

Chapter 12

Locating Subscriber Information

This chapter describes how to use the network information collector (NIC) to locate subscriber information for an application and discusses strategies for implementing a NIC configuration. The chapter includes information about the NIC sample data provided with the SDX software; reviewing this data will help you plan a NIC configuration for your network. This chapter contains the following sections:

- Locating Subscriber Management Information on page 219
- Mapping Subscribers to a Managing SAE on page 220
- High Availability for NIC on page 222
- Planning a NIC Implementation on page 224
- Before You Configure NIC Hosts on page 227
- Configuring NIC Hosts to Resolve Requests on page 227
- Specifying a Router Initialization Script on page 228
- Configuring Operating Parameters for NIC Hosts on page 229
- Modifying Basic Configuration for a NIC Host on page 233
- Starting NIC on a System on page 243
- Configuring NIC Replication on page 243
- Changing NIC Configurations on page 243

Locating Subscriber Management Information

For services to be activated for a subscriber session, applications such as volume-tracking applications, Dynamic Service Activator, the Enterprise Manager Portal, or a residential portal need to locate the SAE that manages the subscriber.

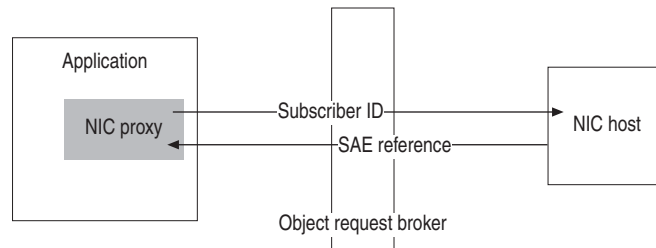
The network information collector (NIC) is the component that locates which SAE manages the subscriber. The NIC uses information that identifies the subscriber to identify the managing SAE. A NIC is similar to a Domain Name System (DNS) in that a NIC processes resolution requests. Rather than translating hostnames to IP addresses and vice versa, the NIC resolves an identifier for a subscriber to a reference for the SAE that manages the subscriber.

NIC operates on a client/server model. A NIC host is the server—the component that processes resolution requests. A NIC proxy, a library within an application that interacts with a NIC host, is the client—the component requesting data resolution. A NIC proxy is so-named because it requests information on behalf of an application.

A NIC proxy and a NIC host communicate with each other through Common Object Request Broker Architecture (CORBA). When you use NIC, it manages CORBA interactions for you; you do not need to understand CORBA to use the NIC.

Figure 16 shows that NIC proxies and NIC hosts communicate through CORBA, with the NIC proxy providing an identifier for a subscriber and the NIC host returning a reference to the SAE that manages the subscriber.

Figure 16: Communication Between a NIC Proxy and a NIC Host



00156800

Mapping Subscribers to a Managing SAE

A NIC collects information about the state of the network and can provide mapping from a specified type of network data, known as a *key*, to another type of network data, known as a *value*. Applications can use a NIC proxy to submit a key to a NIC host. The NIC host obtains a corresponding value from other components within NIC and returns it through the NIC proxy to the application. A typical use of a NIC is for a residential portal application to submit a subscriber's IP address and for the NIC to return the interoperable object reference (IOR) of the SAE managing that subscriber.

NIC Proxies

Typically, an application supports one NIC proxy for each type of data request. A NIC proxy caches resolution results for a period of time so that it can resolve future requests without consulting the NIC host, thereby decreasing traffic between the NIC proxy and the NIC host. Applications that use NIC proxies communicate with the proxy to delete any invalidate cache entries. Caching lets you optimize resolution performance for your network configuration and system resources.

You configure a NIC proxy when you configure that application. SDX applications such as volume-tracking applications, and Dynamic Service Activator contain NIC proxies. If you are writing an external application that will interact with a NIC, you must include NIC proxies in the application. See *Chapter 14, Developing Applications That Use a NIC*.

NIC Hosts

NIC hosts collect and store SDX information, and respond to requests from NIC proxies. The components in a NIC host that manage this process are:

- NIC agents—Collect data from SDX components, publish data, and make data available to NIC resolvers
- NIC resolvers—Process resolution requests

NIC Agents

NIC agents collect information about the state of the network from many data sources on the network. Table 21 describes the types of agents supplied with NIC.

Table 21: Types of NIC Agents

Type of Agent	Type of Information the Agent Makes Available
Consolidator agent	Summary information received from other agents.
Directory agent	Specified directory entries and changes to directory entries.
Router access agent	Information from JUNOS routing tables.
SAE plug-in agent	Subscriber information and interface information for SAE-managed subscribers and interfaces.

NIC Resolvers

NIC resolvers manage information to resolve requests by:

- Receiving and storing information about the state of the network from components within NIC and other NIC resolvers
- Requesting information from NIC agents and other NIC resolvers
- Receiving requests from the NIC proxies or other NIC resolvers
- Processing requests and sending responses to the requesters

High Availability for NIC

NIC supports several mechanisms to maintain high availability. We recommend that you use NIC replication to keep a NIC configuration highly available. NIC replication uses groups of NIC hosts that share the same configuration for NIC resolutions to respond to resolution requests.

