///var/acp/sra.ior
- Property name—ACP.syncRateAdapter.ior

Configuring SRC-ACP Redundancy

To configure SRC-ACP redundancy:

1. Access SDX Admin.
2. In the navigation pane, highlight the entry *I = ACP, ou = staticConfiguration, ou = Configuration, o = Management, o = umc*.
3. Click the Main tab in the ACP Configuration pane.
4. Edit or accept the default values for the properties that configure SRC-ACP redundancy. See *SRC-ACP Redundancy Properties* on page 367.

SRC-ACP Redundancy Properties

In SDX Admin, you can modify the following SRC-ACP properties in the content pane for an SRC-ACP configuration.

ACP.redundancy.enable

- Enables or disables SRC-ACP redundancy.
- Value
 - Yes—Enable redundancy.
 - No—Disable redundancy.
- Default—No

ACP.redundancy.local.ior

- In a redundant SRC-ACP configuration, exports the object reference for this SRC-ACP through a local file or COS naming service.
- Value—See value for the field ACP.ior on page 366.
- Default—None
- Example—corbaname::cosHost#0000000000000035...

ACP.redundancy.remote.ior

- In a redundant SRC-ACP configuration, exports the object reference for the other SRC-ACP through a local file or COS naming service.
- Value—See value for the field ACP.ior on page 366.
- Default—None
- Example—corbaname:rir#0000000000000035...

ACP.IgnoreUserOutOfSync

- Specifies whether user tracking events should be ignored when they raise an OutOfSync exception to the SAE when state synchronization is enabled. SRC-ACP raises an OutOfSync exception when SRC-ACP handles service tracking or authentication events without receiving a user start event first.
- Value
 - true—Ignore user tracking events that raise an OutOfSync exception.
 - false—Tracks all events; SRC-ACP raises an OutOfSync exception.
- Default—false

ACP.redundancy.bkpns.ior

- In a redundant SRC-ACP configuration, exports the object reference for the backup naming service through a local file or COS naming service. The primary SRC-ACP registers the IOR and redundancy IOR to both naming services, while the secondary SRC-ACP registers the redundancy IOR to both naming services.
- Value—See value for the field ACP.ior on page 366.
- Default—None
- Example—corbaname::cosHost#00000000000000035...

Configuring State Synchronization

Enabling state synchronization can affect performance because of resource consumption. To configure state synchronization with SAE:

1. Access SDX Admin.
2. In the navigation pane, highlight the entry *I = ACP, ou = staticConfiguration, ou = Configuration, o = Management, o = umc*.
3. Click the Main tab in the ACP Configuration pane.
4. Edit or accept the default values for the properties that configure state synchronization. See *State Synchronization Properties* on page 368.

State Synchronization Properties

In SDX Admin, you can modify the following SRC-ACP properties in the content pane for an SRC-ACP configuration.

ACP.stateSync

- Enables or disables SRC-ACP state synchronization with the SAE.
- Value
 - Yes—Enable state synchronization.
 - No—Disable state synchronization.
- Default—Yes

ACP.stateSyncBulkSize

- Number of events the SAE sends to SRC-ACP in a single method call during state synchronization.
- Value—Integer
- Default—1

ACP.redundancy.community.heartbeat

- Time interval for community members to check each other's availability when both redundancy and state synchronization are enabled.
- Value—Number of seconds in the range 0–4294967295
- Default—30

ACP.redundancy.community.acquire_timeout

- Time to wait before trying to reacquire the distributed lock when both redundancy and state synchronization are enabled.
- Value—Number of seconds in the range 0–4294967295
- Default—15

ACP.redundancy.community.blackout_time

- Time to wait before regaining control when both redundancy and state synchronization are enabled.
- Value—Number of seconds in the range 0–4294967295
- Default—30

Configuring Connections to the Subscribers' Directory

To configure how SRC-ACP connects to the directory that contains subscriber information:

1. Access SDX Admin.
2. In the navigation pane, highlight the entry *I = ACP, ou = staticConfiguration, ou = Configuration, o = Management, o = umc*.
3. Click the Main tab in the ACP Configuration pane.
4. Edit or accept the default values for the properties that configure connections to the subscriber's directory. See *Subscriber Directory Properties* on page 370.

Subscriber Directory Properties

In SDX Admin, you can modify the following SRC-ACP properties in the content pane for an SRC-ACP configuration.



NOTE: In the following descriptions, use the property name with the GlobalUserDatabase prefix if one directory supports all the components in the network. Use the property name with the <vrGroupName> prefix if you have partitioned the directory to provide information for different parts of the network through different VRs. For more information, see *Working with Partitioned Directories* on page 374.

