



## show smds addresses through waas export

---

- [show smds addresses, on page 3](#)
- [show smds map, on page 4](#)
- [show smds traffic, on page 5](#)
- [show srtp, on page 7](#)
- [show vc-group, on page 8](#)
- [show vfi, on page 9](#)
- [show waas accelerator, on page 14](#)
- [show waas alarms, on page 18](#)
- [show waas auto-discovery, on page 20](#)
- [show waas cache http-express metadacache, on page 23](#)
- [show waas connection, on page 26](#)
- [show waas statistics accelerator, on page 34](#)
- [show waas statistics aoim, on page 41](#)
- [show waas statistics application, on page 45](#)
- [show waas statistics auto-discovery, on page 48](#)
- [show waas statistics class, on page 53](#)
- [show waas statistics dre, on page 56](#)
- [show waas statistics errors, on page 60](#)
- [show waas statistics global, on page 63](#)
- [show waas statistics lz, on page 66](#)
- [show waas statistics pass-through, on page 68](#)
- [show waas statistics peer, on page 71](#)
- [show waas status, on page 74](#)
- [show waas token, on page 77](#)
- [show x25 context, on page 79](#)
- [show x25 cug, on page 82](#)
- [show x25 hunt-group, on page 85](#)
- [show x25 interface, on page 87](#)
- [show x25 map, on page 88](#)
- [show x25 profile, on page 91](#)
- [show x25 remote-red, on page 94](#)
- [show x25 route, on page 95](#)
- [show x25 services, on page 96](#)

- [show x25 vc](#), on page 97
- [show x25 xot](#), on page 105
- [show x28 hunt-group](#), on page 107
- [show x29 access-lists](#), on page 109
- [show xconnect](#), on page 111
- [shutdown \(FR-ATM\)](#), on page 124
- [skeptical interval \(OTV\)](#), on page 126
- [smds address](#), on page 127
- [smds dxi](#), on page 128
- [smds enable-arp](#), on page 130
- [smds glean](#), on page 131
- [smds multicast](#), on page 132
- [smds multicast arp](#), on page 134
- [smds multicast bridge](#), on page 135
- [smds multicast ip](#), on page 137
- [smds static-map](#), on page 139
- [snmp-server enable traps waas](#), on page 141
- [source-interface loopback](#), on page 143
- [spf-interval \(OTV\)](#), on page 144
- [status admin-down disconnect](#), on page 145
- [suppress-server-encoding enable](#), on page 146
- [tfo auto-discovery blacklist](#), on page 147
- [tfo optimize](#), on page 149
- [threshold de](#), on page 151
- [threshold ecn](#), on page 153
- [timeout setup](#), on page 155
- [vc-group](#), on page 156
- [vpls-id](#), on page 158
- [waas cm-register url](#), on page 160
- [waas config](#), on page 162
- [waas enable](#), on page 163
- [waas-ssl-trustpoint](#), on page 164

# show smds addresses

To display the individual addresses and the interface they are associated with, use the **show smds addresses** privileged EXEC command.

**show smds addresses**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
10.0	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 Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

## Examples

The following is sample output from the **show smds addresses** command:

```
Router# show smds addresses
SMDS address - Serial0 c141.5555.1212.FFFF
```

The table below describes the fields shown in the display.

**Table 1: show smds addresses Field Descriptions**

Field	Description
Serial0	Interface to which this SMDS address has been assigned.
c141.5555.1212	SMDS address that has been assigned to the interface.

## show smds map

To display all Switched Multimegabit Data Service (SMDS) addresses that are mapped to higher-level protocol addresses, use the **show smds map** privileged EXEC command.

### show smds map

#### Syntax Description

This command has no arguments or keywords.

#### Command Modes

Privileged EXEC

#### Command History

Release	Modification
10.0	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 Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

#### Examples

The following is sample output from the **show smds map** command:

```
Router# show smds map
Serial0: ARP maps to e180.0999.9999.FFFF multicast
Serial0: IP maps to e180.0999.9999.FFFF 172.16.42.112 255.255.255.0 multicast
Serial0: IPX 1ABC.000.0c00.d8db maps to c111.1111.1111.1111 -- dynamic, TTL: 4 min
```

The table below describes the fields shown in the output.

**Table 2: show smds map Field Descriptions**

Field	Description
Serial0	Name of interface on which SMDS has been enabled.
ARP maps to	Higher-level protocol address that maps to this particular SMDS address.
e180.0999.9999.FFFF	SMDS address. Includes all SMDS addresses entered with either the <b>smds static-map</b> command (static) or <b>smds multicast</b> command (multicast).
172.16.42.112	IP address.
255.255.255.0	Subnet mask for the IP address.
static/dynamic	The address was obtained from a static map or dynamic map.
TTL	Time to live.

## show smds traffic

To display statistics about Switched Multimegabit Data Service (SMDS) packets the router has received, use the **show smds traffic** privileged EXEC command.

**show smds traffic**

### Syntax Description

This command has no arguments or keywords.

### Command Modes

Privileged EXEC

### Command History

Release	Modification
10.0	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 Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

### Examples

The following is sample output from the **show smds traffic** command:

```
Router# show smds traffic
624363 Input packets
759695 Output packets
2 DXI heartbeat sent
0 DXI heartbeat received
0 DXI DSU polls received
0 DXI DSU polls sent
0 DXI invalid test frames
0 Bad BA size errors
0 Bad Header extension errors
65 Invalid address errors
1 Bad tag errors
```

The table below describes the fields shown in the output.

**Table 3: show smds traffic Field Descriptions**

Field	Description
Input packets	Number of input packets.
Output packets	Number of output packets.
DXI heartbeat sent	Number of Data Exchange Interface (DXI) heartbeat polls transmitted.
DXI heartbeat received	Number of DXI heartbeat polls received.
DXI DSU polls sent	Number of DXI Data Service Unit (DSU) polls sent.
DXI DSU polls received	Number of DXI DSU polls received.

Field	Description
DXI invalid test frames	Number of invalid test frames seen.
Bad BA size errors	Number of packets that have a size less than 32 or greater than 9188 bytes.
DXI Header extension errors	Number of extended SMDS Interface Protocol (SIP) Layer 3 header errors.
DXI Invalid address errors	Number of address errors.
Bad tag errors	Status indicating the number of errors that occur when there is a mismatch between the Tag value in the header and the BeTag value in the trailer of an SMDS frame. This usually indicates that there is a misconfiguration (that is, a DXI is connected to a non-DXI) or that the SMDS data service unit (SDSU) is scrambling the Layer 2 protocol data units (PDUs).

# show srcp

To display Simple Resource Coordination Protocol (SRCP) information, use the **show srcp** command in user EXEC or privileged EXEC mode.

## show srcp

### Syntax Description

This command has no arguments or keywords.

### 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.

### Examples

The following is sample output for **show srcp** command:

```
Router# show srcp
SRCP Admin State ACTIVE, Oper State ACTIVE
SRCP UDP port 2428
```

The table below describes the fields shown in the display.

**Table 4: show srcp Field Descriptions**

Field	Description
SRCP Admin State	Administrative state of the SRCP daemon.
Oper State	Operational state of the SRCP daemon.
SRCP UDP Port	The User Datagram Protocol (UDP) port used for the specified connection.

### Related Commands

Command	Description
<b>debug srcp</b>	Enables debug traces for SRCP errors, events, media, packets, and parser.
<b>srcp</b>	Allocates resources for the SRCP and starts the daemon.

# show vc-group

To display the names of all virtual circuit (VC) groups, use the **show vc-group** command in user EXEC or privileged EXEC mode.

**show vc-group** [*group-name*]

## Syntax Description

<i>group-name</i>	(Optional) Name defined by the <b>vc-group</b> command. If this argument is not specified, the names of all VC groups in the system are displayed.
-------------------	--

## Command Default

The names of all VC groups in the system are displayed.

## Command Modes

User EXEC  
Privileged EXEC

## Command History

Release	Modification
12.1(2)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 Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

## Examples

The following example shows the default display of the **show vc-group** EXEC command:

```
Router# show vc-group
Name of All VC Groups:
=====
network-1
```

## Related Commands

Command	Description
<b>show atm pvc</b>	Displays all ATM PVCs, SVCs, and traffic information.
<b>show frame-relay pvc</b>	Displays statistics about Frame Relay interfaces.
<b>vc-group</b>	Assigns multiple Frame Relay DLCIs to a VC group.



# show vfi

To display information related to a virtual forwarding instance (VFI), use the **show vfi** command in privileged EXEC mode.

```
show vfi [{checkpoint [summary] | mac static address | memory [detail] | name vfi-name
[ {checkpoint | mac static address} ] | neighbor ip-addr vcid vcid mac static address}]
```

## Syntax Description

<b>checkpoint</b>	(Optional) Displays VFI checkpoint information.
<b>summary</b>	(Optional) Displays a summary of VFI checkpoint information.
<b>mac static address</b>	(Optional) Displays static MAC addresses in a bridge domain.
<b>memory</b>	(Optional) Displays VFI memory usage.
<b>detail</b>	(Optional) Displays details of VFI memory usage.
<b>name</b>	(Optional) Displays information for the specified VFI.
<i>vfi-name</i>	(Optional) Name of a specific VFI.
<b>neighbor</b>	(Optional) Displays VFI neighbor information.
<i>ip-addr</i>	(Optional) IP address of the neighbor (remote peer).
<b>vcid</b>	(Optional) Displays the virtual circuit (VC) ID for a peer.
<i>vcid</i>	(Optional) Integer from 1 to 4294967295 that identifies the virtual circuit.

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
12.2(33)SRA	This command was updated to display the Virtual Private Network (VPN) ID.
12.2(33)SRC	This command was modified. The <b>name</b> keyword was added.
12.2(33)SRE	This command was modified. The following keywords and arguments were added: <b>address</b> , <b>checkpoint</b> , <b>detail</b> , <b>mac</b> , <b>memory</b> , <b>neighbor ip-addr</b> , <b>static</b> , <b>summary</b> , and <b>vcid vcid</b> .
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.
Cisco IOS XE Release 3.7S	This command was integrated into Cisco IOS XE Release 3.7S.

## Usage Guidelines

Use this command to verify VFI configurations and for troubleshooting.

## Examples

The following example shows status for a VFI named VPLS-2. The VC ID in the output represents the VPN ID; the virtual circuit is identified by the combination of the destination address and the virtual circuit ID.

```
Router# show vfi name VPLS-2
VFI name: VPLS-2, state: up
VPN ID: 100
Local attachment circuits:
  Vlan2
Neighbors connected via pseudowires:
Peer Address      VC ID      Split-horizon
10.1.1.1          2          Y
10.1.1.2          2          Y
10.2.2.3          2          N
```

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

**Table 5: show vfi name Field Descriptions**

Field	Description
VFI name	The name assigned to the VFI.
state	The status of the VFI (up or down).
Local attachment circuits	The interface or VLAN assigned to the VFI.
Peer Address	The IP address of the peer router.
VC ID	The VC ID assigned to the pseudowire.
Split-horizon	Indicates whether split horizon is enabled (Y) or disabled (N).

The following is sample output from the show vfi command. For the Virtual Private LAN Service (VPLS) autodiscovery feature, the command output from the command output includes autodiscovery information, as shown in the following example:



**Note** VPLS autodiscovery is not supported in Cisco IOS Release 12.2(50)SY.

```
Router# show vfi
Legend: RT= Route-target, S=Split-horizon, Y=Yes, N=No
VFI name: VPLS1, state: up, type: multipoint
VPN ID: 10, VPLS-ID: 9:10
RD: 9:10, RT: 10.10.10.10:150
Local attachment circuits:
  Ethernet0/0.2
Neighbors connected via pseudowires:
Peer Address      VC ID      Discovered Router ID      S
10.7.7.1          10         10.7.7.1                  Y
10.7.7.2          10         10.1.1.2                  Y
10.7.7.3          10         10.1.1.3                  Y
10.7.7.4          10         10.1.1.4                  Y
10.7.7.5          10         -                          Y
VFI name: VPLS2 state: up, type: multipoint
VPN ID: 11, VPLS-ID: 10.9.9.9:2345
```

```

RD: 10:11, RT: 10.4.4.4:151
Local attachment circuits:
  Ethernet0/0.3
Neighbors connected via pseudowires:
Peer Address      VC ID      Discovered Router ID      S
10.7.7.1          11         10.7.7.1                   Y
10.7.7.2          11         10.1.1.5                    Y

```

The table below describes the significant fields in the output related to VPLS autodiscovery.

**Table 6: show vfi Field Descriptions for VPLS Autodiscovery**

Field	Description
VPLS-ID	The identifier of the VPLS domain. VPLS autodiscovery automatically generates a VPLS ID using the Border Gateway Protocol (BGP) autonomous system number and the configured VFI VPN ID.
RD	The route distinguisher (RD) to distribute endpoint information. VPLS autodiscovery automatically generates an RD using the BGP autonomous system number and the configured VFI VPN ID.
RT	The route target (RT). VPLS autodiscovery automatically generates a route target using the lower 6 bytes of the RD and VPLS ID.
Discovered Router ID	A unique identifier assigned to the PE router. VPLS autodiscovery automatically generates the router ID using the Multiprotocol Label Switching (MPLS) global router ID.

The following is sample output from the **show vfi** command for a specified VFI named H-VPLS-A-VFI. Because the optional **name** keyword is entered, the checkpoint information for the specific VFI is displayed.

```

Router# show vfi name H-VPLS-A-VFI checkpoint
VFI Active RP
Checkpointing: Allowed
ISSU Client id: 2092, Session id: 65543, Compatible with peer
VFI VFI AC VFI PW
Bulk-sync 1 1 3
Checkpoint failures: 0 3 21
Recovered at switchover: 0 0 0
Recovery failures: 0 0 0
Legend: C=Checkpointed
VFI name: H-VPLS-A-VFI, state: up, type: multipoint
VPN ID: 12, Internal ID 1 C
Local attachment circuits:
Vlan200 16387 / 8195 C
Neighbors connected via pseudowires:
Peer ID VC ID SSM IDs
10.0.0.12 12 4096 / 12292 C
10.0.0.15 12 8193 / 16389 C
10.0.0.14 12 12290 / 20486 C

```

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

**Table 7: show vfi name checkpointing Field Descriptions**

Field	Description
Checkpointing	Specifies whether checkpointing is allowed on this VFI.
ISSU Client id	The ID number assigned to the In-Service Software Upgrade (ISSU) client.
Session id	The current VFI session ID number.
VFI	Status of the VFI.
VFI AC	Status of the Attachment Circuit (AC).
VFI PW	Status of the pseudowire for this VFI.
Checkpoint failures	The number of checkpoint failures on this interface.
Recovered at switchover	The number of checkpoint failures recovered on this interface at switchover.
Recovery failures	The number of checkpoint failures recovered on this interface.
VFI name	The name assigned to the VFI.
state	Status of the VFI (up or down).
type	VFI type.
VPN ID	The ID number of the VPN.
Local attachment circuits	The Interface or VLAN assigned to the VFI.
Peer ID	The IP address of the peer router.
VC ID	The VC ID assigned to the pseudowire.

The following is sample output from the **show vfi** command using the **memory** and **detail** keywords.

```
Router# show vfi memory detail
VFI memory                In-use Asked-For/Allocated Count  Size  Cfg/Max
-----
VFI structs                In-use Asked-For/Allocated Count  Size  Cfg/Max
-----
vfi_context_t             :      --      --/--          --    52  --/--
vfi_circuit_retry         :      --      --/--          --    24  --/--
Total allocated: 0.000 Mb, 0 Kb, 0 bytes
```

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

**Table 8: show vfi memory detail Field Descriptions**

Field	Description
VFI memory	Amount of memory available for use.
In-use	Amount of memory actively used.

Field	Description
Asked-For/Allocated	Amount of memory originally requested/amount of memory allocated.
Count	Number of pieces of this named memory that exist.
Size	Size of the memory allocated by the system for this chunk.
Config/Max	Number of chunklets per chunk.
VFI structs	Data structures being used.
Total allocated	Total allocated memory.

**Related Commands**

Command	Description
<b>show checkpoint</b>	Displays information about the Checkpoint Facility (CF) subsystem on a Cisco CMTS.
<b>show xconnect</b>	Displays information about xconnect attachment circuits and pseudowires.

# show waas accelerator

To display information about WAAS Express accelerators, use the **show waas accelerator** command in privileged EXEC mode.

**show waas accelerator** [{**detail** | **cifs-express** | **http-express** | **ssl-express**}]

## Syntax Description

<b>detail</b>	(Optional) Displays detailed information about the status and configuration of an accelerator.
<b>cifs-express</b>	(Optional) Displays status and configuration information about Common Internet File System (CIFS)-Express accelerator.
<b>http-express</b>	(Optional) Displays status and configuration information about HTTP-Express accelerator.
<b>ssl-express</b>	(Optional) Displays status and configuration information about Secure Sockets Layer (SSL)-Express accelerator.

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
15.2(3)T	This command was introduced.

## Examples

The following is sample output from the **show waas accelerator** command:

```
Router# show waas accelerator

Accelerator   Config State   Operational State
-----
http-express  Enabled        Shutdown
cifs-express  Disabled       Shutdown
ssl-express   Disabled       Shutdown
```

The table below describes the fields shown in the display.

**Table 9: show waas accelerator Field Descriptions**

Field	Description
Accelerator	Lists the name of accelerator—CIFS-Express, HTTP-Express, SSL-Express—configured on the WAAS Express device.
Config State	Configuration status of the accelerator, enabled or disabled.
Operational State	Operational status of the accelerator, running or shutdown.

The following is sample output from the **show waas accelerator cifs-express** command:

```
Router# show waas accelerator cifs-express

Accelerator   Config State   Operational State
-----
cifs-express  Disabled       Shutdown
```

```
CIFS-Express:
Accelerator Config Item      Value
-----
Read-Ahead Optimization     Enabled
    Read-Ahead size:        190
Async-Write Optimization     Enabled
    Quota threshold:        20
Ads Negative Cache Optimization Enabled
    Timeout:                 3
```

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

**Table 10: show waas accelerator cifs-express Field Descriptions**

Field	Description
Read-Ahead Optimization	Configuration status of the read ahead feature.
Read-Ahead size	Configured value, in KB, of the data to read ahead per file.
Async-Write Optimization	Configuration status of the async write feature.
Quota threshold	Configured value, in MB, of the quota threshold for async write optimization.
Ads Negative Cache Optimization	Configuration status of the alternate data stream negative caching feature.
Timeout	Configured timeout value, in seconds, for negative caching entries.

The following is sample output from the **show waas accelerator http-express** command:

```
Router# show waas accelerator http-express

Accelerator      Config State      Operational State
-----
http-express     Disabled          Shutdown

HTTP-Express:
Accelerator Config Item      Value
-----
Suppress Server Encoding     Disabled
DRE Hints                     Enabled
Metadatacache                Disabled
    MaxAge                    86400
    MinAge                     60
    Filter-extension           All
    Redirect                   Enabled
    Unauthorized               Enabled
    Conditional                 Enabled
HTTPS Metadatacache          Disabled
```

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

**Table 11: show waas accelerator http-express Field Descriptions**

Field	Description
Suppress Server Encoding	Configuration status of the server encoding suppression feature.