High Availability in Existing NIC Configurations

If you have a previous NIC configuration, you may be using:

- NIC host redundancy in which a set of NIC hosts provide redundancy
- Redundancy for SAE plug-in agents in which a set of SAE plug-in agents provide redundancy

If you have an SAE plug-in agent that uses agent redundancy, we recommend that you enable state synchronization for the agent and use NIC replication.

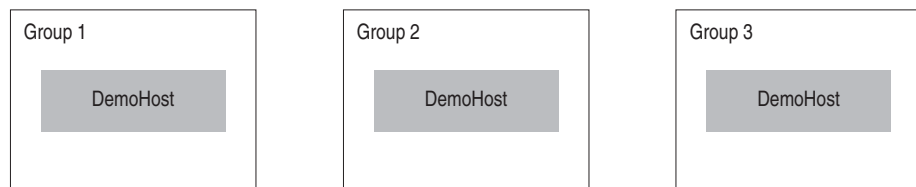
NIC Replication

NIC replication uses the concept of a group to identify a NIC host that has a particular configuration. A group contains one or more NIC hosts; each NIC host in a group is unique, for example each NIC host could reside on a different system. A NIC proxy contacts specified groups that contains hosts with the same configuration to locate a managing SAE.

For example, a group might include the host DemoHost, but not two instances of DemoHost. Typically, each NIC host in a group is located in the same point of presence (POP). However, a machine can support only one NIC host. The SDX software stores groups in the directory in *ou = dynamicConfiguration*, *ou = Configuration*, *o = Management*, *o = umc*.

For example, Figure 17 shows three NIC groups with each group containing a NIC host that has the same configuration.

Figure 17: NIC Groups



g015900

Groups let you:

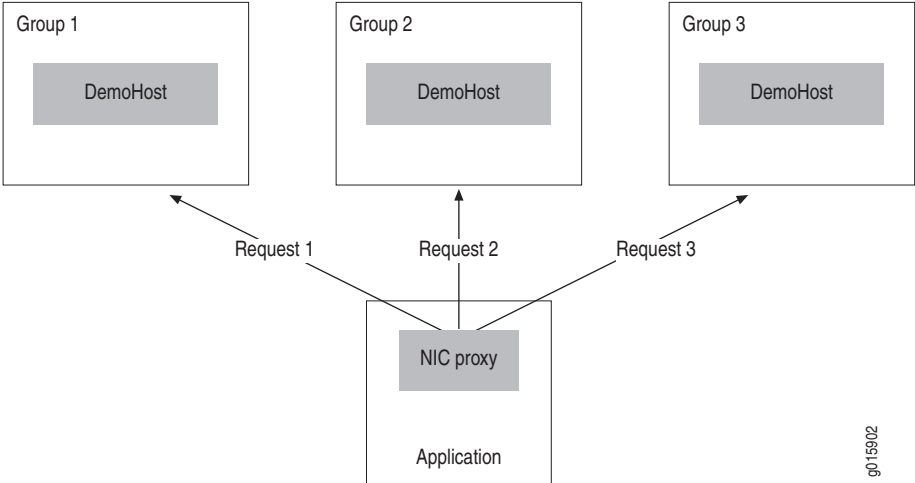
- Distribute network and processing load between two or more groups
- Provide failover protection if one group becomes unavailable

With NIC replication, a NIC proxy can contact multiple NIC hosts that are assigned to different groups. When a NIC proxy is configured to contact more than one group, the NIC configuration on a NIC host in each group should be equivalent—the NIC hosts should use the same configuration scenarios.

A NIC proxy selects a group by using the method specified in the configuration for the proxy; for example, the NIC proxy can randomly choose a group from a list. The NIC proxy then sends resolution requests to the corresponding host in that group. If a NIC proxy submits high numbers of resolution requests to the NIC host, you can configure the NIC proxy to randomly pick a NIC host or to pick a NIC host in a cyclic order to decrease the probability that one NIC host manages all the resolution requests.

Figure 18 shows resolution requests sent using a round-robin selection.

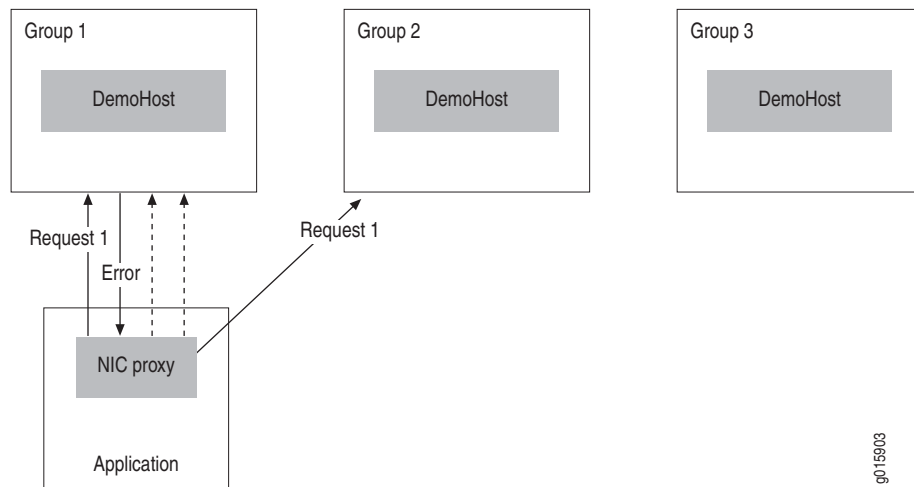
Figure 18: NIC Group Selection by Round-Robin