server.address

- List of primary and redundant servers that manage data for subscribers.
- Value—List of IP addresses or hostnames separated by spaces
- Default—127.0.0.1
- Example—10.227.7.153

server.port

- TCP port for the directory.
- Value—Valid TCP port number
- Default—389

server.baseDN

- DN of the root of the directory.
- Value—List of attribute = value pairs separated by commas
- Default—*o = users, o = umc*

server.authDN

- DN used to authorize connections to the directory.
- Value—List of attribute = value pairs separated by commas
- Default—*cn = umcadmin, o = umc*

server.password

- Password used to authorize connections to the directory.
- Value—Text string
- Default—admin123

server.event_baseDN

- DN of the directory that contains event information.
- Value—DN
- Default—*o = umc*

des.enable_eventing

- Enables or disables directory eventing.
- Value
 - Yes—Enable directory eventing.
 - No—Disable directory eventing.
- Default—Yes

des.pollinginterval

- Time interval at which the SRC component polls the directory.
- Value—Number of seconds in the range 15–2147483647
- Default—30

server.intf_eventing

- Enables or disables directory eventing for congestion points.
- Value
 - Yes—Enable directory eventing.
 - No—Disable directory eventing.
- Default—No

Configuring Connections to the Services' Directory

To configure how SRC-ACP connects to the directory that contains information about services:

1. Access SDX Admin.
2. In the navigation pane, highlight the entry *I = ACP, ou = staticConfiguration, ou = Configuration, o = Management, o = umc*.
3. Click the Main tab in the ACP Configuration pane.
4. Edit or accept the default values for the properties that configure connections to the service's directory. See *Service Directory Properties* on page 372.

Service Directory Properties

In SDX Admin, you can modify the following SRC-ACP properties in the content pane for an SRC-ACP configuration.



NOTE: In the following descriptions, use the property name with the GlobalServiceDatabase prefix if one directory supports all the components in the network. Use the property name with the <vrGroupName> prefix if you have partitioned the directory to provide information for different parts of the network through different VRs. For more information, see *Working with Partitioned Directories* on page 374.

server.address

- List of primary and redundant servers that manage data for services.
- Value—List of IP addresses or hostnames separated by spaces
- Default—127.0.0.1
- Example—10.227.7.153 10.227.7.125

server.port

- TCP port for the directory.
- Value—Valid TCP port number
- Default—389

server.baseDN

- DN of the root of the directory that stores data about services.
- Value—List of attribute = value pairs separated by commas
- Default—*o = services, o = umc*

server.authDN

- DN that SRC-ACP uses to authorize connections to the directory that stores data about services.
- Value—List of attribute = value pairs separated by commas
- Example—*cn = umcadmin, o = umc*

server.password

- Password that SRC-ACP uses to authorize connections to the directory that stores data about services.
- Value—Text string
- Default—admin123

server.event_baseDN

- DN of the directory that contains event information for services.
- Value—DN
- Example—*o = umc*

des.enable_eventing

- Enables or disables directory eventing.
- Value
 - Yes—Enable directory eventing
 - No—Disable directory eventing
- Default—Yes

des.pollinginterval

- Time interval at which SRC-ACP polls the directory.
- Value—Number of seconds in the range 15–2147483647
- Default—30

server.intfBaseDN

- DN of the directory that contains information about network interfaces for edge congestion points.
- Value—DN
- Default—*o = AdmissionControl, o = umc*

server.congestionPointBaseDN

- DN of the directory that contains information about network interfaces for backbone congestion point objects.
- Value—DN
- Default—*o = CongestionPoints, o = umc*

eventing.reloadCongestionPoints

- Specifies whether SRC-ACP detects changes in the backbone congestion point for a service while SRC-ACP is operative.
- Value
 - Yes—SRC-ACP uses new information for the backbone congestion point as soon as SRC-ACP detects a change to the data in the directory.
 - No—SRC-ACP uses new information for the backbone congestion point only after you stop and restart SRC-ACP.
- Guidelines—Set this field to Yes only when you want to modify a congestion point (see [on page 394](#)). When you have modified the congestion point, reset this field to No.
- Default—No

server.intf_eventing

- Enables or disables directory eventing for congestion points.
- Value
 - Yes—Enable directory eventing.
 - No—Disable directory eventing.
- Default—No

Configuring Eventing Properties for Databases

You can configure all directory eventing properties with SDX Admin for the subscriber and service databases. For information about configuring directory eventing properties, see *SRC-PE Getting Started Guide, Chapter 37, Distributing Directory Changes to SRC Components on a Solaris Platform*. If one directory supports all the components in the network, use the following constructions for the properties:

- GlobalUserDatabase.des. <property >
- GlobalServiceDatabase.des. <property >

If, however, you have partitioned the directory, see *Working with Partitioned Directories on page 374*.



NOTE: For SRC-ACP, always set the value of the des.dispatcher_pool_size property to 1.

Working with Partitioned Directories

If you have partitioned the directory to provide information for different parts of the network through different VRs, you must define the Data Manager properties with SDX Admin. To do so:

1. Access SDX Admin.
2. In the navigation pane, highlight the entry *I = ACP, ou = staticConfiguration, ou = Configuration, o = Management, o = umc*.
3. Click the Main tab in the ACP Configuration pane.
4. Define the name of the VR group for each directory in the Property field by using the following formats.

- VrUserDatabase. <vrGroupName >
- VrServiceDatabase. <vrGroupName >

<vrGroupName > is an arbitrary name that identifies the group of VRs in the partition.

5. Define the VRs in the group by defining the property <vrGroupName > .vrs.

- Define the properties for connecting to the subscribers' directory and the services' directory by using the following format:

```
< vrGroupName > < property > = < value >
```

For information about these properties, see *Configuring Connections to the Subscribers' Directory* on page 369 and *Configuring Connections to the Services' Directory* on page 371.