Field	Description
DRE Hints	Configuration status of the Data Redundancy Elimination (DRE) hints feature.
Metadatacache	Configuration status of HTTP metadata caching.
MaxAge	Configured maximum time, in seconds, for which cache entries are retained in the metadata cache table.
MinAge	Configured minimum time, in seconds, for which cache entries are retained in the metadata cache table.
Filter-extension	File extensions for which the metadata cache will be stored.
Redirect	Configuration status of the HTTP URL redirect feature.
Unauthorized	Configuration status of the HTTP authentication-redirect feature.
Conditional	Configuration status of the HTTP conditional requests feature.
HTTPS Metadatacache	Configuration status of HTTPS metadata caching.

The following is sample output from the **show waas accelerator ssl-express** command. The fields in the display are self-explanatory.

```
Router# show waas accelerator ssl-express

Accelerator      Config State      Operational State
-----
ssl-express      Enabled           Running
```

#### Related Commands

Command	Description
<b>clear waas</b>	Clears information about WAAS Express closed connections, statistics, cache, or tokens.
<b>debug waas</b>	Displays debugging information for different WAAS Express modules.
<b>show waas alarms</b>	Displays WAAS Express status and alarms.
<b>show waas auto-discovery</b>	Displays information about WAAS Express autodiscovery.
<b>show waas statistics accelerator</b>	Displays statistical information about WAAS Express accelerators.
<b>show waas statistics aoim</b>	Displays WAAS Express peer information and negotiated capabilities.
<b>show waas statistics application</b>	Displays WAAS Express policy application statistics.
<b>show waas statistics auto-discovery</b>	Displays WAAS Express autodiscovery statistics.
<b>show waas statistics class</b>	Displays statistics for the WAAS Express class map.



<b>Command</b>	<b>Description</b>
<b>show waas statistics dre</b>	Displays WAAS Express DRE statistics.
<b>show waas statistics errors</b>	Displays WAAS Express error statistics.
<b>show waas statistics global</b>	Displays global WAAS Express statistics.
<b>show waas statistics lz</b>	Displays WAAS Express LZ statistics.
<b>show waas statistics pass-through</b>	Displays WAAS Express connections placed in a pass-through mode.
<b>show waas statistics peer</b>	Displays inbound and outbound statistics for peer WAAS Express devices.
<b>show waas status</b>	Displays the status of WAAS Express.
<b>show waas token</b>	Displays the value of the configuration token used by the WAAS Central Manager.
<b>waas cm-register url</b>	Registers a device with the WAAS Central Manager.

# show waas alarms

To display WAAS Express status and alarms, use the **show waas alarms** command in privileged EXEC mode.

**show waas alarms**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
15.1(2)T	This command was introduced.
15.2(3)T	This command was modified. The output was enhanced to display the status and alarms for Secure Sockets Layer (SSL)-Express accelerator parameters.

## Usage Guidelines

Use this command to display the status of the WAAS Express device and display the alarms that are enabled in the system.

## Examples

The following output from the **show waas alarms** command shows that alarms are enabled when the WAAS Express feature license expires:

```
Device# show waas alarms

Alarms
  Connection limit exceeded:           off
  Too many peers discovered:          off
  WAAS license expired:                off
  WAAS license revoked:                off
  WAAS license deleted:                on
  WAAS SSL-Express CA enrolled trustpoint deleted: off
  WAAS SSL-Express router certificate deleted: off
  High CPU:                             off
```

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

**Table 12: show waas alarms Field Descriptions**

Field	Description
Connection limit exceeded	Device exceeds the connection limit.
High CPU	CPU reaches maximum utilization.

## Related Commands

Command	Description
<b>clear waas</b>	Clears WAAS Express statistics and closed connections information.
<b>debug waas</b>	Displays debugging information for different WAAS Express modules.

<b>Command</b>	<b>Description</b>
<b>show waas auto-discovery</b>	Displays information about WAAS Express autodiscovery.
<b>show waas connection</b>	Displays information about WAAS Express connections.
<b>show waas statistics aoim</b>	Displays WAAS Express peer information and negotiated capabilities.
<b>show waas statistics application</b>	Displays WAAS Express policy application statistics.
<b>show waas statistics auto-discovery</b>	Displays WAAS Express autodiscovery statistics.
<b>show waas statistics class</b>	Displays statistics for the WAAS Express class map.
<b>show waas statistics dre</b>	Displays WAAS Express DRE statistics.
<b>show waas statistics errors</b>	Displays WAAS Express error statistics.
<b>show waas statistics global</b>	Displays global WAAS Express statistics.
<b>show waas statistics lz</b>	Displays WAAS Express LZ statistics.
<b>show waas statistics pass-through</b>	Displays WAAS Express connections placed in a pass-through mode.
<b>show waas statistics peer</b>	Displays inbound and outbound statistics for peer WAAS Express devices.
<b>show waas status</b>	Displays the status of WAAS Express.
<b>show waas token</b>	Displays the value of the configuration token used by the WAAS Central Manager.
<b>waas cm-register url</b>	Registers a device with the WAAS Central Manager.

# show waas auto-discovery

To display autodiscovery information for the WAAS Express device, use the **show waas auto-discovery** command in privileged EXEC mode.

**show waas auto-discovery** {**list** | **blacklist**}

## Syntax Description

<b>list</b>	Displays the relevant autodiscovery states for the current connections.
<b>blacklist</b>	Displays the autodiscovery blocked list including the server address and state (grey or black).

## Command Default

Autodiscovery information for the WAAS Express device is displayed with the associated connection states.

## Command Modes

Privileged EXEC (#)

## Command History

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

## Usage Guidelines

Use this command to display connections being optimized and connections on which optimization is being negotiated.

## Examples

The following is sample output from the **show waas auto-discovery list** command:

```
Router> enable
Router# show waas auto-discovery list
E: Established, S: Syn, A: Ack, F: Fin, R: Reset M: eMbyronic
s: sent, r: received, O: Options, P: Passthrough
  Src-IP:Port      Dst-IP:Port      Orig-St  Term-St
  192.168.111.111:65531      192.168.200.200:65531      Sr      SOs
```

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

**Table 13: show waas auto-discovery list Field Descriptions**

Field	Description
Src-IP:Port	Source IP port number
Dst-IP:Port	Destination IP port number
Orig-St	Originating state
Term-St	Terminating state

The following is sample output from the **show waas auto-discovery blacklist** command:

```
Router> enable
Router# show waas auto-discovery blacklist
```

```

Server IP          Insert Time      State
192.168.111.111:65531  Tue Jul 27 16:16:19 2010  Grey

```

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

**Table 14: show waas auto-discovery blacklist Field Descriptions**

Field	Description
Server IP	The server address.
Insert Time	The blocked list insert time.
State	<ul style="list-style-type: none"> <li>• Grey indicates that one acknowledgment was received without option 33. Grey also indicates that WAAS Express is in the validation state to add the IP address to the blocked list.</li> <li>• Black indicates that two acknowledgments were received without option 33. Black also indicates that packets are dropped with WAAS Express TCP options and are added to the blocked list. This enables WAAS Express to perform optimization.</li> </ul>

#### Related Commands

Command	Description
<b>clear waas</b>	Clears WAAS Express statistics and closed connections information.
<b>debug waas</b>	Displays debugging information for different WAAS Express modules.
<b>show waas alarms</b>	Displays WAAS Express status and alarms.
<b>show waas connection</b>	Displays information about WAAS Express connections.
<b>show waas statistics aaim</b>	Displays WAAS Express peer information and negotiated capabilities.
<b>show waas statistics application</b>	Displays WAAS Express policy application statistics.
<b>show waas statistics auto-discovery</b>	Displays WAAS Express autodiscovery statistics.
<b>show waas statistics class</b>	Displays statistics for the WAAS Express class map.
<b>show waas statistics dre</b>	Displays WAAS Express DRE statistics.
<b>show waas statistics errors</b>	Displays WAAS Express error statistics.
<b>show waas statistics global</b>	Displays global WAAS Express statistics.
<b>show waas statistics lz</b>	Displays WAAS Express LZ statistics.
<b>show waas statistics pass-through</b>	Displays WAAS Express connections placed in a pass-through mode.
<b>show waas statistics peer</b>	Displays inbound and outbound statistics for peer WAAS Express devices.
<b>show waas status</b>	Displays the status of WAAS Express.

Command	Description
show waas token	Displays the value of the configuration token used by the WAAS Central Manager.
waas cm-register url	Registers a device with the WAAS Central Manager.

## show waas cache http-express metadatabacache

To display WAAS Express HTTP metadata cache entries, use the **show waas cache http-express metadatabacache** command in privileged EXEC mode.

**show waas cache http-express metadatabacache** {**all** | **conditional-response** | **redirect-response** | **unauthorized-response**}

Syntax Description	all	Displays all types of metadata caches.
	<b>conditional-response</b>	Displays conditional-response metadata cache entries.
	<b>redirect-response</b>	Displays redirect-response metadata cache entries.
	<b>unauthorized-response</b>	Displays unauthorized-response metadata cache entries.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	15.2(3)T	This command was introduced.

### Examples

The following is sample output from the **show waas cache http-express metadatabacache all** command:

```
Device# show waas cache http-express metadatabacache all

Redirect cache
Active HTTP entries: 0, Active HTTPS entries: 0 Max Entries: 400

Conditional cache
Active HTTP entries: 0, Active HTTPS entries: 0 Max Entries: 2800

Unauthorized cache
Active HTTP entries: 0, Active HTTPS entries: 0 Max Entries: 800
```

The table below describes the fields shown in the display.

**Table 15: show waas cache http-express metadatabacache all Field Descriptions**

Field	Description
<b>Redirect cache</b>	
Active HTTP entries	Displays the number of current HTTP redirect cache entries. The cache entries are also displayed.
Active HTTPS entries	Displays the number of current HTTPS redirect cache entries. The cache entries are not displayed.
Max Entries	Displays the maximum number of redirect cache entries allowed.
<b>Conditional cache</b>	

Field	Description
Active HTTP entries	Displays the number of current HTTP conditional cache entries. The cache entries are also displayed.
Active HTTPS entries	Displays the number of current HTTPS conditional cache entries. The cache entries are not displayed.
Max Entries	Displays the maximum number of conditional cache entries allowed.
<b>Unauthorized cache</b>	
Active HTTP entries	Displays the number of current HTTP unauthorized cache entries. The cache entries are also displayed.
Active HTTPS entries	Displays the number of current HTTPS unauthorized cache entries. The cache entries are not displayed.
Max Entries	Displays the maximum number of unauthorized cache entries allowed.

**Related Commands**

Command	Description
<b>clear waas</b>	Clears information about WAAS Express closed connections, statistics, cache, or tokens.
<b>debug waas</b>	Displays debugging information for different WAAS Express modules.
<b>show waas alarms</b>	Displays WAAS Express status and alarms.
<b>show waas auto-discovery</b>	Displays information about WAAS Express autodiscovery.
<b>show waas statistics aoim</b>	Displays WAAS Express peer information and negotiated capabilities.
<b>show waas statistics application</b>	Displays WAAS Express policy application statistics.
<b>show waas statistics auto-discovery</b>	Displays WAAS Express autodiscovery statistics.
<b>show waas statistics class</b>	Displays statistics for the WAAS Express class map.
<b>show waas statistics dre</b>	Displays WAAS Express DRE statistics.
<b>show waas statistics errors</b>	Displays WAAS Express error statistics.
<b>show waas statistics global</b>	Displays global WAAS Express statistics.
<b>show waas statistics lz</b>	Displays WAAS Express LZ statistics.
<b>show waas statistics pass-through</b>	Displays WAAS Express connections placed in a pass-through mode.
<b>show waas statistics peer</b>	Displays inbound and outbound statistics for peer WAAS Express devices.



<b>Command</b>	<b>Description</b>
<b>show waas status</b>	Displays the status of WAAS Express.
<b>show waas token</b>	Displays the value of the configuration token used by the WAAS Central Manager.
<b>waas cm-register url</b>	Registers a device with the WAAS Central Manager.

## show waas connection

To display the information for a Wide-Area Application Services (WAAS) Express connection, use the **show waas connection** command in privileged EXEC mode.

**show waas connection** [**closed**] [**conn-id** *conn-id*] [**client-ip** *client-ip*] [**client-port** *client-port*] [**server-ip** *server-ip*] [**server-port** *server-port*] [**peer-id** *peer-id*] [{**brief** | **detailed**}]

### Syntax Description

<b>closed</b>	(Optional) Displays the list of closed connections.
<b>conn-id</b> <i>conn-id</i>	(Optional) Displays connection information for the specified connection ID.
<b>client-ip</b> <i>client-ip</i>	(Optional) Displays connection information for the specified client.
<b>client-port</b> <i>client-port</i>	(Optional) Displays connection information for the specified client port.
<b>server-ip</b> <i>server-ip</i>	(Optional) Displays connection information for the specified server.
<b>server-port</b> <i>server-port</i>	(Optional) Displays connection information for the specified server port.
<b>peer-id</b> <i>peer-id</i>	(Optional) Displays connection information for the specified peer.
<b>brief</b>	(Optional) Displays the connection summary.
<b>detailed</b>	(Optional) Displays information in a detailed format.

### Command Default

For each connection, the following information is displayed:

- Connection ID
- Destination IP address and port number
- Negotiated policy
- Peer ID
- Source IP address and port number

### Command Modes

Privileged EXEC (#)

### Command History

Release	Modification
15.1(2)T	This command was introduced.
15.2(3)T	This command was modified. The output was enhanced to display connection details for the following three WAAS Express accelerators: Common Internet File System (CIFS)-Express, Secure Sockets Layer (SSL)-Express, and HTTP-Express.
15.2(4)M	This command was modified. The output was modified to display time in the Coordinated Universal Time (UTC) format.

### Usage Guidelines

Use this command to display the following WAAS Express connection information:

- Client and server information
- Compression used to optimize traffic
- Time when a connection was initiated and closed
- Reason for closing a connection

## Examples

The following is sample output from the **show waas connection** command:

```
Device# show waas connection
```

```
ConnID Source IP:Port      Dest IP:Port      PeerID Accel
1 192.168.20.99:51558 192.168.40.99:80 0021.5586.13df  TLD
```

The following is sample output from the **show waas connection detailed** command:

```
Device# show waas connection detailed
```

```
connection ID:                6
Peer Id:                      0016.9d39.20bd
Connection Type:              External
Start Time:                   03:16:07 UTC Jan 7 2012
Source IP Address:            192.168.22.99
Source Port Number:           43526
Destination IP Address:       192.168.42.99
Destination Port Number:      443
Application Name:             SSL
Classifier Name:               HTTPS
Peer Policy:                   TFO
Configured Policy:             TFO
Negotiated Policy:             TFO, LZ, DRE
Configured Accelerator:        SSL-Express
Derived Accelerator:           SSL-Express
Applied Accelerator:           SSL-Express, HTTP-Express
Hist. Accelerator:             None
Bytes Read Orig:               1905360
Bytes Written Orig:            1054
Bytes Read Opt:                28103
Bytes Written Opt:              56378
Auto-discovery information:
  Orig-St                      E
  Term-St                      EO
TFO information:
  TFO Frames Read:              215
  TFO Frames Written:           232
LZ section

Encode stats
  Bytes in                      265204
  Bytes out                     37421
  Bypass bytes                   8988
  Compression gain                85%
  Avg Latency in Cef              0 usec
  Avg Latency in Proc             722 usec

Decode stats
  Bytes in                       68
  Bytes out                      72
  Bypass bytes                    9642
  Compression gain                 5%
  Avg Latency in Cef              0 usec
```

```

      Avg Latency in Proc          1 usec
DRE section

  Encode stats
    R-tx total                    0
    R-tx chunk-miss               0
    R-tx collision                 0
    Bytes in                      1884160
    Bytes out                     273638
    Bypass bytes                   467
    Compression gain               85%
    Avg latency                    1774 usec

  Decode stats
    Nacks generated               0
    Bytes in                      72
    Bytes out                     25
    Bypass bytes                   0
    Compression gain               0%
    Avg latency                    53 usec
SSL-Express AO section

  LAN Bytes read                  1905360
  LAN Bytes written               1054
  WAN Bytes read                  28103
  WAN Bytes written               58250

  LAN Handshake Bytes read       262
  LAN Handshake Bytes written    932
  WAN Handshake Bytes read       1362
  WAN Handshake Bytes written    340

  C2S version                     SSL 3.0
  W2W version                     TLS 1.0
  C2S cipher                      rsa-with-aes-128-cbc-sha
  W2W cipher                      rsa-with-aes-128-cbc-sha
HTTP-Express AO section

  LAN Bytes read                  1884627
  LAN Bytes written               25
  WAN Bytes read                  25
  WAN Bytes written               1884627

```

The following is sample output from the **show waas connection closed detailed** command:

```

Device# show waas connection closed detailed

connection ID:                    2
Peer Id:                          0016.9d39.2209
Connection Type:                  External
Start Time:                      01:03:54 UTC May 18 2012
End Time:                        01:03:55 UTC May 18 2012
End Reason:                       Closed.
Source IP Address:                192.168.12.99
Source Port Number:               38798
Destination IP Address:           192.168.32.99
Destination Port Number:          8080
Application Name:                 Web
Classifier Name:                   HTTP
Peer Policy:                      TFO, LZ, DRE
Configured Policy:                TFO, LZ, DRE
Negotiated Policy:                TFO, LZ, DRE
Configured Accelerator:           HTTP-Express
Derived Accelerator:              HTTP-Express
Applied Accelerator:              HTTP-Express, SSL-Express

```

```

Hist. Accelerator:           None
Bytes Read Orig:            691
Bytes Written Orig:         1969
Bytes Read Opt:             2910
Bytes Written Opt:          1301
Auto-discovery information:
  Orig-St                   E
  Term-St                   EO
TFO information:
  TFO Frames Read:         4
  TFO Frames Written:      2
  TFO EOT State:          CONN_CLOSE
  TFO EOT:                RS AR RR AS LFR LFS WFR WFS
LZ section

```

```

Encode stats
  Bytes in                  0
  Bytes out                  0
  Bypass bytes              400
  Compression gain          0%
  Avg Latency in Cef        0 usec
  Avg Latency in Proc       13 usec

```

```

Decode stats
  Bytes in                  329
  Bytes out                  393
  Bypass bytes              63
  Compression gain          16%
  Avg Latency in Cef        2 usec
  Avg Latency in Proc       3 usec

```

DRE section

```

Encode stats
  R-tx total                0
  R-tx chunk-miss           0
  R-tx collision            0
  Bytes in                  0
  Bytes out                  0
  Bypass bytes              314
  Compression gain          0%
  Avg latency               0 usec

```

```

Decode stats
  Nacks generated          0
  Bytes in                  399
  Bytes out                  332
  Bypass bytes              0
  Compression gain          0%
  Avg latency               23 usec

```

SSL-Express AO section

```

LAN Bytes read              548
LAN Bytes written           1892
WAN Bytes read              2688
WAN Bytes written           1030

```

```

LAN Handshake Bytes read   314
LAN Handshake Bytes written 1509
WAN Handshake Bytes read   2077
WAN Handshake Bytes written 392

```

```

C2S version                 SSL 3.0
W2W version                 TLS 1.0
C2S cipher                  dhe-rsa-with-aes-256-cbc-sha

```

```

W2W cipher                rsa-with-aes-128-cbc-sha
HTTP-Express AO section

LAN Bytes read            310
LAN Bytes written         328
WAN Bytes read            332
WAN Bytes written         314

```

Table 16: show waas connection Field Descriptions

Field	Description
ConnID	Connection ID.
Source IP:Port	Source IP address and port number.
Dest IP:Port	Destination IP address and port number.
PeerID	Peer ID.
Accel	Type of accelerator(s) used in the connection. Possible values include the following: <ul style="list-style-type: none"> <li>• C—CIFS-Express accelerator</li> <li>• D—Data Redundancy Elimination (DRE)</li> <li>• G—Generic</li> <li>• H—HTTP-Express accelerator</li> <li>• L—Lempel-Ziv (LZ)</li> <li>• S—SSL-Express accelerator</li> <li>• T—Transport Flow Optimization (TFO)</li> </ul>
connection ID	Connection ID.
Peer Id	IP address of a peer.
Connection Type	Type of connection established with a peer.
Start Time	Date and time when a connection was initiated.
End Time	Date and time when a connection was terminated.
Source IP Address	Source IP address.
Source Port Number	Source IP port number.
Destination IP Address	Destination IP address.
Destination Port Number	Destination IP port number.
Application Name	Name of the application traffic on a connection.
Classifier Name	Name of the application classifier on a connection.