If the NIC host fails to respond to a specified number of resolution requests, the NIC proxy stops sending resolution requests to the unavailable NIC host and sends the resolution requests to another NIC host. The NIC proxy continues to poll the unavailable NIC host to determine its availability. When the NIC host becomes available, the NIC proxy can again send resolution requests to that host.

Figure 19 shows a NIC proxy that sends a resolution request to Group 1, receives an error message, then send two more resolution requests before sending a request to Group 2 rather than Group 1. When Group 1 is available again, the NIC proxy will send the request to Group 1.

Figure 19: NIC Resolution Request



You configure NIC replication for hosts, then configure NIC proxies to use replication.

Although you can distribute agents and resolvers among different hosts as shown in the configuration for the NIC hosts OnePopBO and OnePopH1 in the sample data, we recommend that you use the DemoHost configuration, which centralizes the configuration for agents and resolvers.

Planning a NIC Implementation

The SDX software provides standard NIC configuration scenarios that you can modify to meet the requirements for your environment. Which scenarios you choose depends on the applications you use.

If the resolution scenarios do not provide the type of resolution needed, we recommend that you consult Juniper Professional Services. If you want to customize configuration of the scenarios provided, see *Chapter 17, Customizing NIC Configuration*.

To plan your NIC implementation:

1. Review the resolution scenarios available in the NIC sample data, and select the scenario that best fits the requirements for your application.

Table 22 describes the resolution scenarios available in the NIC sample data. In most cases, one of the basic configuration scenarios provides the type of resolution needed.

2. Determine the number of NIC proxies that you will need to access NIC hosts, and estimate the amount of traffic between the NIC proxies and the NIC hosts. If you expect heavy traffic between NIC proxies and NIC hosts, configure a number of NIC hosts to share the traffic load and processing.
3. Determine which NIC hosts to assign to a group to provide NIC replication; choose names for these groups.
4. If you have not done so already, determine which systems are to run NIC hosts.

Table 22: NIC Configuration Scenarios

Configuration Scenario	Sample Configuration File to Use	Type of Resolution	Notes
Basic Configuration Scenarios			
For JUNOS local configuration for PPP and DHCP subscribers. Sample use: DSL providers for residential customers.	<i>OnePop.xml</i>	Subscriber IP address to SAE IOR	Simplest configuration. IP pools configured locally on each VR with IP addresses from a static pool of IP addresses configured on the virtual router.
For subscribers who have assigned IP addresses (assigned external to the SAE). Sample use: A PCMM environment when the SAE acts as both a policy server and application manager.	<i>OnePopDynamicIp.xml</i>	Subscriber IP address to SAE IOR	
For resolution of a subscriber login name to an SAE IOR, and of a subscriber IP address to a subscriber login name. Sample use: Support for tracking subscriber bandwidth usage or for using a billing model. You can use volume-tracking applications (VTAs) with this scenario.	<i>OnePopLogin.xml</i>	Subscriber login name to SAE IOR	Uses two resolvers. Use a separate NIC proxy for each resolution.
For subscribers who connect through a CMTS device. Sample use: In a PCMM environment in which the policy server is separate from the application server. This scenario can be used when the configuration includes Juniper Policy Server or another policy server, and the SAE is an application manager.	<i>OnePopPcmm.xml</i>	Subscriber IP address to SAE IOR	

Table 22: NIC Configuration Scenarios (continued)

Configuration Scenario	Sample Configuration File to Use	Type of Resolution	Notes
<p>For a router configuration in which VRs share IP pools.</p> <p>Sample use:</p> <ul style="list-style-type: none"> ■ Services for enterprise subscribers. ■ Support for two different proxies: <ul style="list-style-type: none"> ■ Subscriber DN to SAE IOR ■ Subscriber IP address to SAE IOR 	<i>OnePopDnSharedIp.xml</i>	Subscriber DN or subscriber IP address to SAE IOR	Includes resolution available in <i>OnePopSharedIp.xml</i> and adds resolution from a subscriber DN.
<p>For a router configuration in which pools can be shared among routers. Pools can be assigned by RADIUS or by a DHCP server.</p> <p>Sample use:</p> <p>Support for DHCP and PPP connections for residential subscribers.</p>	<i>OnePopSharedIp.xml</i>	Subscriber IP address to SAE IOR	
<p>For enterprise customers.</p>	<i>OnePopAllRealms.xml</i>	Subscriber IP address to SAE IOR	The scenario combines the OnePop and OnePopSharedIp scenarios and adds resolution from a subscriber DN.
Advanced Configuration Scenarios			
<p>For two POPs that share a back office.</p> <p>Sample use:</p> <p>Support for a deployment that has a back office that connects to NIC hosts at other sites.</p>	<i>MultiPop.xml</i>	Subscriber IP address to SAE IOR	<p>You can deploy this scenario in an environment that has a number of POPs; for example, a configuration in which there are two POPs with NIC proxy communication to a back office, which in turn communicates with the POP hosts. The POP hosts each support parallel hosts and agents and manage resolutions in the same way.</p> <p>You can add POPs by copying the configuration for one POP and modifying the configuration to suit your environment.</p>

