Configuring Extensible Messaging Control Protocol

There are two methods for clients to interact with a service routing-enabled network:

- Through the internal Cisco IOS API for service routing, which is available only for clients implemented within Cisco IOS software
- Through the Extensible Messaging Client Protocol (XMCP), also referred to as the External Client protocol, which is available to any client running anywhere within the network on any platform

Cisco SAF Clients connect to the Cisco SAF network in one of two ways:

- Reside on the same router as a Cisco SAF Forwarder, in which case the Cisco SAF Client uses an internal API to connect to a Cisco SAF Forwarder.
- Be external to a Cisco SAF Forwarder. In this configuration, the SAF Client is referred to as a Cisco SAF External Client, and it requires a protocol interface for connecting to the Cisco SAF Forwarder.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisite for XMCP

- Before configuring XMCP, you should understand the concepts in the “Cisco SAF Overview” section, particularly the “Cisco SAF Client Overview” and “External Cisco SAF Client (XMCP) Overview” sections.
- This section covers configuration of the XMCP server functionality in Cisco IOS software. To configure a specific device or software (such as Cisco Unified Communications Manager) as an XMCP client, refer to the documentation for that device or software. Note that some client documentation may refer to configuring a “client-label”. A client-label should be configured with the same identifier as the username.
- Before configuring an XMCP client to connect to a Cisco router configured as an XMCP server, ensure that you have configured IP routing between the client device and the Cisco router.
- Any device configured as an XMCP server should also be configured as a Cisco SAF Forwarder. (See “Configuring a Cisco SAF Forwarder”). You can configure the Cisco SAF Forwarder before or after you configure XMCP.

Information About XMCP

Once the XMCP session has been established successfully, the XMCP client may send XMCP publish, unpublish, subscribe, and unsubscribe requests. When the server receives and successfully authenticates these requests, it translates the requests into the equivalent Cisco SAF Client requests and sends them to the Cisco SAF Forwarder. Similarly, Cisco SAF Client notify requests from the forwarder will be translated into XMCP notify requests and sent to the XMCP client.

How to Configure XMCP

There are two methods for clients to interact with a service routing-enabled network:

- Through the internal Cisco IOS API for service routing, which is available only for clients implemented within Cisco IOS software.
- Through the Extensible Messaging Client Protocol (XMCP), also referred to as the External Client protocol, which is available to any client running anywhere within the network on any platform.

Configuring a Basic XMCP Server

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **service-routing xmcp listen**
4. **client username** *username* **password** *password*
5. **domain** *domain-number* {**default** | **only**}
6. **end**
7. **show service-routing xmcp server**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**service-routing xmcp listen** **Example:** `Router(config)# service-routing xmcp listen`	Enables the XMCP server, and enters XMCP configuration mode. The XMCP server will: • Listen on its default port (4788) • Accept connections in any VRF (virtual routing forwarding) instance
Step 4	**client username** *username* **password** *password* **Example:** `Router(config-xmcp)# client username exampleuser password examplepassword`	Defines a username and password pair that an XMCP client can use to authenticate this server, and enters XMCP client configuration mode. • By default, no username or password is defined; therefore, you must configure at least one **client** command to have a functioning XMCP server. • The password range is from 11 to 62 characters.

	Command or Action	Purpose
Step 5	**domain** *domain-number* {**default** | **only**} **Example:** `Router(config-xmcp-client)# domain 100 only`	(Optional) Defines the service-routing domain to which all clients using the given username and password pair will be assigned. • This pair corresponds to a SAF autonomous-system, so if you have configured this router as a SAF forwarder (see the "Configuring a Cisco SAF Forwarder" section), you should use the same SAF forwarder autonomous-system number as the domain number used here. • If you do not configure this command, clients will default to domain 7177.
Step 6	**end** **Example:** `Router(config-xmcp-client)# end`	Exits XMCP client configuration mode and returns to privileged EXEC mode.
Step 7	**show service-routing xmcp server** **Example:** `Router# show service-routing xmcp server`	Displays a summary of the XMCP server configuration and the number of connected clients.

