showvlangroupthroughswitchportport-security violation

show vasi pair

To display the status of a VRF-Aware Service Infrastructure (VASI) pair, use the **show vasi pair**command in privileged EXEC mode.

show vasi pair status [*number*]

Syntax Description

status	Displays the VASI pair status.
number	(Optional) VASI pair number. The range is from 1 to 256.

Command Default

If no interface is specified, all VASI interfaces are displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 2.6	This command was introduced.

Examples

The following is sample output from the **show vasi pair** command:

```
Router# show vasi pair status 100
Pair name     Left state            Right state           Pair state
------------------------------------------------------------------------------
VASIPair100   down                  not configured        need vasiright100
```

The table below describes the significant fields shown in the display.

Table 1: show vasi pair status Field Descriptions

Field	Description
Pair name	Name of the VASI interface pair.
Left state	State of the vasileft interface. The values are as follows: • admin down--interface is administratively down. • down--interface is down. • not configure--interface is not configured. • up--interface is operational and up.

Field	Description
Right state	State of the vasiright interface. The values are as follows: • admin down--interface is administratively down. • down--interface is down. • not configure--interface is not configured. • up--interface is operational and up.
Pair state	Vasi pair status. Possible values are as follows: • need vasileft--vasileft interface is not configured. • need vasiright--vasiright interface is not configured. • up-- both interfaces are up and operational. • vasileft down--vasileft interface state is down • vasiright down--vasiright interface state is down

Related Commands

debug adjacency (vasi)	Displays debugging information for VASI adjacency.
debug interface (vasi)	Displays debugging information for VASI interface descriptor block.
debug vasi	Displays VASI debugging information.
interface (vasi)	Configures a VASI virtual interface.

show vlan group

To display the VLANs mapped to VLAN groups, use the **show vlan group** command in privileged EXEC mode.

show vlan group [**group-name** *group-name*]

Syntax Description

group-name *group-name*	(Optional) Displays the VLANs mapped to the specified VLAN group.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SXI1	This command was introduced.

Usage Guidelines

The **show vlan group** command displays the existing VLAN groups and lists the VLANs and VLAN ranges that are members of each VLAN group. If the **group-name**keyword is entered, only the members of the VLAN group specified by the *group-name* argument are displayed.

Examples

This example shows how to display the members of a specified VLAN group:

```
Router# show vlan group group-name ganymede
Group Name Vlans Mapped
---------------- --------------------
ganymede         7-9
```

Related Commands

Command	Description
vlan group	Creates or modifies a VLAN group.

show vtemplate

To display information about all configured virtual templates, use the **show vtemplate**command in privileged EXEC mode.

show vtemplate

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(7)DC	This command was introduced on the Cisco 6400 NRP.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3(14)T	The show display was modified to display the interface type of the virtual template and to provide counters on a per-interface-type basis for IPsec virtual tunnel interfaces.
12.2(33)SRA	This comand was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This comand was integrated into Cisco IOS Release 12.2(33)SXH.

Examples

The following is sample output from the **show vtemplate** command:

```
Router# show vtemplate
Virtual access subinterface creation is globally enabled
         Active     Active    Subint  Pre-clone Pre-clone Interface
       Interface Subinterface Capable Available   Limit     Type
       --------- ------------ ------- --------- --------- ---------
Vt1            0            0   Yes          --        --   Serial
Vt2            0            0   Yes          --        --   Serial
Vt4            0            0   Yes          --        --   Serial
Vt21           0            0    No          --        --   Tunnel
Vt22           0            0   Yes          --        --   Ether
Vt23           0            0   Yes          --        --   Serial
Vt24           0            0   Yes          --        --   Serial
Usage Summary
                              Interface   Subinterface
                              ---------   ------------
Current Serial  in use                1              0
Current Serial  free                  0              3
Current Ether   in use                0              0
Current Ether   free                  0              0
Current Tunnel  in use                0              0
Current Tunnel  free                  0              0
Total                                 1              3
Cumulative created                    8              4
Cumulative freed                      0              4
Base virtual access interfaces: 1
```

```
Total create or clone requests: 0
Current request queue size: 0
Current free pending: 0
Maximum request duration: 0 msec
Average request duration: 0 msec
Last request duration: 0 msec
Maximum processing duration: 0 msec
Average processing duration: 0 msec
Last processing duration: 0 msec
Last processing duration:0 msec
```

The table below describes the significant fields shown in the example.

Table 2: show vtemplate Field Descriptions

Field	Description
Virtual access subinterface creation is globally...	The configured setting of the **virtual-template**command. Virtual access subinterface creation may be enabled or disabled.
Active Interface	The number of virtual access interfaces that are cloned from the specified virtual template.
Active Subinterface	The number of virtual access subinterfaces that are cloned from the specified virtual template.
Subint Capable	Specifies if the configuration of the virtual template is supported on the virtual access subinterface.
Pre-clone Available	The number of precloned virtual access interfaces currently available for use for the particular virtual template.
Pre-clone Limit	The number of precloned virtual access interfaces available for that particular virtual template.
Current in use	The number of virtual access interfaces and subinterfaces that are currently in use.
Current free	The number of virtual access interfaces and subinterfaces that are no longer in use.
Total	The total number of virtual access interfaces and subinterfaces that exist.
Cumulative created	The number of requests for a virtual access interface or subinterface that have been satisfied.
Cumulative freed	The number of times that the application using the virtual access interface or subinterface has been freed.

Field	Description
Base virtual-access interfaces	This field specifies the number of base virtual access interfaces. The base virtual access interface is used to create virtual access subinterfaces. There is one base virtual access interface per application that supports subinterfaces. A base virtual access interface can be identified from the output of the **show interfaces virtual-access** command.
Total create or clone requests	The number of requests that have been made through the asynchronous request API of the virtual template manager.
Current request queue size	The number of items in the virtual template manager work queue.
Current free pending	The number of virtual access interfaces whose final freeing is pending. These virtual access interfaces cannot currently be freed because they are still in use.
Maximum request duration	The maximum time that it took from the time that the asynchronous request was made until the application was notified that the request was done.
Average request duration	The average time that it took from the time that the asynchronous request was made until the application was notified that the request was done.
Last request duration	The time that it took from the time that the asynchronous request was made until the application was notified that the request was done for the most recent request.
Maximum processing duration	The maximum time that the virtual template manager spent satisfying the request.
Average processing duration	The average time that the virtual template manager spent satisfying the request.
Last processing duration	The time that the virtual template manager spent satisfying the request for the most recent request.

Related Commands

Command	Description
clear counters	Clears interface counters.

Command	Description
show interfaces virtual-access	Displays status, traffic data, and configuration information about a specified virtual access interface.
virtual-template	Specifies which virtual template will be used to clone virtual access interfaces.

show webvpn context

To display the operational status and configuration parameters for Secure Socket Layer (SSL) virtual private network (VPN) context configurations, use the **show webvpn context** command in privileged EXEC mode.

show webvpn context [*name*| **brief**]

Syntax Description

name	(Optional) Name of the context for which output will be filtered to display detailed information.
brief	(Optional) Filters the output to display a summary of SSL VPN context configuration.

Command Default

If no arguments or keywords are specified, the output displays general information about the operational status of all SSL VPN contexts.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(6)T	This command was introduced.
15.0(1)M	This command was modified. The **brief**keyword was added.

Usage Guidelines

Entering a context name displays more detailed information, such as the operational status and specific configuration information for the named context.

Examples

The following output is an example of brief information that can be displayed for system security officer (SSO) servers configured for the SSL VPN context:

```
Router# show webvpn context brief
Codes: AS - Admin Status, OS - Operation Status
       VHost - Virtual Host
Context Name        Gateway  Domain/VHost      VRF      AS    OS
------------        -------  ------------      -------  ----  --------
Default_context     n/a      n/a               n/a      down  down
con-1               gw-1     one               -        up    up
con-2               -        -                 -        down  down
```

The table below describes the significant fields shown in the display.

Table 3: show webvpn context brief Field Descriptions

Field	Description
Context Name	Displays the name of the context.
Gateway	Displays the name of the associated gateway. n/a is displayed if no gateway is associated.
Domain/VHost	Displays the SSL VPN domain or virtual hostname.
VRF	Displays the VPN routing and forwarding (VRF) instance, if configured, that is associated with the context configuration.
AS	Displays the administrative status of the SSL VPN context. The status is displayed as "up" or "down."
OS	Displays the operational status of the SSL VPN context. The status is displayed as "up" or "down."

The following is sample output from the **show webvpn context** command entered with the name of a specific SSL VPN context:

```
Router# show webvpn context 1234567891234567891second
Admin Status: down
Operation Status: down
Error and Event Logging: Disabled
CSD Status: Disabled
Certificate authentication type: All attributes (like CRL) are verified
AAA Authentication List not configured
AAA Authorization List not configured
AAA Accounting List not configured
AAA Authentication Domain not configured
Authentication mode: AAA authentication
Default Group Policy not configured
Not associated with any WebVPN Gateway
Domain Name and Virtual Host not configured
Maximum Users Allowed: 1000 (default)
NAT Address not configured
VRF Name not configured
Virtual Template not configured
```

The table below describes the significant fields shown in the display.

Table 4: show webvpn context (Specific WebVPN Context) Field Descriptions

Field	Description
Admin Status	Administrative status of the context. The status is displayed as "up" or "down." The **inservice** command is used to configure this configuration parameter.

Field	Description
Operation Status	Displays the operational status of the SSL VPN. The status is displayed as "up" or "down." The context and the associated gateway must both be in an enabled state for the operational status to be "up."
CSD Status	Displays the status of Cisco Secure Desktop (CSD). The status is displayed as "Enabled" or "Disabled."
Certificate authentication type	Displays the certification authority (CA) type.
AAA Authentication List...	Displays the authentication list if configured.
AAA Authentication Domain...	Displays the authentication, authorization, and accounting (AAA) domain if configured.
Default Group Policy	Name of the group policy configured under the named context.
Domain Name	Domain name or virtual hostname configured under the named context.
Maximum Users Allowed	Displays the maximum number of user sessions that can be configured.
NAT Address...	Displays the Network Address Translation (NAT) address if configured.
VRF	Displays the VRF, if configured, that is associated with the context configuration.

Related Commands

Command	Description
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

show webvpn gateway

To display the status of a SSL VPN gateway, use the **show webvpn gateway** command in privileged EXEC mode.

show webvpn gateway [*name*]

Syntax Description

name	(Optional) Filters the output to display more detailed information about the named gateway.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

Entering this command without specifying a gateway name, displays general the operational status of all SSL VPN gateways. Entering a gateway name displays the IP address and CA trustpoint.

Examples

The following is sample output from the **show webvpn gateway** command:

```
Router# show webvpn gateway

Gateway Name                        Admin  Operation
------------                        -----  ---------
GW_1                                up     up
GW_2                                down   down
```

The table below describes the significant fields shown in the display.

Table 5: show webvpn gateway Field Descriptions

Field	Description
Gateway Name	Name of the gateway.
Admin	The administrative status of the gateway, displayed as "up" or "down." Administrative status is configured with the **inservice** command.

Field	Description
Operation	The operational status of the gateway, displayed as "up" or "down." The gateway must be "inservice" and configured with a valid IP address to be in an "up" state.

The following is sample output from the **show webvpn gateway**command, entered with a specific SSL VPN gateway name:

```
Router# show webvpn gateway
 GW_1

Admin Status: up
Operation Status: up
IP: 10.1.1.1, port: 443
SSL Trustpoint: TP-self-signed-26793562
```

The table below describes the significant fields shown in the display.

Table 6: show webvpn gateway name Field Descriptions

Field	Description
Admin Status	The administrative status of the gateway, displayed as "up" or "down." Administrative status is configured with the **inservice** command.
Operation Status	The operational status of the gateway, displayed as "up" or "down." The gateway must be "inservice" and configured with a valid IP address to be in an "up" state.
IP: ... port: ...	The configured IP address and port number of the WebVPN gateway. The default port number 443.
SSL Trustpoint:	Configures the CA certificate trust point.

Related Commands

Command	Description
webvpn gateway	Enters webvpn gateway configuration mode to configure a SSL VPN gateway.

show webvpn install

To display the installation status of SVC or CSD client software packages, use the **show webvpn install** command in EXEC mode.

show webvpn install {**file** *name*| **package** {**csd| svc**}| **status** {**csd| svc**}}

Syntax Description

file *name*	Displays file attribute information about the named software package file.
package {**csd** | **svc**	Displays information about either the CSD or SVC software installation package.
status {**csd** | **svc**}	Displays file attribute information about the CSD or SVC software package.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

This command is used to display information about Cisco Secure Desktop (CSD) and SSL VPN Client (SVC) software pages that are locally cached for distribution to remote SSL VPN clients. This information includes software versions and build dates.

Examples

The following is sample output from the **show webvpn install** command, entered with the **file** keyword:

```
Router# show webvpn install file \webvpn\stc\version.txt

SSLVPN File \webvpn\stc\version.txt installed:
CISCO STC win2k+ 1.0.0
1,1,0,116
Fri 06/03/2005 03:02:46.43
```

The table below describes the significant fields shown in the display.

Table 7: show webvpn install file Field Descriptions

Field	Description
SSLVPN File	The local path to the specified installation package file. File attributes, such as the name, build number, and installation date are deployed following this line.

The following is sample output from the **show webvpn install** command, entered with the **package svc**keywords:

```
Router# show webvpn install package svc

SSLVPN Package SSL-VPN-Client installed:
File: \webvpn\stc\1\binaries\detectvm.class, size: 555
File: \webvpn\stc\1\binaries\java.htm, size: 309
File: \webvpn\stc\1\binaries\main.js, size: 8049
File: \webvpn\stc\1\binaries\ocx.htm, size: 244
File: \webvpn\stc\1\binaries\setup.cab, size: 176132
File: \webvpn\stc\1\binaries\stc.exe, size: 94696
File: \webvpn\stc\1\binaries\stcjava.cab, size: 7166
File: \webvpn\stc\1\binaries\stcjava.jar, size: 4846
File: \webvpn\stc\1\binaries\stcweb.cab, size: 13678
File: \webvpn\stc\1\binaries\update.txt, size: 11
File: \webvpn\stc\1\empty.html, size: 153
File: \webvpn\stc\1\images\alert.gif, size: 2042
File: \webvpn\stc\1\images\buttons.gif, size: 1842
File: \webvpn\stc\1\images\loading.gif, size: 313
File: \webvpn\stc\1\images\title.gif, size: 2739
File: \webvpn\stc\1\index.html, size: 4725
File: \webvpn\stc\2\index.html, size: 325
File: \webvpn\stc\version.txt, size: 63
Total files: 18
```

The table below describes the significant fields shown in the display.

Table 8: show webvpn install package Field Descriptions

Field	Description
SSLVPN Package SSL-VPN-Client installed:	Displays the installation status of the CSD or SVC software package as "installed" or "NONE."
File: ... size: ...	The path, name, and size of each installation file.
Total files:	Total number in the package.

The following is sample output from the **show webvpn install** command, entered with the **status svc** keywords:

```
Router# show webvpn install status svc

SSLVPN Package SSL-VPN-Client version installed:
CISCO STC win2k+ 1.0.0
1,0,2,127
Fri 07/22/2005 12:14:45.43
```

The table below describes the significant fields shown in the display.

Table 9: show webvpn install stats Field Descriptions

Field	Description
SSLVPN Package	The SVC or CSD package file status is displayed as "installed" or "NONE." File attributes, such as the name, build number, and installation date are displayed following this line.

Related Commands

Command	Description
webvpn install	Installs a CSD or SVC package file to a WebVPN gateway for distribution to remote users.

show webvpn license

To display the available count and the current usage, use the **show webvpn license**command in privileged EXEC mode.

show webvpn license

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

Use the **show webvpn license** command to display the available count and the current usage. To display the current license type and time period left in the case of a nonpermanent licence, use the **show license**command.

Examples

The following is sample output from the **show webvpn license** command:

```
Router# show webvpn license
Available license count : 200
Reserved license count  : 200
In-use count : 3
```

The above output is self-explanatory.

Related Commands

Command	Description
debug webvpn license	Displays debug messages related to license operations, events, and errors.

show webvpn nbns

To display information in the NetBIOS Name Service (NBNS) cache, use the **show webvpn nbns** command in privileged EXEC mode.

show webvpn nbns context {**all**| *name*}

Syntax Description

context *name*	Filters the output to display NBNS information for the named context.
context all	Displays NBNS information for all contexts.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

This command is used to display information about NBNS cache entries. The NetBIOS name, IP address of the Windows Internet Name Service (WINS) server, and associated time stamps.

Examples

The following is sample output from the **show webvpn nbns** command, entered with the **context** and **all** keywords:

```
Router# show webvpn nbns context all

NetBIOS name        IP Address       Timestamp
0 total entries
NetBIOS name        IP Address       Timestamp
0 total entries
NetBIOS name        IP Address       Timestamp
0 total entries
```

The table below describes the significant fields shown in the display.

Table 10: show webvpn nbns context all Field Descriptions

Field	Description
NetBIOS name	NetBIOS name.

Field	Description
IP Address	The IP address of the WINs server.
Timestamp	Time stamp for the last entry.
... total entries	Total number of NetBIOS cache entries.

Related Commands

Command	Description
nbns-list	Enters webvpn NBNS list configuration mode to configure a NBNS server list for CIFS name resolution.
webvpn install	Installs a CSD or Cisco AnyConnect VPN Client package file to a SSL VPN gateway for distribution to end users.

show webvpn policy

To display the context configuration associated with a policy group, use the **show webvpn policy** command in user EXEC or privileged EXEC mode.

show webvpn policy group *name* **context** {**all**| *name*} **[detail]**

Syntax Description

group *name*	Displays information for the named policy group.
context all	Displays information for all context configurations with which the policy group is associated.
context *name*	Displays information for the named context configuration.
detail	(Optional) Displays detailed information about the user session.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.4(11)T	This command was modified. An output example was added for Single SignOn (SSO) server information.
15.1(1)T	This command was modified. The **detail** keyword was added. The output was modified to display the webvpn home page configuration.

Usage Guidelines

This command is used to display configuration settings that apply only to the policy group. This command can also be used to display all contexts for which the policy group is configured.

Examples

The following is sample output from the **show webvpn policy**command:

```
Router# show webvpn policy group group1 context all
WEBVPN: group policy = group1 ; context = context1
      url list name = "web-url"
      cifs url list name = "cifs-url"
      idle timeout = 2100 sec
      session timeout = Disabled
      port forward name = "pflist"
      functions =
                file-access
```

```
            file-browse
            file-entry
            svc-enabled
      citrix disabled
      address pool name = "70pool"
      svc home page = "http://wiki-eng.cisco.com/engwiki/SSLVPNTech"
      webvpn home page = "http://192.0.2.0", redirection time = 10
      dpd client timeout = 300 sec
      dpd gateway timeout = 300 sec
      keepalive interval = 30 sec
      SSLVPN Full Tunnel mtu size = 1406 bytes
      keep sslvpn client installed = enabled
      rekey interval = 3600 sec
      rekey method =
      lease duration = 43200 sec
      msie-proxy = auto
      ie proxy server = "test.com:80"
      split include = 209.165.200.225 255.255.255.224
      split include = 209.165.200.226 255.255.255.224
```

See the table below for the field description.

```
The following sample output displays information about an SSO server configured for a policy
 group of the SSL VPN context:
Router# show webvpn policy group ONE context all
WV: group policy = sso ; context = test_sso
  idle timeout = 2100 sec
  session timeout = 43200 sec
  sso server name = "server2
  citrix disabled
  dpd client timeout = 300 sec
  dpd gateway timeout = 300 sec
  keep sslvpn client installed = disabled
  rekey interval = 3600 sec
  rekey method =
  lease duration = 43200 sec
```

The table below describes the significant fields shown in the displays.

Table 11: show webvpn policy Field Descriptions

Field	Description
group policy	Name of the policy group.
context	Name of the Secure Socket Layer (SSL) Virtual Private Network (VPN) context.
url list name	Name of the URL list.
cifs url list name	Name of the Common Internet File System (CIFS) URL list.
idle timeout	Length of time that a remote-user session can remain idle.
session timeout	Length of time that a remote-user session can remain active.
port forward name	Name of the port-forwarding list configured with the **port-forward** command.

Field	Description
citrix	Support for Citrix applications, shown as "disabled" or "enabled."
address pool name	Name of the address pool configured.
svc home page	URL of the SSL VPN Client (SVC) configured.
webvpn home page	URL of the WebVPN configured using the **webvpn-homepage** command.
dpd client timeout	Length of time that a session will be maintained with a nonresponsive end user (remote client).
dpd gateway timeout	Length of the time that a session will be maintained with a nonresponsive SSL VPN gateway.
keepalive interval	Keepalive interval, in seconds.
SSLVPN Full Tunnel mtu size	MTU, in bytes.
keep sslvpn client installed	Cisco AnyConnect VPN Client software installation policy on the end user (remote PC). "enabled" indicates that Cisco AnyConnect VPN Client software remains installed after the SSL VPN session is terminated. "disabled" indicates that Cisco AnyConnect VPN Client software is pushed to the end user each time a connection is established.
rekey interval	Length of time between tunnel key refresh cycles.
rekey method	Tunnel key authentication method.
lease duration	Tunnel key lifetime.
sso server name	Name of the SSO server.