Table 22: NIC Configuration Scenarios (continued)

Configuration Scenario	Sample Configuration File to Use	Type of Resolution	Notes
For subscribers who have assigned IP addresses (assigned external to the SAE). Assigned IP subscribers are supported on JUNOSe routers.	<i>OnePopAssignedIp.xml</i>	Assigned subscriber IP address to SAE IOR	Similar to <i>OnePopDynamicIp.xml</i> . Uses SNMP with OSPF routing tables on a JUNOSe router.
Sample uses:			
<ul style="list-style-type: none"> ■ A signaled proxy application such as voice over IP. ■ DSL providers for residential customers. 			

Before You Configure NIC Hosts

Before you configure NIC hosts:

- Install and configure the main SDX components, such as SAEs and the directory (see *SDX Software Basics Guide*).
- Install the sample data (see *SDX Software Basics Guide, Chapter 7, Defining an Initial Configuration*).
- Install the NIC software (UMCnic package) on each system that is to support a NIC host.



NOTE: A machine can support only one NIC host.

- Understand how to use SDX Configuration Editor to create new configuration files, modify configuration files, and export files to the directory (see *SDX Software Basics Guide, Chapter 14, Using SDX Configuration Editor*).

Configuring NIC Hosts to Resolve Requests

Tasks to configure a NIC host are:

1. Specifying a Router Initialization Script on page 228
2. Configuring Operating Parameters for NIC Hosts on page 229
3. Modifying Basic Configuration for a NIC Host on page 233
4. Starting NIC on a System on page 243
5. Configuring NIC Replication on page 243

Specifying a Router Initialization Script

The NIC resolutions map virtual routers (VRs) to SAEs. For these resolutions, use a router initialization script that associates each VR with the SAE that manages it. Which router initialization script you use depends on whether the SAE obtains IP pools from JUNOS VRs:

- **poolPublisher** router initialization script—Used when the SAE obtains IP pools locally from JUNOS VRs.
- **iorPublisher** router initialization script—Use when the router is one of the following:
 - JUNOS routers that do not supply IP addresses from local pools
 - JUNOS routing platforms
 - CMTS devices

For the following resolutions, IP addresses are obtained from local address pools. If you use one of these scenarios, use a **poolPublisher** router initialization script.

- OnePop
- OnePopDynamicIp

For the following resolutions, routers (including all JUNOS routing platforms and CMTS devices) do not supply IP addresses from local pools in your network. If you use one of these scenarios, and use an **iorPublisher** router initialization script.

- OnePopSharedIp
- OnePopAssignedIP
- OnePopLogin
- OnePopDnSharedIp
- OnePopPcmm

For the following resolutions, either a **poolPublisher** router initialization script or an **iorPublisher** router initialization script can be used, depending on router configuration.

- OnePopAllRealms
- MultiPop

For information about how to select an initialization script for the SAE, see *SDX Components Guide, Vol. 1, Chapter 2, Configuring the SAE*.

Modifying Information About IP Pools

The **poolPublisher** script enables the SAE to obtain data from the VR through Simple Network Management Protocol (SNMP), and the SAE stores that information in the directory. The SAE runs the script when a Common Open Policy Service (COPS) connection is established to the JUNOSe router. Consequently, if you modify information about IP pools on a VR after the COPS connection is established, the SAE does not automatically register the changes, and you must update the directory.

To update the directory with the local IP addresses that a VR provides, you can use either SDX Admin or the **poolRepublish** command. For information about this procedure, see *SDX Objects Guide, Chapter 5, Managing Routers and Virtual Routers*.