- Define directory eventing properties for the subscriber's directory and the services' directory by using the format

```
< vrGroupName > . < des.Name > .des. < property > = < value >
```

For more information, see *Configuring Eventing Properties for Databases* on page 374.

<vrGroupName>.vrs

- List of VRs that support the user database or the service database.
- Value—List of VRs separated by spaces in the format:

```
< vrName > @ < routerName >
```

 - < vrName > —Name of VR configured on the router
 - < routerName > —Name of router on which the VR is configured
- Example—vrdb1.vrs = default@erx1 default@erx2 vr1@erx3

Example In this example, the name of the VR group is vr1, and the group contains one VR called bigfoot@erx1.

```
VrUserDatabase.vr1
vr1.factory.class.name = net.juniper.smgmt.acp.UserLdapDataManagerFactory
vr1.server.address = 127.0.0.1
vr1.server.port = 389
vr1.server.baseDN = o=users,o=umc
vr1.server.authDN = cn=umcadmin,o=umc
vr1.server.password = admin123
vr1.server.event_baseDN = o=umc
vr1.server.signatureDN = o=umc
vr1.des.enable_eventing = true
vr1.des.pollinginterval = 30
vr1.des.delegate_factory_initial = com.sun.jndi.ldap.LdapCtxFactory
vr1.des.connection_pool_size = 1
vr1.des.dispatcher_pool_size = 1
vr1.des.fake_delete = false
vr1.des.show_fake_delete = false
vr1.vrs = bigfoot@default
```

Configuring SRC-ACP Scripts and Classification

To configure scripts and classification, see *Configuring SRC-ACP Scripts and Classification* on page 305.

Configuring SRC-ACP to Manage the Edge Network

To configure SRC-ACP to manage the edge network you must:

1. Configure network interfaces that represent locations of congestion points in the directory.
2. Configure guaranteed bandwidths for subscribers.
3. Assign network interfaces to subscribers.
4. Configure guaranteed bandwidths for services.

See the following sections for details about these procedures.

You can configure objects in the directory by means of an LDAP client or by means of a network management database. These sections provide information about the LDAP attributes you must configure and their positions in the LDAP schema, as well as details on how to configure objects with SDX Admin. For detailed information about the LDAP schema, see the documentation on the SRC software distribution in the folder */SDK/doc/ldap*.

Configuring Network Interfaces in the Directory

You must add network interfaces to the directory. For the edge network, you do so by specifying in the DN *o = Admission Control, o = umc* the network interfaces of the routers and the switches in the access network between subscribers and the SRC network. Table 18 shows the object class for network interfaces and the associated attributes.

Table 18: SRC-ACP Information for Network Interfaces

Information	Mandatory or Optional Information	LDAP Schema
Network interface	Mandatory	networkInterface (object class)
Provisioned downstream bandwidth	Mandatory	downstreamProvisionedRate (attribute)
Provisioned upstream bandwidth	Mandatory	upstreamProvisionedRate (attribute)
List of downstream background bandwidths Entries separated by commas in the LDAP schema	Optional (For information about background bandwidths, see <i>Allocating Bandwidth to Applications Not Controlled by SRC-ACP</i> on page 277.)	downstreamBackgroundRate (attribute)
List of upstream background bandwidths Entries separated by commas in the LDAP schema	Optional (For information about background bandwidths, see <i>Allocating Bandwidth to Applications Not Controlled by SRC-ACP</i> on page 277.)	upstreamBackgroundRate (attribute)

To configure a network interface with SDX Admin:

1. Access SDX Admin.
2. In the navigation pane, highlight the entry *o = Admission Control, o = umc*, and right-click.

3. Select **New > NetworkDevice**.

The New Network Device dialog box appears.

4. Enter the name of the network device, and click **OK**.

An object for the new network device appears in the navigation pane, and basic details for the new network device appear in the Main tab of the NetworkDevice pane.

5. (Optional) Enter a description for the network device in the Description field, and click Save in the NetworkDevice pane.

6. In the navigation pane, highlight the network device, and right-click.

7. Select **New > Network Interface**.

The New Network Interface dialog box appears.

8. Enter the name of the network interface, and click **OK**.

An object for the new network interface appears in the navigation pane, and basic details for the new network interface appear in the Main tab of the NetworkInterface pane.

NetworkInterface	
Main Meta Data	
Name	FE 4/2
Downstream Prov. Rate	
Upstream Prov. Rate	
Downstream Background Bandwidth	
Upstream Background Bandwidth	

9. Complete the fields using the information in *Bandwidth for Network Interfaces* on page 377.
10. Click **Save** in the NetworkInterface pane.

Bandwidth for Network Interfaces

Use the fields in this section to define bandwidth for network interfaces.

Downstream Prov. Rate

- Provisioned downstream bandwidth.
- Value—Number of bits per second

Upstream Prov. Rate

- Provisioned upstream bandwidth.
- Value—Number of bits per second

Downstream Background Bandwidth

- Downstream background bandwidths.
- Value—List of bandwidths separated by commas.
- Guidelines—Optional. For information about background bandwidths, see *Allocating Bandwidth to Applications Not Controlled by SRC-ACP* on page 277.