Related Commands

Command	Description
policy group	Enters SSL VPN group policy configuration mode to configure a group policy.

show webvpn session

To display Secure Sockets Layer Virtual Private Network (SSL VPN) user session information, use the **show webvpn session** command in user EXEC or privileged EXEC mode.

show webvpn session [**user** *user-name*] **context** {*context-name*| **all**} **[detail]**

Syntax Description

user	(Optional) Displays detailed information about the named user session.
user-name	(Optional) Name of the user.
context	Displays a list of active users for only the named context.
context-name	Name of the context.
all	Displays a list of active users sessions for all locally configured contexts.
detail	(Optional) Displays detailed information about the user session.

Command Default

Session information is not displayed.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.4(6)T	This command was introduced.
15.1(1)T	This command was modified. The **detail**keyword was added.

Usage Guidelines

This command is used to list active SSL VPN connections or to display context configuration policies that apply to the specified end user.

The **show webvpn session** command provides detailed information about the user session. These details include the username, assigned IP addess, group policy, login time, hash algorithms used for the session, number of clientless tunnels, and the number of full tunnels enabled for the user.

This command is applicable only for user session statistics and tunnel statistics.

Examples

The following is sample output from the **show webvpn session** command. The output is filtered to display user session information for only the specified context.

```
Router# show webvpn session context context1

WebVPN context name: context1
Client_Login_Name  Client_IP_Address  No_of_Connections  Created  Last_Used
user1              192.0.2.1                  2         04:47:16  00:01:26
user2              192.0.2.2                  2         04:48:36  00:01:56
```

The table below describes the significant fields shown in the display.

Table 12: show webvpn session Field Descriptions

Field	Description
WebVPN context name	Name of the context.
Client_Login_Name	Login name for the end user (remote PC or device).
Client_IP_Address	IP address of the remote user.
No_of_Connections	Number of times the remote user has connected.
Created	Time, in hh:mm:ss, when the remote connection was established.
Last_Used	Time, in hh:mm:ss, that the user connection last generated network activity.

The following is sample output from the **show webvpn session** command. The output is filtered to display session information for a specific user.

```
Router# show webvpn session user user1 context all

Session Type      : Full Tunnel
Client User-Agent : Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.1.5)
Username          : test                 Num Connection : 1
Public IP         : 192.0.2.0            VRF Name       : None
Context           : context1             Policy Group   : default
Last-Used         : 00:00:42             Created        : *09:50:38.191 UTC Thu Jan 21 2010
Session Timeout   : Disabled             Idle Timeout   : 2100
DPD GW Timeout    : 300                  DPD CL Timeout : 300
Address Pool      : varun                MTU Size       : 1206
Rekey Time        : 3600                 Rekey Method   :
Lease Duration    : 43200
Tunnel IP         : 209.165.200.225      Netmask        : 255.255.255.224
Rx IP Packets     : 0                    Tx IP Packets  : 1
CSTP Started      : 00:01:42             Last-Received  : 00:01:42
CSTP DPD-Req sent : 0                    Virtual Access : 1
Msie-ProxyServer  : None                 Msie-PxyPolicy : Disabled
Msie-Exception    :
Split Include     : 209.165.200.224 255.255.255.224
Client Ports      : 2538
DTLS Port         : 2547
```

The table below describes the significant fields shown in the display.

Table 13: show webvpn session user context all Field Descriptions

Field	Description
Session Type	Mode used to access SSL VPN.
Client User-Agent	The client user-agent header.
Username	Name of the end user.
Num Connection	Number of times the remote user has connected.
Public IP	Public IP address.
VRF Name	Name of the virtual routing and forwarding (VRF) interface.
Context	Name of the context to which user policies apply.
Policy Group	Name of the policy group to which the user belongs.
Last-Used	Time, in hh:mm:ss, that the user connection last generated network activity.
Created	Time, in hh:mm:ss, when the remote connection was established.
Session Timeout	Length of time that a remote-user session can remain active.
Idle Timeout	Length of time that a remote-user session can remain idle.
DPD GW Timeout	Length of time that a Dead Peer Detection (DPD) gateway can remain idle.
DPD CL Timeout	Length of time that a DPD client can remain idle.
Address Pool	Name of the address pool configured.
MTU Size	Size of the maximum transmission unit (MTU).
Rekey Time	Time at which the tunnel key is refreshed.
Rekey Method	Tunnel key authentication method.
Lease Duration	Tunnel key lifetime.
Tunnel IP	IP address of the SSL VPN tunnel.
Netmask	Network mask used.

Field	Description
Rx IP Packets	Number of IP packets sent.
Tx IP Packets	Number of IP packets received.
CSTP Started	Time at which the Cisco SSL Tunnel Protocol (CSTP) frames were sent to the client.
Last-Received	Time when the CSTP frame was received.
CSTP DPD-Req sent	Time at which the CSTP request was sent to the client.
Virtual Access	Total number of virtual access interfaces created.
Msie-ProxyServer	Number of Microsoft Internet Explorer (MSIE) proxy servers configured for policy group end users.
Msie-PxyPolicy	Status of the MSIE policy: Enabled or Disabled.
Msie-Exception	MS Proxy exceptions.
Split Include	IP address from which the traffic is resolved through the Cisco AnyConnect VPN Client tunnel.
Client Ports	Local TCP port used on the client host.
DTLS Port	Datagram Transport Layer Security (DTLS) port.

The following is sample output from the show webvpn session user context all detail command:

```
Router# show webvpn session user user1 context all detail
Session Type      : Full Tunnel
Client User-Agent : Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:10.0.0.1)
Username          : user1                Num Connection : 1
Public IP         : 209.165.200.225      VRF Name       : None
Context           : context1             Policy Group   : default
Last-Used         : 00:00:02             Created        : *09:50:38.191 UTC Thu Jan 21 2010
Session Timeout   : Disabled             Idle Timeout   : 2100
DPD GW Timeout    : 300                  DPD CL Timeout : 300
Address Pool      : varun                MTU Size       : 1206
Rekey Time        : 3600                 Rekey Method   :
Lease Duration    : 43200
Tunnel IP         : 209.165.200.249      Netmask        : 255.255.255.224
Rx IP Packets     : 0                    Tx IP Packets  : 2
CSTP Started      : 00:02:03             Last-Received  : 00:02:03
CSTP DPD-Req sent : 0                    Virtual Access : 1
Msie-ProxyServer  : None                 Msie-PxyPolicy : Disabled
Msie-Exception    :
Split Include     : 209.165.200.250 255.255.255.224
Client Ports      : 2538
DTLS Port         : 2547

Detail Session Statistics for User:: user1
----------------------------------
CSTP Statistics::
Rx CSTP Frames    : 4                  Tx CSTP Frames   : 0
```

```
Rx CSTP Bytes     : 32                Tx CSTP Bytes    : 0
Rx CSTP Data Fr   : 0                 Tx CSTP Data Fr  : 0
Rx CSTP CNTL Fr   : 4                 Tx CSTP CNTL Fr  : 0
Rx CSTP DPD Req   : 0                 Tx CSTP DPD Req  : 0
Rx CSTP DPD Res   : 0                 Tx CSTP DPD Res  : 0
Rx Addr Renew Req : 0                 Tx Address Renew : 0
Rx CDTP Frames    : 2                 Tx CDTP Frames   : 0
Rx CDTP Bytes     : 122               Tx CDTP Bytes    : 0
Rx CDTP Data Fr   : 2                 Tx CDTP Data Fr  : 0
Rx CDTP CNTL Fr   : 0                 Tx CDTP CNTL Fr  : 0
Rx CDTP DPD Req   : 0                 Tx CSTP DPD Req  : 0
Rx CDTP DPD Res   : 0                 Tx CDTP DPD Res  : 0
Rx IP Packets     : 0                 Tx IP Packets    : 2
Rx IP Bytes       : 0                 Tx IP Bytes      : 10
CEF Statistics::
Rx CSTP Data Fr   : 0                 Tx CSTP Data Fr  : 0
Rx CSTP Bytes     : 0                 Tx CSTP Bytes    : 0
```

The table below describes the significant fields shown in the display.

Table 14: show webvpn session user context all detail Field Descriptions

Field	Description
Rx CSTP Frames	Number of CSTP frames received from the client.
Rx CSTP Bytes	Number of CSTP bytes (data plus control frames) received from the client.
Rx CSTP Data Fr	Number of CSTP data frames received from the client.
Rx CSTP CNTL Fr	Number of CSTP control frames received from the client.
Rx CSTP DPD Req	Number of DPD requests received at the gateway.
Rx CSTP DPD Res	Number of times the gateway processed a CSTP DPD request frame.
Rx Addr Renew Req	Number of address renew requests received at the gateway.
Rx CDTP Frames	Number of Cisco Dynamic Trunking Protocol (CDTP) frames received from the client.
Rx CDTP Bytes	Number of CDTP bytes received from the client.
Rx CDTP Data Fr	Number of CDTP data frames received from the client.
Rx CDTP CNTL Fr	Number of CDTP control frames received from the client.
Rx CDTP DPD Req	Number of CDTP DPD requests received at the gateway.

Field	Description
Rx CDTP DPD Res	Number of times the gateway processed a CDTP DPD request frame.
Rx IP Packets	Total number of IP packets received.
Rx IP Bytes	Total number of IP bytes received.
Tx CSTP Frames	Number of CSTP frames transmitted to the client.
Tx CSTP Bytes	Number of CSTP bytes (data plus control frames) transmitted to the client.
Tx CSTP Data Fr	Number of CSTP data frames transmitted to the client.
Tx CSTP CNTL Fr	Number of CSTP control frames transmitted to the client.
Tx CSTP DPD Req	Number of DPD requests transmitted from the gateway.
Tx CSTP DPD Res	Number of times the gateway processed a CSTP DPD request frame.
Tx Address Renew	Number of address renew requests transmitted at the gateway.
Tx CDTP Frames	Number of CDTP frames transmitted to the client.
Tx CDTP Bytes	Number of CDTP bytes transmitted to the client.
Tx CDTP Data Fr	Number of CDTP data frames transmitted to the client.
Tx CDTP CNTL Fr	Number of CDTP control frames transmitted to the client.
Tx CDTP DPD Req	Number of CDTP DPD requests transmitted to the gateway.
Tx CDTP DPD Res	Number of times the gateway processed a CDTP DPD request frame.
Tx IP Packets	Total number of IP packets transmitted.
Tx IP Bytes	Total number of IP bytes transmitted.
CEF Statistics	Cisco Express Forwarding statistics.

show webvpn sessions

Note Effective with Cisco IOS Release 12.4(6)T, the **show webvpn sessions** command is replaced by the **show webvpn session** command. See the **show webvpn session** command for more information.

To display information about WebVPN sessions, use the **show webvpn sessions** command in privileged EXEC mode.

show webvpn sessions

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(6)T	This command was replaced by the **show webvpn session** command.

Examples

The following output example displays information about a WebVPN session:

```
Router# show webvpn sessions
WebVPN domain name: cisco.com
Client Login Name          Client IP Address     Number of Connections
webuser                    172.16.163.142       4
    Created 00:14:25, Last-used 00:00:10
    Client Port: 2366
    Client Port: 2386
    Client Port: 2396
    Client Port: 2486
browseruser                172.16.163.142      2
    Created 00:00:09, Last-used 00:00:08
    Client Port: 2431
    Client Port: 2432
```

The table below describes the significant fields shown in the display

Table 15: show webvpn sessions Field Descriptions

Field	Description
Client Login Name	Username used to log in to the WebVPN gateway.
Client IP Address	IP address of the host from which the user is connecting.

Field	Description
Number of Connections	Number of active TCP connections by the user at this point.
Created	Provides the time that has elapsed since the user logged in (in HH:MM:SS format).
Client Port	Local TCP port used on the client host.

Related Commands

Command	Description
show webvpn statistics	Displays WebVPN statistics.

show webvpn statistics

Note Effective with Cisco IOS Release 12.4(6)T, the **show webvpn statistics** command is replaced by the **show webvpn stats**command. See the **show webvpn stats** command for more information.

To display WebVPN statistics, use the **show webvpn statistics** command in privileged EXEC mode.

show webvpn statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(6)T	This command was replaced by the **show webvpn stats**command.

Examples

The following is sample output using the **show webvpn statistics** command:

```
Router# show webvpn statistics
Active user sessions: 2
Active user TCP connections: 6
Authentication failures: 3
Terminated user sessions: 0
```

The table below describes the significant fields shown in the display.

Table 16: show webvpn statistics Field Descriptions

Field	Description
Active user sessions	Number of users who are logged into the system.
Active user TCP connections	Number of TCP user connections that are used by the user session.
Authentication failures	Number of authentication failures to the gateway.
Terminated user sessions	Number of users who logged in and logged out after the statistics were cleared.

Related Commands

Command	Description
show webvpn sessions	Displays information about WebVPN sessions.

show webvpn stats

To display Secure Socket Layer Virtual Private Network (SSL VPN) application and network statistics, use the **show webvpn stats** command in privileged EXEC mode.

show webvpn stats [**cifs**| **citrix**| **mangle**| **port-forward**| **sso**| **tunnel**] **[detail]** [**context** {**all**| *name*}]

Syntax Description

cifs	(Optional) Displays Windows file share (Common Internet File System [CIFS]) statistics.
citrix	(Optional) Displays Citrix application statistics.
mangle	(Optional) Displays URL mangling statistics.
port-forward	(Optional) Displays port forwarding statistics.
sso	(Optional) Displays statistics for the Single SignOn (SSO) server.
tunnel	(Optional) Displays VPN tunnel statistics.
detail	(Optional) Displays detailed information.
context all | *name*	(Optional) Displays information for a specific context or all contexts.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.4(11)T	The **sso** keyword was added for Cisco 6500 Catalyst switches.
12.4(15)T	Output information was added for Cisco Express Forwarding (CEF).

Usage Guidelines

This command is used to display SSL VPN application, authentication, and network statistics and counters.

Examples

The following is sample output from the **show webvpn stats** command entered with the **detail** and **context** keywords:

```
Router# show webvpn stats detail context context1
WebVPN context name : context1
User session statistics:
    Active user sessions     : 0          AAA pending reqs         : 0
    Peak user sessions       : 0          Peak time                : never
    Active user TCP conns    : 0          Terminated user sessions : 0
    Session alloc failures   : 0          Authentication failures  : 0
    VPN session timeout      : 0          VPN idle timeout         : 0
    User cleared VPN sessions: 0          Exceeded ctx user limit  : 0
    CEF switched packets - client: 0         , server: 0
    CEF punted packets - client: 0         , server: 0
Mangling statistics:
    Relative urls            : 0          Absolute urls            : 0
    Non-http(s) absolute urls: 0          Non-standard path urls   : 0
    Interesting tags         : 0          Uninteresting tags       : 0
    Interesting attributes   : 0          Uninteresting attributes : 0
    Embedded script statement: 0          Embedded style statement : 0
    Inline scripts           : 0          Inline styles            : 0
    HTML comments            : 0          HTTP/1.0 requests        : 0
    HTTP/1.1 requests        : 0          Unknown HTTP version     : 0
    GET requests             : 0          POST requests            : 0
    CONNECT requests         : 0          Other request methods    : 0
    Through requests         : 0          Gateway requests         : 0
    Pipelined requests       : 0          Req with header size >1K : 0
    Processed req hdr bytes  : 0          Processed req body bytes : 0
    HTTP/1.0 responses       : 0          HTTP/1.1 responses       : 0
    HTML responses           : 0          CSS responses            : 0
    XML responses            : 0          JS responses             : 0
    Other content type resp  : 0          Chunked encoding resp    : 0
    Resp with encoded content: 0          Resp with content length : 0
    Close after response     : 0          Resp with header size >1K: 0
    Processed resp hdr size  : 0          Processed resp body bytes: 0
    Backend https response   : 0          Chunked encoding requests: 0
CIFS statistics:
  SMB related Per Context:
    TCP VC's                 : 0          UDP VC's                 : 0
    Active VC's              : 0          Active Contexts          : 0
    Aborted Conns            : 0
  NetBIOS related Per Context:
    Name Queries             : 0          Name Replies             : 0
    NB DGM Requests          : 0          NB DGM Replies           : 0
    NB TCP Connect Fails     : 0          NB Name Resolution Fails : 0
  HTTP related Per Context:
    Requests                 : 0          Request Bytes RX         : 0
    Request Packets RX       : 0          Response Bytes TX        : 0
    Response Packets TX      : 0          Active Connections       : 0
    Active CIFS context      : 0          Requests Dropped         : 0

Socket statistics:
    Sockets in use           : 0          Sock Usr Blocks in use   : 0
    Sock Data Buffers in use : 0          Sock Buf desc in use     : 0
    Select timers in use     : 0          Sock Select Timeouts     : 0
    Sock Tx Blocked          : 0          Sock Tx Unblocked        : 0
    Sock Rx Blocked          : 0          Sock Rx Unblocked        : 0
    Sock UDP Connects        : 0          Sock UDP Disconnects     : 0
    Sock Premature Close     : 0          Sock Pipe Errors         : 0
    Sock Select Timeout Errs : 0
Port Forward statistics:
    Connections serviced     : 0          Server Aborts (idle)     : 0
  Client                                Server
    in pkts                  : 0          out pkts                 : 0
    in bytes                 : 0          out bytes                : 0
    out pkts                 : 0          in pkts                  : 0
    out bytes                : 0          in bytes                 : 0
WEBVPN Citrix statistics:
Connections serviced : 0
```

```
              Server                    Client
  Packets in  : 0                        0
  Packets out : 0                        0
  Bytes in    : 0                        0
  Bytes out   : 0                        0
Tunnel Statistics:
    Active connections       : 0
    Peak connections         : 0          Peak time                : never
    Connect succeed          : 0          Connect failed           : 0
    Reconnect succeed        : 0          Reconnect failed         : 0
    SVCIP install IOS succeed: 0          SVCIP install IOS failed : 0
    SVCIP clear IOS succeed  : 0          SVCIP clear IOS failed   : 0
    SVCIP install TCP succeed: 0          SVCIP install TCP failed : 0
    DPD timeout              : 0
  Client                                 Server
    in  CSTP frames          : 0          out IP pkts              : 0
    in  CSTP data            : 0          out stitched pkts        : 0
    in  CSTP control         : 0          out copied pkts          : 0
    in  CSTP Addr Reqs       : 0          out bad pkts             : 0
    in  CSTP DPD Reqs        : 0          out filtered pkts        : 0
    in  CSTP DPD Resps       : 0          out non fwded pkts       : 0
    in  CSTP Msg Reqs        : 0          out forwarded pkts       : 0
    in  CSTP bytes           : 0          out IP bytes             : 0
    out CSTP frames          : 0          in  IP pkts              : 0
    out CSTP data            : 0          in  invalid pkts         : 0
    out CSTP control         : 0          in  congested pkts       : 0
    out CSTP Addr Resps      : 0          in  bad pkts             : 0
    out CSTP DPD Reqs        : 0          in  nonfwded pkts        : 0
    out CSTP DPD Resps       : 0          in  forwarded pkts       : 0
    out CSTP Msg Reqs        : 0
    out CSTP bytes           : 0          in  IP bytes             : 0
```

The table below describes significant fields in the **show webvpn stats detail context**display.

Table 17: show webvpn stats detail context Field Descriptions

Field	Description
WebVPN context name	Name of the context.
User session statistics:	
Active user sessions	Total number of currently active user sessions on the gateway.
Peak user sessions	Maximum number of simultaneous user sessions on the gateway since the gateway came up.
Active user TCP conns	Total number of currently active TCP connections that were initiated from the client side toward the SSL VPN gateway.

Field	Description
Session alloc failures	Total number of session allocation failures that were initiated from the client side. These failures occur because of a lack of memory on the gateway. Examples: • No free slot in session table • No memory for session allocation • No memory for gateway cookie allocation • Not enough memory on the gateway
VPN session timeout	Information about the number of times the web VPN session timer has expired. This value reflects the full total for all the contexts that are configured at the gateway. The session timer is off by default, and it is enabled when an administrator intentionally uses the command-line interface (CLI) timeout session *number* argument under the **group policy** command submode.
User cleared VPN sessions	Total number of user-removed (or cleared) VPN sessions on the gateway. For example, if any user sessions are cleared using the CLI command **clear webvpn session** *user-name* **context** *context-name*, the counter is incremented by one.
AAA pending reqs	Total number of pending authentication, authorization, and accounting (AAA) requests on the gateway.
Peak time	Time elapsed since the peak number of simultaneous user sessions were observed on the gateway.
Terminated user sessions	Total number of expired user sessions on the gateway. Examples: • User logout sessions • Session cookie removed
Authentication failures	Total number of authentication failures on the gateway. Examples: • Wrong username and password • Empty username and password field

Field	Description
VPN idle timeout	Number of times the idle timer expired for all the contexts configured at the security gateway. Idle time refers to the time for which an active session can be left unattended (maximum time for which a session is up even though no traffic flows through the connection).
Exceeded ctx user limit	Total number of denied logins on the gateway that exceeded the context maximum user limit.
CEF switched packets (for client and server)	Packets that were CEF-switched.
CEF punted packets (for client and server)	Packets that could not be CEF-switched in a box with CEF switching enabled and that were "punted" to the next switching level.
Mangling statistics:	
Relative urls	Number of URLs that point to a file/directory in relation to the present file/directory.
Non-http(s) absolute urls	Number of non-HTTP- relative URLs that are mangled.
Interesting tags	Number of HTTP, Cascade Style Sheets (CSS), or JavaScript tags that are mangled.
Interesting attributes	HTTP attributes, JavaScript, or CSS attributes that are mangled.
Embedded script statement	Embedded JavaScripts that were mangled.
Inline scripts	Number of inline CSSs that were mangled.
HTML comments	Number of HTML comments that were encountered.
HTTP/1.1 requests	Number of HTTP 1.1 requests that were encountered.
GET requests	Number of HTTP 1.0 or 1.1 GET requests that were encountered.
CONNECT requests	Number of HTTP 1.0 or 1.1 CONNECT requests that were encountered.
Pipelined requests	Number of requests dropped due to pipelines (pipelined requests are currently not supported).
Processed req hdr bytes	Total number of bytes in the requests made by the HTTP header to the backend server.