Configuring Operating Parameters for NIC Hosts

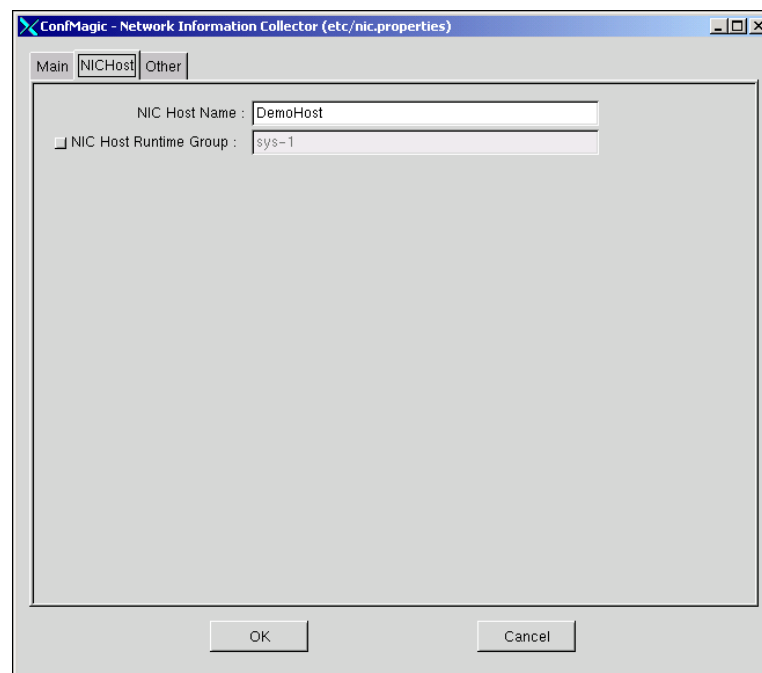
The operating parameters define how the NIC host interacts with other SDX components, such as the directory.

To configure the operating parameters:

1. Log in as **root**.
2. Start the local configuration tool in the directory where you installed the NIC.

/opt/UMC/nic/etc/config

The Network Information Collector window appears.



3. Configure the fields in each tab of this window. The following sections describe the properties on each tab:
 - Configuring Directory Connections on page 230
 - Specifying NIC Host Information on page 231
 - Configuring Additional NIC Host Properties on page 232
4. Click OK.



NOTE: If you change any of the NIC operating parameters, restart NIC for the changes to take effect.

Configuring Directory Connections

In the Main tab, configure directory connection properties. Use the following field descriptions to configure these properties.

Primary Directory Server

- Location of the directory server in URL string format.
- Value—URL in the format [ldap | ldaps]:// { < host > } : < portNumber >
 - ldap—LDAP connection (not secure)
 - ldaps—Secure LDAP connection
 - < host > —Name or IP address of the host that supports the directory
 - < portNumber > —Number of the TCP/IP port
- Default— ldap://127.0.0.1:389/
- Example—ldaps://192.0.2.10:389/

Backup Directory Servers

- List of redundant directories.
- Value—List of URLs separated by semicolons; for format of the URL, see the field Primary Directory Server on page 230.
- Example—ldaps://192.0.2.10:389/

Base DN

- Location in the directory in which the SDX data is stored.
- Value—DN
- Example—o = UMC

Bind DN

- DN that contains the username that the directory server uses to authenticate the NIC host.
- Value— < DN > , < base >
- Example—*cn = nic, ou = Components, o = Operators, < base >*

Bind Password

- Password that the directory server uses to authenticate the NIC host.
- Value—Text string or Base64 string
- Example—*nic*

Static Configuration DN

- DN of the location in which the NIC configuration is stored.
- Value—DN
- Example—*l = OnePop, l = NIC, ou = staticConfiguration, ou = Configuration, o = Management, o = umc*

Dynamic Configuration DN

- DN of the location in which data that the NIC automatically generates is stored.
- Value—DN
- Example—*ou = dynamicConfiguration, ou = Configuration, o = Management, o = umc*

Connect Timeout(s)

- Time that the NIC waits for the directory server to respond when it tries to connect to the directory.
- Value—Time in seconds
- Example—*10*

Specifying NIC Host Information

In the NIC Host tab, specify the name of the NIC host and the name of the group to which this host belongs for NIC replication. Use the following field descriptions to configure these properties.

NIC Host Name

- Name of the NIC host that you configured.
- Value—Text string
- Guidelines—Use the name *DemoHost*. The configuration scenarios all use *DemoHost* as the NIC hostname.
- Default—No value
- Example—*DemoHost*

NIC Host Runtime Group

- Group to which this NIC host belongs if you configure NIC replication.
- Value—Text string
- Default—No value
- Example—ontarioHosts

Configuring Additional NIC Host Properties

In the Other tab, configure Java properties and SNMP connection properties for the NIC host. Use the following field descriptions to configure these properties.

NIC Host Java

- Path to the JRE.
- Value—Path (absolute or relative) to the directory that contains the JRE
- Example—`../jre/bin`

JVM Max Heap

- Maximum memory size available to the JRE.
- Value—Capacity in MB
- Guidelines—By default, the JRE can allocate 160 MB. Change this value if you experience problems because of lack of memory. Set to a value lower than the available physical memory to avoid low performance because of disk swapping.
- Default—160 MB

Enable Sysman Clients

- Whether or not there is support for viewing SNMP counters with an SNMP browser.
- Value
 - Yes—Enabled
 - No—Disabled
- Default—No

Sysman IOR

- Folder that contains the IOR file for the NIC. The NIC writes its object references to this folder, and the SNMP agent discovers NIC components by monitoring the NIC IOR file in this folder.
- Value—Path to the folder that contains the IOR
- Guidelines—By default, the NIC IOR file is in the *var* folder, which is relative to the SNMP agent installation folder (*opt/UMC/agent*). You need to change this property only if you installed the SNMP agent in a folder other than the default folder, or if you previously changed this property and now need it to point to the folder where the IOR file currently resides.
- Default—*/opt/UMC/agent/var*

Modifying Basic Configuration for a NIC Host

You can configure one NIC host on a machine. You configure a NIC host by modifying a configuration scenario provided in the NIC sample data. Use the configuration for the NIC host DemoHost. This configuration is intended for use with NIC replication.