Upstream Background Bandwidth

- Upstream background bandwidths.
- Value—List of bandwidths separated by commas.
- Guidelines—Optional. For information about background bandwidths, see *Allocating Bandwidth to Applications Not Controlled by SRC-ACP* on page 277.

Configuring Bandwidths for Subscribers

You must configure bandwidths for subscribers that SRC-ACP manages in the edge region of the network.

If the access network between the subscriber and the router uses ATM, and all the traffic coming from one DSLAM travels on a single virtual path, you do not need to provision bandwidths for each subscriber. In this case, SRC-ACP can derive the congestion points from the router (see *Deriving Edge Congestion Points* on page 275.)

However, if the access network uses a protocol other than ATM, you must provide the information shown in Table 19 for each subscriber.

Table 19: SRC-ACP Information for Subscribers

Information	LDAP Attributes
Provisioned downstream bandwidth	downstreamProvisionedRate
Provisioned upstream bandwidth	upstreamProvisionedRate
Actual downstream bandwidth for current subscriber session	downstreamSyncRate
Actual upstream bandwidth for current subscriber session	upstreamSyncRate
List of DNs of interfaces associated with congestion points	networkInterfaceRef

To configure bandwidths for subscribers with SDX Admin:

1. Access SDX Admin.
2. In the navigation pane, highlight the entry for the residential subscriber in *o = users, o = umc*.
3. Click the **Admission Control** tab in the User pane.
4. Enter the values for the fields using the information in *Bandwidth for Subscribers* on page 379.
5. Click **Save** in the User pane.

Figure 46: Admission Control Tab in User Pane
Bandwidth for Subscribers

Use the fields in this section to configure bandwidths for subscribers.

Downstream Prov. Rate

- Provisioned downstream bandwidth.
- Value—Number of bits per second
- Guidelines—Mandatory. This rate is used if the subscriber bandwidth settings are not provided by remote update (through the API for ACP) or by the Downstream Sync Rate value.
- Default—No value

Upstream Prov. Rate

- Provisioned upstream bandwidth.
- Value—Number of bits per second
- Guidelines—Mandatory. This rate is used if the subscriber bandwidth settings are not provided by remote update (through the API for ACP) or by the Upstream Sync Rate value.
- Default—No value

Downstream Sync Rate

- Actual downstream bandwidth for the current subscriber session.
- Value—Number of bits per second
- Guidelines—If you do not set this value and it is not provided by remote update (through the API for ACP), then the Downstream Prov. Rate value is used.
- Default—No value

Upstream Sync Rate

- Actual upstream bandwidth for the current subscriber session.
- Value—Number of bits per second
- Guidelines—If you do not set this value and it is not provided by remote update (through the API for ACP), then the Upstream Prov. Rate value is used.
- Default—No value

Assigning Network Interfaces to Subscribers

You must assign to the subscriber object interfaces (including the router interfaces) for all congestion points between the subscriber and the router. Table 19 on page 378 shows the LDAP attribute for this type of network interface.



NOTE: You must define the interface in the directory before you can assign it to a residential subscriber (see Configuring Network Interfaces in the Directory on page 376).

To assign an interface with SDX Admin:

1. Start at the Admission Control pane for the subscriber (see Figure 46).
2. Click the  icon below the Interfaces field.

The Select Object dialog box appears.

3. Select the network device on which the interface is located.

You can shift-click or control-click network devices to select multiple options.

4. Click **OK**.

The network devices appear in the User pane.

5. Click **Add**.

The network devices appear in the Scopes field of the pane.

6. Highlight a network device.
7. Modify the DN of the network device to include the interface location.
8. Click **Modify**.

Repeat Steps 6 to 8 for each interface associated with a congestion point for this subscriber.

Configuring Bandwidths for Services

Upstream and downstream bandwidths must be specified for services that SRC-ACP manages. You can obtain bandwidths for services in two ways:

- Provide static values through the directory.
- Allow the values to be provided through the SAE core API.

For example, a business partner may need to specify the required values for a particular piece of content through the SAE core API.

Table 20 shows the LDAP attributes for these services.

Table 20: SRC-ACP Information for Services

Information	LDAP Attributes
Required downstream bandwidth	sspRequiredDownstreamBandwidth
Required upstream bandwidth	sspRequiredUpstreamBandwidth

To configure values for services with SDX Admin:

1. Access SDX Admin.
2. In the navigation pane, highlight the entry for the service in *o = Services*, *o = umc*.
3. Click the **Admission Control** tab in the SSP Service pane.

4. Enter the values for the Required Downstream Bandwidth and the Required Upstream Bandwidth fields.
5. Click **Save** in the SSP Service pane.

Configuring SRC-ACP to Manage the Backbone Network

To configure SRC-ACP to manage the backbone network, you must:

1. Configure network interfaces that represent locations of congestion points in the directory.
2. (Optional) Configure an action congestion point.
3. Configure guaranteed bandwidths for services.
4. Assign network interfaces to services.
5. Create congestion points in the directory.
6. Assign network interfaces to congestion points.

Refer to the following sections for details about these procedures.