Field	Description
HTML /1.0 responses	Number of HTTP 1.0 responses that were encountered.
HTML responses	Total number of HTML pages that were received at the gateway.
XML responses	Total number of XML pages/responses that were received at the gateway.
Other content type resp	Total number of responses that were received other than HTML, XML, JavaScript, or CSS.
Resp with encoded content	Number of supported responses that were already encoded by the backend server.
Processed resp hdr size	Number of bytes in the headers of HTTP responses that were processed at the gateway.
Backend https response	Number of HTTP pages sent to the client by the backend server.
Absolute urls	Number of absolute HTTP URLs that were mangled.
Non-standard path urls	Number of non-HTTP-relative URLs that were mangled.
Uninteresting tags	HTTP attributes, JavaScript, or CSS attributes that were mangled.
Uninteresting attributes	Number of attributes that were not mangled (for instance, XML attributes).
Embedded style statement	Embedded CSS and other styling sheets that were mangled.
Inline styles	Number of inline CSSs that were mangled.
HTTP/1.0 requests	Number of HTTP 1.0 requests that were encountered.
Unknown HTTP version	Number of HTTP version requests other than 1.0 and 1.1.
POST requests	Number of HTTP 1.0 or 1.1 POST requests that were encountered.
Other request methods	Number of non- (1.0 or 1.1) HTTP requests plus the number of requests other than GET, POST, or CONNECT.

Field	Description
Gateway requests	Number of requests made explicitly to the gateway.
Req with header size >1K	Number of requests to the backend server having a header size greater than 1024 bytes.
Processed req body bytes	Total number of bytes processed while parsing HTML requests (body means the total bytes processed or read in an HTML request excluding the header).
HTTP/1.1 responses	Number of HTTP 1.1 responses that were received at the gateway.
CSS responses	Total number of CSS tags that were received.
JS responses	Total number of JavaScript responses that were received at the gateway.
Chunked encoding resp	Number of times transfer encoding was set to "chunked" in an HTTP response.
Resp with content length	Number of non-zero content-length responses.
Resp with header size > 1K	Responses received at the gateway with a header size greater than 1 kilobyte.
Processed resp body bytes	Total number of bytes that were processed in responses (number of bytes in the bodies of the messages).
Chunked encoding requests	Number of requests that were chunk encoded.
CIFS statistics:	
SMB related Per Context:	
TCP VC's	Backend TCP connections established successfully (thus far).
Active VC's	Currently active TCP/User Datagram Protocol (UDP) connections.
Aborted Conns	Number of TCP-aborted connections (thus far).
UDP VC's	Backend TCP connections established successfully (thus far).
Active Contexts	Currently active Server Message Block (SMB) contexts.

Field	Description
NetBIOS related Per Context:	
Name Queries	NetBIOS name service (NBNS) name queries that have been sent.
NB DGM Requests	NetBios datagram service-related GET backup browser-list queries that have been sent.
NB TCP Connect Fails	NetBios TCP connections that failed.
Name Replies	NBNS name-query replies that have been received. Mismatch indicates that browsers/primary domain controller (PDC)/servers could not be contacted.
NB DGM Replies	NetBIOS datagram service-related GET backup browser replies were received. Request/reply mismatch indicates that a browse domain attempt would not work.
NB Name Resolution Fails	NetBIOS name resolution requests sent to the PDC failed.
HTTP related Per Context:	
Requests	Number of HTTP requests made per a CIFS application context.
Request Packets RX	Number of HTTP packets received per a CIFS application context.
Response Packets TX	Number of HTTP packets sent per a CIFS application context.
Active CIFS context	Number of active CIFS application module contexts on which CIFS requests are being processed.
Request Bytes RX	Number of HTTP bytes received per a CIFS application context.
Response Bytes TX	Number of HTTP bytes sent per a CIFS application context.
Active Connections	Number of active CIFS connections.
Requests Dropped	Number of HTTP requests dropped per CIFS application context.
Socket statistics:	

Field	Description
Sockets in use	Number of sockets that are in use by SSL VPN socket layer.
Sock Data Buffers in use	Number of data buffers that are used by the socket layer.
Select timers in use	Number of socket select timers that are in use.
Sock TX Blocked	Number of times an application send was blocked by TCP congestion control.
Sock Rx Blocked	Number of times an application blocked further reception of data from the TCP layer. The blocking indicates application buffer starvation or a processing limit.
Sock UDP Connects	Number of UDP connects to the gateway.
Sock Premature Close	Number of times an application received a Closed connection before it could be established.
Sock Select Timeout Errs	Number of times a socket select timeout error occurred.
Sock Usr Blocks in use	Number of user blocks in use.
Sock Buf desc in use	Number of socket buffer descriptors in use.
Sock Select Timeouts	Number of times an application timed out while waiting for a reply in a request/reply exchange or while waiting for a TCP connection to be established.
Sock Tx Unblocked	Number of times an application send resumed after being blocked due to TCP congestion control. If the transmit blocked and unblocked do not match after a sufficient period of time, the transaction is stalled.
Sock Rx Unblocked	Number of times an application resumed further reception of data from the TCP layer. If receive blocked and unblocked do not match after a sufficient period of time, the transaction is stalled.
Sock UDP Disconnects	Number of UDP disconnects to the gateway.
Sock Pipe Errors	Number of times socket pipe establishment failed.
WEBVPN Citrix statistics:	
Server	

Field	Description
Packets in	Number of packets received from the server.
Packets out	Number of packets sent to the server.
Bytes in	Number of bytes received from the server.
Bytes out	Number of bytes sent to the server.
Client	
Packets in	Number of packets received from the client.
Packets out	Number of packets sent to the client.
Bytes in	Number of bytes received from the server.
Bytes out	Number of bytes sent to the client.
Tunnel Statistics:	
Active connections	Number of active tunnels.
Peak connections	Maximum number of simultaneously active tunnels as observed since the last reboot of the Cisco IOS router or last counter reset.
Connect succeed	Number of tunnel connections that have succeeded since the last reboot of the Cisco IOS router or last counter reset.
Reconnect succeed	Number of tunnel connections that have succeeded in reconnecting since the last reboot of the Cisco IOS router or last counter reset.
SVCIP install IOS succeed	Number of times, during the SSL VPN Client (SVC)/AnyConnect package installation, that the frame IP address or allocated IP address is used (IP address sticky).
SVCIP clear IOS succeed	Number of times an SVC IP address is successfully removed from the IP alias on the core.
SVCIP install TCP succeed	Number of tunnel connections that have succeeded since the last reboot of the Cisco IOS router or last counter reset.
DPD timeout	Number of Dead Peer Detection (DPD) timeout sessions.

Field	Description
Peak time	Absolute timestamp when the peak full-tunnel connections were observed.
Connect failed	Number of tunnel connections that have failed since the last reboot of the Cisco IOS router or last counter reset.
Reconnect failed	Number of tunnel connections that have failed in reconnecting since the last reboot of the Cisco IOS router or last counter reset.
SVCIP install IOS failed	Total number of times, during the SVC/AnyConnect installation, that an IP assignment from the pool fails or failed to configure an IP address to the virtual route forwarding (VRF) table.
SVCIP clear IOS failed	Number of times an STC IP address could not be removed from the IP alias on the core.
SVCIP install TCP failed	Number of tunnel connections that have failed since the last reboot of the Cisco IOS router or last counter reset.
Client	
in CSTP frames	Number of Cisco SSL Tunnel Protocol (CSTP) frames from the client.
in CSTP data	Number of CSTP data frames from the client.
in CSTP control	Number of CSTP control frames from the client.
in CSTP Addr Reqs	Number of IP address renewal requests received by the gateway.
in CSTP DPD Reqs	Number of DPD requests received at the gateway.
in CSTP DPD Resps	Number of DPD responses received at the gateway (The client sends the DPD requests, the gateway responds to the transmission, and the client responds back. It is this response that is counted here.)
in CSTP Msg Reqs	Number of times a CSTP message control frame is received at the gateway.
in CSTP bytes	Number of CSTP bytes (data+control frames) from the client.
out CSTP frames	Number of CSTP frames to the client.

Field	Description
out CSTP data	Number of CSTP data frames to the client.
out CSTP control	Number of CSTP control frames to the client.
out CSTP DPD Reqs	Number of times at-gateway CSTP control frames were generated.
out CSTP DPD Resps	Number of times the gateway processed a CSTP DPD request frame.
out CSTP Msg Reqs	Number of times the gateway generated a CSTP message (MSG) frame.
out CSTP bytes	Number of CSTP bytes (data+control frames) to the client.
Server	
out IP pkts	IP datagrams that are successfully forwarded to the server.
out bad pkts	Number of times a bad tunneled IP packet was dropped at the gateway.
out filtered pkts	Number of times a tunneled IP packet was dropped at the gateway due to a named or numbered ACL that was configured at the gateway.
out non fwded pkts	Number of times a tunneled IP packet could not be forwarded due to routing issues.
out forwarded pkts	Number of times a tunneled IP packet was successfully forwarded by the gateway.
out IP bytes	IP datagram bytes that are successfully forwarded to the server.
in IP pkts	IP datagrams that are successfully received from the server.
in IP bytes	IP datagram bytes that are successfully received from the server.

The following example displays SSO statistics:

```
Router# show webvpn stats sso
   Auth Requests            : 4          Pending Auth Requests      : 0
   Successful Requests      : 1          Failed Requests            : 3
   Retranmissions           : 0          DNS Errors                 : 0
```

```
   Connection Errors        : 0          Request Timeouts           : 0
   Unknown Responses        : 0
```

The table below describes significant fields in the **show webvpn stats sso**display.

Table 18: show webvpn stats sso Field Descriptions

Field	Description
Auth Requests	Number of SSO authentication requests.
Successful Requests	Number of SSO authentication requests that passed successfully.
Retransmissions	Total number of times authentication requests were resent for authentication. The resending occurs when the SSO timer expires and no response is received from the SSO server for authentication requests.
Connection Errors	Number of failures to sign on to the SSO server.
Unknown Responses	Number of times an SSO authentication request yielded results other than failure or success (includes errors, such as access control list [ACL] errors).
Pending Auth Requests	Total number of SSO authentication requests pending to be processed for authentication.
Failed Requests	Number of times SSO authentication failed.
DNS Errors	Number of times an SSO server could not be resolved.
Request Timeouts	Number of times an SSO authentication request timed out.

The following example displays information about CEF:

```
Router# show webvpn stats
User session statistics:
   Active user sessions     : 1          AAA pending reqs         : 0
   Peak user sessions       : 1          Peak time                : 00:12:01
   Active user TCP conns    : 1          Terminated user sessions : 1
   Session alloc failures   : 0          Authentication failures  : 0
   VPN session timeout      : 0          VPN idle timeout         : 0
   User cleared VPN sessions: 0          Exceeded ctx user limit  : 0
   Exceeded total user limit: 0
   Client process rcvd pkts : 37         Server process rcvd pkts : 0
   Client process sent pkts : 1052       Server process sent pkts : 0
   Client CEF received pkts : 69         Server CEF received pkts : 0
   Client CEF rcv punt pkts : 1          Server CEF rcv punt pkts : 0
   Client CEF sent pkts     : 1102       Server CEF sent pkts     : 0
   Client CEF sent punt pkts: 448        Server CEF sent punt pkts: 0

   SSLVPN appl bufs inuse   : 0          SSLVPN eng  bufs inuse   : 0
  Active server TCP conns   : 0
```

The table below describes fields in the **show webvpn stats** display.

Table 19: show webvpn stats Field Descriptions

Field	Description
User session statistics:	
Active user sessions	Total number of currently active user sessions on the gateway.
Peak user sessions	Maximum number of simultaneous user sessions on the gateway since the gateway came up.
Active user TCP conns	Total number of currently active TCP connections that were initiated from the client side toward the SSL VPN gateway.
Session alloc failures	Total number of session allocation failures that were initiated from the client side. These failures occur because of a lack of memory on the gateway. Examples: • No free slot in session table • No memory for session allocation • No memory for gateway cookie allocation Not enough memory on the gateway
VPN session timeout	Information about the number of times the web VPN session timer has expired. This value reflects the full total for all the contexts that are configured at the gateway. The session timer is OFF by default, and it is enabled when an administrator intentionally uses the CLI timeout session *number* argument under the **group policy** command submode.
User cleared VPN sessions	Total number of user-removed (or cleared) VPN sessions on the gateway. For example, if any user sessions are cleared using the CLI command **clear webvpn session** *user-name* **context** *context-name*, the counter is incremented by one.
Exceeded total user limit	Total number of denied logins on the gateway. An SSL VPN gateway can support the maximum user sessions (up to 1000).
Client process rcvd pkts	Total number of packets that were received from the client on the SSL VPN gateway.
Client process sent pkts	Total number of data packets that were sent to the client side from the SSL VPN gateway.

Field	Description
Client CEF received pkts	Total number of CEF-related packets that were received from the client on the gateway.
Client CEF rcv punt pkts	Total number of punt packets that were received from the client on the gateway. Punting is defined as the handling of CEF-intended data on the slower path (called the process path). Punting occurs when the data is not handled by the CEF path. Example: • If any control packets are received on the CEF path, those packets will punt to the slower path (process path), which is not handled by the CEF path.
Client CEF sent pkts	Total number of data packets that were sent via the CEF path to the client side from the gateway.
Client CEF sent punt pkts	Total number of punt packets (data sent via a slow path) that were sent to the client from the gateway.
SSLVPN appl bufs inuse	Total number of buffers that are allocated for data or application processing on the gateway.
Active server TCP conns	Total number of currently active TCP connections on the gateway that were initiated from the server side toward the SSL VPN gateway.
AAA pending reqs	Total number of pending AAA requests on the gateway.
Peak time	Time elapsed since the peak number of simultaneous user sessions were observed on the gateway.
Terminated user sessions	Total number of expired user sessions on the gateway. Examples: • User logout sessions • Session cookie removed
Authentication failures	Total number of authentication failures on the gateway. Examples: • Wrong username and password • Empty username and password field

Field	Description
VPN idle timeout	Number of times the idle timer expired for all the contexts configured at the security gateway. Idle time refers to the time for which an active session can be left unattended (maximum time for which a session is up even though no traffic flows through the connection).
Exceeded ctx user limit	Total number of denied logins on the gateway that exceeded the context maximum user limit.
Server process rcvd pkts	Total number of control packets that were received from the server side of the SSL VPN gateway.
Server process sent pkts	Total number of control packets that were sent to the server side from the SSL VPN gateway.
Server CEF received pkts	Total number of data CEF-related packets that were received from the server side of the SSL VPN gateway.
Server CEF rcv punt pkts	Total number of punt packets that were received from the server on the SSL VPN gateway.
Server CEF sent pkts	Total number of data (CEF-related) packets that were sent to the server from the SSL VPN gateway.
Server CEF sent punt pkts	Total number of punt packets that were sent to the server side from the SSL VPN gateway.
SSLVPN eng bufs inuse	Total number of buffers that were allocated for engine processing on the gateway.

Related Commands

Command	Description
clear webvpn stats	Clears application and access counters on an SSL VPN gateway.

show wlccp wds

To display information either about the wireless domain services (WDS) device or about client devices, use the **show wlccp wds**command in privileged EXEC mode.

show wlccp wds [**ap**| **mn**] **[detail]** [**mac-addr mac-address**]

Syntax Description

ap	(Optional) Displays access points participating in Cisco Centralized Key Management.
mn	(Optional) Displays cached information about client devices, also called mobile nodes.
detail	(Optional) Displays the lifetime of the client, the service set identifier (SSID), and the virtual VLAN ID.
mac-addr	(Optional) Displays information about a specific client device.
mac-address	Client's MAC address.

Command Default

If you do not enter any options with the **show wlccp wds** command, this command displays the IP address of the WDS device, the MAC address, the priority, and the interface state. If the interface state is backup, the command also displays the IP address of the current WDS device, the MAC address, and the priority.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(11)JA	This command was introduced.
12.3(11)T	This command was implemented on the following platforms: Cisco 2600XM, Cisco 2691, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3700, and Cisco 3800 series routers.

Usage Guidelines

To show information about the WDS device, do not enter any keywords with this command.

Examples

The following command entry displays information about the WDS device:

```
Router# show wlccp wds ap
```

The following command entry displays cached information, including details, about the client device with the specified MAC address:

```
Router# show wlccp wds mn detail mac-addr 00-05-C2-00-01-F5
```

The following is sample output from the **show wlccp wds** command:

```
Router# show wlccp wds
      MAC:0001.28e0.a400, IP-ADDR:10.0.0.1       , Priority:255
      Interface Vlan1, State:Administratively StandAlone - ACTIVE
      AP Count:1   , MN Count:0   , MAX AP Count:50
```

The table below describes the significant fields shown in the display.

Table 20: show wlccp wds Field Descriptions

Field	Description
MAC	MAC address of the interface on which the WDS is configured.
IP-ADDR	IP address of the interface on which the WDS is configured.
Priority	Priority of the WDS.
Interface	Interface on which the WDS is configured.
State	State of the WDS. The state can be INITIALIZATION, BACKUP, or ACTIVE.
AP Count	Number of access points registered to the WDS.
MN Count	Number of mobile nodes registered to the WDS.
MAX AP Count	Maximum number of access points that can be registered.

Related Commands

Command	Description
debug wlccp packet	Displays packet traffic to and from the WDS router.
debug wlccp wds	Displays either WDS debug state or WDS statistics messages.

Command	Description
wlccp authentication-server client	Configures the list of servers to be used for 802.1X authentication.
wlccp authentication-server infrastructure	Configures the list of servers to be used for 802.1X authentication for the wireless infrastructure devices.
wlccp wds priority interface	Enables a wireless device such as an access point or a wireless-aware router to be a WDS candidate.

show xsm status

To display information and subscription status of the XML Subscription Manager (XSM) server and clients (such as VPN Device Manager [VDM]), and to display a list of XML data from the XSM server, use the **show xsm status**command in privileged EXEC mode.

show xsm status

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(6)E	This command was introduced.
12.2(9)YE	This command was integrated into Cisco IOS Release 12.2(9)YE.
12.2(9)YO1	This command was integrated into Cisco IOS Release 12.2(9)YO1.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to display the following information: which subsystems and histories are enabled or disabled (XSM, Embedded Device Manager [EDM], VDM), XSM client version, number of XSM sessions, duration of XSM session, session IDs, client version and IP address, configuration and monitor privilege levels, and list of subscribed XML Request Descriptors (XRDs).

Examples

The following example shows one XSM session (Session ID = 2) active on the Cisco device for the XSM client at IP address 172.17.129.134, and how long this session has been connected to the XSM server (Session 2: Connected since 22:47:07 UTC Mon Jan 8 2001). The output shows that the XSM, VDM, and EDM subsystems, and EDM and VDM history collecting are enabled. XSM configuration privilege level is set at 15, with XSM monitor privilege level set at 1.

This output also shows the active XRDs (and their version) for Session 2:

```
Router# show xsm status
XSM subsystem is Enabled.
```

```
VDM subsystem is Enabled.
EDM subsystem is Enabled.
EDM History is Enabled.
VDM History is Enabled.
XSM privilege configuration level 15.
XSM privilege monitor level 1.
Number of XSM Sessions : 1.
  Session ID = 2.
    XSM Client v0.0(0.0)- @ 172.17.129.134
    Connected since 22:47:07 UTC Mon Jan 8 2001
    List of subscribed xrds:
    0 ) device-about                              v1.0
    1 ) ios-image                                 v1.0
    2 ) if-list                                   v1.0
    3 ) device-health                             v1.0
    4 ) ike-stats                                 v1.0
    5 ) ike                                       v1.0
    6 ) ipsec-topn-tunnels-by-traffic             v1.0
    7 ) ipsec-topn-tunnels-by-duration            v1.0
    8 ) ipsec-stats                               v1.0
    9 ) crypto-maps                               v1.0
    10) ipsec                                     v1.0
```

The table below describes the significant fields shown in the display. (See documention of the **show xsm xrd-list** command for a full description of subscribed XRDs).

Table 21: show xsm status Field Descriptions

Field	Description
XSM privilege configuration level	XSM configuration privilege level.
XSM privilege monitor level	XSM monitor privilege level.
Number of XSM Sessions	Total number of concurrent XSM sessions.
Session ID	Specific XSM session number.
XSM Client	Version and IP address of the XSM client.
Connected since	Start time for each session connection to the XSM server.
List of subscribed xrds	Details XRDs available from the XSM server (see **show xsm xrd-list** command for complete list of XRDs).

Related Commands

Command	Description
clear xsm	Clears XSM client sessions.
show xsm xrd-list	Displays all XRDs for clients subscribed to the XSM server.
xsm	Enables XSM client access to the router.

Command	Description
xsm privilege configuration level	Enables configuration privilege level to subscribe to XRDs.
xsm privilege monitor level	Enables monitor privilege level to subscribe to XRDs.

show xsm xrd-list

To display all XML Request Descriptors (XRDs) for XML Subscription Manager (XSM) clients (such as the VPN Device Manager [VDM]) made available by subscription to the XSM server and to identify the required privilege levels, use the **show xsm xrd-list** command in privileged EXEC mode.

show xsm xrd-list

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(6)E	This command was introduced.
12.2(9)YE	This command was integrated into Cisco IOS Release 12.2(9)YE.
12.2(9)YO1	This command was integrated into Cisco IOS Release 12.2(9)YO1.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to display the XRD version and minimum privilege level and type (configuration or monitor) required to view each XRD.