Field	Description
Peer Policy	Names of optimization policies that a peer WAAS device requires on a particular connection.
Configured Policy	Names of optimization policies configured on a connection.
Negotiated Policy	Names of optimization policies derived from configured and peer policies.
Configured Accelerator	Accelerators configured locally on a device.
Derived Accelerator	Accelerator derived after negotiation with a peer.
Applied Accelerator	Accelerator applied to the current flow.
Hist. Accelerator	Accelerators historically used.
Bytes Read Orig	Number of bytes received on the unoptimized side (LAN).
Bytes Written Orig	Number of bytes sent on the unoptimized side.
Bytes Read Opt	Number of bytes received on the optimized side (WAN).
Bytes Written Opt	Number of bytes sent on the optimized side (WAN).
<b>Auto-discovery information</b>	
Orig-St	Originating state.
Term-St	Terminating state.
<b>LZ section</b>	Displays LZ compression or decompression statistics.
Encode stats Bytes in Bytes out	Number of bytes encoded using the LZ compression and resulting number of output bytes.
Bypass bytes	Number of bytes that bypassed the LZ module due to low compressibility.
Avg Latency in Cef	Latency, in microseconds, introduced by LZ compression while compressing data in the Cisco Express Forwarding packet path.
Avg Latency in Proc	Latency, in microseconds, introduced by LZ compression while compressing data in the process path.
Decode stats Bytes in Bytes out	Number of bytes decoded using the DRE compression and the resulting number of output bytes.
<b>DRE section</b>	Displays DRE compression or decompression statistics.
R-tx total	Total number of retransmissions.
R-tx chunk-miss	Number of DRE message retransmissions due to missing chunks.

Field	Description
R-tx collision	Number of DRE message retransmissions due to signature collisions.
Avg latency	Average time, in microseconds, taken to compress, send, decompress, and display data using DRE.
Nacks generated	Number of negative acknowledgment (NACK) messages generated.
<b>SSL-Express AO section</b>	Displays SSL-Express accelerator (also known as application optimizer [AO]) optimization statistics.
C2S version	SSL version used on the client-to-server (C2S) connection.
W2W version	SSL version used on the WAN-to-WAN (W2W) connection.
<b>HTTP-Express AO section</b>	Displays HTTP-Express accelerator optimization statistics.

**Related Commands**

Command	Description
<b>clear waas</b>	Clears information about WAAS Express closed connections, statistics, cache, or tokens.
<b>debug waas</b>	Displays debugging information about different WAAS Express modules.
<b>show waas alarms</b>	Displays WAAS Express status and alarms.
<b>show waas auto-discovery</b>	Displays autodiscovery information about the WAAS Express device.
<b>show waas statistics aoim</b>	Displays WAAS Express peer information and negotiated capabilities.
<b>show waas statistics application</b>	Displays WAAS Express policy application statistics.
<b>show waas statistics auto-discovery</b>	Displays autodiscovery statistics for a WAAS Express device.
<b>show waas statistics class</b>	Displays statistical information about the class in WAAS Express.
<b>show waas statistics dre</b>	Displays DRE statistics for a WAAS Express device.
<b>show waas statistics errors</b>	Displays error statistics for a WAAS Express device.
<b>show waas statistics global</b>	Displays global statistics for a WAAS Express device.
<b>show waas statistics lz</b>	Displays LZ statistics for a WAAS Express device.
<b>show waas statistics pass-through</b>	Displays pass-through statistics for a WAAS Express device.



<b>Command</b>	<b>Description</b>
<b>show waas statistics peer</b>	Displays inbound and outbound statistics for peer WAEs devices.
<b>show waas status</b>	Displays the status of WAAS Express.
<b>show waas token</b>	Displays the value of the WAAS Express configuration token.
<b>waas cm-register url</b>	Registers a device with the WAAS Central Manager.

## show waas statistics accelerator

To display statistical information about Wide-Area Application Services (WAAS) Express accelerators, use the **show waas statistics accelerator** command in privileged EXEC mode.

**show waas statistics accelerator** {**cifs-express** [**detail**] | **http-express** [{**debug** | **detail** | **https**}] | **ssl-express** [{**ciphers** | **debug** | **peering**}]}

### Syntax Description

<b>cifs-express</b>	Displays Common Internet File System (CIFS)-Express accelerator statistics.
<b>detail</b>	(Optional) Displays CIFS-Express accelerator statistics in detailed format.
<b>http-express</b>	Displays Hypertext Transfer Protocol (HTTP)-Express accelerator statistics.
<b>debug</b>	(Optional) Displays HTTP-Express accelerator debugging information.
<b>detail</b>	(Optional) Displays HTTP-Express accelerator statistics in detailed format.
<b>https</b>	(Optional) Displays HTTP Secure (HTTPS) statistics.
<b>ssl-express</b>	Displays Secure Sockets Layer (SSL)-Express accelerator statistics.
<b>ciphers</b>	(Optional) Displays a list of ciphers.
<b>debug</b>	(Optional) Displays SSL-Express accelerator debugging information.
<b>peering</b>	(Optional) Displays information about WAAS-to-WAAS sessions.

### Command Modes

Privileged EXEC (#)

### Command History

Release	Modification
15.2(3)T	This command was introduced.
15.2(4)M	This command was modified. The HTTP-Express accelerator <b>debug</b> keyword was added. The output of this command was modified to display time in the Coordinated Universal Time (UTC) format.

### Examples

The following is sample output from the **show waas statistics accelerator cifs-express detail** command:

```
Device# show waas statistics accelerator cifs-express detail

CIFS-Express AO Statistics detail

Parameter                               Value
-----
Time Accelerator was started:            00:58:58 UTC May 18 2012
Time Statistics were Last Reset/Cleared: 00:58:58 UTC May 18 2012
Total Handled Connections:                0
Total Optimized Connections:              0
Total Dropped Connections:                0
Current Active Connections:                0
```

```

Current pipe through connections: 0
Maximum Active Connections: 0
Total LAN bytes read: 0
Total LAN bytes written: 0
Total WAN bytes read: 0
Total WAN bytes written: 0
Messages received from the LAN: 0
Messages sent to the LAN: 0
Messages received from the WAN: 0
Messages sent to the WAN: 0
Disk space query Messages sent to the WAN: 0
Unsupported dialects / CIFS version: 0
Currently active unsupported dialects / CIFS version: 0
Unsupported due to signing: 0
Total Number of Bytes Read by Clients: 0
Total Number of Bytes Written by Clients: 0
Total Number of Bytes Read from File Servers: 0
Total Number of Bytes Written to File Servers: 0
Number of current active commands: 0
    
```

```

Request types          Frequency
-----
CLOSE:                0
OPEN_ANDX:            0
READ_ANDX:            0
WRITE_ANDX:           0
TRANS2:               0
NT_TRANS:             0
TREE_CONNECT:         0
TREE_DISCONNECT:     0
NEGOTIATE:            0
SETUP_ANDX:           0
LOGOFF_ANDX:          0
NT_CREATE_ANDX:      0
WRITE:                0
CANCEL:               0
RENAME:               0
LOCKING_ANDX:         0
SESSION_SETUP WITH TREE_CONNECT: 0
ECHO:                 0
OTHER ANDX:           0
OTHER:                0
    
```

```

Read Ahead:
Parameter          Value
-----
Passed through FIDs: 0
Optimized FIDs:    0
Reads served:      0
  Local replies:   0
  Accelerated replies: 0
  Passed through replies: 0
Read-aheads sent:  0
Served file ranges: 0
No fid:            0
Wrong locking level: 0
Optimization disabled: 0
Optimization disabled (pipeline): 0
Read-ahead processing error: 0
Invalidate LRU cache due to out of buf: 0
Read-ahead responses with NULL fid: 0
Allocates RA buffers: 0
RA buffers pending for delete: 0
    
```

```

Async Write:
Parameter                               Value
-----
Writes served:                           0
  Local replies:                          0
  Not a file:                              0
  No oplock:                               0
  No quota:                                0
  Andx command:                            0
  No tid:                                   0
Outstanding writes:                       0
Async errors:                             0

Negative-Cache:
Parameter                               Value
-----
Current entries:                          0
Entries added:                             0
Entries removed:                           0
ADS opens served:                          0
  Local replies:                           0
  Entry timed out:                          0
  Not in cache:                             0
  Invalidated:                              0
  Flow miss-match:                          0
  Not a file or ADS:                        0

```

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

**Table 17: show waas statistics accelerator cifs-express detail Field Descriptions**

Field	Description
Time Accelerator was started	Time and date stamp when an accelerator (also known as an application optimizer [AO]) was started. The value is updated if the accelerator is restarted.
Time Statistics were Last Reset/Cleared	Time when the statistics were last reset or cleared.
Total Handled Connections	Number of connections handled since an accelerator was started or the statistics were reset.
Total Optimized Connections	Number of connections previously or currently optimized by an accelerator.
Total Connections Handed-off with Compression Policies Unchanged	Number of connections initially accepted by the accelerator but later handed off for generic optimization without policy changes so that currently negotiated policies are used for compression (Data Redundancy Elimination [DRE] or Lempel-Ziv [LZ]).
Total Dropped Connections	Number of connections dropped for reasons other than client or server socket errors.
Current Active Connections	Number of connections currently established on the WAN that are either in use or free for fast connection use.
Maximum Active Connections	Highest number of active connections since the accelerator was last started or restarted.

Field	Description
Total LAN bytes read	Number of bytes read by an accelerator from the original side of the flow.
Total LAN bytes written	Number of bytes written by an accelerator on the original side of the flow.
Total WAN bytes read	Number of bytes read by an accelerator from the optimized side of the flow.
Total WAN bytes written	Number of bytes written by an accelerator on the optimized side of the flow.
Local replies	Number of requests that resulted in the WAAS Express generating a local reply.
Messages received from the LAN	Number of CIFS messages received from the LAN.
Messages sent to the LAN	Number of CIFS messages sent to the LAN.
Messages received from the WAN	Number of CIFS messages received from the WAN.
Messages sent to the WAN	Number of CIFS messages sent to the WAN.
Disk space query Messages sent to the WAN	Number of messages sent over the WAN to query disk space on a remote server.
Unsupported dialects / CIFS version	Number of unsupported dialects of Server Message Block (SMB) or unsupported CIFS version.
Currently active unsupported dialects / CIFS version	Number of unsupported dialects of SMB or unsupported CIFS version in active connections.
Unsupported due to signing	Number of unsupported flows due to SMB packet signing.
<b>Read Ahead Parameter</b>	
Passed through FIDs	Number of file IDs (FIDs) passed through.
Optimized FIDs	Number of FIDs optimized.
Reads served	Number of reads served locally.
Local replies	Number of local replies sent to a client.
Accelerated replies	Number of accelerated replies sent to clients.
Passed through replies	Number of replies passed through to a WAN.
Read-aheads sent	Number of read-ahead requests sent over a WAN.
Served file ranges	Number of nonoverlapping file ranges served.
No fid	Number of read requests received without an FID.

Field	Description
Wrong locking level	Number of read requests received without an opportunistic locking (oplock) level.
Optimization disabled	Number of flows for which optimization is disabled based on the global configuration.
Optimization disabled (pipeline)	Number of flows for which read-ahead optimization is disabled since pipelining was detected.
Read-ahead processing error	Number of error messages generated while processing read requests.
Invalidate LRU cache due to out of buf	Number of least recently used (LRU) cache entries invalidated to make space for new entries in the buffer.
Read-ahead responses with NULL fid	Number of read responses received with a NULL FID.
Allocates RA buffers	Number of read-ahead buffers allocated.
RA buffers pending for delete	Number of read-ahead buffers pending deletion after successfully sending the entire data in buffers.
<b>Async Write Parameter</b>	
Writes served	Number of async writes served.
Local replies	Number of local replies sent to clients.
Not a file	Number of write requests for processing an unknown file in sync mode.
No oplock	Number of write requests received without an oplock level.
No quota	Number of flows not optimized because a disk space quota is not allocated on a remote server.
Andx command	Number of AndX requests received.
No tid	Number of failures that occurred while finding a tree ID (TID).
Async errors	Number of async errors encountered.
<b>Negative-Cache Parameter</b>	
Current entries	Number of entries in the negative cache.
Entries added	Number of entries added to the negative cache.
Entries removed	Number of entries removed from the negative cache.
ADS opens served	Number of alternate-data-stream (ADS) open requests handled.
Entry timed out	Number of timed-out entries in the cache.
Not in cache	Number of cache misses.

Field	Description
Invalidated	Number of invalidated entries in the cache.
Flow miss-match	Number of times that a matching flow ID entry is not found in the cache.
Not a file or ADS	Number of requests that are not in the form of a regular file or an alternate data stream.

**Related Commands**

Command	Description
<b>clear waas</b>	Clears information about WAAS Express closed connections, statistics, cache, or tokens.
<b>debug waas</b>	Displays debugging information about different WAAS Express modules.
<b>show waas accelerator</b>	Displays information about WAAS Express accelerators.
<b>show waas alarms</b>	Displays WAAS Express status and alarms.
<b>show waas auto-discovery</b>	Displays autodiscovery information about the WAAS Express device.
<b>show waas statistics aoim</b>	Displays WAAS Express peer information and negotiated capabilities.
<b>show waas statistics application</b>	Displays WAAS Express policy application statistics.
<b>show waas statistics auto-discovery</b>	Displays autodiscovery statistics for a WAAS Express device.
<b>show waas statistics class</b>	Displays statistical information about the class in WAAS Express.
<b>show waas statistics dre</b>	Displays DRE statistics for a WAAS Express device.
<b>show waas statistics errors</b>	Displays error statistics for a WAAS Express device.
<b>show waas statistics global</b>	Displays global statistics for a WAAS Express device.
<b>show waas statistics lz</b>	Displays LZ statistics for a WAAS Express device.
<b>show waas statistics pass-through</b>	Displays pass-through statistics for a WAAS Express device.
<b>show waas statistics peer</b>	Displays inbound and outbound statistics for peer WAEs devices.
<b>show waas status</b>	Displays the status of WAAS Express.
<b>show waas token</b>	Displays the value of the WAAS Express configuration token.

Command	Description
waas cm-register url	Registers a device with the WAAS Central Manager.



## show waas statistics aoim

To display WAAS Express peer information and negotiated capabilities, use the **show waas statistics aoim** command in privileged EXEC mode.

**show waas statistics aoim**

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	15.1(2)T	This command was introduced.
	15.2(2)T	This command was modified. The command output was updated to display information about HTTP and SSL Application Optimizers (AOs).

**Usage Guidelines** This command displays information about the peer and the negotiations.

### Examples

The following example shows how to display WAAS peer information and negotiated capabilities:

```
Device> enable
Device# show waas statistics aoim

Total number of peer syncs:                1
Current number of peer syncs in progress:  0
Number of peers:                          1
Number of local application optimizations (AO): 3
Number of AO discovery successful:         1
Number of AO discovery failure:           0

Local AO statistics
  Local AO:                                TFO
    Total number of incompatible connections: 0
    Version:                               0.11
    Registered:                            Yes
  Local AO:                                HTTP
    Total number of incompatible connections: 0
    Version:                               1.1
    Registered:                            Yes
  Local AO:                                SSL
    Total number of incompatible connections: 0
    Version:                               1.0
    Registered:                            Yes

Peer AOIM Statistics
Number of Peers:                          1
  Peer:                                    0021.5586.1399
  Peer IP:                                 50.0.0.2
  Peer Expiry Time:                       00:00:04
  Peer Compatible:                         Yes
  Peer active connections:                 0
  Peer Aoim Version:                      1.0
  Peer sync in progress:                   No
  Peer valid:                              Yes
```

```

Peer Software Version:      4.4.0 (b168)
Peer AOs:
  Peer AO:                  TFO
    Compatible:             Yes
    Version:                 0.20
  Peer AO:                  HTTP
    Compatible:             Yes
    Version:                 1.3
  Peer AO:                  SSL
    Compatible:             Yes
    Version:                 1.0

```

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

**Table 18: show waas statistics aoim Field Descriptions**

Field	Description
Total number of peer syncs	Number of times the AO Information Manager (AOIM) on the WAAS device has synchronized with a peer WAAS device.
Current number of peer syncs in progress	Number of currently active peer synchronization is in progress.
Number of peers	Number of known or encountered peer WAAS devices.
Number of local application optimizations (AO)	Number of locally registered AOs on the WAAS device.
Number of AO discovery successful	Number of times AO discovery succeeded on peer WAAS devices.
Number of AO discovery failure	Number of times AO discovery failed on peer WAAS devices. Possible reasons include AO not enabled, AO not running on the peer Wide-area Application Engine (WAE), or license not configured for the AO.
Local AO statistics	
Local AO	Name of the locally registered AO. The possible values include TFO, HTTP, and SSL.
Total number of incompatible connections	Number of times a connection was not passed to the locally registered AO due to software incompatibility with the peer AO after synchronization with the peer WAAS device was complete.
Version	Software version of the locally registered AO.
Registered	Registration status of the locally registered AO.
Number of Peers	Number of peer WAAS devices encountered.
Peer	MAC address of the peer WAAS device, and whether it has been formally registered with the AO information database.
Peer IP	IP address of the primary network interface of the peer WAAS device.
Peer Expiry Time	Time elapsed since the last AOIM negotiation with the peer WAAS device.