To configure a NIC host by modifying a sample scenario:

1. Start SDX Configuration Editor, and set the editing level to Basic.

In SDX Configuration Editor, select Windows, then Preference, then SDX System Configuration, and then Basic for Editing Level.
2. In the NIC folder, open the configuration file whose name matches the scenario you want to modify for your configuration.
3. Click the Hosts tab, and review NIC host configurations. No changes should be needed.
4. Ignore entries on the Redundancy tab and on the Realms tab.
5. Update NIC agent configuration to define properties specific to your environment, such as directory properties. See the following sections:
 - Overview of NIC Agent Configuration on page 233
 - Configuring Consolidator Agents on page 235
 - Configuring Directory Agents on page 235
 - Configuring Router Access Agents on page 238
 - Configuring SAE Plug-In Agents on page 240
6. Save the NIC configuration file.
7. Export the NIC configuration file to the directory.

Overview of NIC Agent Configuration

You use the basic configuration for each NIC agent, but modify properties such as directory properties to make the agent configuration compatible with your SDX configuration. The NIC configuration scenario that you use determines which agents appear in your configuration.

Table 23 lists all agents that are available in the various configuration scenarios.

Table 23: NIC Agents

Agent Name	Type of Agent	Type of Information
DnVr	SAE plug-in	Mappings of enterprise access DNs to VRs
Enterprise	Directory	List of enterprise names
InterfaceIdInterface	SAE plug-in	Receives interface tracking events and stores mappings of interface identifiers to interface names
IpLoginName	SAE plug-in	Mappings of IP addresses to login names
IpVr	SAE plug-in	Mappings of IP addresses to VRs
LoginNameVr	SAE plug-in	Mappings of login names to VRs
PoolInterfaceId	Router access	Mappings of IP pools to interface identifiers
PoolVr	Directory	Mappings of IP pools to VRs
Router	Consolidator	Based on information it receives from the InterfaceIdInterface agent, publishes names of routers in a POP
VrSaeld	Directory	Reads information about virtual routers and the mappings between virtual routers and SAEs

Table 24 shows the types of agents that each configuration scenario uses.

Table 24: Agents in Configuration Scenarios

Sample Configuration File	Directory Agents	Consolidator Agents	SAE Plug-In Agents	Router Access Agents
<i>OnePop.xml</i>	PoolVr, VrSaeld			
<i>OnePopAssignedIp.xml</i>	VrSaeld	Router	InterfaceIdInterface	PoolInterfaceId
<i>OnePopDnSharedIp.xml</i>	PoolVr, VrSaeld, Enterprise			
<i>OnePopDynamicIp.xml</i>	PoolVr, VrSaeld			
<i>OnePopLogin.xml</i>	Pool, VrSaeld		IpLoginName, LoginNameVr	
<i>OnePopPcmm.xml</i>	PoolVr, VrSaeld			
<i>OnePopSharedIp.xml</i>	PoolVr, VrSaeld		IpVr	
<i>MultiPop.xml</i>	PoolVr, VrSaeld, site-specific versions of PoolVr and VrSaeld		IpVr	
<i>OnePopAllRealms.xml</i>	PoolVr, VrSaeld, Enterprise		IpVr	



NOTE: If you use a configuration scenario that includes an SAE plug-in agent, make sure that your network has a CORBA naming server that includes the names of the servers that host the SAE plug-in agents. The SDX software distribution includes a CORBA naming server in the omniORB package.

Configuring Consolidator Agents

To modify the configuration for consolidator agents in Configuration Editor:

- Review the value for the Source Agent field in the Consolidator Agent area of the Agents pane, and modify if needed.

Consolidator Agent (Router)

Source Agent: /agents/InterfaceIdInterface

Source Agent

- Path to the agent for which this consolidator agent publishes data.
- Value—Text string
- Default—No value
- Example—/agents/InterfaceIdInterface
- Property name—sourceAgent

Configuring Directory Agents

To modify the configuration for directory agents in Configuration Editor:

- Review the values for the fields in the Directory Client Agent area of the Agents pane, and modify if needed.

Directory Client Agent (VrSaeId)

Search Base: o=Network,<base>

Search Filter: <objectclass=umcVirtualRouter> Disable

Search Scope: SubTree Disable

Server URL: ldap://127.0.0.1:389/

Backup Servers URL: Disable

Authentication DN: cn=nic,ou=Components,o=Operators,<base>

Password: *** Show

The following list describes fields that appear in the Directory Client Agent area of the Agents pane.