Examples

The following example shows some active XRDs on the XSM server. The end of each line displays the following:

- XRD version number.
- XRD privilege type (configuration or monitor), indicating the privilege level required.

This example displays all available XRDs because both relevant commands (**xsm edm** and **xsm vdm**) have been configured. However, if one command is not configured, only an abbreviated XRD list will appear.

```
Router# show xsm xrd-list
```

```
List of all available xrds:
0 ) vlan-db                                 v1.0  privilege=configuration
1 ) entity                                  v1.0  privilege=configuration
2 ) ip                                      v1.0  privilege=configuration
3 ) ios-users                               v1.0  privilege=configuration
4 ) device-about                            v1.0  privilege=monitor
5 ) ios-image                               v1.0  privilege=configuration
6 ) if-stats                                v1.0  privilege=monitor
7 ) if-list                                 v1.0  privilege=configuration
8 ) device-health                           v1.0  privilege=monitor
9 ) time                                    v1.0  privilege=monitor
10) access-lists                            v1.0  privilege=configuration
11) ike-topn-tunnels-by-traffic             v1.0  privilege=monitor
12) ike-topn-tunnels-by-errors              v1.0  privilege=monitor
13) ike-topn-tunnels-by-duration            v1.0  privilege=monitor
14) ike-stats                               v1.0  privilege=monitor
15) ike                                     v1.0  privilege=configuration
16) certificate-authorities                 v1.0  privilege=configuration
17) ipsec-topn-tunnels-by-traffic           v1.0  privilege=monitor
18) ipsec-topn-tunnels-by-errors            v1.0  privilege=monitor
19) ipsec-topn-tunnels-by-duration          v1.0  privilege=monitor
20) ipsec-stats                             v1.0  privilege=monitor
21) crypto-maps                             v1.0  privilege=configuration
22) ipsec                                   v1.0  privilege=configuration
23) vdm-history                             v1.0  privilege=configuration
24) gre-tunnels                             v1.0  privilege=monitor
end list.
```

The table below describes (in alphabetical order) typical XRDs shown in the display.

Table 22: show xsm xrd-list Field Descriptions

Field	Descriptions
access-lists	IOS access control list (ACL) configuration.
certificate-authorities	IOS certificate authority (CA) configuration.
crypto-maps	IOS Crypto Map configuration.
device-about	General network device information.
device-health	General network device health statistics.
edm-history	Selected, historical statistics related to general embedded device management. (This field is not shown in the example above.)
entity	Summary of all physical and logical entities within a device.
gre-tunnels	All current GRE tunnels and respective statistics.
if-list	List of all interfaces and their respective IOS configurations.
if-stats	Statistics for all interfaces and their respective IOS configurations.
ike	IOS Internet Key Exchange (IKE) configuration.

Field	Descriptions
ike-stats	Statistics related to IKE.
ike-topn-tunnels-by-duration	Top 10 IKE tunnels by duration (time).
ike-topn-tunnels-by-errors	Top 10 IKE tunnels by errors.
ike-topn-tunnels-by-traffic	Top 10 IKE tunnels by traffic volume.
ios-image	Information about the current running IOS image.
ios-users	Local IOS user configuration.
ip	IOS IP configuration statistics.
ipsec	IOS IPSec configuration.
ipsec-stats	Interface name and IPSec input and output statistics including: number of packets, dropped packets, octets and errors.
ipsec-topn-tunnels-by-duration	Top 10 IPSec tunnels by duration.
ipsec-topn-tunnels-by-errors	Top 10 IPSec tunnels by errors.
ipsec-topn-tunnels-by-traffic	Top 10 IPSec tunnels by traffic.
time	Device's clock reading in UTC.
vdm-history	Selected, historical VPN-related statistics.
vlan-db	VLAN database configuration (switches only).
xsm-session	Status of the current XSM session and related subscriptions. (This field is not shown in the example above.)

Related Commands

Command	Description
clear xsm	Clears XSM client sessions.
show xsm status	Displays information and status about clients subscribed to the XSM server.
xsm	Enables XSM client access to the router.

Command	Description
xsm privilege configuration level	Enables configuration privilege level to subscribe to XRDs.
xsm privilege monitor level	Enables monitor privilege level to subscribe to XRDs.

show zone security

To display zone security information, use the **show zone security**command in user EXEC or privileged EXEC mode.

show zone security [*security-zone-name*]

Syntax Description

security-zone-name	(Optional) The security zone name.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
12.4(24)T	This command was introduced in a release earlier than Cisco IOS Release 12.4(24)T.
Cisco IOS 2.1 XE	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

Use this command to display zone security information.

Examples

The following is sample output from the **show zone security**command. The fields are self-explanatory.

```
Router# show zone security
zone self
Description: System defined zone
```

show zone-pair security

To display the source zone, destination zone, and policy attached to the zone-pair, use the **show zone-pair security** command in privileged EXEC mode. To disable the display, use the **no** form of this command.

show zone-pair security [**source** *source-zone-name*] [**destination** *destination-zone-name*]

no show zone-pair security [**source** *source-zone-name*] [**destination** *destination-zone-name*]

Syntax Description

source *source-zone-name*	(Optional) Name of the source zone.
destination *destination-zone-name*	(Optional) Name of the destination zone.

Command Default

If you do not specify a source or destination zone, the system displays all the zone-pairs for the source, destination, and the associated policy.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(6)T	This command was introduced.

Examples

The following example displays the source zone, destination zone, and policy attached to the zone-pair:

```
Router# show zone-pair security source z1 destination z2
zone-pair name zp
  Source-Zone z1  Destination-Zone z2
  service-policy p1
```

The table below describes the significant fields shown in the display.

Table 23: show zone-pair security Field Descriptions

Field	Description
zone-pair name	Name of the zone-pair.
Source-Zone	Name of the source zone.
Destination-Zone	Name of the destination zone.
service-policy	Name of the service policy.

shutdown (firewall)

To shut down a group manually, use the **shutdown**command in redundancy application group configuration mode. To enable a redundancy group, use the **no** form of this command.

shutdown

no shutdown

Syntax Description

This command has no arguments or keywords.

Command Default

The group is active.

Command Modes

Redundancy application group configuration (config-red-app-grp)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Usage Guidelines

When a group is shut down, it does not participate in the role negotiation. The group remains in the shutdown state until you execute the **no shutdown**command.

Examples

The following example shows how to shut down a group named group1:

```
Router# configure terminal
Router(config)# redundancy
Router(config-red)# application redundancy
Router(config-red-app)# group 1
Router(config-red-app-grp)# shutdown
```

Related Commands

Command	Description
application redundancy	Enters redundancy application configuration mode.
group(firewall)	Enters redundancy application group configuration mode.
name	Configures the redundancy group with a name.
preempt	Enables preemption on the redundancy group.

shutdown (cs-server)

To allow a certificate server to be disabled without removing the configuration, use the **shutdown**command in certificate server configuration mode. To reenable the certificate server, use the **no** form of this command.

shutdown

no shutdown

Syntax Description

This command has no arguments or keywords.

Command Default

no shutdown

Command Modes

Certificate server configuration (cs-server)

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

You must configure the **crypto pki server** command with the name of the certificate server in order to enter certificate server configuration mode and configure this command.

You should issue the **no shutdown** command only after you have completely configured your certificate server.

The **shutdown** command disables the certificate server. If you prefer to disable simple certificate enrollment protocol (SCEP) but still want the certificate server for manual certificate enrollment, use the **no ip http server** command.

Examples

To ensure that the specified URL is working correctly, configure the **database url** command before you issue the **no shutdown** command on the certificate server for the first time. If the URL is broken, you will see output as follows:

```
Router(config)# crypto pki server mycs
Router(cs-server)# database url ftp://myftpserver
Router(cs-server)# no shutdown
% Once you start the server, you can no longer change some of
% the configuration.
Are you sure you want to do this? [yes/no]: yes

Translating "myftpserver"
% Failed to generate CA certificate - 0xFFFFFFFF
% The Certificate Server has been disabled.
```

Related Commands

Command	Description
auto-rollover	Enables the automated CA certificate rollover functionality.
cdp-url	Specifies a CDP to be used in certificates that are issued by the certificate server.
crl (cs-server)	Specifies the CRL PKI CS.
crypto pki server	Enables a CS and enters certificate server configuration mode, or immediately generates shadow CA credentials
database archive	Specifies the CA certificate and CA key archive format--and the password--to encrypt this CA certificate and CA key archive file.
database level	Controls what type of data is stored in the certificate enrollment database.
database url	Specifies the location where database entries for the CS is stored or published.
database username	Specifies the requirement of a username or password to be issued when accessing the primary database location.
default (cs-server)	Resets the value of the CS configuration command to its default.
grant auto rollover	Enables automatic granting of certificate reenrollment requests for a Cisco IOS subordinate CA server or RA mode CA.
grant auto trustpoint	Specifies the CA trustpoint of another vendor from which the Cisco IOS certificate server automatically grants certificate enrollment requests.

Command	Description
grant none	Specifies all certificate requests to be rejected.
grant ra-auto	Specifies that all enrollment requests from an RA be granted automatically.
hash (cs-server)	Specifies the cryptographic hash function the Cisco IOS certificate server uses to sign certificates issued by the CA.
issuer-name	Specifies the DN as the CA issuer name for the CS.
lifetime (cs-server)	Specifies the lifetime of the CA or a certificate.
mode ra	Enters the PKI server into RA certificate server mode.
mode sub-cs	Enters the PKI server into sub-certificate server mode
redundancy (cs-server)	Specifies that the active CS is synchronized to the standby CS.
serial-number (cs-server)	Specifies whether the router serial number should be included in the certificate request.
show (cs-server)	Displays the PKI CS configuration.

single-connection

To enable all TACACS packets to be sent to the same server using a single TCP connection, use the **single-connection**command in TACACS+ server configuration mode. To disable this feature, use the **no** form of this command.

single-connection

no single-connection

Syntax Description

This command has no arguments or keywords.

Command Default

TACACS packets are not sent on a single TCP connection.

Command Modes

TACACS+ server configuration (config-server-tacacs)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.

Usage Guidelines

Use the **single-connection** command to multiplex all TACACS packets to the same server over a single TCP connection.

Examples

The following example shows how to multiplex all TACACS packets over a single TCP connection to the TACACS server:

```
Router (config)# tacacs server server1
Router(config-server-tacacs)# single-connection
```

Related Commands

Command	Description
tacacs server	Configures the TACACS+ server for IPv6 or IPv4 and enters config server tacacs mode.

signature

To specify a signature for which the command-line interface (CLI) user tunings will be changed, use the **signature** command in signature-definition-signature (config-sigdef-sig) configuration mode. To remove the CLI user tunings and revert to the default values, use the **no** version of this command.

signature *signature-id* [*subsignature-id*]

no signature *signature-id* [*subsignature-id*]

Syntax Description

signature-id subsignature-id	Signature number. If a subsignature is not specified, the default is 0. For example, if signature 1105 is specified without a subsignature, the router will interpret the signature as 1105:0.

Command Default

Default signature parameters cannot be changed.

Command Modes

Signature-definition-signature configuration (config-sigdef-sig)

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Use the **signature** command to specify a signature whose CLI user tunings are to be customized. Thereafter, you can begin to specify which signature parameters (user tunings) are to be changed.

Examples

The following example shows how to modify signature 5081/0 to "produce alert" and "reset tcp connection":

```
Router(config)# ip ips signature-definition
Router(config-sigdef-sig)# signature 5081 0
Router(config-sigdef-action)# engine
Router(config-sigdef-action-engine)# event-action produce-alert reset-tcp-connection
Router(config-sigdef-action-engine)# ^Z
Do you want to accept these changes:[confirmm]y
```

Related Commands

Command	Description
ip ips signature-definition	Enters signature-definition-signature configuration mode, which allows you to define a signature for CLI user tunings.

slave (IKEv2 cluster)

To define settings for slave gateways in an Internet Key Exchange Version 2 (IKEv2) cluster, use the **slave** command in IKEv2 cluster configuration mode. To restore the default settings, use the **no** form of this command.

slave {**hello** *milliseconds*| **max-session** *number*| **priority** *number*| **update** *milliseconds*}

no slave {**hello**| **max-session**| **priority**| **update**}

Syntax Description

hello *milliseconds*	Specifies the hello interval, in milliseconds, for a slave gateway. The range is from 100 to 30000. The default is 1000.
max-session *number*	Specifies the maximum number of security associations (SA) allowed on a slave. The range is from 1 to 100000. **Note** This keyword is mandatory.
priority *number*	Specifies the priority of the slave. The range is from 1 to 100. The default is 100.
update *milliseconds*	Specifies the interval, in milliseconds, between two update messages for a slave gateway. The range is from 100 to 60000. The default is 3000.

Command Default

The default slave settings are used.

Command Modes

IKEv2 cluster configuration (config-ikev2-cluster)

Command History

Release	Modification
15.2(4)M	This command was introduced.

Usage Guidelines

You must enable the **crypto ikev2 cluster** command before enabling the **slave** command.

Examples

The following example shows how to set the priority setting to 90 for the IKEv2 slave gateway:

```
Device(config)# crypto ikev2 cluster
Device(config-ikev2-cluster)# slave priority 90
```

Related Commands

Command	Description
crypto ikev2 cluster	Defines an IKEv2 cluster policy in an HSRP cluster.

smart-tunnel list

To configure the smart tunnel list and enable it within a policy group, use the **smart-tunnel list** command in WebVPN context configuration mode or WebVPN group policy configuration mode. To disable the smart tunnel configuration, use the **no** form of this command.

smart-tunnel list *name*

no smart-tunnel list

Syntax Description

name	Smart tunnel list name.

Command Default

No smart tunnel list is created and enabled.

Command Modes

WebVPN context configuration mode (config-webvpn-context) WebVPN group policy configuration mode (config-webvpn-group)

Command History

Release	Modification
15.1(3)T	This command was introduced.

Usage Guidelines

Before a smart tunnel list can be enabled within a group policy, it must be created. Applications that are to be directed to the smart tunnel then must be specified within the list. This list must later be applied to the group policy.

Note To remove a smart tunnel list, first use the **no smart-tunnel list** command in WebVPN group policy configuration mode, and then use the **no smart-tunnel list**command in WebVPN context configuration mode.

Examples

The following example shows how to create a smart tunnel list named "st1" and configure the applications for smart tunneling:

```
Router(config)# webvpn context sslgw
Router(config-webvpn-context)# smart-tunnel list st1
Router(config-webvpn-smart-tunnel)# appl ie ieexplore.exe windows
Router(config-webvpn-smart-tunnel)# appl telnet telnet.exe windows
```

The following example shows how to enable the smart tunnel list "st1" within a group policy:

```
Router(config)# webvpn context sslgw
```

```
Router(config-webvpn-context)# policy group new
Router(config-webvpn-group)# smart-tunnel list st1
```

Related Commands

Command	Description
webvpn context	Configures the SSL VPN context.
app (webvpn)	Configures applications to access smart tunnel.

smartcard-removal-disconnect

To terminate a session on removing the smart card, use the **smarcard-removal-disconnect** command in IKEv2 authorization policy configuration mode. To disable session termination, use the **no** form of this command.

smartcard-removal-disconnect

Syntax Description

This command has no arguments or keywords

Command Default

The session is not terminated.

Command Modes

IKEv2 authorization policy configuration (config-ikev2-author-policy)

Command History

Release	Modification
15.2(1)T	This command was introduced.

Usage Guidelines

Before using this command, you must first configure the **crypto ikev2 authorization policy** command. The parameter set by this command is sent to the client via the nonstandard Cisco unity configuration attribute. This command specifies that the client should terminate the session on removing the smart card.

Examples

The following example show how to configure the smartcard-removal-disconnect command:

```
Router(config)# crypto ikev2 authorization policy policy1
Router(config-ikev2-profile)# smartcard-removal-disconnect
```

Related Commands

Command	Description
crypto ikev2 authorization policy	Specifies an IKEv2 authorization policy.

snmp-server enable traps gdoi

To enable Group Domain of Interpretation (GDOI) Simple Network Management Protocol (SNMP) notifications for Cisco Group Encrypted Transport VPN (GET VPN), use the **snmp-server enable traps gdoi** command in global configuration mode. To disable GDOI SNMP notifications, use the **no** form of this command.

snmp-server enable traps gdoi [*notification-type*]

no snmp-server enable traps gdoi [*notification-type*]

Syntax Description

notification-type	(Optional) Specifies the particular SNMP notifications to be enabled. If you use the command without keywords, all GDOI notifications are enabled. You can specify any combination of the following types in any order: • **gm-incomplete-cfg—**A group member (GM) sent an error notification because of a missing configuration. • **gm-re-register—**A GM began the reregistration process with a key server (KS.) • **gm-registration-complete—**A GM completed registration to a KS. • **gm-rekey-fail—**A GM sent an error notification because it cannot process and install a rekey. • **gm-rekey-rcvd—**A rekey message was received by a GM. • **gm-start-registration—**A GM first sent a registration request to a KS. • **ks-new-registration—**A KS first received a registration request from a GM. • **ks-no-rsa-keys—**An error notification was received from a KS because of missing RSA keys. • **ks-reg-complete—**A GM completed registration to a KS. • **ks-rekey-pushed—**A rekey message was sent by the KS.

Command Default

No GDOI SNMP notifications are enabled.

Command Modes Global configuration (config)

Command History

Release	Modification
15.2(1)T	This command was introduced.
Cisco IOS XE Release 3.8S	This command was integrated into Cisco IOS XE Release 3.8S.

Usage Guidelines This command configures notifications for RFC 3547, *The Group Domain of Interpretation*; it supports only the objects related to the GDOI MIB IETF standard.

The GDOI MIB consists of objects and notifications that include information about GDOI groups, GM and KS peers, and the policies that are created or downloaded. Only "get" operations are supported by the GDOI MIB.

The command configures two kinds of notifications—those generated by the KS and those generated by each GM.

For more information about GDOI MIB support for GET VPN, see the *Cisco Group Encrypted Transport VPN Configuration Guide.*.

For a complete description of the notification types and additional MIB functions, refer to the CISCO-GDOI-MIB.my file.

Examples The following example shows how to enable GDOI MIB notifications for when a GM begins the reregistration process with a KS and when a GM completes registration to a KS:

```
Device(config)# snmp-server enable traps gdoi gm-re-register gm-registration-complete
```

The following example shows how to enable the GDOI MIB notification for when a GM sends an error notification because it cannot process and install a rekey:

```
Device(config)# snmp-server enable traps gdoi gm-rekey-fail
```

The following example shows how to enable GDOI MIB notifications for when a KS first receives a registration request from a GM and a group member completes registration to the KS:

```
Device(config)# snmp-server enable traps gdoi ks-new-registration ks-reg-complete
```

The following example shows how to enable the GDOI MIB notification for when an error is received from the KS because of missing RSA keys:

```
Device(config)# snmp-server enable traps gdoi ks-no-rsa-keys
```

Related Commands

Command	Description
snmp-server community	Specifies the community access string to define the relationship between the SNMP manager and the SNMP agent to permit access to SNMP.
snmp-server host	Specifies the recipient (host) of an SNMP notification operation.

snmp-server enable traps ipsec

To enable the router to send IP Security (IPSec) Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps ipsec**command in global configuration mode. To disable IPSec SNMP notifications, use the **no**form of this command.

snmp-server enable traps ipsec [**cryptomap** [**add**| **delete**| **attach**| **detach**]| **tunnel** [**start**| **stop**]| **too-many-sas**]

no snmp-server enable traps ipsec [**cryptomap** [**add**| **delete**| **attach**| **detach**]| **tunnel** [**start**| **stop**]| **too-many-sas**]

Syntax Description

cryptomap add	(Optional) Notifications for cipsCryptomapAdded { cipsMIBNotifications 3 } events are generated, as defined in the CISCO-IPSEC-MIB. These notifications are generated when a new cryptomap is added to the specified cryptomap set.
cryptomap delete	(Optional) Notifications for cipsCryptomapDeleted { cipsMIBNotifications 4 } events are generated, as defined in the CISCO-IPSEC-MIB. These notifications are generated when a cryptomap is removed from the specified cryptomap set.
cryptomap attach	(Optional) Notifications for cipsCryptomapSetAttached { cipsMIBNotifications 5 } events are generated, as defined in the CISCO-IPSEC-MIB. These notifications are generated when a cryptomap set is attached to an active interface of the managed entity.
cryptomap detach	(Optional) Notifications for cipsCryptomapSetDetached { cipsMIBNotifications 6 } events are generated, as defined in the CISCO-IPSEC-MIB. These notifications are generated when a cryptomap set is detached from an interface to which it was previously bound.
tunnel start	(Optional) Notifications for cipSecTunnelStart { cipSecMIBNotifications 7 } events are generated, as defined in the CISCO-IPSEC-FLOW-MONITOR-MIB. These notifications are generated when an IPsec Phase-2 Tunnel becomes active.

tunnel stop	(Optional) Notifications for cipSecTunnelStop { cipSecMIBNotifications 8 } events are generated, as defined in the CISCO-IPSEC-FLOW-MONITOR-MIB. These notifications are generated when an IPsec Phase-2 Tunnel becomes inactive.
too-many-sas	(Optional) Notifications for cipsTooManySAs { cipsMIBNotifications 7 } events are generated, as defined in the CISCO-IPSEC-MIB.my. These notifications are generated when an attempt to make a new security association (SA) is made but there is insufficient memory on the device.