Field	Description
Peer Compatible	Compatibility status of the peer WAAS device. The compatibility of the peer WAAS device depends on the TFO version. If the TFO version on the peer WAAS device is incompatible with the local TFO version, the peer is considered incompatible and connections with this peer are not optimized.
Peer active connections	Number of active connections with the peer.
Peer Aoim Version	The AOIM module version on the peer WAAS device negotiated during AOIM handshake.
Peer sync in progress	Indicates whether synchronization with the peer WAAS device is in progress.
Peer valid	Indicates the validity of the entry in the peer table.
Peer Software Version	Software version and build number of IOS WAAS running on the peer WAAS device.
Peer AO	Name of the registered AO on the peer WAAS device. The possible values include TFO, HTTP, and SSL.
Compatible	<p>Compatibility status of the AO on the peer WAAS device with a matching, locally registered AO. Possible values include Y (yes/compatible), N (no/incompatible), and U (unknown). The compatibility status may be unknown if no matching AO is registered locally. The AO compatibility status is discovered during AOIM negotiation.</p> <ul style="list-style-type: none"> <li>• If a peer WAAS device is incompatible (indicated by the Peer Compatible field), connections with the peer are not optimized, even if a peer AO on this peer WAAS device is compatible with a matching, locally registered AO.</li> <li>• If the peer is compatible but a peer AO is not, then the peer AO is not negotiated during autodiscovery. However, connections with the peer are optimized.</li> </ul>
Version	Software version of the registered AO on the peer WAAS device.

**Related Commands**

Command	Description
<b>clear waas</b>	Clears WAAS Express statistics and closed connections information.
<b>debug waas</b>	Displays debugging information for different WAAS Express modules.
<b>show waas alarms</b>	Displays WAAS Express status and alarms.
<b>show waas auto-discovery</b>	Displays autodiscovery information for the WAAS Express device.
<b>show waas connection</b>	Displays WAAS Express connection details.

<b>Command</b>	<b>Description</b>
<b>show waas statistics application</b>	Displays WAAS Express policy application statistics.
<b>show waas statistics auto-discovery</b>	Displays the autodiscovery statistics for a WAAS Express device.
<b>show waas statistics class</b>	Displays statistics information about the class in WAAS Express.
<b>show waas statistics dre</b>	Displays DRE statistics for a WAAS Express device.
<b>show waas statistics errors</b>	Displays error statistics for a WAAS Express device.
<b>show waas statistics global</b>	Displays global statistics for a WAAS Express device.
<b>show waas statistics lz</b>	Displays the LZ compression statistics for a WAAS Express device.
<b>show waas statistics pass-through</b>	Displays the pass-through statistics for a WAAS Express device.
<b>show waas statistics peer</b>	Displays inbound and outbound statistics for peer WAE devices.
<b>show waas status</b>	Displays the status of WAAS Express.
<b>show waas token</b>	Displays the value of WAAS Express configuration token.
<b>waas cm-register url</b>	Registers a device with the WAAS Central Manager.

## show waas statistics application

To display WAAS Express policy application statistics, use the **show waas statistics application** command in privileged EXEC mode.

**show waas statistics application** [**app-name** *app-name*]

<b>Syntax Description</b>	<b>app-name</b> <i>app-name</i> (Optional) Displays statistics for a specific WAAS policy application.
---------------------------	--

**Command Default** Statistics are displayed for all WAAS policy applications.

**Command Modes** Privileged EXEC (#)

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	15.1(2)T	This command was introduced.

**Usage Guidelines** Use this command to display statistical information about the WAAS policies.

**Examples** The following is sample output from the **show waas statistics application** command:

```
Router> enable
Router# show waas statistics application waas-default
Application:      waas-default
TCP Data Volumes
Connection Type   Inbound          Outbound
Opt TCP Plus      5054526          13969693
Orig TCP Plus     35202552         35202552
Opt TCP Only      0                0
Orig TCP Only     0                0
Internal Client   0                0
Internal Server   0                0
TCP Connection Counts
Connection Type   Active           Completed
Opt TCP Plus     0                18
Opt TCP Only     0                0
Internal Client  0                0
Internal Server  0                0
Pass Through Connection Counts
Connection Type   Completed
PT Asymmetric     0
PT Capabilities   0
PT Intermediate   0
PT_Other          0
Connection Reset: 0
Cleared connections 0
```

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

Table 19: show waas statistics application Field Descriptions

Field	Description
Opt TCP Plus Bytes	Inbound/outbound optimized (WAN) TCP bytes.
Opt TCP Plus Packets	Inbound/outbound optimized (WAN) TCP packets.
Orig TCP Plus Bytes	Inbound/outbound originating (LAN) TCP bytes.
Orig TCP Plus Packets	Inbound/outbound originating (LAN) TCP packets.
Opt TCP Only Bytes	Inbound/outbound optimized (WAN) TCP bytes.
Opt TCP Only Packets	Inbound/outbound optimized (WAN) TCP packets.
Orig TCP Only Bytes	Inbound/outbound originating (LAN) TCP bytes.
Orig TCP Only Packets	Inbound/outbound originating (LAN) TCP packets.
Internal Client Bytes	Packets terminating at the router where the router is a client.
Internal Server Bytes	Packets terminating at the router where the router is the server (WCM-NGWO).
Opt TCP Plus	Optimized TCP plus connection count.
Opt TCP Only	Optimized TCP only connection count.
Internal Client	Internal client connection count.
Internal Server	Internal server connection count.
PT Asymmetric	Pass-through asymmetric connection count.
PT Capabilities	Pass-through incompatible connection count.
PT Intermediate	Pass-through intermediate connection count.
PT_Other	Pass-through other connection count.

## Related Commands

Command	Description
<b>clear waas</b>	Clears WAAS Express statistics and closed connections information.
<b>debug waas</b>	Displays debugging information for different WAAS Express modules.
<b>show waas alarms</b>	Displays WAAS Express status and alarms.
<b>show waas auto-discovery</b>	Displays information about WAAS Express autodiscovery.
<b>show waas connection</b>	Displays information about WAAS Express connections.
<b>show waas statistics aoim</b>	Displays WAAS Express peer information and negotiated capabilities.

<b>Command</b>	<b>Description</b>
<b>show waas statistics auto-discovery</b>	Displays WAAS Express autodiscovery statistics.
<b>show waas statistics class</b>	Displays statistics for the WAAS Express class map.
<b>show waas statistics dre</b>	Displays WAAS Express DRE statistics.
<b>show waas statistics errors</b>	Displays WAAS Express error statistics.
<b>show waas statistics global</b>	Displays global WAAS Express statistics.
<b>show waas statistics lz</b>	Displays WAAS Express LZ statistics.
<b>show waas statistics pass-through</b>	Displays WAAS Express connections placed in a pass-through mode.
<b>show waas statistics peer</b>	Displays inbound and outbound statistics for peer WAAS Express devices.
<b>show waas status</b>	Displays the status of WAAS Express.
<b>show waas token</b>	Displays the value of the configuration token used by the WAAS Central Manager.
<b>waas cm-register url</b>	Registers a device with the WAAS Central Manager.

# show waas statistics auto-discovery

To display the autodiscovery statistics for a WAAS Express device, use the **show waas statistics auto-discovery** command in privileged EXEC mode.

**show waas statistics auto-discovery** [**blacklist**]

## Syntax Description

<b>blacklist</b>	(Optional) Displays blocked list tables lookups, size, and the maximum hold time.
------------------	---

## Command Modes

Privileged EXEC (#)

## Command History

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

## Usage Guidelines

Use this command to display statistics for autodiscovery states, success, and failures.

## Examples

The following is sample output from the **show waas statistics auto-discovery** command:

```
Router> enable
Router# show waas statistics auto-discovery
Packets:
Total Sent:          3
Total Received:     3
Ack dropped in synack received state: 0
Non Syn dropped in nostate state: 0
Aoim sync syn-ack drop: 0
Aoim sync ack drop: 0
Auto discovery failure:
Total Failure:      0
Insufficient option space: 0
Invalid connection state: 0
Sequence number override: 0
Connection split failed: 0
Set sequence number failed: 0
Get sequence number failed: 0
Setting BIC failed: 0
External module init failed: 0
Deleting options failed: 0
Set window size failed: 0
AOIM handover failed: 0
AOIM force sync failed: 0
AOIM peer addition failed: 0
AOIM synchronization reset: 0
TFO handover failed: 0
Setting timestamp failed: 0
Setting window scale failed: 0
Setting send window failed: 0
Setting sack failed: 0
Setting keepalive failed: 0
FD association failed: 0
Auto discovery success SYN retransmission:
Zero retransmit: 1
```



```

One retransmit:          0
Two+ retransmit:        0
Auto discovery Miscellaneous:
RST received:           0
SYNs with our device id:      0
Zero device ID:         0
Non standard option length:    0
Replication mode turned on:    0
ADM mode turned on:         0
Capabilities mismatch:      0
Intermediate device:       0
Invalid option content:     0
Version mismatch:          0
Peer AOIM incompatible:     0
Peer AOIM in progress:     0
AOIM peertable full:       0
AOIM multiple sync request passthrough: 0
No peer:                  0
Missing Ack conf:         0

```

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

**Table 20: show waas statistics auto-discovery Field Descriptions**

Field	Description
Packets: Total Sent	Packets sent by autodiscovery.
Total Received	Packets received by autodiscovery.
Ack dropped in synack received state	Acknowledgment packet dropped within an AD state.
Non Syn dropped in nostate state	Nonsynchronization control packet dropped since no synchronization packet has been received.
Aoim sync syn-ack drop	Synchronization and acknowledgment dropped while AOIM synchronization is in progress.
Aoim sync ack drop	Acknowledgment dropped while AOIM synchronization is in progress.
Auto discovery failure: Total Failure	Number of failed flows.
Insufficient option space	Unable to add TCP options.
Invalid connection state	Connection state invalid.
Sequence number override	Sequence numbers out of sync.
Connection split failed	Unable to connect to a proxy.
Set sequence number failed	Sequence number bump failed.
Get sequence number failed	Unable to read sequence number.

Field	Description
Setting BIC failed	Binary Increased Congestion Control (BIC) initialization failure.
External module init failed	Module initialization failure.
Deleting options failed	WAAS Express TCP option deletion failure.
Set window size failed	Window size adjustment failure.
AOIM handover failed	AOIM handover failure.
AOIM force sync failed	AOIM sync failure.
AOIM peer addition failed	AOIM peer could not be added.
TFO handover failed	TFO handover failure.
Setting timestamp failed	Unable to set the time stamp.
Setting window scale failed	Unable to set the windows scale.
Setting send window failed	Unable to set send the window on connection.
Setting sack failed	Unable to set the Selective Acknowledgment (SACK) on connection.
Setting keepalive failed	Failure to initialize keepalive.
FD association failed	Unable to associate file descriptor.
Auto discovery success SYN retransmission: Zero retransmit	Connections optimized for which a single synchronization was received.
One retransmit	Connections optimized for which a retransmitted synchronization was received.
Two+ retransmit	Two or more synchronization retransmissions.
Auto discovery Miscellaneous: RST received	Reset received during autodiscovery.
SYNs with our device id	Indicates synchronization with the WAAS Express device.
Zero device ID	Zero device ID advertised.
Non standard option length	Invalid WAAS Express TCP option.
Replication mode turned on	Connection bypass due to replication mode turned on.
ADM mode turned on	Connection bypass due to directed mode turned on.
Capabilities mismatch	Advertised capability mismatch.

Field	Description
Intermediate device	Intermediate WAAS Express device.
Invalid option content	Invalid WAAS Express TCP option.
Version mismatch	Administrative distance (AD) version mismatch.
Peer AOIM incompatible	Peer AOIM incompatible.
Peer AOIM in progress	Peer AOIM synchronization in progress.
AOIM peertable full	AOIM peer table full.
AOIM multiple sync request passthrough	Pass through requested due to multiple simultaneous AOIM synchronization requests.
No peer	No peer for this connection.
Missing Ack conf	Missing autodiscovery confirmation.

The following is sample output from the **show waas statistics auto-discovery blacklist** command:

```
Router> enable
Router# show waas statistics auto-discovery
  blacklist
Auto-Discovery Blacklist Table Statistics
Operation Status:          1
Total Lookups:             0
Hits:                      0
Miss (Grey Entry):        0
Miss (No Entry):          0
Table Insertions:         0
Total Entries (Free & Used): 1024
Current Free Entries:     1024
Current Used Entries:      0
Peak Used Entries:        0
Oldest Entry Hold Time (sec): 3600
IP Address Retrieval Failure: 0
Unexpected Threshold:     0
```

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

**Table 21: show waas statistics auto-discovery blacklist Field Descriptions**

Field	Description
Operation Status	Indicates whether the blocked list is enabled, which is 1.
Total Lookups	Total number of blocked list lookups.
Hits	The number of blocked list hits.
Miss (Grey Entry)	Hits in the grey list.
Miss (No Entry)	No blocked list found.

Field	Description
Table Insertions	Blocked list insertions.
Total Entries (Free & Used)	Total possible entries.
Current Free Entries	Free entries.
Current Used Entries	Used entries.
Peak Used Entries	Peak used entries.
Oldest Entry Hold Time (sec)	Active entry time period.
IP Address Retrieval Failure	Unable to locate IP address.
Unexpected Threshold	Invalid blocked list threshold.

**Related Commands**

Command	Description
<b>clear waas</b>	Clears WAAS Express statistics and closed connections information.
<b>debug waas</b>	Displays debugging information for different WAAS Express modules.
<b>show waas alarms</b>	Displays WAAS Express status and alarms.
<b>show waas auto-discovery</b>	Displays information about WAAS Express autodiscovery.
<b>show waas connection</b>	Displays information about WAAS Express connections.
<b>show waas statistics aoim</b>	Displays WAAS Express peer information and negotiated capabilities.
<b>show waas statistics application</b>	Displays WAAS Express policy application statistics.
<b>show waas statistics class</b>	Displays statistics for the WAAS Express class map.
<b>show waas statistics dre</b>	Displays WAAS Express DRE statistics.
<b>show waas statistics errors</b>	Displays WAAS Express error statistics.
<b>show waas statistics global</b>	Displays global WAAS Express statistics.
<b>show waas statistics lz</b>	Displays WAAS Express LZ statistics.
<b>show waas statistics pass-through</b>	Displays WAAS Express connections placed in a pass-through mode.
<b>show waas statistics peer</b>	Displays inbound and outbound statistics for peer WAAS Express devices.
<b>show waas status</b>	Displays the status of WAAS Express.
<b>show waas token</b>	Displays the value of the configuration token used by the WAAS Central Manager.
<b>waas cm-register url</b>	Registers a device with the WAAS Central Manager.

## show waas statistics class

To display statistical information about the class in WAAS Express, use the **show waas statistics class** command in privileged EXEC mode.

```
show waas statistics class [class-name class-name]
```

### Syntax Description

<b>class-name</b> <i>class-name</i>	(Optional) Specifies the class-name.
-------------------------------------	--------------------------------------

### Command Modes

Privileged EXEC (#)

### Command History

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

### Usage Guidelines

This command displays statistical information about the class specified in WAAS Express. If a class name is not specified, the command displays the output for all the classes in WAAS Express.

### Examples

The following is sample output from the **show waas statistics class** command:

```
Router> enable
Router# show waas statistics class
Number of Classes :          3
Class                FTP-Control
TCP Data Volumes
Connection Type      Inbound                               Outbound
Opt TCP Plus         0                               0
Orig TCP Plus        0                               0
Opt TCP Only         0                               0
Orig TCP Only        0                               0
Internal Client      0                               0
Internal Server      0                               0
TCP Connection Counts
Connection Type      Active                               Completed
Opt TCP Plus         0                               0
Opt TCP Only         0                               0
Internal Client      0                               0
Internal Server      0                               0
Pass Through Connection Counts
Connection Type      Completed
PT Asymmetric        0
PT Capabilities      11
PT Intermediate      0
PT_Other              0
Connection Reset:    0

Class                waas-default
TCP Data Volumes
Connection Type      Inbound                               Outbound
Opt TCP Plus         0                               0
Orig TCP Plus        0                               0
Opt TCP Only         0                               0
Orig TCP Only        0                               0
```

```

Internal Client      0
Internal Server     0

TCP Connection Counts
Connection Type     Active           Completed
Opt TCP Plus       0                0
Opt TCP Only       0                0
Internal Client    0                0
Internal Server    0                0

Pass Through Connection Counts
Connection Type     Completed
PT Asymmetric      0
PT Capabilities    0
PT Intermediate    0
PT_Other           0
Connection Reset:  0

Class              FTP-Data
TCP Data Volumes
Connection Type     Inbound           Outbound
Opt TCP Plus       722              573
Orig TCP Plus      0                24
Opt TCP Only       0                0
Orig TCP Only      0                0
Internal Client    0                0
Internal Server    0                0

TCP Connection Counts
Connection Type     Active           Completed
Opt TCP Plus       0                4
Opt TCP Only       0                0

```

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

**Table 22: show waas statistics class Field Descriptions**

Field	Description
Class	The class name.
TCP Data Volumes	Indicates the volume of data in terms of connections, optimizations, and so on.
Connection Type	The type of connection.
Opt TCP Plus	Optimized TCP plus connection count.
Orig TCP Plus	Inbound/outbound originating TCP packets.
Opt TCP Only	Optimized TCP only connection count.
Orig TCP Only	Inbound/outbound originating TCP packets.
Internal Client	Internal client connection count.
Internal Server	Internal server connection count.
PT Asymmetric	Pass-through asymmetric connection count.
PT Capabilities	Pass-through incompatible connection count.

Field	Description
PT_Intermediate	Pass-through intermediate connection count.
PT_Other	Pass-through other connection count.

**Related Commands**

Command	Description
<b>clear waas</b>	Clears WAAS Express statistics and closed connections information.
<b>debug waas</b>	Displays debugging information for different WAAS Express modules.
<b>show waas alarms</b>	Displays WAAS Express status and alarms.
<b>show waas auto-discovery</b>	Displays information about WAAS Express autodiscovery.
<b>show waas connection</b>	Displays information about WAAS Express connections.
<b>show waas statistics aoim</b>	Displays WAAS Express peer information and negotiated capabilities.
<b>show waas statistics application</b>	Displays WAAS Express policy application statistics.
<b>show waas statistics auto-discovery</b>	Displays WAAS Express autodiscovery statistics.
<b>show waas statistics dre</b>	Displays WAAS Express DRE statistics.
<b>show waas statistics errors</b>	Displays WAAS Express error statistics.
<b>show waas statistics global</b>	Displays global WAAS Express statistics.
<b>show waas statistics lz</b>	Displays WAAS Express LZ statistics.
<b>show waas statistics pass-through</b>	Displays WAAS Express connections placed in a pass-through mode.
<b>show waas statistics peer</b>	Displays inbound and outbound statistics for peer WAAS Express devices.
<b>show waas status</b>	Displays the status of WAAS Express.
<b>show waas token</b>	Displays the value of the configuration token used by the WAAS Central Manager.
<b>waas cm-register url</b>	Registers a device with the WAAS Central Manager.