NOTE: You can configure objects in the directory by means of an LDAP browser or by means of a network management database. These sections provide information about the LDAP attributes that you must configure and their positions in the LDAP schema, as well as details on how to configure objects with SDX Admin. For detailed information about the LDAP schema, see the documentation in the SRC software distribution in the folder `/SDK/doc/ldap`.

Configuring Network Interfaces in the Directory

You configure network interfaces in the directory in the same way for edge and backbone congestion points. However, for backbone congestion points, you can add only VRs and their interfaces. For information about this procedure, see *Configuring Network Interfaces in the Directory* on page 376.

Extending SRC-ACP Congestion Points

You can extend SRC-ACP congestion points to initialize and execute applications defined in a backbone congestion point. SRC-ACP provides a service provider interface (SPI) to:

- Create custom congestion point applications that authorize service activation and track service start and stop events.
- Obtain congestion point information from remote update.
- Retrieve congestion point status.
- Track congestion point state.

The SPI for ACP provides a Java interface that a congestion point application implements. For information about the SPI for ACP, see the documentation in the SRC application library distribution in the folder `SDK/doc/acp`.

The implementation of the SPI for ACP can be a customized application that performs certain tasks, such as creating or removing congestion points on the router. SRC-ACP acts as an interface tracking plug-in, and interface tracking events are treated as remote updates for congestion points when they are created, modified, or removed.

SRC-ACP supports applications written in Java or Jython. For scripts written in Java, you must compile and package the implemented SPI for ACP to make it available for use by SRC-ACP. A Java implementation can include more than one Java archive (JAR) file.

To use congestion point applications with SRC-ACP, configure an action congestion point that references the script (see *Configuring Action Congestion Points* on page 383).

Configuring Action Congestion Points

You can define an application in a backbone congestion point so that SRC-ACP can execute it in a predefined manner. Backbone congestion points that are configured to run an application are called action congestion points. If you want to use an action congestion point to execute an application that requires real-time congestion point status, you must enable SRC-ACP state synchronization with the SAE (see *Configuring State Synchronization* on page 368).

Before you configure an action congestion point, make sure that you know the location of the application file.

To configure an action congestion point with SDX Admin:

1. Access SDX Admin.
2. In the navigation pane, highlight the entry for the network interface in *o = Admission Control, o = umc*.
3. Click the **Action** tab.

The Action tab appears in the NetworkInterface pane.

4. In the Type field, select one of the following file types that the application uses:
 - URL—URL to identify the location of script file
 - Python—Python source code
 - Java Class—Compiled Java class file
 - Java Archive—Java archive file (.jar)
5. In the Class Name field, enter the class name of the Java or Python class implementing the SPI.
6. In the File/URL field, enter the URL, or click **Load** to add a file.
 - If the type is URL, enter the URL.
 - If the type is not URL, click Load.

The Load data dialog box appears. For information about loading scripts, see *Managing Files from the Load Data Dialog Box* on page 385.

The URL or the content of the script file appears in the File/URL box.

If you want to remove the URL or file, click **Clear**.

7. In the entry box below the Parameters field, enter the parameter as an attribute = value pair, and click **Add**.

The entry appears in the Parameters field.

To modify the entry:

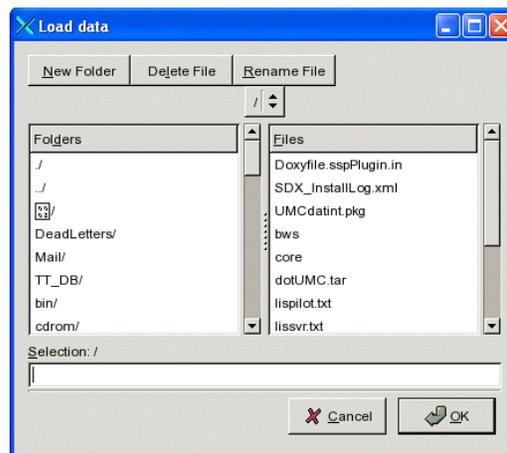
- Highlight the entry so that it appears in the entry box below the Parameters field.
- Make your changes to the entry, and click **Add** to add a new entry, or click **Modify** to change the selected entry.

The modified entry appears in the Parameters field.

8. Click **Save** in the NetworkInterface pane.

Managing Files from the Load Data Dialog Box

If you click **Load** in the Files/URL box, the Load data dialog box appears.



You can manipulate files and folders from the Load data dialog box.

- To load a file:
 1. Select the directory that contains the script that implements the application, and then select the file.

or

Type the path to the script file in the Selection box.

If a JAVA implementation includes more than one JAR file, use commas to separate file URL entries, or enter one URL per line.

2. Click **OK**.

The content of the script file appears in the File/URL box.

- To create a new folder, click **New Folder**.
- To remove a file, select a file or enter its path in the Selection box, and click **Delete File**.

- To rename a file:
 1. In the Files list, select a file, and click **Rename File**.
The Rename File dialog box appears.
 2. Enter the new filename, and click **OK**.

Configuring Bandwidths for Services

You configure bandwidths for services in the same way for edge and backbone congestion points. For information about this procedure, see *Configuring Bandwidths for Services* on page 381.

Configuring Congestion Points for Services

You must assign a congestion point to each service that SRC-ACP manages. Table 21 shows the LDAP attributes for a backbone congestion point.