Command Default

SNMP notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.1(11b)E	This command was integrated into Cisco IOS Release 12.1(11b)E.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests.

A cryptomap is a table that maps an IPSec Phase-2 tunnel to the corresponding IPSec Policy element.

For a complete description of the notification types and additional MIB functions, refer to the CISCO-IP-SEC.my and CISCO-IPSEC-FLOW-MONITOR-MIB.my files, available on Cisco.com through:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

The **snmp-server enable traps ipsec** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send SNMP notifications, you must configure at least one **snmp-server host** command.

Examples

In the following example, the router is configured to send IPSec MIB inform notifications to the host nms.cisco.com using the community string named "public":

```
snmp-server enable traps ipsec
snmp-server host nms.cisco.com informs public ipsec
```

Related Commands

Command	Description
snmp-server enable traps isakmps	Controls the sending of (ISAKMP) SNMP notifications
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server trap-source	Specifies the interface that an SNMP trap should originate from.

snmp-server enable traps isakmp

To enable the router to send IP Security (IPSec) Internet Security Association and Key Exchange Protocol (ISAKMP) Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps isakmp**command in global configuration mode. To disable ISAKMP IPSec SNMP notifications, use the **no**form of this command.

snmp-server enable traps isakmp [**policy** {**add**| **delete**}| **tunnel** {**start**| **stop**}]

no snmp-server enable traps isakmp [**policy** {**add**| **delete**}| **tunnel** {**start**| **stop**}]

Syntax Description

policy add	(Optional) Notifcations for cipsIsakmpPolicyAdded { cipsMIBNotifications 1 } events are generated, as defined in the CISCO-IPSEC-MIB. These notifications are generated when a new ISAKMP policy element is defined on the managed entity. The context of the event includes the updated number of ISAKMP policy elements currently available.
policy delete	(Optional) Notifcations for cipsIsakmpPolicyDeleted { cipsMIBNotifications 2 } events are generated, as defined in the CISCO-IPSEC-MIB. These notifications are generated when an existing ISAKMP policy element is deleted on the managed entity. The context of the event includes the updated number of ISAKMP policy elements currently available.
tunnel start	(Optional) Notifications for cikeTunnelStart { cipSecMIBNotifications 1 } events are generated, as defined by in the CISCO-IPSEC-FLOW-MONITOR-MIB.my. These notifications are generated when an IPsec Phase-1 IKE Tunnel becomes active.
tunnel stop	(Optional) Notifications for cikeTunnelStop { cipSecMIBNotifications 2 } events are generated, as defined by in the CISCO-IPSEC-FLOW-MONITOR-MIB.my. These notifications are generated when an IPsec Phase-1 IKE Tunnel becomes inactive.

Command Default

SNMP notifications are disabled by default.

If no keywords are specified, all available ISAKMP traps are enabled (or disabled if the **no** form is used).

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.1(11b)E	This command was integrated into Cisco IOS Release 12.1(11b)E
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both ISAKMP trap and inform requests.

For a complete description of these notifications and additional MIB functions, refer to the CISCO-IPSEC-MIB.myand CISCO-IPSEC-FLOW-MONITOR-MIB.my files, available on Cisco.com through:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

The **snmp-server enable traps isakmp** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send SNMP notifications, you must configure at least one **snmp-server host** command.

Examples

In the following example, the router is configured to send IPSec MIB inform notifications to the host nms.cisco.com using the community string named "public":

```
snmp-server enable traps isakmp
snmp-server host nms.cisco.com informs public ipsec
```

Related Commands

Command	Description
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server trap-source	Specifies the interface that an SNMP trap should originate from.

snmp-server enable traps nhrp

To enable Simple Network Management Protocol (SNMP) notifications for the Next Hop Resolution Protocol (NHRP), use the **snmp-server enable traps nhrp** command in global configuration mode. To disable SNMP NHRP notifications, use the **no** form of this command.

snmp-server enable traps nhrp [**nhc** [**down**| **up**]| **nhp** [**down**| **up**]| **nhs** [**down**| **up**]| **quota-exceeded**]

no snmp-server enable traps nhrp [**nhc** [**down**| **up**]| **nhp** [**down**| **up**]| **nhs** [**down**| **up**]| **quota-exceeded**]

Syntax Description

nhc	(Optional) Enables Next Hop Client (NHC) notifications.
down	(Optional) Enables notifications for when the client, peer, or server interface is declared 'down'.
up	(Optional) Enables notifications for when the client, peer, or server interface is declared 'up'.
nhp	(Optional) Enables Next Hop Peer (NHP) notifications.
nhs	(Optional) Enables Next Hop Server (NHS) notifications.
quota-exceeded	(Optional) Enables notifications for when the rate limit set on NHRP packets is exceeded on the interface.

Command Default

No notifications (traps) are enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

By default all notifications (traps) are disabled. You must explicitly enable any notifications that you need in your system. After you enable traps in your system, you can use the **snmp-server host traps** command to control which traps are sent to a particular trap receiver.

The **snmp-server host traps nhrp** command enables the default NHRP traps only (it does not enable all NHRP traps). The default traps include the NHS, NHC, and quota-exceeded traps.

Examples

The following example shows how to enable the default NHRP traps, and how to send these NHRP traps to the notification receiver with the IP address 192.40.3.130 using the community string public:

```
Router(config)# snmp-server enable traps nhrp
Router(config)# snmp-server host 192.40.3.130 traps version 2c public nhrp
```

The following example shows how to disable NHC traps and enable rate limit traps:

```
Router(config)# no snmp-server enable traps nhrp nhc
Router(config)# snmp-server enable traps nhrp quota-exceeded
```

Related Commands

Command	Description
debug snmp mib nhrp	Displays messages about the SNMP NHRP MIB.
snmp-server host	Specifies the recipient of an SNMP notification operation.

snmp trap ip verify drop-rate

To configure the router to send a Simple Network Management Protocol (SNMP) notification when the Unicast Reverse Path Forwarding (RPF) drop rate exceeds the configured threshold, use the **snmp trap ip verify drop-rate**command in interface configuration mode. To disable SNMP notification, use the **no** form of this command.

snmp trap ip verify drop-rate

no snmp trap ip verify drop-rate

Syntax Description

This command has no arguments or keywords.

Command Default

No SNMP notifications are sent.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(31)SB2	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
12.2(33)SXI2	This command was integrated into Cisco IOS Release 12.2(33)SXI2.

Usage Guidelines

This command enables cipUrpfIfDropRateNotify notification. This notification is sent when the Unicast RPF drop rate exceeds the threshold.

Examples

The following example shows how to configure SNMP notification for the Unicast RPF drop rate on Ethernet interface 3/0:

```
Router> enable
Router# configure terminal
Router(config)# interface ethernet 3/0
Router(config-if)# snmp trap ip verify drop-rate
```

Related Commands

Command	Description
ip verify drop-rate compute window	Configures the interval of time over which the Unicast RPF drop count used in the drop rate computation is collected.

Command	Description
ip verify unicast notification threshold	Configures the Unicast RPF drop count threshold which, when exceeded, triggers a notification.

source

To sequentially number the source address, use the **source** command in IKEv2 FlexVPN client profile configuration mode. To remove the sequence, use the **no** form of this command.

source *sequence interface* **track** *track-number*

no source *sequence*

Syntax Description

sequence	Assigns a sequence number.
interface	Interface type and number.
track *track-number*	Tracks the source address with a track number.

Command Default

The track status is always up.

Command Modes

IKEv2 FlexVPN client profile configuration (config-ikev2-flexvpn)

Command History

Release	Modification
15.2(1)T	This command was introduced.
Cisco IOS XE Release 3.7S	This command was integrated into Cisco IOS XE Release 3.7S.

Usage Guidelines

Before you enable this command, you must configure the **crypto ikev2 client flexvpn** command.

The source address is the one with the lowest sequence number for which track object is in the UP state only if the source IP address is available in the tunnel VRF of the tunnel interface. If a session is UP for a source, the source is said to be a "Current active source".

Note Any changes to this command terminates the active session.

Examples

The following example shows how to define a static peer:

```
Router(config)# crypto ikev2 client flexvpn client1
Router(config-ikev2-flexvpn)# source 1 Ethernet 0/1 track 11
```

Related Commands

Command	Description
crypto ikev2 client flexvpn	Defines an IKEv2 FlexVPN client profile.

source interface

To specify the address of an interface to be used as the source address for all outgoing TCP connections associated with a trustpoint, use the **source interface** command in ca-trustpoint configuration mode. To disable the interface that was specified, use the **no** form of this command.

source interface *interface-name*

no source interface *interface-name*

Syntax Description

interface-name	Interface address to be used as the source address for all outgoing TCP connections associated with a trustpoint.

Command Default

If this command is not specified, the address of the outgoing interface is used.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.

Usage Guidelines

This command must be used following the **crypto ca trustpoint** command. If this command is used and the address of the outgoing interface is specified, the router uses the specified address (or address of the specified interface) as the source address for any datagrams that are sent to the certification authority (CA) server or Lightweight Directory Access Protocol (LDAP) server during authentication, enrollment, and if appropriate, when obtaining certificate revocation lists (CRLs).

Examples

In the following example, the router is located in a branch office. The router uses IP Security (IPSec) to communicate with the main office. Ethernet 1 is the "outside" interface that connects to the Internet Service Provider (ISP). Ethernet 0 is the interface connected to the LAN of the branch office. To access the CA server located in the main office the router needs to send its IP datagrams out interface Ethernet 1 (address 10.2.2.205) using the IPSec tunnel. Address 10.2.2.205 is assigned by the ISP. Address 10.2.2.205 is not a part of the branch office or main office.

The CA cannot access any address outside the company because of a firewall. The CA sees a message coming from 10.2.2.205 and cannot respond (that is, it does not know that the router is located in a branch office at address 10.1.1.1, which it is able to reach).

Adding the **source interface** command tells the router to use address 10.1.1.1 as the source address of the IP datagram that it sends to the CA. The CA is able to respond to 10.1.1.1.

This scenario is configured using the **source interface** command and the interface addresses as described above.

```
crypto ca trustpoint ms-ca
 enrollment url http://yourname:80/certsrv/mscep/mscep.dll
 source interface ethernet0
!
interface ethernet 0
 description inside interface
 ip address 10.1.1.1 255.255.255.0
!
interface ethernet 1
 description outside interface
 ip address 10.2.2.205 255.255.255.0
 crypto map main-office
```

Related Commands

Command	Description
crypto ca trustpoint	Declares the CA that your router should use.

source interface (ca-trustpool)

To specify the source interface to be used for certificate revocation list (CRL) retrieval, online certificate status protocol (OCSP) status, or the downloading of a certificate authority (CA) certificate bundle for the public key infrastructure (PKI) trustpool, use the **source interface** command in ca-trustpool configuration mode. To disable the interface that was specified, use the **no** form of this command.

source interface *name number*

no source interface *name number*

Syntax Description

interface-name	Interface type used as the source address for the PKI trustpool.
interface	Interface number or slot and port of this interface.

Command Default

No source interface is specified.

Command Modes

Ca-trustpool configuration (ca-trustpool)

Command History

Release	Modification
15.2(2)T	This command was introduced.
15.1(1)SY	This command was integrated into Cisco IOS 15.1(1)SY.

Usage Guidelines

Before you can configure this command, you must enable the **crypto pki trustpool policy** command, which enters ca-trustpool configuration mode.

Examples

```
Router(config)# crypto pki trustpool policy
Router(ca-trustpool)# source interface tunnel 1
```

Related Commands

Command	Description
cabundle url	Configures the URL from which the PKI trustpool CA bundle is downloaded.

Command	Description
chain-validation	Enables chain validation from the peer's certificate to the root CA certificate in the PKI trustpool.
crl	Specifes the CRL query and cache options for the PKI trustpool.
crypto pki trustpool import	Manually imports (downloads) the CA certificate bundle into the PKI trustpool to update or replace the existing CA bundle.
crypto pki trustpool policy	Configures PKI trustpool policy parameters.
default	Resets the value of a ca-trustpool configuration command to its default.
match	Enables the use of certificate maps for the PKI trustpool.
ocsp	Specifies OCSP settings for the PKI trustpool.
revocation-check	Disables revocation checking when the PKI trustpool policy is being used.
show	Displays the PKI trustpool policy of the router in ca-trustpool configuration mode.
show crypto pki trustpool	Displays the PKI trustpool certificates of the router and optionally shows the PKI trustpool policy.
source interface	Specifies the source interface to be used for CRL retrieval, OCSP status, or the downloading of a CA certificate bundle for the PKI trustpool.
storage	Specifies a file system location where PKI trustpool certificates are stored on the router.

Command	Description
vrf	Specifies the VRF instance to be used for CRL retrieval.

source interface (Diameter peer)

To configure the interface to be used for the Diameter peer connection, use the **source interface** command in Diameter peer configuration mode. To disable the interface configuration, use the **no** form of this command.

source interface interface

no source interface interface

Syntax Description

interface	Source address and port that initiate the TCP connection to the peer.

Command Default

No source interface is defined.

Command Modes

Diameter peer configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

The Diameter client uses the configured source address and port to initiate a TCP connection to the Diameter peer.

Examples

The following example shows how to configure a source address and port on the Diameter client:

```
Router (config-dia-peer)# source interface
 interface_01
```

Related Commands

Command	Description
diameter peer	Configures a Diameter peer and enters Diameter peer configuration submode.
show diameter peer	Displays the Diameter peer configuration.

source-interface (URL parameter-map)

To specify the interface whose IP address will be used as the source IP address while making a TCP connection to the URL filter server, use the **source-interface** command in URL parameter-map configuration mode. To stop using the IP address of the specified interface, use the **no** form of this command.

source-interface *interface-name*

no source-interface *interface-name*

Syntax Description

interface-name	Name of the interface.

Command Default

None

Command Modes

URL parameter-map configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

When you are creating or modifying a URL parameter map, you can enter the **source-interface** subcommand after you enter the **parameter-map type urlfilter** command.

Examples

The following example specifies that the IP address of Ethernet0 will be used as the source IP address while making a TCP connection to the URL filter server:

```
parameter-map type urlfilter u1
 source-interface ethernet0
```

Related Commands

Command	Description
parameter-map type urlfilter	Creates or modifies a parameter map for URL filtering parameters

source (parameter-map)

To configure the source for content scan redirection, use the **source** command in parameter-map type inspect configuration mode. To disable the source for content scan redirection, use the **no** form of this command.

source {**address ipv4** *address* | **interface** *type number*}

no source address ipv4 *address*

Syntax Description

address	Specifies the source address.
ipv4 *address*	Specifies the IPv4 address of the source.
interface	Specifies the interface.
type	Interface type. For more information, use the question mark (?) online help function.
number	Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.

Command Default

A source for content scan redirection is not configured.

Command Modes

Parameter-map type inspect configuration (config-profile)

Command History

Release	Modification
15.2(1)T1	This command was introduced.

Usage Guidelines

The **source** command configures an interface or an IP address as the source from which packets to ScanSafe will originate from the router. The IP address that is configured in this command must be the IP addresses that is associated with the interface on which **content-scan out** command is configured.

Examples

The following example shows how to configure a source for content scan redirection:

```
Router(config)# parameter-map type content-scan global
Router(config-profile)# source address ipv4 10.1.1.1
```

Related Commands

Command	Description
content-scan out	Enables content scanning on an egress interface.
parameter-map type inspect global	Configures a global content-scan parameter map and enters parameter-map type inspect configuration mode.

split-dns

To specify a domain name that must be tunneled or resolved to the private network, use the **split-dns** command in Internet Security Association Key Management Protocol (ISAKMP) group configuration mode or IKEv2 authorization policy configuration mode. To remove a domain name, use the **no** form of this command.

split-dns *domain-name*

no split-dns *domain-name*

Syntax Description

domain-name	Name of the Domain Name System (DNS) domain that must be tunneled or resolved to the private network.

Command Default

All domain names are resolved via the public DNS server.

Command Modes

ISAKMP group configuration (config-isakmp-group)

IKEv2 authorization policy configuration (config-ikev2-author-policy)

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware.

Usage Guidelines

If you configure the **split-dns** command, the split-dns attribute will be added to the policy group. The attribute will include the list of domain names that you configured. All other names will be resolved via the public DNS server.

You must enable the **crypto isakmp client configuration group** or **crypto ikev2 authorization policy** command, which specifies group policy information that needs to be defined or changed, before enabling the **split-dns** command.

Note If you have to configure more than one domain name, you have to add a **split-dns** command line for each.

Examples

The following example shows that the domain names "green.com" and "acme.org" will be added to the policy group:

```
Router (config)# crypto isakmp client configuration group cisco
Router (config-isakmp-group)# key cisco
Router (config-isakmp-group)# dns 10.2.2.2 10.2.2.3
Router (config-isakmp-group)# wins 10.6.6.6
Router (config-isakmp-group)# domain cisco.com
Router (config-isakmp-group)# pool green
Router (config-isakmp-group)# acl 199
Router (config-isakmp-group)# split-dns green.com
Router (config-isakmp-group)# split-dns acme.org
```

Related Commands

Command	Description
acl	Configures split tunneling.
crypto ikev2 authorization policy	Specifies an IKEv2 authorization policy.
crypto isakmp client configuration group	Specifies group policy information that needs to be defined or changed.

ssh

To start an encrypted session with a remote networking device, use the **ssh** command in user EXEC or privileged EXEC mode.

ssh [**-v** {**1**| **2**}| **-c** {**aes128-ctr**| **aes192-ctr**| **aes256-ctr**| **aes128-cbc**| **3des-cbc**| **aes192-cbc**| **aes256-cbc**}| **-l** *user-id*| **-l** *user-id*:*vrf-name number ip-address ip-address*| **-l** *user-id*:*rotary number ip-address*| **-m** {**hmac-md5**| **hmac-md5-96**| **hmac-sha1**| **hmac-sha1-96**}| **-o numberofpasswordprompts** *n* {**hmac-md5**| **hmac-md5-96**| **hmac-sha1**| **hmac-sha1-96**}| **-p** *port-num*] {*ip-addr* |*hostname* [**command**| **-vrf**]

Syntax Description

-v	(Optional) Specifies the version of Secure Shell (SSH) to use to connect to the server. • **1** --Connects using SSH Version 1. • **2** --Connects using SSH Version 2.
-c {aes128-ctr | aes192-ctr | aes256-ctr | aes128-cbc | 3des-cbc | aes192-cbc | aes256-cbc}	(Optional) Specifies the crypto algorithms Data Encryption Standard (DES), Triple DES (3DES), or Advanced Encryption Standard (AES) to use for encrypting data. AES algorithms are **aes128-ctr**, **aes192-ctr**, **aes256-ctr**, **aes128-cbc**, **aes192-cbc**, and **aes256-cbc**. • To use SSH Version 1, you must have an encryption image running on the device. Cisco software images that include encryption have the designators “k8” (DES) or “k9” (3DES). • SSH Version 2 supports only the following crypto algorithms: **aes128-ctr**, **aes192-ctr**, **aes256-ctr**, **aes128-cbc**, **aes192-cbc**, and **aes256-cbc**, and **3des-cbc**. SSH Version 2 is supported only in 3DES images. • If you do not specify the **-c** keyword, during negotiation the remote networking device sends all the supported crypto algorithms. • If you configure the **-c** keyword and the server does not support the argument that you have shown (**des**, **3des**,**aes128-ctr**, **aes192-ctr**, **aes256-ctr**, **aes128-cbc**, **aes192-cbc**, or **aes256-cbc**), the remote networking device closes the connection.

-l *user-id*	(Optional) Specifies the user ID to use when logging in on the remote networking device running the SSH server. If no user ID is specified, the default is the current user ID.
-l *user-id* **:** *vrf-namenumber ip-address*	(Optional) Specifies the user ID when configuring reverse SSH by including port information in the *user-id* field. • **:** --Signifies that a VRF name, number, and terminal IP address will follow the user ID. • *vrf-name* --User-specific VRF. • *number* --Terminal or auxiliary line number. • *ip-address* --IP address of the terminal server. **Note** The *user-id* argument and **:** *number ip-address* delimiter and arguments must be used if you are configuring reverse SSH by including port information in the *user-id* field (a method that is easier than the longer method of listing each terminal or auxiliary line on a separate command configuration line).The VRF name allows SSH to establish sessions with hosts whose addresses are in a VRF instance.
-l *user-id* **:rotary** *number ip-address*	(Optional) Specifies that the terminal lines are to be grouped under the rotary group for reverse SSH. • **:rotary** --Signifies that a rotary group number and terminal IP address will follow. • *number* --Terminal or auxiliary line number. • *ip-address* --IP address of the terminal server. **Note** The *user-id* argument and the **:rotary** *number ip-address* delimiter and arguments must be used if you are configuring reverse SSH by including rotary information in the *user-id* field (a process that is easier than the longer process of listing each terminal or auxiliary line on a separate command configuration line).