NOTE: If the SDX Configuration Editor editing level is set to Expert, you can view and change values for fields for directory eventing properties. This section does not list these fields.

For more information about the following directory eventing properties, see *SDX Components Guide, Vol. 1, Chapter 11, Configuring the Directory Eventing System*

Search Base

- DN of the location in the directory from which the agent should read information.
- Value— < DN > , < base >
- Default—No value
- Example—*o = Network, < base >*
- Property name—baseDN

Search Filter

- Directory search filter that the agent should use.
- Value—LDAP search filter
- Guidelines—Optional field.
- Default—No value
- Example—(objectclass = umcVirtualRouter)
- Property name—searchFilter

Search Scope

- Location in the directory relative to the base DN from which the NIC agent can retrieve information.
- Value—One of the following options:
 - Object—Entry specified in the Search Base field only
 - Level—Entry specified in the Search Base field and objects that are subordinate by one level
 - Subtree—Subtree of entry specified in the Search Base field
- Guidelines—Optional field.
- Default—Subtree
- Property name—searchScope

Server URL

- Location of the directory in URL string format.
- Value—Location of the directory that stores configuration information in URL string format `ldap:// <host> : <portNumber>`
 - `<host>` —IP address or name of directory host
 - `<portNumber>` —Number of TCP/IP port
- Default—No value
- Example—`ldap://127.0.0.1:389/`
- Property name—`java.naming.provider.url`

Backup Servers URL

- List of redundant directories.
- Value—List of URLs separated by semicolons
- Default—No value
- Example—`ldap://127.0.0.1:389/`
- Property name—`net.juniper.smgmt.des.backup_provider_urls`

Authentication DN

- DN that contains the username that the directory server uses to authenticate the NIC agent.
- Value—`<DN> , <base>`
- Default—No value
- Example—`cn = nic, ou = Components, o = Operators, <base>`
- Property name—`java.naming.security.principal`

Password

- Password that the directory server uses to authenticate the NIC agent.
- Value—Text string or Base64 string
- Default—No value
- Example—`nic`
- Property name—`java.naming.security.credentials`

Managing Directory Changes for the Directory Agent

The NIC directory agent does not support dynamic changes to a directory entry that result in the entry's being removed from its search filter.

If you require such changes, you must restart the NIC host containing this agent for the changes to take effect. For example, consider the MultiPop scenario provided as part of the NIC sample data. If you remove the POP-Ottawa scope from the directory entry with the following DN:

```
virtualRouterName=default, orderedCimKeys=Ottawa_ERX_Node, o=Network,
o=umc
```

then the OttawaPoolVr and OttawaVrSaeId agents will not dynamically detect the change. You must restart OttawaHost for the changes to take effect.

Configuring Router Access Agents

To modify the configuration for router access agents in Configuration Editor:

- Review the values for the fields in the Router Access Agent area of the Agents pane, and modify if needed.

Router Access Agent (PoolInterfaceId)	
Primary Router Id	10.227.7.109
Snmp Port	161 Disable
Local Port	162 Enable
Snmp Community String	public Disable
Snmp Timeout Value	5 Disable
Snmp Retries Value	3 Disable

The following list describes the fields that appear in the Router Access Agent area of the Agents pane.

Primary Router ID

- IP address of the JUNOSe router on which the Open Shortest Path First (OSPF) link-state advertisement (LSA) database resides.
- Value—IP address
- Example—127.0.0.1
- Property name—snmpRouterId

SNMP Port

- TCP port on the JUNOSe router to which the agent connects.
- Value—Number of TCP port
- Default—161
- Property name—snmpPort

Local Port

- TCP/IP port on which the agent listens for SNMP traps.
- Value—Number of TCP port
- Default—162
- Property name—localPort

SNMP Community String

- SNMP community string that identifies the group of JUNOSe routers with which the agent can establish SNMP sessions.
- Value—Text string
- Default—Public
- Property name—snmpCommunityString

SNMP Timeout Value

- Time after which the agent terminates SNMP operation.
- Value—Number of seconds in the range 0–4294967295
- Default—5
- Property name—snmpTimeout

SNMP Retries Value

- Number of times that the agent tries to complete an SNMP operation.
- Value—Integer in the range 0–4294967295
- Default—3
- Property name—snmpRetries

Configuring SAE Plug-In Agents

To modify the configuration for SAE plug-in agents in Configuration Editor:

- Review the values for the fields in the SAE Plug-In Agent area of the Agents pane, and modify if needed.

The following list describes all fields that appear in the SAE Plug-in Agent area of the Agents pane.

