CHAPTER 24

Using SNMP Services

CWCS provides support for SNMPv1, SNMPv2c, and SNMPv3.

SNMPv3 support is new in this version of CWCS. SNMP v3 support enhances the security of SNMP operation over the existing support for the SNMPv1/v2c model. It provides the degree of authentication and privacy required to perform network management operations securely.

CWCS SNMPv3 support allows you to:

- Address threats like information modification, masquerade, and disclosure and message stream modification.
- Do SNMP requests using SNMPv3.
- Automatically discover SNMP engine parameters.
- Get and Set SNMPv3 engine parameters.
- Handle SNMPv3-related error conditions.
- Set the number of outstanding requests.
- Automatically re-localize keys.
- Use existing support for SNMPv1/SNMPv2c.

The following topics describe how to use CWCS SNMP Services with your application:

For basic information on CWCS SNMP Services, see the "About SNMP Service Components" section on page 6-15.

For more information about CWCS SNMP Services, see:

- *SNMPOnJava: Changes for SNMPv3 (authNoPriv)DS: EDCS-309325*

Why SNMPv3?

SNMPv3 is included in this release of CWCS to address threats not addressed in the existing SNMPv1/v2c model:

- **Information Modification:** An entity can alter an in-transit message generated by an authorized entity in such a way as to effect unauthorized management operations, including the setting of object values.

- **Masquerade**: Management operations not authorized for some user may be attempted by assuming the identity of an authorized user.
- **Disclosure**: An entity can eavesdrop on the exchanges between managed agents and a management station and thereby learn the values of managed objects or learn of trap events.
- **Message Stream Modification**: The SNMP is designed to operate over a connection- less transport service, which may operate over any sub-network service.There is a threat that SNMP messages could be reordered,delayed,or duplicated to effect unauthorized management operations.

The SNMPv3 security model addresses the above threats in the following ways:

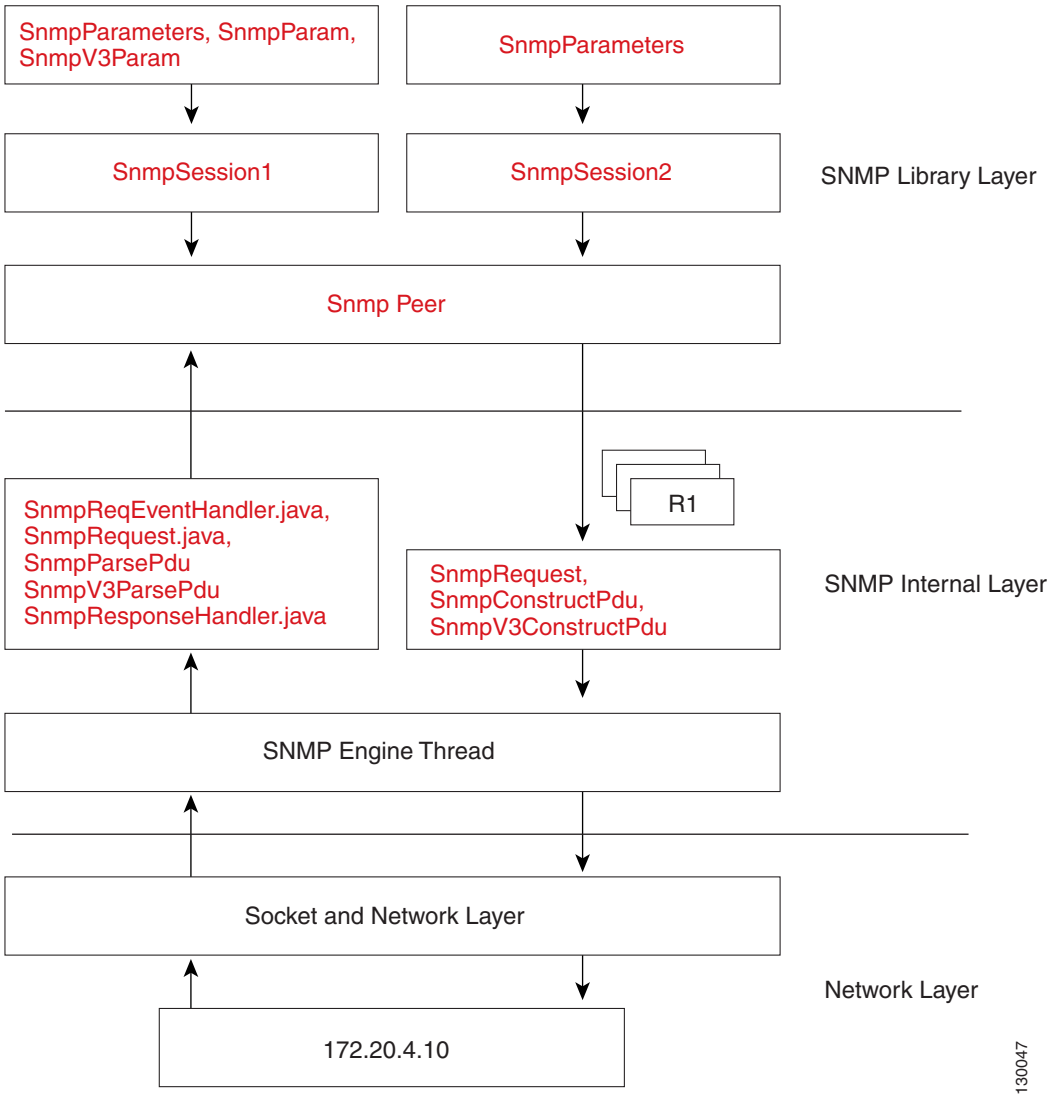
- Verify that each received SNMP message has not been modified during its transmission through the network.
- Verify the identity of the user who generates the SNMP requests.
- Detect received SNMP messages requesting or containing management information, whose time of generation was not recent.