-m {**hmac-md5** | **hmac-md5-96** | **hmac-sha1** | **hmac-sha1-96**}	(Optional) Specifies a Hashed Message Authentication Code (HMAC) algorithm. • SSH Version 1 does not support HMACs. • If you do not specify the **-m** keyword, the remote device sends all the supported HMAC algorithms during negotiation. If you specify the **-m** keyword and the server does not support the algorithm that you have shown (**hmac-md5**, **hmac-md5-96**, **hmac-sha1**, and **hmac-sha1-96**), the remote device closes the connection.
-o numberofpasswordprompts *n*	(Optional) Specifies the number of password prompts that the software generates before ending the session. The SSH server may also apply a limit to the number of attempts. If the limit set by the server is less than the value specified by the **-o numberofpasswordprompts** keyword, the limit set by the server takes precedence. The default is 3 attempts, which is also the Cisco IOS SSH server default. The range of values is from 1 to 5.
-p *port-num*	(Optional) Indicates the desired port number for the remote host. The default port number is 22.
ip-addr | *hostname*	Specifies the IPv4 or IPv6 address or hostname of the remote networking device.
command	(Optional) Specifies the Cisco IOS command that you want to run on the remote networking device. If the remote host is not running Cisco IOS software, this may be any command recognized by the remote host. If the command includes spaces, you must enclose the command in quotation marks.
-vrf	(Optional) Adds VRF awareness to SSH client-side functionality. The VRF instance name in the client is provided with the IP address to look up the correct routing table and establish a connection.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.2(8)T	This command was modified. Support for IPv6 addresses was added.
12.0(21)ST	This command was modified. IPv6 address support was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was modified. IPv6 address support was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was modified. IPv6 address support was integrated into Cisco IOS Release 12.2(14)S.
12.2(17a)SX	This command was integrated into Cisco IOS Release 12.2(17a)SX.
12.3(7)T	This command was modified to include Secure Shell Version 2 support. The **-c** keyword was expanded to include support for the following cryptic algorithms: aes128-cbc, aes192-cbc, and aes256-cbc. The **-m** keyword was added, with the following algorithms: hmac-md5, hmac-md5-96, hmac-sha1, and hmac-sha1-96. The **-v**keyword and **1** and **2** arguments were added.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.3(11)T	The **-l** *userid***:***number ip-address and* **-l** *userid***:rotary** *number ip-address* keyword and argument options were added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.3(7)JA	This command was integrated into Cisco IOS Release 12.3(7)JA.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	The**-l** *userid***:***vrfname number ip-address* keyword and argument options were added
Cisco IOS XE Release 2.4	This command was integrated into Cisco IOS XE Release 2.4.
15.3(2)S	This command was modified. SSH version 2 supports counter-based AES encryption for 128-, 192-, and 256-bit key length.
Cisco IOS XE Release 3.9S	This command was modified. SSH version 2 supports counter-based AES encryption for 128-, 192-, and 256-bit key length.

Release	Modification
15.2(2)SA2	This command was implemented on the Cisco ME 2600X Series Ethernet Access Switches.

Usage Guidelines

The **ssh** command enables a Cisco device to make a secure, encrypted connection to another Cisco device running an SSH Version 1 or Version 2 server. This connection provides functionality that is similar to that of an outbound Telnet connection except that the connection is encrypted. With authentication and encryption, the SSH client allows for a secure communication over an insecure network.

Note SSH Version 1 is supported on DES (56-bit) and 3DES (168-bit) data encryption software images only. In DES software images, DES is the only encryption algorithm available. In 3DES software images, both DES and 3DES encryption algorithms are available.

- SSH Version 2 supports only the following crypto algorithms: aes128-ctr, aes192-ctr, aes256-ctr, aes128-cbc, aes192-cbc, and aes256-cbc. SSH Version 2 is supported only in 3DES images.
- SSH Version 1 does not support HMAC algorithms.

Examples

The following example illustrates the initiation of a secure session between the local device and the remote host HQhost to run the **show users** command. The result of the **show users** command is a list of valid users who are logged in to HQhost. The remote host will prompt for the adminHQ password to authenticate the user adminHQ. If the authentication step is successful, the remote host will return the result of the **show users** command to the local device and will then close the session.

```
Device# ssh -l adminHQ HQhost "show users"
```

The following example illustrates the initiation of a secure session between the local device and the edge device HQedge to run the **show ip route** command. In this example, the edge device prompts for the adminHQ password to authenticate the user. If the authentication step is successful, the edge device will return the result of the **show ip route** command to the local device.

```
Device#ssh -l adminHQ HQedge "show ip route"
```

The following example shows the SSH client using 3DES to initiate a secure remote command connection with the HQedge device. The SSH server running on HQedge authenticates the session for the admin7 user on the HQedge device using standard authentication methods. The HQedge device must have SSH enabled for authentication to work.

```
Device# ssh -l admin7 -c 3des -o numberofpasswordprompts 5 HQedge
```

The following example shows a secure session between the local device and a remote IPv6 device with the address 2001:DB8:0000:FFFF:FFFF:FFFF:FFFF:FFFF to run the **show running-config** command. In this example, the remote IPv6 device prompts for the adminHQ password to authenticate the user. If the authentication step is successful, the remote IPv6 device will return the result of the **show running-config** command to the local device and will then close the session.

```
Device# ssh -l adminHQ 2001:DB8:0000:FFFF:FFFF:FFFF:FFFF:FFFF "show running-config"
```

The following example shows an SSH Version 2 session using the crypto algorithm aes256-ctr and an HMAC of hmac-sha1-96. The user ID is user2 and the IP address is 10.76.82.24.

```
Device# ssh -v 2 -c aes256-ctr -m hmac-sha1-96 -l user2 10.76.82.24
```

The following example shows how to configure reverse SSH on the SSH client:

```
Device# ssh -l lab:1 device.example.com
```

The following command shows how to connect reverse SSH to the first free line in the rotary group:

```
Device# ssh -l lab:rotary1 device.example.com
```

Related Commands

Command	Description
ip ssh	Configures SSH server control parameters on the device.
show ip route	Displays the contents of the routing table.
show ip ssh	Displays the version and configuration data for SSH.
show running-config	Displays the contents of the running configuration file.
show ssh	Displays the status of SSH server connections.
show users	Displays information about the active lines on a device.

ssid (local RADIUS server group)

To assign up to 20 service set identifiers (SSIDs) to a user group, use the **ssid**command in local RADIUS server group configuration mode. To instruct the access point (AP) to not check if the client has come in on a list of specified SSIDs, use the **no** form of this command.

ssid *ssid-number*

no ssid *ssid-number*

Syntax Description

ssid-number	SSID number of user group members.

Command Default

No default behavior or values

Command Modes

Local RADIUS server group configuration

Command History

Release	Modification
12.2(11)JA	This command was introduced on Cisco Aironet Access Point 1100 and Cisco Aironet Access Point 1200.
12.3(11)T	This command was implemented on the following platforms: Cisco 2600XM, Cisco 2691, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3700, and Cisco 3800 series routers.

Usage Guidelines

You can enter up to 20 SSIDs to limit users to those SSIDs.

Examples

The following example shows that the SSID "green" has been added to the local user group:

```
ssid green
```

Related Commands

Command	Description
block count	Configures the parameters for locking out members of a group to help protect against unauthorized attacks.
clear radius local-server	Clears the statistics display or unblocks a user.
debug radius local-server	Displays the debug information for the local server.

Command	Description
group	Enters user group configuration mode and configures shared setting for a user group.
nas	Adds an access point or router to the list of devices that use the local authentication server.
radius-server host	Specifies the remote RADIUS server host.
radius-server local	Enables the access point or router to be a local authentication server and enters into configuration mode for the authenticator.
reauthentication time	Specifies the time (in seconds) after which access points or wireless-aware routers must reauthenticate the members of a group.
show radius local-server statistics	Displays statistics for a local network access server.
user	Authorizes a user to authenticate using the local authentication server.
vlan	Specifies a VLAN to be used by members of a user group.

ssl encryption

To specify the encryption algorithm that the Secure Sockets Layer (SSL) protocol uses for SSL Virtual Private Network (SSL VPN) connections, use the **ssl encryption**command in webvpn gateway configuration mode. To remove an algorithm from the SSL VPN gateway, use the **no** form of this command.

ssl encryption [3des-sha1] [aes-sha1] [rc4-md5]

no ssl encryption

Syntax Description

3des-sha1	(Optional) Configures the 3 DES-SHA1 encryption algorithm.
aes-sha1	(Optional) Configures the AES-SHA1 encryption algorithm.
rc4-md5	(Optional) Configures the RC4-MD5 encryption algorithm.

Command Default

All algorithms are available in the order shown above.

Command Modes

Webvpn gateway configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

The SSL VPN provides remote-access connectivity from almost any Internet-enabled location using only a Web browser and its native SSL encryption. Configuring this command allows you to restrict the encryption algorithms that SSL uses in Cisco IOS software. The ordering of the algorithms specifies the preference. If you specify this command after you have specified an algorithm, the previous setting is overridden.

Examples

The following example configures the gateway to use, in order, the 3DES-SHA1, AES-SHA1, or RC4-MD5 encryption algorithms for SSL connections:

```
Router(config)# webvpn gateway SSL_GATEWAY

Router(config-webvpn-gateway)#
ssl encryption rc4-md5

Router(config-webvpn-gateway)#
```

Related Commands

Command	Description
webvpn gateway	Defines a SSL VPN gateway and enters webvpn gateway configuration mode.

ssl-proxy module allowed-vlan

To add the VLANs allowed over the trunk to the Secure Socket Layer (SSL) Services Module, enter the **ssl-proxy module allowed-vlan** command in global configuration mode. To remove the SSL Services Module from the specified VLAN, use the **no** form of this command.

ssl-proxy module *mod* **allowed-vlan** *vlan-id*

no ssl-proxy module *mod* **allowed-vlan** *vlan-id*

Syntax Description

mod	Module number.
vlan-id	VLAN number; valid values are from 1 to 4094.

Command Default

This command has no default settings.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXD	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is supported on Cisco 7600 series routers that are configured with a Wireless LAN Services Module (WLSM) only.

One of the allowed VLANs must be the administrative VLAN.

To verify the configuration, enter the **show spanning-tree vlan** command.

To display the spanning-tree state for the specified VLAN, enter the **show ssl-proxy module state** command.

Examples

This example shows how to add an SSL Services Module installed in slot 6 to a specific VLAN:

```
Router (config)# ssl-proxy module 6 allowed-vlan 100
Router (config)#
```

This example shows how to remove the SSL Services Module from the specified VLAN:

```
Router (config)# no ssl-proxy module 6 allowed-vlan 100
Router (config)#
```

Related Commands

Command	Description
show ssl-proxy module state	Displays the spanning-tree state for the specified VLAN.

ssl truspoint

To configure the certificate trustpoint on a SSL VPN gateway, use the **ssl trustpoint**command in webvpn gateway configuration mode. To remove the trustpoint association, use the **no** form of this command.

ssl trustpoint *name*

no ssl trustpoint

Syntax Description

name	Name of the trust point.

Command Default

This command has no default behavior or values.

Command Modes

SSLVPN gateway configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

You can configure a persistent self-signed certificate or an external CA server to generate a valid trustpoint.

Examples

The following example configures a trustpoint named CA_CERT:

```
Router(config)#
webvpn gateway SSL_GATEWAY

Router(config-webvpn-gateway)#
ssl trustpoint CA_CERT
```

Related Commands

Command	Description
webvpn gateway	Defines a SSL VPN gateway and enters webvpn gateway configuration mode.

sso-server

To create a Single SignOn (SSO) server name under a Secure Sockets Layer Virtual Private Network (SSL VPN) context and to enter webvpn sso server configuration mode--and to attach an SSO server to a policy group--use the **sso-server** command in webvpn sso server configuration and group policy configuration modes, respectively. To remove an SSO server name, use the **no** form of this command.

sso-server *name*

no sso-server *name*

Syntax Description

name	Name of the SSO server.

Command Default

A SSO server is not created or attached to a policy group.

Command Modes

Webvpn sso server configuration Group policy configuration

Command Modes

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

The SSO server name is configured under the SSL VPN context in webvpn context configuration mode. All SSO server-related parameters, such as web agent URL and policy server secret key, are configured under the SSO server name. The SSO server name is attached to the policy group in webvpn group policy configuration mode.

Examples

The following example shows that the SSO server "test-sso-server" is created under the SSL VPN context and attached to a policy group named "ONE":

```
webvpn context context1
 sso-server "test-sso-server"
  web-agent-url "http://webagent.example.com"
  secret-key "12345"
  retries 3
  timeout 15
 policy group ONE
  sso-server "test-sso-server"
```

Related Commands

Command	Description
policy group	Enters webvpn group policy configuration mode to configure a policy group.
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

standby-group

To specify a Hot Standby Router Protocol (HSRP) group to be used by a cluster, use the **standby-group** command in IKEv2 cluster configuration mode. To remove a HSRP group, use the **no** form of this command.

standby-group *group-name*

no standby-group

Syntax Description

group-name	HSRP group name.

Command Default

The HSRP group is not specified.

Command Modes

IKEv2 cluster configuration (config-ikev2-cluster)

Command History

Release	Modification
15.2(4)M	This command was introduced.

Usage Guidelines

You must enable the **crypto ikev2 cluster** command before enabling the **standby-group** command.

You must specify the same name that you specified in the *group-name* argument of the **standby name** command.

Examples

The following example shows how to set the HSRP group to group1:

```
Device(config)# crypto ikev2 cluster
Device(config-ikev2-cluster)# standby-group group1
```

Related Commands

Command	Description
crypto ikev2 cluster	Defines an IKEv2 cluster policy in an HSRP cluster.
standby name	Specifies the name of the HSRP standby group.

status

To enter the signature-definition-status configuration mode, which allows you to change the enabled or retired status of an individual signature, use the **status**command in signature-definition-action configuration mode. To return to the default action, use the **no** form of this command.

status

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Signature-definition-action configuration (config-sigdef-action)

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Before issuing the **status** command, you must specify at least one signature via the **signature** command.

Examples

The following example shows how to change the status of signature 9000:0 to enabled:

```
Router(config)# ip ips signature-definition
Router(config-sigdef-sig)# signature 9000 0
Router(config-sigdef-action)# status
Router(config-sigdef-status)# enabled true
```

Related Commands

Command	Description
signature	Specifies a signature for which the CLI user tunings will be changed.

strict-http

To allow HTTP messages to pass through the firewall or to reset the TCP connection when HTTP noncompliant traffic is detected, use the **strict-http**command in appfw-policy-http configuration mode. To disable configured settings, use the **no** form of this command.

strict-http action {**reset**| **allow**} **[alarm]**

no strict-http action {**reset**| **allow**} **[alarm]**

Syntax Description

action	HTTP messages are subject to the specified action (**reset** or **allow**).
reset	Sends a TCP reset notification to the client or server if the HTTP message fails the mode inspection.
allow	Forwards the packet through the firewall.
alarm	(Optional) Generates system logging (syslog) messages for the given action.

Command Default

If this command is not enabled, all traffic will be allowed through the firewall.

Command Modes

appfw-policy-http configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Examples

The following example shows how to define the HTTP application firewall policy "mypolicy." This policy includes all supported HTTP policy rules. After the policy is defined, it is applied to the inspection rule "firewall," which will inspect all HTTP traffic entering the FastEthernet0/0 interface.

```
! Define the HTTP policy.
appfw policy-name mypolicy
 application http
  strict-http action allow alarm
  content-length maximum 1 action allow alarm
  content-type-verification match-req-rsp action allow alarm
  max-header-length request 1 response 1 action allow alarm
  max-uri-length 1 action allow alarm
  port-misuse default action allow alarm
  request-method rfc default action allow alarm
  request-method extension default action allow alarm
  transfer-encoding type default action allow alarm
```

```
!
!
! Apply the policy to an inspection rule.
ip inspect name firewall appfw mypolicy
ip inspect name firewall http
!
!
! Apply the inspection rule to all HTTP traffic entering the FastEthernet0/0 interface.
interface FastEthernet0/0
 ip inspect firewall in
!
!
```

storage

To specify a file system location where public key infrastructure (PKI) trustpool certificates are stored on the router, use the **storage** command in CA-trustpool configuration mode. To remove the file system location that was specified, use the **no** form of this command.

storage *location*

no storage *location*

Syntax Description

location	The file system location where the PKI trustpool certificates are stored. The types of file system locations are specified in the "Usage Guidelines" section.

Command Default

The storage location is not configured.

Command Modes

CA-trustpool configuration mode (ca-trustpool)

Command History

Release	Modification
15.2(2)T	This command was introduced.
15.1(1)SY	This command was integrated into Cisco IOS 15.1(1)SY.

Usage Guidelines

Before you can configure this command, you must enable the **crypto pki trustpool policy** command, which enters ca-trustpool configuration mode.

Previously stored certificates cannot be moved with this command.

The *location* argument specifies the file system storage location. The table below lists the available file system locations:

Table 24: File System Locations

File System	Description
disk0:	Stores the PKI trustpool in the disc0 file system.
disk1:	Stores the PKI trustpool in the disc1 file system.
nvram:	Stores the PKI trustpool in the NVRAM file system.

File System	Description
unix:	Stores the PKI trustpool in the the UNIX file system.
file-system-name =	The named file system that is stored in the PKI trustpool.

Examples

```
Router(config)# crypto pki trustpool policy
Router(ca-trustpool)# storage disk0:crca2048.crl
```

Related Commands

Command	Description
cabundle url	Configures the URL from which the PKI trustpool CA bundle is downloaded.
chain-validation	Enables chain validation from the peer's certificate to the root CA certificate in the PKI trustpool.
crl	Specifes the certificate revocation list (CRL) query and cache options for the PKI trustpool.
crypto pki trustpool import	Manually imports (downloads) the CA certificate bundle into the PKI trustpool to update or replace the existing CA bundle.
crypto pki trustpool policy	Configures PKI trustpool policy parameters.
default	Resets the value of a ca-trustpool configuration command to its default.
match	Enables the use of certificate maps for the PKI trustpool.
ocsp	Specifies OCSP settings for the PKI trustpool.
revocation-check	Disables revocation checking when the PKI trustpool policy is being used.

Command	Description
show	Displays the PKI trustpool policy of the router in ca-trustpool configuration mode.
show crypto pki trustpool	Displays the PKI trustpool certificates of the router and optionally shows the PKI trustpool policy.
source interface	Specifies the source interface to be used for CRL retrieval, OCSP status, or the downloading of a CA certificate bundle for the PKI trustpool.
vrf	Specifies the VRF instance to be used for CRL retrieval.

subject-alt-name

To specify the trustpoint certificate name in the Subject Alternative Name (subjectAltName) field in the X.509 certificate, which is contained in the trustpoint certificate, use the **subject-alt-name**in ca-trustpoint configuration mode. To remove this configuration, use the **no** form of this command.

subject-alt-name *name*

no subject-alt-name *name*

Syntax Description

name	Specifies the trustpoint certificate name.

Command Default

The Subject Alternative Name field is not included in the X.509 certificate.

Command Modes

Ca-trustpoint (ca-trustpoint)

Command History

Release	Modification
15.1(3)T	This command was introduced.

Usage Guidelines

The **subject-alt-name**command is used to create a self-signed trustpoint certificate for the router that contains the trustpoint name in the Subject Alternative Name (subjectAltName) field. This Subject Alternative Name can be used only when the trustpoint enrollment option is specified for self-signed enrollment in the trustpoint policy.

Note The Subject Alternative Name field in the X.509 certificate is defined in RFC 2511.