## show waas statistics dre

To display WAAS Express Data Redundancy Elimination (DRE) statistics for a WAAS Express device, use the **show waas statistics dre** command in privileged EXEC mode.

**show waas statistics dre [peer]**

### Syntax Description

<b>peer</b>	(Optional) Displays DRE peer statistics.
-------------	--

### Command Modes

Privileged EXEC (#)

### Command History

Release	Modification
15.1(2)T	This command was introduced.
15.2(3)T	This command was modified. The output was enhanced to display upload DRE information.

### Examples

The following is sample output from the **show waas statistics dre** command:

```
Device# show waas statistics dre

DRE Status:                               Enabled
Cache
  Cache Status:                           Ready
  Oldest data age:                         00:07:35
  Total data storage size:                 1468006400
  Total index size:                       11513600
AckQ size:                                 5242880
AckQ in storage:                          0
AckQ full:                                0
AckQ high:                                0
WaitQ size:                               0
WaitQ in storage:                         0
Connections
  Total:                                  24
  Active:                                 0
Encode Statistics
  Dre msgs:                                0
  R-tx total:                              0
  R-tx chunk-miss:                         0
  R-tx collision:                          0
  Bytes in:                                67344
  Bytes out:                                8840
  Bypass bytes:                            35714
  Bytes Matched:                           59355
  Bytes Skipped:                            0
  Compression gain:                        86%
  Average latency:                          2191 usec
Encode Message Size Distribution:
  0-1K   = 4                               %
  1-5K   = 31                              %
  5-15K  = 14                              %
  15-25K = 0                               %
  25-40K = 0                               %
  >40K   = 0                               %
```



```

Decode Statistics
  Dre msgs:                318
  Nacks generated:         0
  Bytes in:                8494760
  Bytes out:              13780812
  Bypass bytes:           35556
  Compression gain:       38%
  Average latency:        1471 usec
  Decode Message Size Distribution:
    0-1K   = 4           %
    1-5K   = 0           %
    5-15K  = 5           %
    15-25K = 9           %
    25-40K = 23          %
    >40K   = 55          %

```

The following is sample output from the **show waas statistics dre peer** command:

```

Device# show waas statistics dre peer

DRE Status:                Enabled

Current number of connected peers    0
Current number of active peers      1

Peer-ID                    0016.9d38.ca1d
Hostname                   WAE2.cisco.com
IP reported from peer      20.0.0.2
Peer version               4.4.0 (b167)

Cache:
  Cache in storage         614017 B
  Age                     21:22:40

AckQ:
  AckQ in storage         0 B

WaitQ:
  WaitQ in storage        756 B
  WaitQ size              0 B

Sync-clock:
  Local-head              457161116 ms
  Local-tail              457438528 ms
  Remote-head             372192000 ms
  Remote-head-safe        4294967296 ms

Encode Statistics
  DRE msgs:                64
  R-tx total:              0
  R-tx chunk-miss:         0
  R-tx collision:          0
  Bytes in:                67344
  Bytes out:               8840
  Bypass bytes:           35714
  Compression gain:       86%

Decode Statistics
  Dre msgs:                14
  Bytes in:                490
  Bytes out:               416
  Bypass bytes:            0
  Compression gain:        0%
  Nacks generated:         0

```

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

Table 23: show waas statistics dre Field Descriptions

Field	Description
Cache	Displays DRE cache statistics.
AckQ size	The maximum size of the DRE ACK queue (AckQ). The AckQ is an internal data structure used by DRE.
AckQ in storage	The current size of the DRE AckQ.
AckQ full	The number of times the DRE AckQ became full.
AckQ high	The number of times the size of DRE AckQ has reached the high water mark.
WaitQ size	The maximum size of the DRE wait queue (WaitQ). The WaitQ is an internal data structure used by DRE.
WaitQ in storage	The current size of the DRE WaitQ.
Connections	Total number of connections completed.
Dre msgs	The number of DRE messages encoded/decoded by DRE.
R-tx total	Total number of retransmissions.
R-tx chunk-miss	Number of DRE message retransmissions due to missing chunks.
R-tx collision	Number of DRE message retransmissions due to signature collisions.
Bytes in Bytes out	Number of bytes encoded/decoded using the DRE compression and the resulting output bytes.
Bypass bytes	Number of bytes bypassed by DRE.
Bytes Matched	Number of bytes that matched the DRE cache.
Bytes Skipped	Number of bytes skipped by DRE encoder due to hints received from accelerators.
Compression gain	The compression gain achieved by DRE. It is calculated by using the following percentage: $(\text{Bytes\_in} \times 100) / (\text{Bytes\_in} + \text{Bytes\_out})$
Average latency	The interval of the number of bytes encoded or decoded using the DRE compression.
Nacks generated	Number of negative acknowledgement (NACK) messages generated.
Message size distribution	Indicates the distribution of messages across bytes in percentages.

Related Commands	Command	Description
	<b>clear waas</b>	Clears WAAS Express statistics and closed connections information.
	<b>debug waas</b>	Displays debugging information for different WAAS Express modules.
	<b>dre upload</b>	Enables DRE in the uplink direction.
	<b>show waas alarms</b>	Displays WAAS Express status and alarms.
	<b>show waas auto-discovery</b>	Displays information about WAAS Express autodiscovery.
	<b>show waas connection</b>	Displays information about WAAS Express connections.
	<b>show waas statistics aoim</b>	Displays WAAS Express peer information and negotiated capabilities.
	<b>show waas statistics application</b>	Displays WAAS Express policy application statistics.
	<b>show waas statistics auto-discovery</b>	Displays WAAS Express autodiscovery statistics.
	<b>show waas statistics class</b>	Displays statistics for the WAAS Express class map.
	<b>show waas statistics errors</b>	Displays WAAS Express error statistics.
	<b>show waas statistics global</b>	Displays global WAAS Express statistics.
	<b>show waas statistics lz</b>	Displays WAAS Express LZ statistics.
	<b>show waas statistics pass-through</b>	Displays WAAS Express connections placed in a pass-through mode.
	<b>show waas statistics peer</b>	Displays inbound and outbound statistics for peer WAAS Express devices.
	<b>show waas status</b>	Displays the status of WAAS Express.
	<b>show waas token</b>	Displays the value of the configuration token used by the WAAS Central Manager.
	<b>waas cm-register url</b>	Registers a device with the WAAS Central Manager.

## show waas statistics errors

To display error statistics for a WAAS Express device, use the **show waas statistics errors** command in privileged EXEC mode.

**show waas statistics errors**

### Syntax Description

This command has no arguments or keywords.

### Command Modes

Privileged EXEC (#)

### Command History

Release	Modification
15.1(2)T	This command was introduced.
15.2(3)T	This command was modified. The output was enhanced to display error statistics for Secure Sockets Layer (SSL)-Express accelerator.

### Examples

The following example shows how to display WAAS Express error statistics:

```
Device# show waas statistics errors

Unexpected EOT message:                0
TFO close failure:                     0
DRE message delayed for transmission:  0
Invalid input for TFO decode:          0
RST ignored because EOT ACK sent:      0
RST ignored because EOT REQ sent:      0
Unknown TCP Control packet received:   0
DRE encode failed:                     0
Connection reset by peer:              0
Connection timed out:                  0
No data to read:                        0
Buffer allocation failed:               0
Error reading input particle:           0
Received control packet when expecting data: 0
Return value not handled:              0
Lock condition:                         0
Out of transmit buffers:                0
Error received from L4F:                0
Error writing data:                      0
Error processing data:                   0
Error processing control packet:         0
Error sending data:                     0
Unable to find peer in table:           0
Flow semaphore acquisition failures:     0
Encryption/decryption failure:          0
Error processing SSL packet:            0
SSL-Express AO failed to allocate packet: 0
SSL-Express AO failed to allocate sub-block: 0
SSL-Express AO received invalid packet:  0
SSL-Express AO vector copy failed:      0
SSL-Express AO invalid record length in LAN-WAN: 0
SSL-Express AO invalid record length in WAN-LAN: 0
SSL-Express AO failed to retrieve sub-block: 0
SSL-Express AO invalid session received on WAN: 0
SSL-Express AO invalid packet in pipe queue: 0
```

```

SSL-Express AO invalid packet in receive queue:      0
SSL-Express AO encountered misbehaving client:      0
SSL-Express AO Packet enqueue to queue failed:      0
SSL-Express AO Connection closed during SSL handshake: 0
SSL-Express AO Connection reset when pending data:  0
SSL-Express AO received invalid protocol in key-packet:0
SSL-Express AO session create failed:               0
SSL-Express AO received invalid SSL record:         0
SSL-Express AO session delete failed:               0
SSL-Express AO failed to load key-packet:           0
SSL-Express AO memory allocation failed:             0
SSL-Express AO W2W handshake failed:                0
SSL-Express AO encountered rehandshake on W2W session: 0
SSL-Express AO W2W session setup failed:            0
SSL-Express AO received invalid module:             0
SSL-Express AO Encrypt/decrypt allocation failures:  0

```

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

**Table 24: show waas statistics errors Field Descriptions**

Field	Description
Unexpected EOT message	Number of messages generated during End of Transmission (EOT) handshake.
TFO close failure	Number of messages generated during failure of Transport Flow Optimization (TFO) to close connection during EOT handshake.
Error reading input particle	Number of error messages generated while reading noncontiguous packets.
Lock condition	Number of messages generated when a client resets a connection while data is pending for that connection.
Error received from L4F	Number of error messages received from Layer 4 forwarding (L4F).
Flow semaphore acquisition failures	Number of messages generated during failure of flow synchronization check logic.
SSL-Express AO vector copy failed	Number of messages generated during failure to copy data from one set of buffers to another set of buffers. Accelerators are also known as application optimizers (AOs).
SSL-Express AO Packet enqueue to queue failed	Number of messages generated during failure to insert packet to a FIFO queue.

#### Related Commands

Command	Description
<b>clear waas</b>	Clears WAAS Express statistics and closed connections information.
<b>debug waas</b>	Displays debugging information for different WAAS Express modules.
<b>show waas alarms</b>	Displays WAAS Express status and alarms.

<b>Command</b>	<b>Description</b>
<b>show waas auto-discovery</b>	Displays information about WAAS Express autodiscovery.
<b>show waas connection</b>	Displays information about WAAS Express connections.
<b>show waas statistics aoim</b>	Displays WAAS Express peer information and negotiated capabilities.
<b>show waas statistics application</b>	Displays WAAS Express policy application statistics.
<b>show waas statistics auto-discovery</b>	Displays WAAS Express autodiscovery statistics.
<b>show waas statistics class</b>	Displays statistics for the WAAS Express class map.
<b>show waas statistics dre</b>	Displays WAAS Express DRE statistics.
<b>show waas statistics global</b>	Displays global WAAS Express statistics.
<b>show waas statistics lz</b>	Displays WAAS Express LZ statistics.
<b>show waas statistics pass-through</b>	Displays WAAS Express connections placed in a pass-through mode.
<b>show waas statistics peer</b>	Displays inbound and outbound statistics for peer WAAS Express devices.
<b>show waas status</b>	Displays the status of WAAS Express.
<b>show waas token</b>	Displays the value of the configuration token used by the WAAS Central Manager.
<b>waas cm-register url</b>	Registers a device with the WAAS Central Manager.

# show waas statistics global

To display global statistics for a WAAS Express device, use the **show waas statistics global** command in privileged EXEC mode.

**show waas statistics global**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
15.1(2)T	This command was introduced.
15.2(3)T	This command was modified. The output was enhanced to display the Cleared Connections field.

## Examples

The following example shows how to display global statistics for a WAAS Express device:

```
Device# show waas statistics global
```

```
TCP Data Volumes
Connection Type      Inbound      Outbound
Opt TCP Plus         0             0
Orig TCP Plus        0             0
Opt TCP Only         244          161
Orig TCP Only        0             0
Internal Client      0             0
Internal Server      0             0
```

```
TCP Connection Counts
Connection Type      Active      Completed
Opt TCP Plus         0           0
Opt TCP Only         0           1
Internal Client      0           0
Internal Server      0           0
```

```
Pass Through Connection Counts
Connection Type      Completed
PT Asymmetric        0
PT Capabilities      0
PT Intermediate      0
PT_Other              0
Connection Reset:   1
Cleared connections  0
```

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

**Table 25: show waas statistics global Field Descriptions**

Field	Description
TCP Data Volumes	Volume of data in terms of connections, optimizations, and so on.

Field	Description
Connection Type	Type of connection.
Opt TCP Plus	Optimized TCP plus connection count.
Orig TCP Plus	Inbound/outbound originating TCP packets.
Opt TCP Only	Optimized TCP-only connection count.
Orig TCP Only	Inbound/outbound originating TCP-only packets.
Internal Client	Internal client connection count.
Internal Server	Internal server connection count.
TCP Connection Counts	Number of TCP connections intercepted by WAAS Express.
Pass Through Connection Counts	Number of connections made to pass through.
PT Asymmetric	Number of connections made to pass through due to asymmetric route detection during the autodiscovery phase.
PT Capabilities	Number of connections made to pass through due to the configured policy on the device.
PT Intermediate	Number of connections made to pass through because this WAAS Express device lies between two other WAAS Express devices that are closer to the client and the server, but farthest from each other in the network.
PT_Other	Number of connections made to pass through due to other reasons. For more details, see the <b>show waas statistics pass-through</b> command output.
Connection Reset	Number of connections reset by the WAAS Express device.
Cleared connections	Number of connections cleared or reset by an administrator using the <b>clear waas connection</b> command.

#### Related Commands

Command	Description
<b>clear waas</b>	Clears WAAS Express statistics and closed connections information.
<b>debug waas</b>	Displays debugging information for different WAAS Express modules.
<b>show waas alarms</b>	Displays WAAS Express status and alarms.
<b>show waas auto-discovery</b>	Displays information about WAAS Express autodiscovery.
<b>show waas connection</b>	Displays information about WAAS Express connections.



<b>Command</b>	<b>Description</b>
<b>show waas statistics aoim</b>	Displays WAAS Express peer information and negotiated capabilities.
<b>show waas statistics application</b>	Displays WAAS Express policy application statistics.
<b>show waas statistics auto-discovery</b>	Displays WAAS Express autodiscovery statistics.
<b>show waas statistics class</b>	Displays statistics for the WAAS Express class map.
<b>show waas statistics dre</b>	Displays WAAS Express DRE statistics.
<b>show waas statistics errors</b>	Displays WAAS Express error statistics.
<b>show waas statistics lz</b>	Displays WAAS Express LZ statistics.
<b>show waas statistics pass-through</b>	Displays WAAS Express connections placed in a pass-through mode.
<b>show waas statistics peer</b>	Displays inbound and outbound statistics for peer WAAS Express devices.
<b>show waas status</b>	Displays the status of WAAS Express.
<b>show waas token</b>	Displays the value of the configuration token used by the WAAS Central Manager.
<b>waas cm-register url</b>	Registers a device with the WAAS Central Manager.

## show waas statistics lz

To display the Lempel-Ziv compression statistics for a WAAS Express device, use the **show waas statistics lz** command in privileged EXEC mode.

**show waas statistics lz**

### Syntax Description

This command has no arguments or keywords.

### Command Modes

Privileged EXEC (#)

### Command History

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

### Examples

The following example shows how to display WAAS Express LZ statistics:

```
Router> enable
Router# show waas statistics lz
LZ Status:          Enabled
Memory used        30328 KB
Connections
  Total:           75
  Active:          0
Encode Statistics
  Bytes in:        0
  Bytes out:       0
  Bypass bytes:    10886
  Compression gain: 0%
  Average latency in CEF path: 0 usec
  Average latency in process path: 293 usec
Decode Statistics
  Bytes in:        25595
  Bytes out:       71977
  Bypass bytes:    776
  Compression gain: 64%
  Average latency in CEF path: 37 usec
  Average latency in process path: 9 usec
```

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

**Table 26: show waas statistics lz Field Descriptions**

Field	Description
Memory used	Memory usage
Connections:	LZ connection statistics
Encode Statistics	Displays the number of bytes encoded using the LZ compression, and the resulting output bytes.
Bypass bytes	Number of bytes that bypassed the LZ module due to low compressibility.

Field	Description
Compression gain	Compression gain achieve by encoding or decoding. This does not include bytes that LZ bypassed.
Average latency in CEF path	The interval, in milliseconds, between bytes encoded using the LZ compression.
Average latency in process path	The interval, in milliseconds, between bytes encoded using the LZ compression.
Decode Statistics	Displays the number of bytes decoded and the resulting output bytes.

**Related Commands**

Command	Description
<b>clear waas</b>	Clears WAAS Express statistics and closed connections information.
<b>debug waas</b>	Displays debugging information for different WAAS Express modules.
<b>show waas alarms</b>	Displays WAAS Express status and alarms.
<b>show waas auto-discovery</b>	Displays information about WAAS Express autodiscovery.
<b>show waas connection</b>	Displays information about WAAS Express connections.
<b>show waas statistics aoim</b>	Displays WAAS Express peer information and negotiated capabilities.
<b>show waas statistics application</b>	Displays WAAS Express policy application statistics.
<b>show waas statistics auto-discovery</b>	Displays WAAS Express autodiscovery statistics.
<b>show waas statistics class</b>	Displays statistics for the WAAS Express class map.
<b>show waas statistics dre</b>	Displays WAAS Express DRE statistics.
<b>show waas statistics errors</b>	Displays WAAS Express error statistics.
<b>show waas statistics global</b>	Displays global WAAS Express statistics.
<b>show waas statistics pass-through</b>	Displays WAAS Express connections placed in a pass-through mode.
<b>show waas statistics peer</b>	Displays inbound and outbound statistics for peer WAAS Express devices.
<b>show waas status</b>	Displays the status of WAAS Express.
<b>show waas token</b>	Displays the value of the configuration token used by the WAAS Central Manager.
<b>waas cm-register url</b>	Registers a device with the WAAS Central Manager.

## show waas statistics pass-through

To display the pass-through statistics for a WAAS Express device, use the **show waas statistics pass-through** command in privileged EXEC mode.

**show waas statistics pass-through**

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC (#)

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

### Examples

The following is sample output from the **show waas statistics pass-through** command:

```
Router> enable
Router# show waas statistics pass-through
Pass Through Statistics:
Overall:                               1
No Peer:                               0
Rejected due to Capabilities:          0
Rejected due to Resources:             0
Interface Application config:          1
Interface Global config:               0
Asymmetric setup:                      0
Peer sync was in progress:             0
IOS WAAS is intermediate router:       0
Internal error:                        0
Other end is in black list:            0
AD version mismatch:                   0
Incompatable AO:                       0
Connection limit exceeded:             0
AOIM peertable full:                   0
AOIM multiple sync request passthrough: 0
Others:                                 0
```

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

**Table 27: show waas statistics pass-through Field Descriptions**

Field	Description
Overall	Overall connection pass-through's.
No Peer	No peer found for the connection.
Rejected due to Capabilities	Pass-through due to mismatch of capabilities.
Rejected due to Resources	Pass-through due to lack of resources.
Interface Application config	Interface application pass-through.