Table 21: SRC-ACP Information Associated with Backbone Congestion Points

Information	LDAP Attributes
Definition of a backbone congestion point in the format <code><-vrName->/<-serviceName-></code>	congestionPoints
<ul style="list-style-type: none"> ■ To allow the software to automatically define the congestion point, use the entry <code><-vrName->/<-serviceName-></code>. When SRC-ACP starts operating, it will substitute the VR name and the service name from the request for service activation. ■ To restrict the congestion point to a specific VR or service, enter the actual VR name or service name, as shown in the following examples. <ul style="list-style-type: none"> ■ <code>vr1@boston/<-serviceName-></code>—Specifies any service available on VR <code>vr1@boston</code> ■ <code><vrName>/news</code>—Specifies the service <code>news</code> on any VR ■ <code>vr1@boston/news</code>—Specifies the service <code>news</code> available on VR <code>vr1@boston</code> ■ <code>default@ottawa/news</code>—Specifies the service <code>news</code> available either on the default VR or on a router called <code>ottawa</code> 	

To configure values for services with SDX Admin:

1. Access SDX Admin.
2. In the navigation pane, highlight the entry for the service in `o = Services, o = umc`.
3. Click the **Admission Control** tab in the SSP Service pane.
4. In the entry box below the Congestion Points field, enter the name of one congestion point; see Table 21 for information about the format of this entry.
5. Click the **Add** button.

The entry appears in the Congestion Points field.

Configuring Congestion Points in the Directory

You must add backbone congestion points to the directory in $o = \textit{CongestionPoints}$, $o = \textit{umc}$. Table 21 shows the LDAP attribute for a backbone congestion point.

To configure an individual backbone congestion point in the directory with SDX Admin:

1. Access SDX Admin.
2. In the navigation pane, highlight the entry $o = \textit{CongestionPoints}$, $o = \textit{umc}$, and right-click.
3. Select **New > Congestion Point**.

The New Congestion Point dialog box appears.

4. Enter the name of the VR that supports the new congestion point, and click **OK**.

The new object appears in the navigation pane, and basic details for the object appear in the Main tab of the Congestion Point pane.

5. (Optional) Enter a description for the VR in the Description field, and click **Save** in the NetworkDevice pane.
6. In the navigation pane, highlight the VR, and right-click.
7. Select **New > Congestion Point**.

The New Congestion Point dialog box appears.

8. Enter the name of the service, and click **OK**.

The new object appears in the navigation pane, and basic details for the object appear in the Main tab of the Congestion Point pane.

To add all backbone congestion points for all VRs in the directory:

1. Access SDX Admin.
2. In the navigation pane, highlight the entry $o = \textit{CongestionPoints}$, $o = \textit{umc}$, and right-click.
3. Select **New > Create CongestionPoints**.

The VRs and the services they support appear in the folder.

Assigning Interfaces to Congestion Points

You must assign interfaces either to VRs or to individual services under the VRs in *o = CongestionPoints, o = umc*. Services inherit interface assignments from the associated VR unless you assign an interface to the individual service. The LDAP attribute for this network interface is called `interfaceRef` and it lists the DNS of interfaces associated with backbone congestion points.

To assign interfaces to congestion points with SDX Admin:

1. Access SDX Admin.
2. In the navigation pane, highlight the entry in *o = CongestionPoints, o = umc* to which you want to assign the congestion point.

3. Click the  icon below the Interfaces field.

The Select Object dialog box appears.

4. Select the network device on which the interface is located.

You can shift-click or control-click network devices to select multiple options.

5. Click **OK**.

The network devices appear in the User pane.

6. Click **Add**.

The network devices appear in the Scopes field of the pane.

Repeat Steps 3 to 6 for each interface associated with a congestion point for this subscriber.

Defining a Congestion Point Profile

You can create a congestion point profile that automatically performs congestion point classification. This profile supports only access network mode for SRC-ACP.

The congestion point profiles are stored in the directory under *o = congestionPoints, o = umc*.

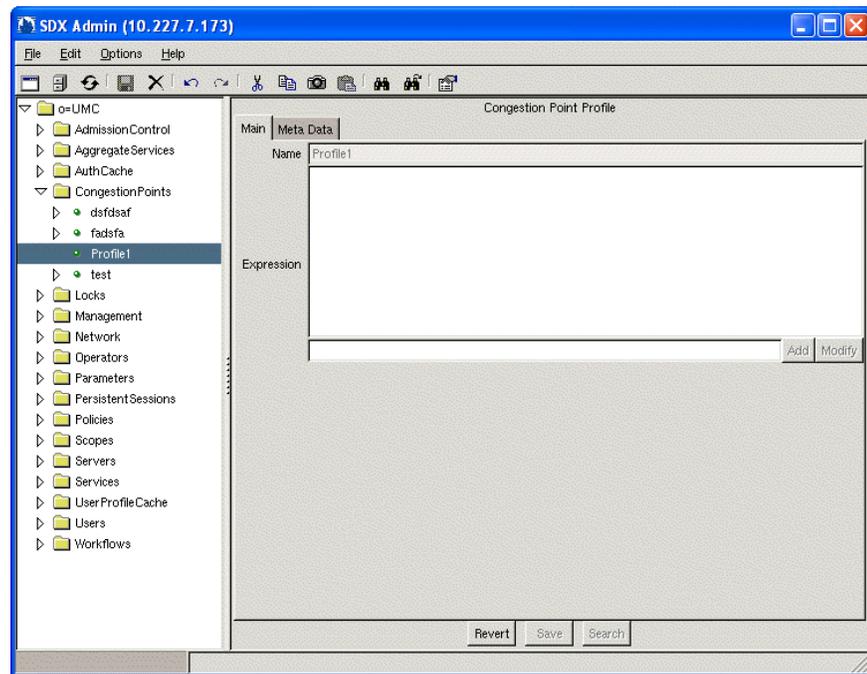
To define a congestion point profile:

1. In SDX Admin under UMC, right-click **CongestionPoints**, select **New**, and then select **Congestion Point Profile**.

The New Congestion Point Profile dialog box appears.

2. In the New Congestion Point Profile dialog box, enter a name for the profile.

The Congestion Point Profile pane appears in the content area.



3. Enter a congestion point expression in the box below the Expression box, and then click **Add**. For information about congestion point expressions, see *Congestion Point Expressions* on page 389.

Congestion Point Expressions

You can enter a congestion point expression by using the syntax listed in this section. You can also embed Python scripting expressions within the congestion point expression.

If you embed Python expressions within a congestion point expression, use the escape sequence `< - then - >` to enclose the Python expression. See *Methods for Use with Scripting Expressions* on page 390 and *Match Criteria for Congestion Point Classification* on page 391.

The syntax for a congestion point expression is:

```
< NetworkDevice > / < NetworkInterface > [ / < CongestionPoint > ]
```

- `< NetworkDevice >` —Network device listed in the directory.

For information about network devices, see *SRC-PE Network Guide, Part 2, Using Juniper Networks Routers in the SRC Network*.

- `< NetworkInterface >` —Network interface listed in the directory.

For information about interfaces, see *SRC-PE Subscribers and Subscriptions Guide, Chapter 7, Classifying Interfaces and Subscribers on a Solaris Platform*.

- `< CongestionPoint >` —(Optional) Name of an instance of congestion point that is automatically created.

If one of the elements with the path contains a slash (/), use a backslash (\) as an escape character for the slash. For example, `\`.

Expressions in Templates for Congestion Point Profiles

You can create a congestion point profile to be used as a template for other profiles. Templates simplify management of congestion points. Rather than configuring each congestion point individually, you can create templates to define common parameters for a class of individual congestion points.

For example, in an environment in which VLAN interfaces GigabitEthernet1/0.1 through GigabitEthernet1/0.1000 have the same available bandwidth, you can specify the characteristics of the VLAN interface once and have SRC-ACP create the congestion points based on the template configuration.

When a congestion point expression has the third element, SRC-ACP uses the `< NetworkDevice > / < NetworkInterface >` part of the expression to load the congestion point from the directory, and uses it as a template to create a congestion point in memory for subscriber. The `< CongestionPoint >` part of the expression distinguishes each congestion point (available bandwidth) created from this template.

Methods for Use with Scripting Expressions

SRC-ACP provides the following methods to use in scripting expressions:

- `slot(nasPortId)`—Collects the slot number from the `nasPortId` or `interfaceName`

Example—`slot("atm 4/5:0.32") = = "4"`

- `port(nasPortId)`—Collects the port number from the `nasPortId` or `interfaceName`

Example—`port("atm 4/5:0.32") = = "5"`

- `l2id(nasPortId)`—Collects the layer 2 ID from the `nasPortId` (VLAN id or ATM vpi.vci)

Example—`l2id("atm 4/5:0.32") = = "0.32"`

- `escape(string)`—Replaces any slash with the escape sequence `\`

Example—`escape("atm 4/5") = = "atm 4\5"`

You can extend the scripting library by creating the file `lib/localCPLib.py` in the ACP installation directory, by default `/opt/UMC/acp/lib/localCPLib.py`. SRC-ACP reads the definitions in this file at startup, after which they are available for processing.

Match Criteria for Congestion Point Classification

You can use the following match criteria in Python scripting expressions for a congestion point expression:

- `ifSessionId`—Identifier for RADIUS accounting on the JUNOS interface.
- `authUserId`—Identifier that a subscriber uses for authentication.
- `domain`—Name of the domain used for secondary authentication.
- `radiusClass`—RADIUS class attribute of the service definition.
- `routerName`—Name of virtual router in the format `<virtualRouter> @ <router>`.
- `interfaceName`—Name of the interface, such as `fastEthernet3/1`.
- `interfaceAlias`—Alias of the interface; that is, the IP description in the interface configuration.
- `interfaceDescr`—SNMP description of the interface, such as `IP3/1`.
- `portId`—Identifier of VLAN or virtual circuit. For a virtual circuit, use the format `<VPI>/<VCI>`.
- `nasPort`—Network access server (NAS) port.
- `sspHost`—Name of host on which SAE is installed.
- `IfRadiusClass`—RADIUS class attribute on the JUNOS interface.
- `ServiceBundle`—Service bundle vendor-specific attribute for RADIUS. A user authorization plug-in returns this attribute to the SAE.
- `loginName`—Subscriber's login name. The format of the login name varies.
- `primaryUserName`—PPP login name or the public DHCP username.
- `accountingId`—Value of directory attribute `accountingUserId`.
- `userDn`—Distinguished name of a subscriber in the directory.
- `userMacAddress`—Media access controller (MAC) address of a DHCP subscriber.
- `dhcpPacket`—Content of the DHCP discover request in the format:
 - First 4 octets—Gateway IP address (`giaddr` field)
 - Remaining octets—DHCP options

For more information, see RFC 2131—Dynamic Host Configuration Protocol (March 1997) and RFC 2132—DHCP Options and BOOTP Vendor Extensions (March 1997).