Note For more information on the User-based Security Model (USM) for SNMPv3, refer to RFC 3414.

How SNMP Support Works

Figure 24-1 shows a high-level system flow for CWCS support of SNMP. The names of classes that were changed to handle SNMPv3 features are shown in red.

Figure 24-1 CWCS Support for SNMP



Using CWCS SNMP Services

CWCS SNMPv3 allows the user to work in the authNoPriv mode of the SNMPv3 security model.This mode provides packet-level security, integrity protection, and replay protection. SNMPv3 support is enabled automatically by passing an SNMPv3 credential to the SNMPOnJava library. The flow of SNMPv3 is intermingled with that of SNMP v1/v2c.

CWCS SNMPv1/v2c/v3 support is provided in the SNMPOnJava library.This library provides a series of APIs for applications to use.The SNMPOnJava library is divided into two main sections:

- The main library: Contains the bulk of the main classes dealing with SNMP. For a summary of the classes in this library, see the "About the SNMP Classes in the Main Library" section on page 24-4.
- The futureapi: Contains credentials-oriented classes and future extensions. For a summary of the classes in this library, see the "About the SNMP Classes in the Futureapi" section on page 24-5.

For details on each of the classes available in the SNMPOnJava library, see: http://mspring-u10.cisco.com/cvw/MOJO/packages.html.

The main features of CWCS support for SNMPv3 include:

- SNMPv3 is available for all applications.
- New APIs are available to get user credentials from applications.
- Applications can directly calculate the localized key from the user password.
- Applications can compute the local notion of an Agent's engine time.
- Automatic re-localization of keys.
- New APIs to expose the SNMPv3-engine-related parameters and localized keys to applications.
- Applications can pass SNMP-engine parameter information and localized keys to the library.
- Backward compatibility with the existing SNMP v1/v2c library.

Note SNMP engine parameters are SnmpEngineID, SnmpEngineTime, SnmpEngineBoots, and local notion of Agent's time.

About the SNMP Classes in the Main Library

The main library contains the classes shown in Table 24-1.