Field	Description
Interface Global config	Global configuration pass-through.
Asymmetric setup	Possible asymmetric setup.
Peer sync was in progress	Pass-through due to AOIM synchronization in progress.
IOS WAAS is intermediate router	Intermediate WAAS Express device.
Internal error	Internal error
Other end is in black list	Blocked list passthrough
AD version mismatch	Autodiscovery version mismatch.
Incomptable AO	Incompatible optimization.
Connection limit exceeded	Connection limited exceeded.
AOIM peertable full	Unable to add more AOIM peers.
AOIM multiple sync request passthrough	Pass through requested due to multiple simultaneous AOIM synchronization requests.
Others	Other conditions.

**Related Commands**

Command	Description
<b>clear waas</b>	Clears WAAS Express statistics and closed connections information.
<b>debug waas</b>	Displays debugging information for different WAAS Express modules.
<b>show waas alarms</b>	Displays WAAS Express status and alarms.
<b>show waas auto-discovery</b>	Displays information about WAAS Express autodiscovery.
<b>show waas connection</b>	Displays information about WAAS Express connections.
<b>show waas statistics aoim</b>	Displays WAAS Express peer information and negotiated capabilities.
<b>show waas statistics application</b>	Displays WAAS Express policy application statistics.
<b>show waas statistics auto-discovery</b>	Displays WAAS Express autodiscovery statistics.
<b>show waas statistics class</b>	Displays statistics for the WAAS Express class map.
<b>show waas statistics dre</b>	Displays WAAS Express DRE statistics.
<b>show waas statistics errors</b>	Displays WAAS Express error statistics.
<b>show waas statistics global</b>	Displays global WAAS Express statistics.

<b>Command</b>	<b>Description</b>
<b>show waas statistics lz</b>	Displays WAAS Express LZ statistics.
<b>show waas statistics peer</b>	Displays inbound and outbound statistics for peer WAAS Express devices.
<b>show waas status</b>	Displays the status of WAAS Express.
<b>show waas token</b>	Displays the value of the configuration token used by the WAAS Central Manager.
<b>waas cm-register url</b>	Registers a device with the WAAS Central Manager.

## show waas statistics peer

To display inbound and outbound statistics for peer Wide-area Application Engines (WAEs) devices, use the **show waas statistics peer** command in privileged EXEC mode.

**show waas statistics peer** [*id peer-id*] [*conn*]

Syntax Description	id <i>peer-id</i>	(Optional) Displays statistics for that peer ID.
	conn	(Optional) Displays current optimized connections to that peer.

**Command Default** Inbound and outbound statistics are displayed for all peer WAE devices. Current optimized connections are not displayed.

**Command Modes** Privileged EXEC (#)

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

**Usage Guidelines** Use this command to display inbound and outbound statistics for all peer WAE devices.

**Examples** The following is sample output from the **show waas statistics peer** command:

```
Router> enable
Router# show waas statistics peer
Number of Peers :          1
Peer:              0021.5586.13df
TCP Data Volumes
Connection Type          Inbound      Outbound
Opt TCP Plus             765708      2698
Orig TCP Plus            335         10486305
Opt TCP Only              0           0
Orig TCP Only            0           0
Internal Client           0           0
Internal Server           0           0
TCP Connection Counts
Connection Type          Active      Completed
Opt TCP Plus             0           2
Opt TCP Only              0           0
Internal Client           0           0
Internal Server           0           0
Pass Through Connection Counts
Connection Type          Completed
PT Asymmetric            0
PT Capabilities           0
PT Intermediate           0
PT_Other                  0
Connection Reset:        1
Connection Closed:       0
```

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

Table 28: show waas statistics peer Field Descriptions

Field	Description
Peer	MAC address of peer
TCP Data Volumes	Indicates the volume of data in terms of connections, optimizations, and so on.
Connection Type	The type of connection.
Opt TCP Plus	Inbound/outbound optimized (WAN) TCP bytes.
Orig TCP Plus	Inbound/outbound originating (LAN) TCP bytes.
Opt TCP Only	Inbound/outbound optimized (WAN) TCP bytes.
Orig TCP Only	Inbound/outbound originating (LAN) TCP bytes.
Internal Client	Packets terminating at the router where the router is a client.
Internal Server	Packets terminating at the router where the router is the server (WCM-NGWO).
Opt TCP Plus	Optimized TCP plus connection count.
Opt TCP Only	Optimized TCP only connection count.
Internal Client	Internal client connection count.
Internal Server	Internal server connection count.
PT Asymmetric	Pass-through asymmetric connection count.
PT Capabilities	Pass-through incompatible connection count.
PT Intermediate	Pass-through intermediate connection count.
PT_Other	Pass-through other connection count.

## Related Commands

Command	Description
<b>clear waas</b>	Clears WAAS Express statistics and closed connections information.
<b>debug waas</b>	Displays debugging information for different WAAS Express modules.
<b>show waas alarms</b>	Displays WAAS Express status and alarms.
<b>show waas auto-discovery</b>	Displays information about WAAS Express autodiscovery.
<b>show waas connection</b>	Displays information about WAAS Express connections.
<b>show waas statistics aoim</b>	Displays WAAS Express peer information and negotiated capabilities.
<b>show waas statistics application</b>	Displays WAAS Express policy application statistics.



<b>Command</b>	<b>Description</b>
<b>show waas statistics auto-discovery</b>	Displays WAAS Express autodiscovery statistics.
<b>show waas statistics class</b>	Displays statistics for the WAAS Express class map.
<b>show waas statistics dre</b>	Displays WAAS Express DRE statistics.
<b>show waas statistics errors</b>	Displays WAAS Express error statistics.
<b>show waas statistics global</b>	Displays global WAAS Express statistics.
<b>show waas statistics lz</b>	Displays WAAS Express LZ statistics.
<b>show waas statistics pass-through</b>	Displays WAAS Express connections placed in a pass-through mode.
<b>show waas status</b>	Displays the status of WAAS Express.
<b>show waas token</b>	Displays the value of the configuration token used by the WAAS Central Manager.
<b>waas cm-register url</b>	Registers a device with the WAAS Central Manager.

## show waas status

To display the status of Wide Area Application Services (WAAS) Express, use the **show waas status** command in privileged EXEC mode.

**show waas status** [**extended**]

### Syntax Description

<b>extended</b>	(Optional) Displays complete status information for WAAS Express in a single request.
-----------------	---

### Command Modes

Privileged EXEC (#)

### Command History

Release	Modification
15.1(2)T	This command was introduced.
15.2(3)T	This command was modified. The output was enhanced to display the status for the following three WAAS Express accelerators: Common Internet File System (CIFS)-Express, Secure Sockets Layer (SSL)-Express, and HTTP-Express.
15.2(4)M3	This command was modified. The <b>extended</b> keyword was added.

### Examples

The following is a sample output from the **show waas status** command. The fields in the output are self-explanatory.

```
Device# show waas status

IOS Version: 15.3(1.12)T
WAAS Express Version: 2.0.0

WAAS Enabled Interface      Policy Map

WAAS Feature License
  License Type:              EvalRightToUse
  Evaluation total period:    8 weeks 4 days
  Evaluation period left:     8 weeks 4 days

DRE Status                  : Disabled
LZ Status                   : Disabled
CIFS-Express AO Status      : Disabled
SSL-Express AO Status       : Disabled
HTTP-Express AO Status      : Disabled

Maximum Flows                : 50
Total Active connections     : 0
Total optimized connections   : 0
```

The possible values for the License Type field include:

- Permanent
- One of the Right to Use (RTU) values: EvalRightToUse or RightToUse

The RTU license is considered to be in evaluation mode for the first 60 days, which is when the License Type field displays the value EvalRightToUse. After 60 days, the RTU license transitions to the value RightToUse.

If the License Type field is RightToUse, the **show waas status** command output does not display the Evaluation total period and Evaluation period left fields.

If the License Type field is EvalRightToUse, the **show waas status** command output also displays the Evaluation total period and Evaluation period left fields.

The following is a sample output from the **show waas status** command with the **extended** keyword. The fields in the output are self-explanatory.

```
Device# show waas status extended

Platform:          Cisco (CISCO3945-CHASSIS)
Hostname:          c3945-5
IOS Version:       15.3(1.12)T
Persistent trustpoint: None
WAAS Express Version: 2.0.0
Device ID:         1cdf.0f58.e400
```

## Related Commands

Command	Description
<b>clear waas</b>	Clears WAAS Express statistics and closed connections information.
<b>debug waas</b>	Displays debugging information for different WAAS Express modules.
<b>show waas alarms</b>	Displays WAAS Express status and alarms.
<b>show waas auto-discovery</b>	Displays information about WAAS Express autodiscovery.
<b>show waas connection</b>	Displays information about WAAS Express connections.
<b>show waas statistics aoim</b>	Displays WAAS Express peer information and negotiated capabilities.
<b>show waas statistics application</b>	Displays WAAS Express policy application statistics.
<b>show waas statistics auto-discovery</b>	Displays WAAS Express autodiscovery statistics.
<b>show waas statistics class</b>	Displays statistics for the WAAS Express class map.
<b>show waas statistics dre</b>	Displays WAAS Express DRE statistics.
<b>show waas statistics errors</b>	Displays WAAS Express error statistics.
<b>show waas statistics global</b>	Displays global WAAS Express statistics.
<b>show waas statistics lz</b>	Displays WAAS Express LZ statistics.
<b>show waas statistics pass-through</b>	Displays WAAS Express connections placed in a pass-through mode.
<b>show waas statistics peer</b>	Displays inbound and outbound statistics for peer WAAS Express devices.

Command	Description
show waas token	Displays the value of the configuration token used by the WAAS Central Manager.

# show waas token

To display the value of the WAAS Express configuration token, use the **show waas alarms** command in privileged EXEC mode.

## show waas token

### Syntax Description

This command has no arguments or keywords.

### Command Modes

Privileged EXEC (#)

### Command History

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

### Usage Guidelines

Use this command to display the values of the WAAS Express configuration token.

### Examples

The following is sample output from the **show waas token** command:

```
Router> enable
Router# show waas token
Config Token: 1292
```

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

**Table 29: show waas token Field Descriptions**

Field	Description
Config Token	Monotonically increasing 32-bit number (unsigned integer).

### Related Commands

Command	Description
<b>clear waas</b>	Clears WAAS Express statistics and closed connections information.
<b>debug waas</b>	Displays debugging information for different WAAS Express modules.
<b>show waas alarms</b>	Displays WAAS Express status and alarms.
<b>show waas auto-discovery</b>	Displays information about WAAS Express autodiscovery.
<b>show waas connection</b>	Displays information about WAAS Express connections.
<b>show waas statistics aaim</b>	Displays WAAS Express peer information and negotiated capabilities.
<b>show waas statistics application</b>	Displays WAAS Express policy application statistics.

<b>Command</b>	<b>Description</b>
<b>show waas statistics auto-discovery</b>	Displays WAAS Express autodiscovery statistics.
<b>show waas statistics class</b>	Displays statistics for the WAAS Express class map.
<b>show waas statistics dre</b>	Displays WAAS Express DRE statistics.
<b>show waas statistics errors</b>	Displays WAAS Express error statistics.
<b>show waas statistics global</b>	Displays global WAAS Express statistics.
<b>show waas statistics lz</b>	Displays WAAS Express LZ statistics.
<b>show waas statistics pass-through</b>	Displays WAAS Express connections placed in a pass-through mode.
<b>show waas statistics peer</b>	Displays inbound and outbound statistics for peer WAAS Express devices.
<b>show waas status</b>	Displays the status of WAAS Express.
<b>waas cm-register url</b>	Registers a device with the WAAS Central Manager.

# show x25 context

To display operating configuration status details of an X.25 link, use the **show x25 context** command in privileged EXEC mode.

**show x25 context** [{**xot** | **interface serial** *number* [**dlci** *number*] | **cmns-interface-type** *number* [**mac** *mac-address*]}]

Syntax Description		
	<b>xot</b>	(Optional) Displays information specific to X.25 over TCP (XOT) contexts.
	<b>interface serial</b> <i>number</i>	(Optional) Specific serial interface.
	<b>dlci</b> <i>number</i>	(Optional) Specific data-link connection identifier (DLCI) link.
	<b>cmns-interface-type</b> <i>number</i>	(Optional) Local Connection Mode Network Service (CMNS) interface type and number. CMNS interface types are Ethernet, Token Ring, and FDDI. The interface numbering scheme depends on the router interface hardware.
	<b>mac</b> <i>mac-address</i>	(Optional) Hardware address of the CMNS interface.

**Command Modes** Privileged EXEC (#)

Command History	Release	Modification
	12.0(3)T	This command was introduced.
	12.1(5)T	This command was modified to display information about X.25 failover.
	12.2(8)T	The <b>xot</b> keyword was added to display information specific to XOT contexts.
	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.

## XOT: Example

The following is sample output from the **show x25 context** command with the **xot** keyword:

```
Router# show x25 context xot

XOT Access-group 2
PROFILE mod128 station DXE/DTE, address 2222, state R1, modulo 128, timer 0
  Defaults: idle VC timeout 0
           input/output window sizes 80/80, packet sizes 256/256
  Timers: T20 180, T21 200, T22 180, T23 180
  RESTARTs 0/0 CALLs 5+0/7+0/0+0 DIAGs 0/0
XOT Access-group 3
station DXE/DTE, address <none>, state R1, modulo 8, timer 0
  Defaults: idle VC timeout 0
           input/output window sizes 2/2, packet sizes 128/128
```

```
Timers: T20 180, T21 200, T22 180, T23 180
RESTARTs 0/0 CALLs 21+0/50+0/0+0 DIAGs 0/0
```

### Serial Interface: Example

The following is sample output from the **show x25 context** command:

```
Router# show x25 context interface serial 1
Serial1 DLCI 20
PROFILE DCE, address <none>, state R1, modulo 8, timer 0
  Defaults: idle VC timeout 0
    input/output window sizes 2/2, packet sizes 128/128
  Timers: T10 60, T11 180, T12 60, T13 60
  Channels: Incoming-only none, Two-way 1-1024, Outgoing-only none
  RESTARTs 1/0 CALLs 0+0/0+0/0+0 DIAGs 0/0
  LAPB DCE, state CONNECT, modulo 8, k 7, N1 12056, N2 20
    T1 3000, T2 0, interface outage (partial T3) 0, T4 0
  VS 7, VR 6, tx NR 6, Remote VR 7, Retransmissions 0
  Queues: U/S frames 0, I frames 0, unack. 0, reTx 0
  IFRAMEs 111/118 RNRs 0/0 REJs 0/0 SABM/Es 14/1 FRMRs 0/0 DISCs 0/0
```

### X.25 Failover: Example

The following is sample output from the **show x25 context** command when the X.25 Failover feature is configured. The “Fail-over delay” field appears when the primary interface has gone down and come back up again. The number of seconds indicates the time remaining until the secondary interface will reset.

```
Router# show x25 context
Serial1 DLCI 33
  PROFILE dxs/DCE, address 3032, state R1, modulo 8, timer 0
    Defaults: idle VC timeout 0
      input/output window sizes 2/2, packet sizes 128/128
    Timers: T20 180, T21 200, T22 180, T23 180
    Channels: Incoming-only none, Two-way 1-4095, Outgoing-only none
    RESTARTs 12/0 CALLs 5+4/0+0/0+0 DIAGs 0/0
    Fail-over delay: 16 seconds remaining on Dialer0
  LAPB dxs/DCE, state CONNECT, modulo 8, k 7, N1 12056, N2 20
    T1 3000, T2 0, interface outage (partial T3) 0, T4 0
  VS 1, VR 1, tx NR 1, Remote VR 1, Retransmissions 0
  Queues: U/S frames 0, I frames 0, unack. 0, reTx 0
  IFRAMEs 97/88 RNRs 0/0 REJs 0/0 SABM/Es 55490/12 FRMRs 186/0 DISCs
```

The following table describes significant fields shown in the displays.

**Table 30: show x25 context Field Descriptions**

Field	Description
XOT Access-group	Number of the XOT access group.
PROFILE	X.25 profile associated with the XOT access group.
address	Address to which the interface is connected.



Field	Description
state	State of the interface. Possible values are as follows: R1-- normal ready state R2--DTE <sup>1</sup> restarting state R3--DCE <sup>2</sup> restarting state If the state is R2 or R3, the interface is awaiting acknowledgment of a Restart packet.
modulo	Modulo packet sequence numbering scheme.
timer	Interface timer value (zero unless the interface state is R2 or R3).
Defaults: idle VC timeout	Inactivity time before clearing the virtual circuit.
input/output window sizes	Default window sizes (in packets) for the interface. The <b>x25 facility</b> interface configuration command can be used to override these default values for the switched virtual circuits originated by the router.
packet sizes	Default maximum packet sizes (in bytes) for the interface. The <b>x25 facility</b> interface configuration command can be used to override these default values for the switched virtual circuits originated by the router.
Timers	Values of the X.25 timers are as follows: T10 through T13 for a DCE device T20 through T23 for a DTE device
Channels	Virtual circuit ranges for this interface.
RESTARTs	Restart packet statistics for the interface using the format Sent/Received.
CALLs	(number of successful calls sent + calls failed)/(calls received + calls failed)/(calls forwarded + calls failed). Calls forwarded are counted as calls sent.
DIAGs	Number of diagnostic messages sent and received.
Fail-over delay	Number of seconds remaining until secondary interface resets.

<sup>1</sup> DTE = data terminal equipment

<sup>2</sup> DCE = data communications equipment

#### Related Commands

Command	Description
<b>show x25 profile</b>	Displays information about configured X.25 profiles.
<b>show x25 vc</b>	Displays information about active X.25 virtual circuits.
<b>x25 profile</b>	Configures an X.25 profile without allocating any hardware-specific information.

## show x25 cug

To display information about all closed user groups (CUGs) or specific CUGs (defined by the local or network CUG number), use the **show x25 cug** command in privileged EXEC mode.

```
show x25 cug {local-cug [number] | network-cug [number]}
```

### Syntax Description

<b>local-cug</b>	Displays CUGs by locally significant CUG identifier.
<i>number</i>	(Optional) Local CUG number (0 to 9999). If you do not specify a CUG number, information for all CUGs will be displayed.
<b>network-cug</b>	Displays CUGs by network-translated CUG identifier.
<i>number</i>	(Optional) Network CUG number (0 to 9999). If you do not specify a CUG number, information for all CUGs will be displayed.