Examples

The following example shows how to create a self-signed trustpoint certificate for the router that contains the trustpoint name in the Subject Alternative Name (subjectAltName) field:

```
Router> enable
Router# configure terminal
Router(config)# crypto pki trustpoint TESTCA
Router(ca-trustpoint)# enrollment selfsigned
Router(ca-trustpoint)# subject-alt-name TESTCA
Router
(ca-trustpoint)#
exit
Router(config)# cypto pki enroll
TESTCA
% Include the router serial number in the subject name? [yes/no]: no
% Include an IP address in the subject name? [no]:
```

```
Generate Self Signed Router Certificate? [yes/no]: yes
Router Self Signed Certificate successfully created
Router(config)# exit
```

The following certificate is created:

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 2 (0x2)
        Signature Algorithm: md5WithRSAEncryption
        Issuer: CN=TESTCA/unstructuredName=r1.cisco.com
        Validity
            Not Before: Mar 22 20:26:20 2010 GMT
            Not After : Jan  1 00:00:00 2020 GMT
        Subject: CN=TESTCA/unstructuredName=r1.cisco.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (512 bit)
                Modulus (512 bit):
                    00:8d:71:2e:3b:eb:a2:e2:f3:44:d9:bc:a9:85:88:
                    f4:a9:bd:c9:7f:f0:69:f5:e7:75:8f:00:f2:8e:3e:
                    2f:ca:5e:c5:08:43:95:8c:a2:6a:ae:ce:a0:ae:82:
                    61:61:ff:4e:8c:8f:89:d1:56:d8:35:34:b7:95:93:
                    1a:72:03:71:fb
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
            CA:TRUE
            X509v3 Subject Alternative Name:
            DNS:TESTCA
            X509v3 Authority Key Identifier:
            keyid:F9:A4:95:87:5F:A4:CA:7D:65:FA:BE:38:20:55:18:F9:4C:6C:D5:F3
            X509v3 Subject Key Identifier:
            F9:A4:95:87:5F:A4:CA:7D:65:FA:BE:38:20:55:18:F9:4C:6C:D5:F3
    Signature Algorithm: md5WithRSAEncryption
        6d:92:e7:a8:a5:1a:5a:ef:13:58:02:1b:79:17:93:41:37:c9:
        2d:9f:1a:a3:f5:3a:73:05:cd:d1:02:84:43:7e:e0:84:07:46:
        55:f9:45:59:51:ba:25:48:6f:d8:e1:0d:35:44:07:5c:16:17:
        35:45:99:e2:80:6e:53:e5:35:76
-----BEGIN CERTIFICATE-----
MIIBszCCAV2gAwIBAgIBAjANBgkqhkiG9w0BAQQFADAuMQ8wDQYDVQQDEwZURVNU
Q0ExGzAZBgkqhkiG9w0BCQIWDHIxLmNpc2NvLmNvbTAeFw0xMDAzMjIyMDI2MjBa
Fw0yMDAxMDEwMDAwMDBaMC4xDzANBgNVBAMTBlRFU1RDQTEbMBkGCSqGSIb3DQEJ
AhYMcjEuY2lzY28uY29tMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAI1xLjvrouLz
RNm8qYWI9Km9yX/wafXndY8A8o4+L8pexQhDlYyiaq7OoK6CYWH/ToyPidFW2DU0
t5WTGnIDcfsCAwEAAaNmMGQwDwYDVR0TAQH/BAUwAwEB/zARBgNVHREECjAIggZU
RVNUQ0EwHwYDVR0jBBgwFoAU+aSVh1+kyn1l+r44IFUY+Uxs1fMwHQYDVR0OBBYE
FPmklYdfpMp9Zfq+OCBVGPlMbNXzMA0GCSqGSIb3DQEBBAUAA0EAbZLnqKUaWu8T
WAIbeReTQTfJLZ8ao/U6cwXN0QKEQ37ghAdGVflFWVG6JUhv2OENNUQHXBYXNUWZ
4oBuU+U1dg==
-----END CERTIFICATE-----
```

Related Commands

Command	Description
cypto pki enroll	Requests the certificates for the router from the trustpoint.
crypto pki trustpoint	Creates a trustpoint and enters ca-trustpoint configuration mode.
enrollment selfsigned	Specifies self-signed enrollment for a trustpoint.

subject-name

To specify the subject name in the certificate request, use the **subject-name** command in ca-trustpoint configuration mode. To clear any subject name from the configuration, use the **no** form of this command.

subject-name [*x.500-name*]

nosubject-name [*x.500-name*]

Syntax Description

x.500-name	(Optional) Specifies the subject name used in the certificate request.

Command Default

If the *x-500-name* argument is not specified, the fully qualified domain name (FQDN), which is the default subject name, will be used.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.4(24)T	Support for IPv6 Secure Neighbor Discovery (SeND) was added.

Usage Guidelines

Before you can issue the subject-name command, you must enable the **crypto ca trustpoint**command, which declares the certification authority (CA) that your router should use and enters ca-trustpoint configuration mode.

The subject-name command is an attribute that can be set for autoenrollment; thus, issuing this command prevents you from being prompted for a subject name during enrollment.

Examples

The following example shows how to specify the subject name for the "frog" certificate:

```
c
rypto ca trustpoint frog
 enrollment url http://frog.phoobin.com/
 subject-name OU=Spiral Dept., O=tiedye.com
 ip-address ethernet-0
 auto-enroll regenerate
 password revokme
```

Related Commands

Command	Description
crypto ca trustpoint	Declares the CA that your router should use.

subnet-acl (IKEv2 profile)

To configure split tunneling, use the **subnet-acl** command in IKEv2 authorization policy configuration mode. To remove this command from your configuration and restore the default value, use the **no** form of this command.

[**ipv6**] **subnet-acl** {*acl-number*| *acl-name*}

no [**ipv6**] **subnet-acl**

Syntax Description

ipv6	(Optional) Specifies an IPv6 attribute. To specify an IPv4 attribute, execute the command without this keyword.
acl-number	Access list number. The range is 100 to 199.
acl-name	Access list name.

Command Default

Split tunneling is disabled.

Command Modes

IKEv2 authorization policy configuration (config-ikev2-author-policy)

Command History

Release	Modification
15.1(3)T	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.
15.2(1)T	This command was modified. The **ipv6** keyword was added.

Usage Guidelines

Use the **subnet-acl** command to specify that the groups of ACLs represent protected subnets for split tunneling. Split tunneling is the ability to have a secure tunnel to the central site and simultaneous clear text tunnels to the Internet.

You must enable the **crypto ikev2 authorization policy** command, which specifies local group policy group authorization parameters that have to be defined or changed, before enabling the **subnet-acl** command.

Examples

The following example shows how to apply split tunneling for the group name "cisco." In this example, all traffic sourced from the client and destined to the subnet 192.168.1.0 will be sent through the VPN tunnel.

```
crypto ikev2 client configuration group cisco
 key cisco
```

```
 dns 10.2.2.2 10.3.2.3
 pool dog
 subnet-acl 199
!
access-list 199 permit ip 192.168.1.0 0.0.0.255 any
```

Related Commands

Command	Description
crypto ikev2 authorization policy	Specifies an IKEv2 client configuration group.

subscriber access pppoe unique-key circuit-id

To specify a unique circuit ID tag for a PPP over Ethernet (PPPoE) user session to be tapped on the router, use the **subscriber access pppoe unique-key circuit-id**command in global configuration mode. To restore the default value, use the **no** form of this command.

subscriber access pppoe unique-key circuit-id

no subscriber access pppoe unique-key circuit-id

Syntax Description

This command has no arguments or keywords.

Command Default

A unique circuit ID tag for PPPoE user session is not specified.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Release 2.6	This command was introduced.

Usage Guidelines

In Cisco IOS XE Release 2.6, a user session is tapped based on the unique PPPoE circuit ID tag. This circuit ID tag serves as a unique parameter for the PPPoE user session on the device. The tapped user session is provisioned through SNMP, and user session data packets and RADIUS authentication data packets are tapped. This command is used in conjunction with the Lawful Intercept feature.

Related Commands

Command	Description
show idmgr session key	Verifies the user session information in the ID Manager (IDMGR) database by specifying the unique circuit ID tag using the **circuit-id** keyword and *circuit-id* argument.

subscriber service

To enable per-subscriber services, use the **subscriber service** command in global configuration mode. To disable per-subscriber services, use the **no** form of this command.

subscriber service {**accounting interim-interval** *minutes*| **coa-rfc-compliant**| **ignore**| **multiple-accept**| **password**| **police**| **session-accounting**| **shaper**| **target-atm-vc**| **vc-ignore-cos**}

no subscriber service {**accounting interim-interval** *minutes*| **coa-rfc-compliant**| **ignore**| **multiple-accept**| **password**| **police**| **session-accounting**| **shaper**| **target-atm-vc**| **vc-ignore-cos**}

Syntax Description

accounting interim-interval *minutes*	Enables the generation of interim service accounting records at periodic intervals for subscribers. The *minutes* argument indicates the number of periodic intervals to send accounting update records from 1 to 71582 minutes.
coa-rfc-compliant	Sends RFC 3576 compliant change of authorization (CoA) NAK messages.
ignore	Ignores any of per-subscriber services.
multiple-accept	Allows multiple services on access-accept.
password	Password to use when downloading services.
police	Quality of service (QoS) RADIUS service police command.
session-accounting	Enables the inclusion of activated services in a session accounting start message.
shaper	QoS RADIUS service shaper command.
target-atm-vc	Enables the QoS service on the target ATM virtual circuit (VC).
vc-ignore-cos	Ignores the set Layer 2 class of service (set-cos) value on the target ATM VC.

Command Default

Service accounting is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Release 12.2(31)ZV1	This command was introduced for session accounting and was implemented on the Cisco 10000 series router for the PRE3.
Cisco IOS XE Release 2.4	This command was integrated into Cisco IOS XE Release 2.4.

Usage Guidelines

The **subscriber service session-accounting** command enables the router to include all activated services in a single accounting Session-Start message for a session.

RADIUS can activate a service using the RADIUS Access-Accept message. When RADIUS activates a service on the router after the router sends the accounting Session-Start message, the router generates an accounting session update that includes all activated services.

When a session stops, all currently active services are included in the accounting session stop record.

The **subscriber service accounting interim-interval**command enables the router to generate interim service accounting records at periodic intervals for subscribers. RADIUS Attribute 85 in the user service profile always takes precedence over the configured interim-interval value. RADIUS Attribute 85 must be in the user service profile. See the RADIUS Attributes Overview and RADIUS IETF Attributes feature document for more information.

Note If RADIUS Attribute 85 is not in the user service profile, then the interim-interval value is used for service interim accounting records. The interim-interval value is configured by either using the **aaa accounting update** command in global configuration mode or the **action-type** command in accounting method list configuration mode. See the Configuring Accounting feature document for more information.

Examples

The following example enables per-service accounting:

```
Router(config)# subscriber service session-accounting
```

Related Commands

Command	Description
bandwidth account	Enables class-based fair queuing and ATM overhead accounting.
shape account	Shapes traffic to the indicated bit rate and enables ATM overhead accounting.

svc address-pool

To configure a pool of IP addresses to be assigned to end users in a policy group, use the **svc address-pool** command in webvpn group policy configuration mode. To remove the address pool from the policy group configuration, use the **no** form of this command.

svc address-pool *name* **netmask** *ip-netmask*

no svc address-pool

Syntax Description

name	Name of the address pool that is configured using the **ip local pool** command.
netmask *ip-netmask*	Specifies the IP netmask that is applied to the address pool.

Command Default

IP address pools are not assigned to end users.

Command Modes

Webvpn group policy configuration (config-webvpn-group)

Command History

Release	Modification
12.4(6)T	This command was introduced.
15.1(1)T	This command was modified. The **netmask** keyword and *ip-netmask* argument were added.
15.1(4)M3	This command was modified. The **netmask** keyword and *ip-netmask* argument were made mandatory.

Usage Guidelines

Before configuring the **svc address-pool** command, use the **ip local pool** command to define the address pool. The standard configuration assumes that the IP addresses in the pool are reachable from a directly connected network.

Configuring Address Pools for Networks That Are Not Directly Connected

If you need to configure an address pool for IP addresses from a network that is not directly connected, perform the following steps:

1. Create a local loopback interface and configure it with an IP address and subnet mask from the address pool.
2. Configure the address pool with the **ip local pool** command. The range of addresses must fall under the subnet mask configured in Step 1.

3 Configure the **svc address-pool** command with the address pool name configured in Step 2.

See the "Examples" section for an example of how to configure a pool of IP addresses to assign to end users in a policy group.

Note The Switched Virtual Circuits (SVC) software or the Secure Sockets Layer VPN (SSL VPN) client is the predecessor of the Cisco AnyConnect VPN Client software.

Examples

Examples

The following example shows how to configure the 192.168.1/24 network as an address pool:

```
Router(config)# ip local pool ADDRESSES 192.168.1.1 192.168.1.254

Router(config)# webvpn context context1

Router(config-webvpn-context)# policy group ONE

Router(config-webvpn-group)# svc address-pool ADDRESSES netmask 255.255.255.0
Router(config-webvpn-group)# end
```

Examples

The following example shows how to configure the 172.16.1/24 network as an address pool. Because the network is not directly connected, a local loopback is configured.

```
Router(config)# interface loopback 0

Router(config-if)# ip address 172.16.1.128 255.255.255.0

Router(config-if)# no shutdown
Router(config-if)# exit

Router(config)# ip local pool ADDRESSES 172.16.1.1 172.16.1.254

Router(config)# webvpn context context1

Router(config-webvpn-context)# policy group ONE

Router(config-webvpn-group)# svc address-pool ADDRESSES
 netmask 255.255.255.0
```

Related Commands

Command	Description
ip local pool	Configures a local pool of IP addresses to be used when a remote peer connects to a point-to-point interface.
policy group	Enters webvpn group policy configuration mode to configure a policy group.
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

svc default-domain

To configure the Cisco AnyConnect VPN Client domain for a policy group, use the **svc default-domain** command in webvpn group policy configuration mode. To remove the domain from the policy group configuration, use the **no** form of this command.

svc default-domain *name*

no svc default-domain

Syntax Description

name	Name of the domain.

Command Default

Cisco AnyConnect VPN Client domain is not configured.

Command Modes

Webvpn group policy configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

Note SVC software, or Secure Sockets Layer Virtual Private Network (SSL VPN) Client, is the predecessor of Cisco AnyConnect VPN Client software.

Examples

The following example configures cisco.com as the default domain:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# svc default-domain cisco.com
```

Related Commands

Command	Description
policy group	Enters webvpn group policy configuration mode to configure a policy group.

Command	Description
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

svc dns-server

To configure Domain Name System (DNS) servers for policy group end users, use the **svc dns-server** command in webvpn group policy configuration mode. To remove a DNS server from the policy group configuration, use the **no** form of this command.

svc dns-server {**primary**| **secondary**} *ip-address*

no svc dns-server {**primary**| **secondary**}

Syntax Description

primary | **secondary**	Configures the primary or secondary DNS server.
ip-address	An IPv4 address is entered to identify the server.

Command Default

DNS servers are not configured.

Command Modes

Webvpn group policy configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelin

Note SVC software, or Secure Sockets Layer Virtual Private Network (SSL VPN) Client, is the predecessor of Cisco AnyConnect VPN Client software.

Examples

The following example configures primary and secondary DNS servers for the policy group:

```
Router(config)# webvpn context context1

Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# svc dns-server primary 192.168.3.1

Router(config-webvpn-group)# svc dns-server secondary 192.168.4.1
```

Related Commands

Command	Description
policy group	Enters webvpn group policy configuration mode to configure a policy group.
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

svc dpd-interval

To configure the dead peer detection (DPD) timer value for the gateway or client, use the **svc dpd-interval**command in webvpn group policy configuration mode. To remove a DPD timer value from the policy group configuration, use the **no** form of this command.

svc dpd-interval {**client**| **gateway**} *seconds*

no svc dpd-interval {**client**| **gateway**}

Syntax Description

client | **gateway**	Specifies the client or gateway.
seconds	Sets the time interval, in seconds, for the DPD timer. A number from 0 through 3600 is entered.

Command Default

The DPD timer is reset every time a packet is received over the Secure Sockets Layer Virtual Private Network (SSL VPN) tunnel from the gateway or end user.

Command Modes

Webvpn group policy configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelin

Note SVC software, or Secure Sockets Layer Virtual Private Network (SSL VPN) Client, is the predecessor of Cisco AnyConnect VPN Client software.

Examples

The following example sets the DPD timer to 30 seconds for a SSL VPN gateway and to 5 minutes for end users (remote PC or device):

```
Router(config)# webvpn context context1

Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# svc dpd-interval gateway 30
Router(config-webvpn-group)# svc dpd-interval client 300
Router(config-webvpn-group)#
```

Related Commands

Command	Description
policy group	Enters webvpn group policy configuration mode to configure a policy group.
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

svc dtls

To enable Datagram Transport Layer Security (DTLS) support on the Cisco IOS Secure Socket Layer Virtual Private Network (SSL VPN), use the **svc dtls** command in WebVPN group policy configuration mode. To disable the configuration, use the **no** form of this command.

svc dtls

no svc dtls

Syntax Description

This command has no arguments or keywords.

Command Default

DTLS is enabled by default on the Cisco ISR G2 series routers (3900, 2900, 1900, 890, and 880) and is disabled on other routers.

Command Modes

WebVPN group policy configuration (config-webvpn-group)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The DTLS Support for IOS SSL VPN feature enables DTLS as a transport protocol for the traffic tunneled through SSL VPN. The DTLS Support for IOS SSL VPN feature is enabled by default on the Cisco IOS SSL VPN. You can use the **no svc dtls** command to disable DTLS support on the SSL VPN.

Examples

The following example shows how to disable DTLS support on the Cisco IOS SSL VPN gateway:

```
Router# configure terminal
Router(config)# webvpn context context1
Router(config-webvpn-context)# policy group group1
Router(config-webvpn-group)# no svc dtls
```

Related Commands

Command	Description
dtls port	Configures a DTLS port.

svc homepage

To configure the URL of the web page that is displayed upon successful user login, use the **svc homepage**command in webvpn group policy configuration mode. To remove the URL from the policy group configuration, use the **no** form of this command.

svc homepage *string*

no svc homepage

Syntax Description

string	The *string* argument is entered as an HTTP URL. The URL can be up to 255 characters in length.

Command Default

URL of the home page is not configured.

Command Modes

Webvpn group policy configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelin

Note SVC software, or Secure Sockets Layer Virtual Private Network (SSL VPN) Client, is the predecessor of Cisco AnyConnect VPN Client software.

Examples

The following example configures www.cisco.com as the Cisco AnyConnect VPN Client home page:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# svc homepage www.cisco.com
```

Related Commands

Command	Description
policy group	Enters webvpn group policy configuration mode to configure a policy group.

Command	Description
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

svc keepalive

To specify the Secure Socket Layer Virtual Private Network Client (SVC) keepalive value, use the **svc keepalive**command in webvpn group policy configuration mode. To return the **svc keepalive** command to its default, use the **no** form of this command.

svc keepalive seconds

no svc keepalive

Syntax Description

seconds	Specifies an SVC keepalive value from 0 to 600 seconds.

Command Default

The SVC is enabled to send keepalive messages by default with a frequency of 30 seconds.

Command Modes

Webvpn group policy configuration (config-webvpn-group)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

You can adjust the frequency of keepalive messages to ensure that an SVC connection through a proxy, IOS firewall, or Network Address Translation (NAT) device remains active, even if the device limits the time that the connection can be idle. Adjusting the frequency also ensures that the SVC does not disconnect and reconnect when the remote user is not actively running a socket-based application, such as Microsoft Outlook or Microsoft Internet Explorer.

If the **svc keepalive** command is configured with a value of **0** seconds, then the keepalive function is disabled.

Note SVC is the predecessor of Cisco AnyConnect VPN Client software.

Examples

In the following example, the security appliance is configured to enable the SVC to send keepalive messages with a frequency of 300 seconds (5 minutes), for the existing group-policy group "ONE":

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# svc keepalive 300
```

Related Commands

Command	Description
policy group	Enters webvpn group policy configuration mode to configure a policy group.
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

svc keep-client-installed

To configure the end user to keep Cisco AnyConnect VPN Client software installed when the SSL VPN connection is not enabled, use the **svc keep-client-installed**command in webvpn group policy configuration mode. To remove the software installation requirement from the policy group configuration, use the **no** form of this command.

svc keep-client-installed

no svc keep-client-installed

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values.

Command Modes

Webvpn group policy configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

The configuration of this command removes the overhead of pushing the Cisco AnyConnect VPN Client software to the end user on each connection attempt.

Note SVC, or Secure Sockets Layer Virtual Private Network (SSL VPN) Client, is the predecessor of Cisco AnyConnect VPN Client software.

Examples

The following example configures end users to keep Cisco AnyConnect VPN Client software installed:

```
Router(config)# webvpn context context1

Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# svc keep-client-installed
```

Related Commands

Command	Description
policy group	Enters webvpn group policy configuration mode to configure a policy group.

Command	Description
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

svc module

To configure Start Before Logon (SBL) functionality support for a Cisco IOS Secure Sockets Layer Virtual Private Network (SSL VPN) headend, use the **svc module** command in webvpn group policy configuration mode. To disable the configuration, use the **no** form of this command.

svc module *module-name*

no svc module

Syntax Description

module-name	Anyconnect module name.

Command Default

The SBL functionality is disabled by default.

Command Modes

Webvpn group policy configuration (config-webvpn-group)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Usage Guidelines

The SBL functionality connects the client PC to the enterprise network even before the users log in to the PC. This functionality allows the administrator to run the logon scripts even if the user is not connected to the enterprise network.

Use the **svc module** command to configure the SBL functionality support for the Cisco IOS SSL VPN headend. This command sets the module in the WebVPN cookie for the AnyConnect client, and thereby helps in downloading the SBL components to the client from the SSL VPN headend.

Examples

The following example shows how to configure the vpn1 AnyConnect module to Cisco IOS SSL VPN headend:

```
Router# configure terminal
Router(config)# webvpn context context1
Router(config-webvpn-context)# policy group group1
Router(config-webvpn-group)# svc module vpn1
```

Related Commands

Command	Description
policy group	Enters webvpn group policy configuration mode to configure a policy group.

svc msie-proxy

To configure Microsoft Internet Explorer (MSIE) browser proxy settings for policy group end users, use the **svc msie-proxy**command in webvpn group policy configuration mode. To remove a MSIE proxy setting from the policy group configuration, use the **no** form of this command.

svc msie-proxy {**server** *host*| **exception** *host*| **option** {**auto**| **bypass-local**| **none**}}

no svc msie-proxy {**server** *host*| **exception** *host*| **option** {**auto**| **bypass-local**| **none**}}

Syntax Description

server *host*	Specifies a MSIE proxy server for policy group end users. The *host* argument specifies the location of the MSIE server. The *host* argument is configured as an IPv4 address or fully qualified domain name, followed by a colon and port number.
exception *host*	Configures the browser not to send traffic for a single Domain Name System (DNS) hostname or IP address through the proxy.
option auto	Configures the browser to automatically detect proxy settings.
option bypass-local	Configures the browser to bypass proxy settings that are configured on the remote user.
option none	Configures the browser to use no proxy settings.

Command Default

MSIE browser proxy settings are not configured for policy group end users.

Command Modes

Webvpn group policy configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

The configuration of this command is applied to end users that use a MSIE browser. The configuration of this command has no effect on any other browser type.

Note SVC, or Secure Sockets Layer Virtual Private Network (SSL VPN) Client, is the predecessor of Cisco AnyConnect VPN Client software.