Configuring an Advanced XMCP Server

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **service-routing xmcp listen** [**ipv4** | **ipv6**] [**port** *port-number*] [**vrf** *vrf-name*]
4. **allow-list** [**ipv4** *acl-name* | **ipv6** *acl-name*]
5. **max-clients** {**unauthenticated** *number* [**total** *number*] | **total** *number* [**unauthenticated** *number*]
6. **client unauthenticated**
7. **client username** *username* {**password** *password* | *encryption-type encrypted-password*}
8. **domain** *domain-number* {**default** | **only**}
9. **nonce** {**lifetime** *seconds* | **none**}
10. **keepalive** *seconds*
11. **exit**
12. **show service-routing xmcp server**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**service-routing xmcp listen** [**ipv4** | **ipv6**] [**port** *port-number*] [**vrf** *vrf-name*] **Example:** `Router(config)# service-routing xmcp listen ipv4 vrf vrf1 port 2000`	Enables the XMCP server, and enters XMCP configuration mode. • If you do not specify either IPv4 or IPv6 to restrict client connections, both will be permitted. • Use the **vrf** keyword to restrict client connections to the specified VRF. If you do not use this keyword, clients may connect from any interface in any VRF. • Use the **port** keyword to change the port number for clients to connect. If you do not use this keyword, the port number defaults to 4788.
Step 4	**allow-list** [**ipv4** *acl-name* | **ipv6** *acl-name*] **Example:** `Router(config-xmcp)# allow-list ipv4 XMCPClientListIPv4`	(Optional) Allows only clients that match the specified access list to connect. All other clients will be denied. If you do not specify an allow list, clients will not be filtered by any access list.

Step 5	**max-clients** {**unauthenticated** *number* [**total** *number*] | **total** *number* [**unauthenticated** *number*]
	
	Example:
	
	`Router(config-xmcp)# max-clients total 100`
	`Router(config-xmcp)# max-clients unauthenticated 5`
	`Router(config-xmcp)# max-clients unauthenticated 10 total 100`
		(Optional) Limits the maximum number of unauthenticated clients and the maximum number of clients of any type.
		
		• When the maximum number of clients connected has been reached, any additional clients will be denied.
		
		• If you do not specify a number of clients, a maximum of 1024 clients may connect, subject to available bandwidth and memory.

Step 6	**client unauthenticated** **Example:** `Router(config-xmcp)# client unauthenticated`	Permit clients to connect without authentication credentials. • This command also enters XMCP client configuration mode to provide additional attributes to apply to clients connecting in this manner. • By default, unauthenticated clients are not permitted and no username or password credentials are considered as valid.

	Command or Action	Purpose
		• You must configure at least one **client** command to have any clients be accepted by the XMCP server.
Step 7	**client username** *username* {**password** *password* | *encryption-type encrypted-password*} **Example:** `Router(config-xmcp-client)# client username example-user password example-password`	Configures a username and password that will be accepted for XMCP (Extensible Messaging Client Protocol) client connections. • Configure one or more **client** commands to permit clients to connect using the given authentication credentials. • By default, unauthenticated clients are not permitted and no username or password credentials are considered as valid. • You must configure at least one **client** command in order to have any clients be accepted by the XMCP server.
Step 8	**domain** *domain-number* {**default** | **only**} **Example:** `Router(config-xmcp-client)# domain 100 default`	(Optional) Defines the domain that clients using the given authentication credentials will be assigned by default, and whether the clients are permitted to request assignment to a different domain. The domain number corresponds to a SAF Forwarder autonomous-system number. By default, clients are assigned to domain 7177, but may request assignment to a different domain. • Use the **default** keyword to select a default domain and permit clients to request a different domain. • Use the **only** keyword to choose a default domain and deny clients to request a different domain.
Step 9	**nonce** {**lifetime** *seconds* | **none**} **Example:** `Router(config-xmcp-client)# nonce lifetime 600`	(Optional) Nonces provide additional session security (for clients that support this feature) against packet spoofing and replay attacks on the server. This feature requires additional bandwidth and CPU resources; therefore, it can be tuned or disabled to meet your security needs. By default, nonces are used for clients that support this feature. Nonces expire every 800 seconds, which requires the client to transition to a new nonce. To disable nonces, use the **nonce none** command. • For higher security (but with higher client bandwidth and CPU usage), configure a shorter nonce lifetime to a minimum of 5 seconds. • For lower security (and with lower client bandwidth and CPU usage), configure a longer nonce lifetime (up to a maximum of 3600 seconds). Nonces are not used for unauthenticated clients; therefore, this command cannot be used in conjunction with the **client unauthenticated** command.
Step 10	**keepalive** *seconds* **Example:** `Router(config-xmcp-client)# keepalive 100`	(Optional) Tunes the keepalive interval for clients using the given authentication credentials. • If the client does not send any messages for the given interval, the XMCP server will assume that the client has failed, terminate the XMCP session, and withdraw any services or subscriptions associated with this client. • By default, clients have a keepalive interval of 30 seconds.