### Command Modes

Privileged EXEC

### Command History

Release	Modification
12.0(7)T	This command was introduced.
12.1(5)T	This command was modified to show information about CUG selection facility suppression.
12.2(13)T	This command was modified to display information about all or specific CUGs configured on terminal lines.
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

You must designate either the local CUG or the network CUG by the choice of keyword. Within that designation you can view all CUGs or a specific CUG defined by its local or network CUG identifier.

### Examples

#### CUG Selection Facility Suppress Option: Example

The following is sample output for the **show x25 cug** command when CUG selection facility is suppressed for all CUGs on serial interface 1/2 and for the preferential CUG on the X.25 profile named "cug".

```
Router# show x25 cug local-cug

X.25 Serial1/2, 2 CUGs subscribed with no public access
CUG selection facility suppressed for all CUGs
local-cug 100 <-> network-cug 10
local-cug 1 <-> network-cug 11
```

```

PROFILE cug, 2 CUGs subscribed with incoming public access
  CUG selection facility suppressed for preferential CUG
  local-cug 0 <-> network-cug 0 , preferential
  local-cug 100 <-> network-cug 100
  local-cug 200 <-> network-cug 200

```

### Local CUG: Example

The following sample output from the **show x25 cug local-cug** command displays information about all local CUGs on configured on the router.

```

Router# show x25 cug local-cug
X.25 Serial1/1, 3 CUGs subscribed with no public access
  local-cug 99 <-> network-cug 9999, no-incoming, preferential
  local-cug 100 <-> network-cug 1000
  local-cug 101 <-> network-cug 1001
PROFILE cugs, 2 CUGs subscribed with with incoming public access
  local-cug 1 <-> network-cug 10, no-outgoing
  local-cug 2 <-> network-cug 20, no-incoming, preferential
Line: 129 aux 0 , 1 CUGs subscribed with outgoing public access
  local-cug 1 <-> network-cug 10
Line: 130 vty 0 , 4 CUGs subscribed with incoming and outgoing public access
  local-cug 1 <-> network-cug 10
  local-cug 50 <-> network-cug 5, preferential
  local-cug 60 <-> network-cug 6, no-incoming
  local-cug 70 <-> network-cug 7, no-outgoing
Line: 131 vty 1 , 1 CUGs subscribed with no public access
  local-cug 1 <-> network-cug 10

```

### Network CUG: Example

The following is sample output from the **show x25 cug network-cug** command specifically for network number 10 showing that local CUG 1 is associated with it.

```

Router# show x25 cug network-cug 10
X.25 Serial1/2, 5 CUGs subscribed with no public access
  network-cug 10 <-> local-cug 1
PROFILE cugs, 2 CUGs subscribed with no public access
  network-cug 10 <-> local-cug 1 , no-outgoing
Line: 129 aux 0 , 1 CUGs subscribed with no public access
  network-cug 10 <-> local-cug 1
Line: 130 vty 0 , 4 CUGs subscribed with incoming and outgoing public access
  network-cug 10 <-> local-cug 1
Line: 131 vty 1 , 1 CUGs subscribed with no public access
  network-cug 10 <-> local-cug 1

```

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

**Table 31: show x25 cug Field Descriptions**

Field	Description
X.25 Serial...	DCE interface with X.25 CUG service subscription.
PROFILE	X.25 profile with X.25 CUG service subscription.
Line	Terminal line with X.25 CUG service subscription.

Field	Description
local-cug	Local CUG details.
network-cug	Network CUG details.
preferential	Identifies which CUG, if any, is preferred. A single CUG listed for an interface is assumed to be preferred.

**Related Commands**

Command	Description
<b>x25 subscribe cug-service</b>	Enables and controls standard CUG behavior on an X.25 DCE interface.
<b>x25 subscribe local-cug</b>	Configures a DCE X.25 interface for a specific CUG subscription.

## show x25 hunt-group

To display hunt groups and view detailed interface statistics and distribution methods, use the **show x25 hunt-group** command in privileged EXEC mode.

```
show x25 hunt-group [name]
```

### Syntax Description

<i>name</i>	(Optional) Displays the specific hunt group named.
-------------	--

### Command Modes

Privileged EXEC

### Command History

Release	Modification
12.0(3)T	This command was introduced.
12.0(5)T	The command output status field was modified to include “unoperational” as a type of interface status.
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 the **clear counters** or the **clear x25** commands in EXEC mode to clear the count of VCs in use in the “status” field and the number of bytes of data transmitted and received in the “traffic” field. Since the “uses” field is a hunt-group-specific counter, it will not be cleared using the **clear counters** or **clear x25** commands. The “uses” field is only cleared at boot time or when the hunt group is defined.

### Examples

The following is sample output from the **show x25 hunt-group** command:

```
Router# show x25 hunt-group

   ID      Type      Target                               uses      status      traffic(out/in)
=====
HG1       rotary   Serial1                             2         next        1158/1691
          Serial2                             2         next        1328/2146
          xot 172.17.125.54                       2         last_used   137/3154
          xot 172.17.125.34                       1         next        137/3154

HG2       vc-count  Serial2                             4         5 VCs       6921/1364
          Serial3                             2         1 VC        70/1259
```

The table below describes significant fields shown in the display.

**Table 32: show x25 hunt-group Field Descriptions**

Field	Description
ID	Hunt group name.

Field	Description
Type	Method of load balancing (rotary or vc-count).
Target	Range of interfaces that a call within the hunt group can go to.
uses	Total number of call attempts (failed plus successful) made to the interface.
status	State of interface at that moment. The status of an interface may be one of the following: <ul style="list-style-type: none"> <li>• next--Interface will be used next for rotary distribution method.</li> <li>• last used--Interface was just used for rotary distribution method.</li> <li>• unavailable--Interface is shutdown.</li> <li>• full--All logical channels on the interface are in use.</li> <li>• # VC--(vc-count only) Number of VCs currently in use on the interface.</li> <li>• unoper--All VCs on the interface are unoperational.</li> </ul>
traffic (out/in)	Number of data bytes transmitted through the interface.

---

**Related Commands**

Command	Description
<b>clear x25</b>	Restarts an X.25 or CMNS service, clears an SVC, or resets a PVC.
<b>x25 hunt-group</b>	Creates and maintains a hunt group.

## show x25 interface

To display information about virtual circuits (VCs) that use an X.25 interface and, optionally, about a specified virtual circuit, use the **show x25 interface EXEC** command.

**show x25 interface** [{*serial number* | *cmns-interface mac mac-address*}]

Syntax Description		
	<i>serial number</i>	(Optional) Keyword <b>serial</b> and number of the serial interface used for X.25.
	<i>cmns-interface mac mac-address</i>	(Optional) Local CMNS interface type and number, plus the MAC address of the remote device. CMNS interface types are Ethernet, Token Ring, or FDDI. The interface numbering scheme depends on the router interface hardware.

### Command Modes

EXEC

### Command History

Release	Modification
11.2	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 Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

### Examples

The following **show x25 interface** sample output displays X.25 information about VCs on serial interface 0:

```
Router# show x25 interface serial 0
SVC 1, State: D1, Interface: Serial0
  Started 00:13:52, last input 00:00:05, output never
  Connects 3334 <-> ip 3.3.3.4
  Call PID ietf, Data PID none
  Window size input: 7, output: 7
  Packet size input: 512, output: 512
  PS: 0 PR: 6 ACK: 1 Remote PR: 0 RCNT: 5 RNR: no
  P/D state timeouts: 0 timer (secs): 0
  data bytes 0/2508 packets 0/54 Resets 0/0 RNRs 0/0 REJs 0/0 INTs 0/0
SVC 32, State: D1, Interface: Serial0.11
  Started 00:16:53, last input 00:00:37, output 00:00:28
  Connects 3334 <-> clns
  Call PID cisco, Data PID none
  Window size input: 7, output: 7
  Packet size input: 512, output: 512
  PS: 5 PR: 4 ACK: 4 Remote PR: 4 RCNT: 0 RNR: no
  P/D state timeouts: 0 timer (secs): 0
  data bytes 378/360 packets 21/20 Resets 0/0 RNRs 0/0 REJs 0/0 INTs 0/0
```

# show x25 map

To display information about configured address maps, use the **show x25 map** command in privileged EXEC mode.

## show x25 map

### Syntax Description

This command has no arguments or keywords.

### Command Modes

Privileged EXEC

### Command History

Release	Modification
10.0	This command was introduced.
12.2(8)T	This command was modified to display record boundary preservation information for address maps.
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

The **show x25 map** command displays information about the following:

- Configured maps (defined by the **x25 map** command)
- Maps implicitly defined by encapsulation permanent virtual circuits (PVCs) (defined by the encapsulating version of the **x25 pvc** command)
- Dynamic maps (from the X.25 Defense Data Network [DDN] or Blacker Front End [BFE] operations)

### Examples

#### Record Boundary Preservation: Examples

The following is sample output of the **show x25 map** command for a router that is configured with record boundary preservation (RBP) using the **x25 pvc rbp remote** command:

```
Router# show x25 map
Serial1/0:-> rbp, destination host 10.0.0.33 port 9999
PVC, 1 VC:1/P
```

The following is sample output of the **show x25 map** command for a router that is configured with RBP using the **x25 map rbp remote** command:

```
Router# show x25 map
Serial3/0:12132 -> rbp, destination host 10.0.0.32 port 9999
permanent, 1 VC:1024
```

The following is sample output of the **show x25 map** command for a router that is configured with RBP using the **x25 pvc rbp local** command:



```
Router# show x25 map
Serial3/0:<- rbp, listening at port 9999
    PVC, 1 VC:2/P
```

The following is sample output of the **show x25 map** command for a router that is configured with RBP using the **x25 map rbp local** command:

```
Router# show x25 map
Serial1/0:12131 <- rbp, listening at port 9999
    permanent, 1 VC:1
```

The table below describes significant fields shown in the display.

**Table 33: show x25 map Field Descriptions for Maps That Use Record Boundary Preservation**

Field	Description
Serial1/0	Interface on which this map is configured.
12131	(For SVCs only) X.121 address of the remote host. If any call user data is configured, it will appear in this field also.
-> rbp	Indicates an outgoing TCP session that is configured to use RBP.
<- rbp	Indicates an incoming TCP session that is configured to use RBP.
destination host 10.0.0.32 port 9999	IP address and port number of the destination host for an outgoing TCP session.
listening at port 9999	Port number on which the router is listening for a TCP connection request for incoming TCP sessions.
permanent	Indicates that the address map was explicitly configured using the <b>x25 map rbp local</b> or <b>x25 rbp remote</b> command.
PVC	Indicates that the address map was created when a PVC was configured using the <b>x25 pvc rbp local</b> or <b>x25 pvc rbp remote</b> command.
1 VC:1	Number of circuits associated with the map, followed by a list of circuit numbers. /P indicates a PVC.

### Typical X.25 Maps: Example

The following is sample output from the **show x25 map** for five maps that were configured with the **x25 map** command:

```
Router# show x25 map
Serial0: X.121 1311001 <--> ip 172.20.170.1
    PERMANENT, BROADCAST, 2 VCS: 3 4
Serial0: X.121 1311005 <--> appletalk 128.1
    PERMANENT
Serial1: X.121 2194441 cud hello <--> pad
    PERMANENT, window size 5 5, accept-reverse, idle 5
Serial1: X.121 1311005 <--> bridge
```

```

PERMANENT, BROADCAST
Serial2: X.121 001003 <--> apollo 1.3,
        appletalk 1.3,
        ip 172.20.1.3,
        decnet 1.3,
        novell 1.0000.0c04.35df,
        vines 00000001:0003,
        xns 1.0000.0c04.35df,
        clns
PERMANENT, NVC 8, 1 VC: 1024

```

The display shows that five maps have been configured for a router: two for serial interface 0, two for serial interface 1, and one for the serial interface 2 (which maps eight protocols to the host).

The table below describes significant fields shown in the display.

**Table 34: show x25 map Field Descriptions for Typical X.25 Maps**

Field	Description
Serial0	Interface on which this map is configured.
X.121 1311001	X.121 address of the mapped encapsulation host.
ip 172.20.170.1	Type and address of the higher-level protocols mapped to the remote host. Bridge maps do not have a higher-level address; all bridge datagrams are sent to the mapped X.121 address. Connectionless Network Service (CLNS) maps refer to a configured neighbor as identified by the X.121 address.
PERMANENT	Address-mapping type that has been configured for the interface in this entry. Possible values include the following: <ul style="list-style-type: none"> <li>• CONSTRUCTED--Derived with the DDN or BFE address conversion scheme.</li> <li>• PERMANENT--Map was entered with the <b>x25 map</b> interface configuration command.</li> <li>• PVC--Map was configured with the <b>x25 pvc</b> interface command.</li> </ul>
BROADCAST	If any options are configured for an address mapping, they are listed; the example shows a map that is configured to forward datagram broadcasts to the mapped host.
2 VCs:	If the map has any active virtual circuits, they are identified.
3 4	Identifies the circuit number of the active virtual circuits. Note that a single protocol virtual circuit can be associated with a multiprotocol map.

## show x25 profile

To view details of X.25 profiles on your router, use the **show x25 profile** command in privileged EXEC mode.

**show x25 profile** [*name*]

### Syntax Description

<i>name</i>	(Optional) Name of X.25 profile.
-------------	----------------------------------

### Command Modes

Privileged EXEC

### Command History

Release	Modification
12.0(3)T	This command was introduced.
12.2(8)T	This command was modified to display the XOT access groups associated with an X.25 profile.
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

When the X.25 profile name is not specified, the output shows all configured profiles for a given interface.

### Examples

The following sample output from the **show x25 profile** command displays details about the X.25 profile called "XOT-DEFAULT":

```
Router# show x25 profile XOT-DEFAULT
X.25 profile name: XOT-DEFAULT
In use by:
  Access-group 2
  Access-group 10
PROFILE dxe/DTE, address 12345, state R/Inactive, modulo 128, timer 0
Defaults: idle VC timeout 0
input/output window sizes 20/20, packet sizes 256/256
Timers: T20 180, T21 200, T22 180, T23 180
Channels: Incoming-only none, Two-way 1-4095, Outgoing-only none
```

The following sample output from the **show x25 profile** command displays all profiles configured on the same interface:

```
Router# show x25 profile
X.25 profile name:NetworkNodeA
Number of references:2
In use by:
  Annex G:Serial1 DLCI 20
  Annex G:Serial1 DLCI 30
PROFILE DCE, address <none>, state R/Inactive, modulo 128, timer 0
Defaults:idle VC timeout 5
input/output window sizes 2/2, packet sizes 128/128
Timers:T10 60, T11 180, T12 60, T13 60
```

```

Channels:Incoming-only none, Two-way 1-128, Outgoing-only none
LAPB DCE, modulo 8, k 7, N1 default, N2 20
T1 3000, T2 0, interface outage (partial T3) 0, T4 0
X.25 profile name:NetworkNodeB
Number of references:1
In use by:
Annex G:Serial1 DLCI 40
PROFILE DTE, address 1111, state R/Inactive, modulo 8, timer 0
Defaults:idle VC timeout 0
input/output window sizes 2/2, packet sizes 128/128
Timers:T20 180, T21 200, T22 180, T23 180
Channels:Incoming-only none, Two-way 1-1024, Outgoing-only none
LAPB DTE, modulo 8, k 7, N1 default, N2 20
T1 3000, T2 0, interface outage (partial T3) 0, T4 0

```

The following table describes significant fields shown in the display.

**Table 35: show x25 profile Field Descriptions**

Field	Description
Number of references	Number of X.25 connections using this profile.
In use by	Shows the interface, XOT access group, and X.25 service using this profile.
address	Address to which interface is connected.
state	State of the interface. Possible values are as follows: R1--normal ready state R2--DTE <sup>3</sup> restarting state R3--DCE <sup>4</sup> restarting state If the state is R2 or R3, the interface is awaiting acknowledgment of a Restart packet.
modulo	Value that determines the packet sequence numbering scheme used.
timer	Interface timer value (zero unless the interface state is R2 or R3).
Defaults: idle VC timeout	Inactivity time before clearing the virtual circuit.
input/output window sizes	Default window sizes (in packets) for the interface. The <b>x25 facility</b> interface configuration command can be used to override these default values for the switched virtual circuits originated by the router.
packet sizes	Default maximum packet sizes (in bytes) for the interface. The <b>x25 facility</b> interface configuration command can be used to override these default values for the switched virtual circuits originated by the router.
Timers	Values of the X.25 timers are as follows: T10 through T13 for a DCE device T20 through T23 for a DTE device
Channels:	Virtual circuit ranges for this interface.

<sup>3</sup> DTE = data terminal equipment

<sup>4</sup> DCE = data communications equipment

Related Commands	Command	Description
	<b>show x25 context</b>	Displays details of an Annex G DLCI link.
	<b>show x25 vc</b>	Displays information about active X.25 virtual circuits.
	<b>x25 profile</b>	Configures an X.25 profile without allocating any hardware-specific information.

# show x25 remote-red



**Note** Effective with Cisco IOS Release 12.2, the **show x25 remote-red** command is not available in Cisco IOS Software.

To display the one-to-one mapping of the host IP addresses and the remote Blacker Front End (BFE) device's IP addresses, use the **show x25 remote-red** command in privileged EXEC mode.

## show x25 remote-red

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC (#)

### Command History

Release	Modification
10.0	This command was introduced.
12.2	This command became unsupported.

### Examples

The following is sample output from the **show x25 remote-red** command:

```
Router# show x25 remote-red
Entry      REMOTE-RED      REMOTE-BLACK    INTERFACE
1          21.0.0.3        21.0.0.7        serial3
2          21.0.0.10       21.0.0.6        serial1
3          21.0.0.24       21.0.0.8        serial3
```

The table below describes significant fields shown in the display.

**Table 36: show x25 remote-red Field Descriptions**

Field	Description
Entry	Address mapping entry.
REMOTE-RED	Host IP address.
REMOTE-BLACK	IP address of the remote BFE device.
INTERFACE	Name of interface through which communication with the remote BFE device will take place.

## show x25 route

To display the X.25 routing table, use the **show x25 route** command in privileged EXEC mode.

**show x25 route**

### Syntax Description

This command has no arguments or keywords.

### Command Modes

Privileged EXEC

### Command History

Release	Modification
10.0	This command was introduced.
12.0(5)T	The <b>dns</b> keyword was added.
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.

### Examples

The following example shows output from the **show x25 route** command:

```
Router# show x25 route
# Match          Substitute          Route To
1 dest ^1311001$      Serial0, 0 uses
2 dest ^1311002$      xot 172.20.170.10
3 dest 444           xot dns \0
4 dest 555           xot dns \0
```

The table below describes significant fields shown in the display.

**Table 37: show x25 route Field Descriptions**

Field	Description
#	Number identifying the entry in the X.25 routing table.
Match	The match criteria and patterns associated with this entry.
Route To	Destination to which the router will forward a call; X.25 destinations identify an interface; CMNS destinations identify an interface and host MAC address; XOT destinations either identify up to six IP addresses (#2), or the <b>x25 route</b> pattern for retrieving up to six IP addresses from the DNS (#3 and #4).