Table 24-1 SNMPOnJava Classes: Main Library

Class	Description
SnmpRequest	Responsible for creating a SNMP request for one or more SNMP operations. In SNMPv3, these classes do SNMP engine parameter discovery like getting the SnmpEngineID, SnmpEngineBoots, and SnmpEngineTime values from the device.They also provide authentication check in addition to error handling.
SnmpPeer	Contains information about the peer, such as the IP address, port number,and parameters like maximum request packet size, maximum number of varbinds, and the permissible outstanding requests to which the SNMP call is to be sent. In SNMPv3, these classes hold the SnmpEngineID.
SnmpParameters	Contains information about credentials(community strings in case of v1/v2c)and the protocol version for an SNMP session. In SNMPv3 ,it holds SNMPv3 credential.
SnmpParam	The base class for all credential-related classes.
Snmpv3Param	Represents the SNMPv3 credential fields. It contains methods and constructors to get credential information from the user.
SnmpMain	Initializes the SNMP environment, which contains default settings for every SNMP call. The initialization tasks include the number of threads for making SNMP calls, mamimum retry, maximum timeout, protocol version, request packet size, retry policy, etc. In SNMPv3, this class holds a new propertyto specify the maximum number of outstanding requests for a peer.
SnmpReqEventhandler	Handles the inherent asynchronous nature of SNMPOnJava. This class calls appropriate methods in other classes to process responses from the Agent. In SNMPv3, this class handles SNMPv3-specific conditions, such as unknown Engine ID, authencity of the received message, etc. It checks the response and updates the SNMP Engine parameters.

Table 24-1 SNMPOnJava Classes: Main Library (continued)

Class	Description
SnmpMultiplexReqDispatcher	Multiplexes one or more SNMP v1/v2c requests. It also prevents multiplexing SNMP v1/v2c and SNMPv3 requests.
Snmpv3ConstructPdu	Constructs the raw SNMPv3 message by translating the higher level information in SnmpRequest and SnmpParameters to the low-level byte stream information required by the device. It encodes the SNMPv3 message parameters – such as msgVersion, msgID, msgSecurityModel, SnmpEngineTime,SnmpEngineBoots, SnmpEngineId, msgAuthentication Parameters(digest), msgUserName, and others – to form a portion of the SNMPv3 message. Encoding the contextEngineName, contextEngineId, and the SNMPv2c PDU forms the remaining portion of the SNMPv3 message.
Snmpv3ParsePdu	Parses the raw SNMPv3 PDU received from the device for SNMPv3 message parameters, such as msgVersion, msgID, msgSecurityModel, SnmpEngineTime and SnmpEngineBoots, SnmpEngineId, msgAuthentication Parameters(digest), msgUserName, etc.
Snmpv3Param	Allows you to assign and fetch SNMPv3 credentials from applications. These include username, mode of SNMPv3 operation, authentication password, the context Engine ID and the context name.
SnmpResponseHandler	Receives the raw datagram object from the Java socket. It forwards the datagram to the appropriate PDU-handling classes, like SnmpV3ParsePdu and SnmpV2cParsePdu, for further processing of the received response.

About the SNMP Classes in the Futureapi

The futureapi library contains the classes shown in Table 24-1.

Table 24-2 SNMPOnJava Classes: Futureapi Library

Class	Description
SnmpCommunityLoader	TheSnmpCommunityLoader class supports the file based SNMPv1/v2c and SNMPv3 credentials.
SnmpCommunity class	TheSnmpCommunity class stores v1/v2c and v3 credentials in its data structures.It also provides methods to assign and fetch the credentials.
SnmpPeerManager class	The SnmpPeerManager class allows you to create and fetch session along with the credential for a device. It also allows you to get the credential directly instead of getting it from theSnmpCommunity class.
SnmpCommand class	The SnmpCommand class allows users to pass their credentials during runtime.It also provides applications a better control to handle the SNMP call.
SnmpFuture class	TheSnmpFuture abstract class is the base class for all future objects handling SNMP operations. In SNMPv3, this class has been modified to handle SNMPv3-specific errors. The BouncyCastle library (a third-party library) is used to perform MD5/SHA-1 digest calculation.