Event Filter

- LDAP filter that restricts the events that the agent collects.
- Value— < pluginAttribute > = < attributeValue >
 - < pluginAttribute > —Plug-in attribute name
 - < attributeValue > —Value of filter
- Default—No value
- Example—PA_USER_TYPE = INTF
- Property name—eventFilter

Number of Events Sent in a Synchronization Call

- Number of events the SAE sends to the agent at one time during state synchronization.
- Value—Integer in the range 1—2147483647
- Guidelines—This field is used if state synchronization is enabled for the SAE plug-in agent. State synchronization is enabled by default
- Default—50
- Property name—stateSyncBulkSize

Configuring the SAE for SAE Plug-In Agents

For each SAE plug-in agent in your configuration, you must also configure a corresponding external plug-in for the SAE. For information about configuring an external plug-in for the SAE, see *SDX Components Guide, Vol. 1, Chapter 5, Configuring Authorization and Accounting Plug-Ins*. Use the following guidelines:

- For the CORBA object reference, use the following construction:


```
<host>:900/NameService#<plugInName>
```

 - <host > —IP address or name of the machine on which you installed the NIC host that supports the agent
 - < plugInName > —Name of the agent
- Specify the plug-in attributes that the agent uses. You must specify the attributes PA_SESSION_ID and PA_ROUTER_NAME, and other attributes that you specified for the agent's network data types and the agent's event filter. Do not, however, specify attributes of type PAT_OPAQUE, such as the attribute PA_DHCP_PACKET.



NOTE: Do not include attributes that are not needed.

Configuring the SAE to Communicate with SAE Plug-In Agents When You Use NIC Replication

You must configure the SAE to communicate with each SAE plug-in agent in each NIC host that you use in the NIC replication. To do so:

1. Create an external plug-in with a unique name in the configuration for the SAE that communicates with the agent.
2. Either configure the agent as a global-user tracking plug-in or as a retailer-specific tracking plug-in.

This action specifies which events the SAE sends to the agents.

3. Repeat Steps 1 to 2 for each SAE plug-in agent in each NIC host that you use in the NIC replication.

For information about these tasks, see *SDX Components Guide, Vol. 1, Chapter 5, Configuring Authorization and Accounting Plug-Ins*. Use the following guidelines to create and configure the external plug-ins.

CORBA Object Reference

- CORBA object reference for the plug-in.
- Value—CORBA object reference in the format:
corbaname::`<host>:900/NameService#<agentName>_<groupName>/saePort<pluginName>`
 - `<host>` —IP address or name of the machine on which you installed the NIC host that supports the agent
 - `<agentName>` —Name of the agent
 - `<groupName>` —Name of the group to which the NIC host that supports the agent belongs
- Default—No value
- Example—`corbaname::192.168.0.100:900/NameService#nicsae_sys-1/saePort`
- Property name—Plugin. `<pluginName>.objectref`
 - `<pluginName>` —Name of the external plug-in that you created, such as `nic1`

Attributes

- Plug-in attributes that the agent uses.
- Value—Comma-separated list of plug-in attributes. For a complete list of attributes, see *SDX Components Guide, Vol. 1, Chapter 5, Configuring Authorization and Accounting Plug-Ins*.
- Guidelines—You must specify the attributes `PA_SESSION_ID`, `PA_ROUTER_NAME`, and other attributes that you specified for the agent's network data types and the agent's event filter. Do not, however, specify attributes of type `PAT_OPAQUE`, such as the attribute `PA_DHCP_PACKET`. Use only the attributes that you need to lessen effect on SDX system performance.
- Default—Comma-separated list of all possible attributes
- Example—`PA_SESSION_ID, PA_ROUTER_NAME`
- Property name—Plugin. `<pluginName>.attr`
 - `<pluginName>` —Name of the external plug-in that you created, such as `nic1`

Global User Tracking Plug-ins

- Tracks all subscriber sessions. These plug-in instances are called after a subscriber session starts and after a subscriber session ends.
- Value—Comma-separated list of plug-in instances
- Default—`fileAcct`
- Example—`fileAcct, nic1, nic2`
- Property name—`User.tracking.plugins`

Starting NIC on a System

After you configure operating parameters for a NIC host and modify basic configuration for a NIC host, start the NIC host.

To start a NIC host:

- Enter the following command:

```
/opt/UMC/nic/etc/nichost start
```

Configuring NIC Replication

You can configure NIC replication for a new NIC configuration and for an established NIC configuration.

To configure NIC replication:

1. Assign NIC hosts to groups:
 - a. Log in as `root` on the machine on which you installed a NIC host.
 - b. Access the operating parameters, and configure the field called NIC Host Runtime group (see *Configuring Operating Parameters for NIC Hosts* on page 229.)
 - c. If the NIC host was already running, restart it.
 - d. Repeat Steps a to c for each NIC host in the group.
2. Configure the NIC proxy to communicate with groups of NIC hosts. See *Chapter 13, Configuring Applications to Communicate with an SAE*.

Changing NIC Configurations

If you change the type of NIC resolution that you use in your network (for example, from the OnePop resolution to the OnePopAllRealms resolution), delete the NIC configuration data for the old resolution from the DN `ou = dynamicConfiguration, ou = Configuration, o = Management, o = umc` in the directory. You can delete the old data with SDX Admin or another LDAP client. If you do not delete the old data, the new NIC configuration may not perform resolutions correctly.