- userType—Type of subscriber.
- sessionId—Identifier of RADIUS session for the subscriber session.
- userIp—IP address of the subscriber.
- nasIp—IP address used to communicate with the server.

Examples of Congestion Profiles

This section provides examples of expressions used in congestion point profiles.

Profile for Gigabit Ethernet Interface

In the following example, a subscriber who is connecting to router test@erx through interface GigabitEthernet1/0.1, has the congestion point:

```
"subInterface=1,interfaceName=GigabitEthernet1/0,orderedCimKeys=test@erx,o=AdmissionControl,o=UMC"
```

This congestion point is created from a congestion point template:

```
"interfaceName=GigabitEthernet1/0,orderedCimKeys=test@erx,o=AdmissionControl,o=UMC"
```

The following congestion point expression is configured for the congestion point profile *cn = vlan*, *o = CongestionPoints*, *o = umc*:



NOTE: The following example is a single expression that should be entered on a single line.

```
<-routerName->/<-interfaceName[:interfaceName.find('.')]>/  
<-interfaceName[interfaceName.find('.')+1:]>
```

Profile That Contains Three Congestion Points

In the following example, a subscriber who is connecting to router test@erx through interface atm 4/5:0.32 will have three congestion points:

- interfaceName=atm4, orderedCimKeys=test@erx, o=AdmissionControl, o=UMC
- interfaceName=atm4/5, orderedCimKeys=test@erx, o=AdmissionControl, o=UMC
- interfaceName=atm4/5:0.32, orderedCimKeys=test@erx, o=AdmissionControl, o=UMC

SRC-ACP automatically appends *o = AdmissionControl*, *o = UMC*.

This profile creates the same congestion points that are created by the ATM autocompletion feature, which is available in this version as well as previous versions of SRC-ACP.

The following congestion point expressions are configured for the congestion point profile *cn = atm*, *o = CongestionPoints*, *o = umc*:

```
<routerName>/<escape(portId.replace(' ',''))>
<routerName>/<escape(portId[:portId.rindex('.')]
.replace(' ',''))>
<routerName>/<escape(portId[:portId.rindex(':')]
.replace(' ',''))>
```

Profile That Uses Congestion Point Templates

In the following example, the congestion points are dynamically created based on templates for the expressions. When you use a template, you specify parameters for the `< NetworkDevice >` / `< NetworkInterface >` part of the expression. This part refers to a network interface object in the directory that defines the parameters of the congestion point; that is, the available bandwidth.

The following congestion point expressions are configured for the congestion point profile *cn = atm*, *o = CongestionPoints*, *o = umc*:

```
<routerName>/VCI/<portId>
<routerName>/VPI/<portId[:portId.rindex('.')
->
<routerName>/PHY/<portId[:portId.rindex(':')
->
```

where:

- VCI—Provides parameters for the virtual channel
- VPI—Provides parameters for the virtual path
- PHY—Provides parameters for the physical interface terminating on a JUNOS router

Changing and Removing a Congestion Point Profile

To change configuration of a congestion point profile:

1. In SDX Admin, select the congestion point profile.
2. In the Congestion Point Profile pane, select the expression to change in the Expression box, and click **Modify**.
3. Make changes to the expression, and click **Add**.

The updated expression appears in the Expression box.

To remove a congestion point profile:

1. In SDX Admin, right-click the congestion point profile.
2. Select **Delete** to remove the profile.

Starting SRC-ACP

To start SRC-ACP:

1. On the SRC-ACP host, log in as `root` or as an authorized nonroot admin user.
2. Start SRC-ACP from its installation directory.

```
cd /opt/UMC/acp/etc  
./acp start
```

Stopping SRC-ACP

To stop SRC-ACP:

1. On the SRC-ACP host, log in as `root` or as an authorized nonroot admin user.
2. Stop SRC-ACP from its installation directory.

```
cd /opt/UMC/acp/etc  
./acp stop
```

Monitoring and Managing SRC-ACP

To monitor admission control, you can use the SRC CLI. See *Chapter 24, Monitoring Admission Control with the SRC CLI*.

You can also use the C-Web interface to monitor admission control. See *Chapter 25, Monitoring Admission Control with the C-Web Interface*.

You can use the SRC CLI or the C-Web interface to:

- Display information about the edge network.
- Display information about the backbone network.
- Display information about subscribers and congestions points obtained through an external application.

To manage admission control, you can use the SRC CLI. See *Chapter 23, Managing SRC-ACP with the SRC CLI*.

You can use the SRC CLI to:

- Reorganize the files that contain ACP data.
- Modify congestion points.