Examples

The following example configures automatic detection of MSIE proxy settings and configures proxy exceptions for traffic from www.example.com and the 10.20.20.1 host:

```
Router(config)# webvpn context context1

Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# svc msie-proxy option auto
Router(config-webvpn-group)# svc msie-proxy exception www.example.com
Router(config-webvpn-group)# svc msie-proxy exception 10.20.20.1
```

The following example configures a connection to an MSIE proxy server through a fully qualified domain name (FQDN) and a port number:

```
Router(config)# webvpn context context1

Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# svc msie-proxy server www.example.com:80
```

The following example configures a connection to an MSIE proxy server through an IP address and port number:

```
Router(config)# webvpn context context1

Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# svc msie-proxy server 10.10.10.1:80
```

Related Commands

Command	Description
policy group	Enters webvpn group policy configuration mode to configure a policy group.
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

svc msie-proxy server

To specify a Microsoft Internet Explorer (MSIE) proxy server for policy group end users, use the **svc msie-proxy server**command in SSLVPN group policy configuration mode. To remove the proxy server from the policy group configuration, use the **no** form of this command.

svc msie-proxy server *host*

no svc msie-proxy server

Syntax Description

host	Specifies the location of the MSIE server. The host argument is configured as an IPv4 address or fully qualified domain name, followed by a colon and port number.

Command Default

No default behavior or values.

Command Modes

SSLVPN group policy configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Examples

The following example configures a connection to an MSIE proxy server through a fully qualified domain name and a port number:

```
Router(config)# webvpn context SSLVPN

Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# svc msie-proxy server www.cisco.com:80
Router(config-webvpn-group)#
```

The following example configures a connection to an MSIE proxy server through an IP address and port number:

```
Router(config)# webvpn context SSLVPN

Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# svc msie-proxy server 10.10.10.1:80
Router(config-webvpn-group)#
```

Related Commands

Command	Description
policy group	Enters SSLVPN group policy configuration mode to configure a group policy.
webvpn context	Enters SSLVPN configuration mode to configure the WebVPN context.

svc mtu

To configure the MTU size for a policy group at the client end, use the **svc mtu** command in webvpn group policy configuration mode. To set the MTU size to its default, use the **no** form of this command.

svc mtu *size*

no svc mtu

Syntax Description

size	Size of MTU, in bytes. Range: 256 to 1406. Default:1406

Command Default

The default MTU size is 1406.

Command Modes

Webvpn group policy configuration (config-webvpn-group)

Command History

Release	Modification
12.4(24)T	This command was introduced.

Usage Guidelines

The maximum size of prefragmented packets that is supported by the adapter is only 1406 bytes. Sending packets larger than 1406 bytes could cause potential problems; as a result, there is a size restriction.

Examples

The following example configures the MTU size to 778 bytes:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# svc mtu 778
```

Related Commands

Command	Description
policy group	Enters webvpn group policy configuration mode to configure a policy group.
webvpn context	Enters webvpn context configuration mode to configure an SSL VPN context.

svc rekey

To configure the time and method that a tunnel key is refreshed for policy group end users, use the **svc rekey**command in webvpn group policy configuration mode. To remove the tunnel key configuration from the policy group configuration, use the **no** form of this command.

svc rekey {**method** {**new-tunnel| ssl**}| **time** *seconds*}

no svc rekey {**method** {**new-tunnel| ssl**}| **time** *seconds*}

Syntax Description

method new-tunnel	Refreshes the tunnel key by creating a new tunnel connection to the end user.
method ssl	Refreshes the tunnel key by renegotiating the Secure Sockets Layer (SSL) session.
time *seconds*	Configures the time interval, in seconds, at which the tunnel key is refreshed. A number from 0 through 43200 seconds is entered.

Command Default

Time and method are not configured.

Command Modes

Webvpn group policy configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

Note SVC, or Secure Sockets Layer Virtual Private Network (SSL VPN) Client, is the predecessor of Cisco AnyConnect VPN Client software.

Examples

The following example configures the tunnel key to be refreshed by initiating a new tunnel connection once an hour:

```
Router(config)# webvpn context context1

Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# svc rekey method new-tunnel
Router(config-webvpn-group)# svc rekey time 3600
```

Related Commands

Command	Description
policy group	Enters webvpn group policy configuration mode to configure a policy group.
webvpn context	Enters webvpn configuration mode to configure the SSL VPN context.

svc split

To enable split tunneling for Cisco AnyConnect VPN Client tunnel clients, use the **svc split**command in webvpn group policy configuration mode. To remove the split tunneling configuration from the policy group configuration, use the **no** form of this command.

svc split {**include**| **exclude [local-lans]**} {*ip-address mask*| **acl** {*access-list-number*| *access-list-name*}}

no svc split {**include**| **exclude [local-lans]**} {*ip-address mask*| **acl**}

Syntax Description

include	Specifies the traffic to be sent over Secure Sockets Layer Virtual Private Network (SSL VPN) tunnel. Traffic from the specified IP address and mask is resolved through the Cisco AnyConnect VPN Client tunnel.
exclude	Specifies the traffic not to be sent over SSL VPN tunnel. Traffic from the specified IP address and mask is not resolved through the Cisco AnyConnect VPN Client tunnel.
local-lans	Specifies the traffic for local LANs not to be sent over SSL VPN tunnel.
ip-address mask	Destination network prefix.
acl	Specifies access-list identifier for classifying the tunnel traffic.
access-list-number	Standard IP access-list number. Range is from 1 to 99.
access-list-name	Access-list name.

Command Default

Split tunneling is not enabled for Cisco AnyConnect VPN Client tunnel clients.

Command Modes

WebVPN group policy configuration (config-webvpn-group)

Command History

Release	Modification
12.4(6)T	This command was introduced.
15.1(1)T	This command was modified. The **acl** keyword and the *access-list* and *access-list-name* arguments were added.

Usage Guidelines

Split tunnel support allows you to configure a policy that permits specific traffic to be carried outside the Cisco AnyConnect VPN Client tunnel. Traffic is either included (resolved in tunnel) or excluded (resolved through the Internet service provider [ISP] or WAN connection). Tunnel resolution configuration is mutually exclusive. An IP address cannot be both included and excluded at the same time. Entering the **local-lans** keyword permits the remote user to access resources on a local LAN, such as a network printer.

Note Switched Virtual Circuits (SVC), or the Secure Sockets Layer Virtual Private Network (SSL VPN) client, is the predecessor of Cisco AnyConnect VPN Client software.

Examples

The following example shows how to configure a list of IP addresses to be resolved over the tunnel (included) and a list to be resolved outside of the tunnel (excluded):

```
Router(config-webvpn-group)# svc split exclude 192.168.1.0 255.255.255.0
Router(config-webvpn-group)# svc split include 172.16.1.0 255.255.255.0
```

Related Commands

Command	Description
policy group	Enters WebVPN group policy configuration mode to configure a policy group.
webvpn context	Enters WebVPN configuration mode to configure the SSL VPN context.

svc split dns

To configure the Secure Sockets Layers Virtual Private Network (SSL VPN) gateway to resolve the specified fully qualified Domain Name System (DNS) names through the Cisco AnyConnect VPN Client tunnel, use the **svc split dns**command in webvpn group policy configuration mode. To remove the split DNS statement from the policy group configuration, use the **no** form of this command.

svc split dns *name*

no svc split dns *name*

Syntax Description

dns *name*	The *name* argument is entered as a fully qualified DNS name.

Command Default

The SSL VPN gateway is not configured to resolve the specified fully qualified DNS names through the Cisco AnyConnect VPN Client tunnel.

Command Modes

Webvpn group policy configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

Entering this command configures the SSL VPN gateway to resolve the specified DNS suffixes (domains) through the tunnel. The gateway automatically incudes the default domain into the list of domains that are resolved through the tunnel. Up to 10 DNS statements can be configured.

Note SVC, or Secure Sockets Layer Virtual Private Network (SSL VPN) Client, is the predecessor of Cisco AnyConnect VPN Client software.

Examples

The following example configures primary and secondary DNS servers for the policy group:

```
Router(config)# webvpn context context1

Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# svc split dns cisco.com
Router(config-webvpn-group)# svc split dns my.company.net
```

Related Commands

Command	Description
policy group	Enters webvpn group policy configuration mode to configure a policy group.
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

svc wins-server

To configure Windows Internet Name Service (WINS) servers for policy group end users, use the **svc wins-server**command in webvpn group policy configuration mode. To remove a WINS server from the policy group configuration, use the **no** form of this command.

svc wins-server {**primary**| **secondary**} *ip-address*

no svc dns-server {**primary**| **secondary**}

Syntax Description

primary | **secondary**	Configures the primary or secondary WINS server.
ip-address	An IPv4 address is entered to identify the server.

Command Default

WINS servers are not configured for policy group end users.

Command Modes

Webvpn group policy configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelin

Note SVC, or Secure Sockets Layer Virtual Private Network (SSL VPN) Client, is the predecessor of Cisco AnyConnect VPN Client software.

Examples

The following example configures primary and secondary WINS servers for the policy group:

```
Router(config)# webvpn context context1

Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# svc wins-server primary 172.31.1.1

Router(config-webvpn-group)# svc wins-server secondary 172.31.2.1
```

Related Commands

Command	Description
policy group	Enters webvpn group policy configuration mode to configure a policy group.
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

switchport port-security

To enable port security on an interface, use the **switchport port-security** command in i nterface configuration mode . To disable port security, use the **no** form of this command.

switchport port-security

no switchport port-security

Syntax Description

This command has no keywords or arguments.

Command Default

D isabled

Command Modes

Interface configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(18)SXE	This command was changed as follows on the Supervisor Engine 720: • With Release 12.2(18)SXE and later releases, port security is supported on trunks. • With Release 12.2(18)SXE and later releases, port security is supported on 802.1Q tunnel ports.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Follow these guidelines when configuring port security:

- With Release 12.2(18)SXE and later releases, port security is supported on trunks.
- With releases earlier than Release 12.2(18)SXE, port security is not supported on trunks.
- With Release 12.2(18)SXE and later releases, port security is supported on 802.1Q tunnel ports.
- With releases earlier than Release 12.2(18)SXE, port security is not supported on 802.1Q tunnel ports.
- A secure port cannot be a destination port for a Switch Port Analyzer (SPAN).
- A secure port cannot belong to an EtherChannel.
- A secure port cannot be a trunk port.

- A secure port cannot be an 802.1X port. If you try to enable 802.1X on a secure port, an error message appears, and 802.1X is not enabled. If you try to change an 802.1X-enabled port to a secure port, an error message appears, and the security settings are not changed.

Examples

This example shows how to enable port security:

```
Router(config-if)#
switchport port-security
```

This example shows how to disable port security:

Related Commands

Command	Description
show port-security	Displays information about the port-security setting.

switchport port-security aging

To configure the port security aging , use the **switchport** port-security aging time command in interface configuration mode . To disable aging, use the **no** form of this command.

switchport port-security aging {**time** *time*| **type** {**absolute| inactivity**}}

no switchport port-security aging

Syntax Description

time *time*	Sets the duration for which all addresses are secured; valid values are from 1 to 1440 minutes.
type	Specifies the type of aging.
absolute	Specifies absolute aging; see the "Usage Guidelines" section for more information.
inactivity	Specifies that the timer starts to run only when there is no traffic; see the "Usage Guidelines" section for more information.

Command Default

The defaults are as follows:

- Disabled.
- If enabled, t he defaults are as follows:
  - *time* is 0.
  - **type** is **absolute**

Command Modes

Interface configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.

Release	Modification
12.2(18)SXE	This command was changed as follows on the Supervisor Engine 720: • With Release 12.2(18)SXE and later releases, port security is supported on trunks. • With Release 12.2(18)SXE and later releases, port security is supported on 802.1Q tunnel ports. • The **type**, **absolute**, and **inactivity** keywords were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Follow these guidelines when configuring port security:

- With Release 12.2(18)SXE and later releases, port security is supported on trunks. With releases earlier than Release 12.2(18)SXE, port security is not supported on trunks.
- With Release 12.2(18)SXE and later releases, port security is supported on 802.1Q tunnel ports. With releases earlier than Release 12.2(18)SXE, port security is not supported on 802.1Q tunnel ports.

You can apply one of two types of aging for automatically learned addresses on a secure port:

- Absolute aging times out the MAC address after the age-time has been exceeded, regardless of the traffic pattern. This default is for any secured port, and the age-time is set to 0.
- Inactivity aging times out the MAC address only after the age_time of inactivity from the corresponding host has been exceeded.

Examples

This example shows how to set the aging time as 2 hours:

```
Router(config-if)# switchport port-security aging time 120
```

This example shows how to set the aging time as 2 minutes:

```
Router(config-if)# switchport port-security aging time 2
```

This example shows how to set the aging type on a port to absolute aging:

```
Router(config-if) switchport port-security aging type absolute
```

This example shows how to set the aging type on a port to inactivity aging:

```
Router(config-if) switchport port-security aging type
 inactivity
```

Related Commands

Command	Description
show port-security	Displays information about the port-security setting.

switchport port-security mac-address

To add a MAC address to the list of secure MAC addresses, use the **switchport port-security mac-address** command. To remove a MAC address from the list of secure MAC addresses, use the **no** form of this command.

switchport port-security mac-address {*mac-addr*| **sticky** [*mac-addr*] [**vlan** *vlan* **[voice]**| *vlan-list*]}

no switchport port-security mac-address {*mac-addr*| **sticky** [*mac-addr*] [**vlan** *vlan* **[voice]**| *vlan-list*]}

Syntax Description

mac-addr	MAC addresses for the interface; valid values are from 1 to 1024.
sticky	Configures the dynamic MAC addresses as sticky on an interface.
vlan *vlan* | *vlan-list*	(Optional) Specifies a VLAN or range of VLANs; see the "Usage Guidelines" section for additional information.

Command Default

MAC-addresses are not classified as secured.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(18)SXE	This command was changed as follows on the Supervisor Engine 720: • With Release 12.2(18)SXE and later releases, port security is supported on trunks. • With Release 12.2(18)SXE and later releases, port security is supported on 802.1Q tunnel ports. • The **vlan** *vlan* | *vlan-list*keyword and arguments were added. • The **sticky** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

If you configure fewer secure MAC addresses than the maximum number of secure MAC addresses on all interfaces, the remaining MAC addresses are dynamically learned.

To clear multiple MAC addresses, you must enter the **no** form of this command once for each MAC address to be cleared.

The *vlan-list* argument is visible only if the port has been configured and is operational as a trunk. Enter the **switchport mode trunk** command and then enter the **switchport nonegotiate** command.

The **sticky** keyword configures the dynamic MAC addresses as sticky on an interface. Sticky MAC addresses configure the static Layer 2 entry to stay sticky to a particular interface. This feature can prevent MAC moves or prevent the entry from being learned on a different interface.

You can configure the sticky feature even when the port security feature is not enabled on the interface. It becomes operational once port security is enabled on the interface.

Note You can enter the **switchport port-security mac-address sticky** command only if sticky is enabled on the interface.

When port security is enabled, disabling the sticky feature causes all configured and learned sticky addresses to be deleted from the configuration and converted into dynamic secure addresses.

When port security is disabled, disabling the sticky feature causes all configured and learned sticky addresses to be deleted from the configuration.

For trunk ports, if you enter the **no switchport port-security mac-address sticky** command, a search is conducted for the MAC address in the native VLAN. An error message is displayed if the MAC address is not found in the native VLAN. You must specify the VLAN in the **no** form of the **switchport port-security mac-address sticky** command to remove the MAC address.

For voice ports, you must specify the **vlan voice** keywords in the **no** form of the command.

Examples

This example shows how to configure a secure MAC address:

```
Router(config-if)# switchport port-security mac-address 1000.2000.3000
```

This example shows how to delete a secure MAC address from the address table:

```
Router(config-if)# no switchport port-security mac-address 1000.2000.3000
```

This example shows how to enable the sticky feature on an interface:

```
Router(config-if)# switchport port-security mac-address sticky
```

This example shows how to disable the sticky feature on an interface:

```
Router(config-if)# no switchport port-security mac-address sticky
```

This example shows how to make a specific MAC address as a sticky address:

```
Router(config-if)# switchport port-security mac-address sticky 0000.0000.0001
```

This example shows how to delete a specific sticky address:

```
Router(config-if)# no switchport port-security mac-address sticky 0000.0000.0001
```

This example shows how to delete all sticky and static addresses that are configured on an interface:

```
Router(config-if)# no switchport port-security mac-address
```

The following example shows how to configure a VLAN in the voice port:

```
Router(config-if)# switch port-security mac-address 0.0.1 vlan voice
```

To remove the MAC address 0.0.1 from the voice port, use the following command:

```
Router(config-if)# no switchport port-security mac-address 0.0.1 vlan voice
```

Related Commands

Command	Description
clear port-security	Deletes configured secure MAC addresses and sticky MAC addresses from the MAC address table.
show port-security	Displays information about the port-security setting.
switchport mode trunk	Configures the port as a trunk member.
switchport nonegotiate	Configures the LAN port into permanent trunking mode.

switchport port-security maximum

To set the maximum number of secure MAC addresses on a port, use the **switchport port-security maximum**command in interface configuration mode. To return to the default settings, use the **no** form of this command.

switchport port-security maximum *maximum* [**vlan** *vlan*| *vlan-list*]

no switchport port-security maximum

Syntax Description

maximum	M aximum number of secure MAC addresses for the interface; valid values are from 1 to 4097.
vlan *vlan* | *vlan-list*	(Optional) Specifies a VLAN or range of VLANs; see the "Usage Guidelines" section for additional information.

Command Default

This command has no default setings .

Command Modes

Interface configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to the Release 12.2(17d)SXB.
12.2(18)SXE	This command was changed as follows on the Supervisor Engine 720 only: • The maximum number of secure MAC addresses was changed from 1024 to 4097. • The **vlan** *vlan* | *vlan-list*keyword and arguments were added. • With Release 12.2(18)SXE and later releases, port security is supported on trunks. • With Release 12.2(18)SXE and later releases, port security is supported on 802.1Q tunnel ports.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

If you enter this command more than once, subsequent use of this command overrides the previous value of *maximum*. If the new *maximum*argument is larger than the current number of the secured addresses on this port, there is no effect except to increase the value of the *maximum*.

If the new *maximum* is smaller than the old *maximum* and there are more secure addresses on the old *maximum*, the command is rejected.

If you configure fewer secure MAC addresses than the maximum number of secure MAC addresses on the port, the remaining MAC addresses are dynamically learned.

Once the maximum number of secure MAC addresses for the port is reached, no more addresses are learned on that port even if the per-VLAN port maximum is different from the aggregate maximum number.

You can override the maximum number of secure MAC addresses for the port for a specific VLAN or VLANs by entering the **switchport port-security maximum** *maximum* **vlan** *vlan* | *vlan-list*command.

The *vlan-list* argument allows you to enter ranges, commas, and delimited entries such as 1,7,9-15,17.

The *vlan-list* argument is visible only if the port has been configured and is operational as a trunk. Enter the **switchport mode trunk** command and then enter the **switchport nonegotiate** command.

Examples

This example shows how to set the maximum number of secure MAC addresses that are allowed on this port:

```
Router(config-if)# switchport port-security maximum 5
```

This command shows how to override the maximum set for a specific VLAN:

```
Router(config-if)# switchport port-security maximum 3 vlan 102
```

Related Commands

Command	Description
show port-security	Display information about the port-security setting.
switchport nonegotiate	Configures the LAN port into permanent trunking mode.

switchport port-security violation

To set the action to be taken when a security violation is detected, use the **switchport port-security violation** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

switchport port-security violation {**shutdown**| **restrict**| **protect**}

no switchport port-security violation {**shutdown**| **restrict**| **protect**}

Syntax Description

shutdown	Shuts down the port if there is a security violation.
restrict	Drops all the packets from the insecure hosts at the port-security process level and increments the security-violation count.
protect	Drops all the packets from the insecure hosts at the port-security process level but does not increment the security-violation count.

Command Default

The port security violation is shutdown.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(18)SXE	This command was changed as follows on the Supervisor Engine 720: • With Release 12.2(18)SXE and later releases, port security is supported on trunks. • With Release 12.2(18)SXE and later releases, port security is supported on 802.1Q tunnel ports.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(14)SXH	**Platform port-security disable traps** was introduced as part of protect violation mode.

Usage Guidelines

When a security violation is detected, one of the following actions occurs:

- Protect--When the number of port-secure MAC addresses reaches the maximum limit that is allowed on the port, the packets with unknown source addresses are dropped until you remove a sufficient number of secure MAC addresses. Platform port-security disable traps is configurable only when the violation mode is set to **protect**. When this option is configured, drop entries will not be installed into hardware for violating addresses, thus allowing traffic to continue to flow to violating address from legitimate ports. To protect switch CPU against overload when this option is enabled, we recommend that you configure the port-security rate-limiter to 2000 packets per second with a burst rate of 10.

Note This feature also permits traffic to legitimate ports from insecure MAC addresses.

- Restrict--A port-security violation restricts data and causes the security-violation counter to increment.
- Shutdown--The interface is error disabled when a security violation occurs.

Note When a secure port is in the error-disabled state, you can bring it out of this state by entering the **errdisable recovery cause psecure-violation** global configuration command or you can manually reenable it by entering the **shutdown** and **no shutdown** commands in interface-configuration mode.

Examples

This example shows how to set the action to be taken when a security violation is detected:

```
Router(config-if)# switchport port-security violation restrict
```

This example allows the traffic to a secured MAC address on one port to flow even in the presence of violations on other ports while in protect mode.

```
Router(config-if)# switchport port-security violation protect
Router(config-if)# platform port-security disable traps
```

Related Commands

Command	Description
show port-security	Displays information about the port-security setting.
errdisable recovery cause psecure-violation (global configuration)	Removes a secure port from an error-disabled state.
platform port-security disable traps	Modifies the behavior of protect violation mode.