	Command or Action	Purpose
Step 11	**exit** **Example:** `Router(config-xmcp-client)# exit`	Exits XMCP client configuration mode and returns to privileged EXEC mode.
Step 12	**show service-routing xmcp server** **Example:** `Router> show service-routing xmcp server`	Displays a summary of the XMCP server configuration and the number of connected clients.

Displaying XMCP Client and Server Information

To display information about connected XMCP clients and servers, use the following commands in user EXEC or privileged EXEC mode. These commands may be used in any order.

SUMMARY STEPS

1. **show service-routing xmcp clients** [*ip-address* | *handle*] [**detail**]
2. **show service-routing xmcp server**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**show service-routing xmcp clients** [*ip-address* | *handle*] [**detail**] **Example:** `Router> show service-routing xmcp clients detail`	Displays information about XMCP clients.
Step 2	**show service-routing xmcp server** **Example:** `Router> show service-routing xmcp server`	Displays information about the XMCP server status.

Configuration Example for XMCP

Example: Configuring an XMCP Server and Cisco SAF Forwarder

The following example, beginning in global configuration mode, shows how to configure a router as both an IPV4 XMCP server and as an IPv4 Cisco SAF forwarder. It maps all XMCP clients to the correct SAF autonomous system.

```
Router(config)# service-routing xmcp listen ipv4
Router(config-xmcp)# client unauthenticated
Router(config-xmcp-client)# client unauthenticated
Router(config-xmcp-client)# domain 1228 only
Router(config-xmcp-client)# client username example password passwordexample
Router(config-xmcp-client)# domain 1228 only
Router(config-xmcp-client)# exit
Router(config-xmcp)# exit
Router(config)# router eigrp saf
Router(config-router)# service-family ipv4 autonomous-system 1228
Router(config-router-sf)# end
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Service Advertisement Framework commands	Cisco IOS Service Advertisement Framework Technology Command Reference

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for XMCP

Table 1: Feature Information for XMCP

Feature Name	Releases	Feature Information
XMCP (Extensible Messaging Client Protocol)	15.2(2)T, 15.2(1)S, 15.2(3)T, 15.2(2)S Cisco IOS XE Release 3.6S, Cisco IOS XE Release 3.3SG 15.2(1)E	An XMCP client sends XMCP publish, unpublish, subscribe, and unsubscribe requests to a server. When the server receives and successfully authenticates these requests, it translates the requests into the equivalent Cisco SAF Client requests and sends them to the Cisco SAF Forwarder. In Cisco IOS XE 3.3 SG, support was added for the Cisco Catalyst 4000 Series Switches. The following commands were introduced or modified: • **allow-list** • **clear service-routing xmcp client** • **client (XMCP)** • **domain** • **keepalive (XMCP)** • **max-clients** • **nonce** • **service-routing xmcp clients** • **service-routingxmcp server**