### Related Commands

Command	Description
<b>x25 route</b>	Creates an entry in the X.25 routing table (to be consulted for forwarding incoming calls and for placing outgoing PAD or protocol translation calls).

## show x25 services

To display information pertaining to the X.25 services, use the **show x25 services** command in user EXEC or privileged EXEC mode.

**show x25 services**

### Syntax Description

This command has no arguments or keywords.

### Command Modes

User EXEC  
Privileged EXEC

### Command History

Release	Modification
11.2	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 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

This command is the default form of the **show x25** command.

### Examples

The following is sample output from the **show x25 services** command:

```
Router# show x25 services
X.25 software, Version 3.0.0.
 3 configurations supporting 3 active contexts
 VCs allocated, freed and in use: 7 - 0 = 7
 VCs active and idle: 4, 3
XOT software, Version 2.0.0.
 VCs allocated, freed and in use: 2 - 1 = 1
 connections in-progress: 0 outgoing and 0 incoming
 active VCs: 1, connected to 1 remote hosts
```

### Related Commands

Command	Description
<b>show x25 interface</b>	Displays information about VCs that use an X.25 interface and, optionally, about a specified VC.
<b>show x25 map</b>	Displays information about configured address maps.
<b>show x25 route</b>	Displays the X.25 routing table.
<b>show x25 vc</b>	Displays information about active SVCs and PVCs.



## show x25 vc

To display information about active switched virtual circuits (SVCs) and permanent virtual circuits (PVCs), use the **show x25 vc** command in privileged EXEC mode.

```
show x25 vc [lcn]
```

### Syntax Description

<i>lcn</i>	(Optional) Logical channel number (LCN).
------------	--

### Command Modes

Privileged EXEC

### Command History

Release	Modification
8.3	This command was introduced in a release prior to Release 8.3.
12.2(8)T	This command was modified to display information about record boundary preservation.
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

To examine a particular virtual circuit number, add an LCN argument to the **show x25 vc** command.

This command displays information about virtual circuits (VCs). VCs may be used for a number of purposes, such as the following:

- Encapsulation traffic
- Traffic switched between X.25 services (X.25, Connection-Mode Network Service [CMNS], and X.25 over TCP/IP [XOT])
- PAD traffic
- QLLC traffic

The connectivity information displayed will vary according to the traffic carried by the VC. For multiprotocol circuits, the output varies depending on the number and identity of the protocols mapped to the X.121 address and the encapsulation method selected for the circuit.

### Record Boundary Preservation: Example

The following is sample output of the **show x25 vc** command for a PVC configured with record boundary preservation (RBP):

```
Router# show x25 vc

PVC 2, State:D1, Interface:Serial3/0
  Started 00:08:08, last input 00:00:01, output 00:00:01
  recordsize:1500, connected
```

```

local address 10.0.0.1 port 9999; remote address 10.0.0.5 port 11029
deferred ack:1
Window size input:2, output:2
Packet size input:128, output:128
PS:2 PR:2 ACK:1 Remote PR:2 RCNT:1 RNR:no
P/D state timeouts:0 timer (secs):0
data bytes 8000/8000 packets 80/80 Resets 9/0 RNRs 0/0 REJs 0/0 INTs 0/0

```

The following table describes the fields shown in the sample output that are typical for virtual circuits.

**Table 38: show x25 vc Field Descriptions**

Field	Description
SVC <i>n</i> or PVC <i>n</i>	Identifies the type of virtual circuit (switched or permanent) and its LCN (also called its “virtual circuit number”).
State	State of the virtual circuit (which is independent of the states of other virtual circuits); D1 is the normal ready state. See the International Telecommunication Union Telecommunication Standardization Sector (ITU-T) <sup>5</sup> X.25 Recommendation for a description of virtual circuit states.
Interface	Interface or subinterface on which the virtual circuit is established.
Started	Time elapsed since the virtual circuit was created.
last input	Time of last input.
output	Time of last output.
Connects...<-->..	Traffic-specific connection information. See the tables below for more information.
D-bit permitted	Indicates that the X.25 D-bit (Delivery Confirmation) may be used on this circuit (displayed as needed).
Fast select VC	Indicates that the Fast Select facility was present on the incoming call (displayed as needed).
Reverse charged	Indicates reverse charged virtual circuit (displayed as needed).
Window size	Window sizes for the virtual circuit.
Packet size	Maximum packet sizes for the virtual circuit.
PS	Current send sequence number.
PR	Current receive sequence number.
ACK	Last acknowledged incoming packet.
Remote PR	Last receive sequence number received from the other end of the circuit.
RCNT	Count of unacknowledged input packets.
RNR	State of the Receiver Not Ready flag; this field is true if the network sends a Receiver-not-Ready packet.

Field	Description
Window is closed	This line appears if the router cannot transmit any more packets until the X.25 Layer 3 peer has acknowledged some outstanding packets.
P/D state timeouts	Number of times a supervisory packet (Reset or Clear) has been retransmitted.
Timer	A nonzero time value indicates that a control packet has not been acknowledged yet or that the virtual circuit is being timed for inactivity.
Reassembly	Number of bytes received and held for reassembly. Packets with the M-bit set are reassembled into datagrams for encapsulation virtual circuits; switched X.25 traffic is not reassembled (and is displayed only when values are not zero).
Held Fragments/Packets	Number of X.25 data fragments to transmit to complete an outgoing datagram, and the number of datagram packets waiting for transmission (displayed only when values are not zero).
data bytes <i>m/n</i> packets <i>p/q</i>	Total number of data bytes sent (m), data bytes received (n), data packets sent (p), and data packets received (q) since the circuit was established.
Resets <i>t/r</i>	Total number of reset packets transmitted/received since the circuit was established.
RNRs <i>t/r</i>	Total number of Receiver Not Ready packets transmitted/received since the circuit was established.
REJs <i>t/r</i>	Total number of Reject packets transmitted/received since the circuit was established.
INTs <i>t/r</i>	Total number of Interrupt packets transmitted/received since the circuit was established.

<sup>5</sup> The ITU-T carries out the functions of the former Consultative Committee for International Telegraph and Telephone (CCITT).

The following table describes the fields specific to VCs configured with record boundary preservation.

**Table 39: show x25 vc Field Descriptions for VCs That Use Record Boundary Preservation**

Field	Description
recordsize	Maximum record size for the session.
connected	Connection status.
local address; port	IP address and port number of the local end of the TCP session.
remote address; port	IP address and port number of the remote end of the TCP session.
input queue	Number of inbound X.25 data packets not yet processed. This field appears in the display only when the value is not zero.
record buffer	Number of bytes of X.25 data in the current partial record (not including data packets in the input queue). This field appears in the display only when the value is not zero.

Field	Description
deferred ack	Number of X.25 data packets that have been received and processed but not yet acknowledged. This field appears in the display only when the value is not zero.

### Encapsulated Traffic: Example

The following is sample output of the **show x25 vc** command used on an encapsulated traffic circuit:

```
Router# show x25 vc 1024
SVC 1024, State: D1, Interface: Serial0
Started 0:00:31, last input 0:00:31, output 0:00:31
Connects 170090 <-->
  compressedtcp 172.20.170.90
  ip 172.20.170.90
Call PID multi, Data PID ietf
Reverse charged
Window size input: 2, output: 2
Packet size input: 128, output: 128
PS: 5 PR: 5 ACK: 4 Remote PR: 5 RCNT: 1 RNR: FALSE
Window is closed
P/D state timeouts: 0 Timer (secs): 0
  data bytes 505/505 packets 5/5 Resets 0/0 RNRs 0/0 REJs 0/0 INTs 0/0
```

The following table describes the connection fields specific to encapsulation traffic.

**Table 40: show x25 vc Encapsulation Traffic Field Descriptions**

Field	Description
170090	The X.121 address of the remote host.
ip 172.20.170.90	The higher-level protocol and address values that are mapped to the virtual circuit.
Call PID	Identifies the method used for protocol identification (PID) in the Call User Data (CUD) field. Because PVCs are not set up using a Call packet, this field is not displayed for encapsulation PVCs. The available methods are as follows: <ul style="list-style-type: none"> <li>• cisco--Cisco's traditional method was used to set up a single protocol virtual circuit.</li> <li>• ietf--The IETF's standard RFC 1356 method was used to set up a single protocol virtual circuit.</li> <li>• snap--The IETF's Subnetwork Access Protocol (SNAP) method for IP encapsulation was used.</li> <li>• multi--the IETF's multiprotocol encapsulation method was used.</li> </ul>
Data PID	Identifies the method used for PID when sending datagrams. The available methods are as follows: <ul style="list-style-type: none"> <li>• none--The virtual circuit is a single-protocol virtual circuit; no PID is used.</li> <li>• ietf--The IETF's standard RFC 1356 method for identifying the protocol is used.</li> <li>• snap--The IETF's SNAP method for identifying IP datagrams is used.</li> </ul>

### Locally Switched X.25 Traffic: Example

The following is sample output of the **show x25 vc** command used on a virtual circuit carrying locally switched X.25 traffic:

```
Router# show x25 vc
PVC 1, State: D1, Interface: Serial2
  Started 0:01:26, last input never, output never
  PVC <--> Serial1 PVC 1, connected
  Window size input: 2, output: 2
  Packet size input: 128, output: 128
  PS: 0 PR: 0 ACK: 0 Remote PR: 0 RCNT: 0 RNR: FALSE
  P/D state timeouts: 0 Timer (secs): 0
  data bytes 0/0 packets 0/0 Resets 0/0 RNRs 0/0 REJs 0/0 INTs 0/0
SVC 5, State: D1, Interface: Serial2
  Started 0:00:16, last input 0:00:15, output 0:00:15
  Connects 170093 <--> 170090 from Serial1 VC 5
  Window size input: 2, output: 2
  Packet size input: 128, output: 128
  PS: 5 PR: 5 ACK: 4 Remote PR: 5 RCNT: 1 RNR: FALSE
  P/D state timeouts: 0 Timer (secs): 0
  data bytes 505/505 packets 5/5 Resets 0/0 RNRs 0/0 REJs 0/0 INTs 0/0
```

The following table describes the connection fields for virtual circuits carrying locally switched X.25 traffic.

**Table 41: show x25 vc Local Traffic Field Descriptions**

Field	Description
PVC <-->	Indicates a switched connection between two PVCs.
Serial1 PVC 1	Identifies the other half of a local PVC connection.
connected	Identifies connection status for a switched connection between two PVCs. See the final table below for PVC status messages.
170093	Identifies the Calling (source) Address of the connection. If a Calling Address Extension was encoded in the call facilities, it is also displayed. If the source host is a CMNS host, its MAC address is also displayed.
170090	Identifies the Called (destination) Address of the connection. If a Called Address Extension was encoded in the call facilities, it is also displayed. If the destination host is a CMNS host, its MAC address is also displayed.
from Serial1	Indicates the direction of the call and the connecting interface.
VC 5	Identifies the circuit type and LCN for the connecting interface. VC indicates an SVC, and PVC indicates a PVC. If the connecting host is a CMNS host, its MAC address is also displayed.

### X.25 Traffic Locally Switched Between PVCs and SVCs: Example

The following is sample output of the **show x25 vc** command used on a virtual circuit carrying locally switched PVC-to-SVC X.25 traffic:

```
Router# show x25 vc
```

```

PVC 5, State: D1, Interface: Serial0
  Started 4d21h, last input 00:00:14, output 00:00:14
  Connects 101600 <--> 201700 from Serial2 VC 700
  D-bit permitted
  Window size input: 2, output: 2
  Packet size input: 128, output: 128
  PS: 5 PR: 5 ACK: 4 Remote PR: 5 RCNT: 1 RNR: no
  P/D state timeouts: 0 timer (secs): 0
  data bytes 1000/1000 packets 10/10 Resets 1/0 RNRs 0/0 REJs 0/0 INTs 0/0
SVC 700, State: D1, Interface: Serial2
  Started 00:00:16, last input 00:00:16, output 00:00:16
  Connects 101600 <--> 201700 from Serial0 PVC 5
  Window size input: 2, output: 2
  Packet size input: 128, output: 128
  PS: 5 PR: 5 ACK: 5 Remote PR: 4 RCNT: 0 RNR: no
  P/D state timeouts: 0 timer (secs): 103
  data bytes 500/500 packets 5/5 Resets 0/0 RNRs 0/0 REJs 0/0 INTs 0/0

```

The following table describes the connection fields for virtual circuits carrying locally switched X.25 traffic between PVCs and SVCs.

**Table 42: show x25 vc Locally Switched PVC-to-SVC Traffic Field Descriptions**

Field	Description
101600	Identifies the Calling (source) Address of the connection. If a Calling Address Extension was encoded in the call facilities, it is also displayed. If the source host is a CMNS host, its MAC address is also displayed.
201700	Identifies the Called (destination) Address of the connection. If a Called Address Extension was encoded in the call facilities, it is also displayed. If the destination host is a CMNS host, its MAC address is also displayed.
from Serial2	Indicates the direction of the call and the connecting interface.
VC 700	Identifies the circuit type and LCN for the connecting interface. VC indicates an SVC and PVC indicates a PVC. If the remote host is a CMNS host, its MAC address is also displayed.

### Remotely Switched X.25 Traffic: Example

The following is sample output from the **show x25 vc** command used on a virtual circuit carrying remotely switched X.25 traffic:

```

Router# show x25 vc
PVC 2, State: D1, Interface: Serial2
  Started 0:01:25, last input never, output never
  PVC <--> [172.20.165.92] Serial2/0 PVC 1 connected
  XOT between 172.20.165.95, 1998 and 172.20.165.92, 27801
  Window size input: 2, output: 2
  Packet size input: 128, output: 128
  PS: 0 PR: 0 ACK: 0 Remote PR: 0 RCNT: 0 RNR: FALSE
  P/D state timeouts: 0 Timer (secs): 0 Reassembly (bytes): 0
  Held Fragments/Packets: 0/0
  data bytes 0/0 packets 0/0 Resets 0/0 RNRs 0/0 REJs 0/0 INTs 0/0
SVC 6, State: D1, Interface: Serial2
  Started 0:00:04, last input 0:00:04, output 0:00:04
  Connects 170093 <--> 170090 from
  XOT between 172.20.165.91, 1998 and 172.20.165.92, 27896
  Window size input: 2, output: 2

```

```

Packet size input: 128, output: 128
PS: 5 PR: 5 ACK: 4 Remote PR: 5 RCNT: 1 RNR: FALSE
P/D state timeouts: 0 Timer (secs): 0 Reassembly (bytes): 0
Held Fragments/Packets: 0/0
data bytes 505/505 packets 5/5 Resets 0/0 RNRs 0/0 REJs 0/0 INTs 0/0

```

The following table describes the connection fields for virtual circuits carrying remotely switched X.25 traffic.

**Table 43: show x25 vc Remote X.25 Traffic Field Descriptions**

Field	Description
PVC	Flags PVC information.
[172.20.165.92]	Indicates the IP address of the router remotely connecting the PVC.
Serial 2/0 PVC 1	Identifies the remote interface and PVC number.
connected	Identifies connection status for a switched connection between two PVCs. See the table below for PVC status messages.
170093	Identifies the Calling (source) Address of the connection. If a Calling Address Extension was encoded in the call facilities, it is also displayed.
170090	Identifies the Called (destination) Address of the connection. If a Called Address Extension was encoded in the call facilities, it is also displayed.
from	Indicates the direction of the call.
XOT between...	Identifies the IP addresses and port numbers of the X.25-over-TCP (XOT) connection.

The following table lists the PVC states that can be reported. These states are also reported by the **debug x25** command in PVC-SETUP packets (for remote PVCs only). Some states apply only to remotely switched PVCs.

**Table 44: X.25 PVC Status Messages**

Status Message	Description
awaiting PVC-SETUP reply	A remote PVC has initiated an XOT TCP connection and is waiting for a reply to the setup message.
can't support flow control values	The window sizes or packet sizes of the PVC cannot be supported by one of its two interfaces.
connected	The PVC is up.
dest. disconnected	The other end has disconnected the PVC.
dest interface is not up	The target interface's X.25 service is down.
dest PVC config mismatch	The targeted PVC is already connected.
mismatched flow control values	The configured flow control values do not match.

Status Message	Description
no such dest. interface	The remote destination interface was reported to be in error by the remote router.
no such dest. PVC	The targeted PVC does not exist.
non-X.25 dest. interface	The target interface is not configured for X.25.
PVC/TCP connect timed out	A remote PVC XOT TCP connection attempt timed out.
PVC/TCP connection refused	A remote PVC XOT TCP connection was tried and refused.
PVC/TCP routing error	A remote PVC XOT TCP connection routing error was reported.
trying to connect via TCP	A remote PVC XOT TCP connection is established and is in the process of connecting.
waiting to connect	The PVC is waiting to be processed for connecting.



## show x25 xot

To display information for all X.25 over TCP (XOT) virtual circuits that match a given criterion, use the **show x25 xot** command in privileged EXEC mode.

```
show x25 xot [local ip-address [port port]] [{remote ip-address [port port] | access-group
[access-group-number]}]
```

Syntax Description		
<b>local</b> <i>ip-address</i> <b>port</b> <i>port</i>	(Optional) Local IP address and optional port number.	
<b>remote</b> <i>ip-address</i> <b>port</b> <i>port</i>	(Optional) Remote IP address and optional port number.	
<b>access-group</b>	(Optional) Displays configuration information about XOT access groups.	
<i>access-group-number</i>	(Optional) Displays configuration information about a specific XOT access group.	

### Command Modes

Privileged EXEC

### Command History

Release	Modification
11.2	This command was introduced.
12.2(8)T	Access group options were added.
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.

### Examples

The following **show x25 xot** sample output displays information about all XOT virtual circuits:

```
Router# show x25 xot
SVC 11, State: D1, Interface: [10.2.2.2,1998/10.2.2.1,11002]
  Started 00:00:08, last input 00:00:08, output 00:00:08
  Line: 0 con 0 Location: Host: 5678
  111 connected to 5678 PAD <--> XOT 2.2.2.2,1998
  Window size input: 2, output: 2
  Packet size input: 128, output: 128
  PS: 2 PR: 3 ACK: 3 Remote PR: 2 RCNT: 0 RNR: no
  P/D state timeouts: 0 timer (secs): 0
  data bytes 54/18 packets 2/3 Resets 0/0 RNRs 0/0 REJs 0/0 INTs 0/0\
```

The following example shows sample output for the **show x25 xot** command with the **access-group** keyword:

```
Router# show x25 xot access-group
xot access-group 1 using built-in default configuration
xot access-group 10 using x.25 profile ocean
xot access-group 55 using x.25 profile river
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>show x25 interface</b>	Displays information about VCs that use an X.25 interface and, optionally, about a specified VC.
<b>show x25 services</b>	Displays information pertaining to the X.25 services.

## show x28 hunt-group

To display the members and status of each member in an X.28 hunt group, use the **show x28 hunt-group** command in user EXEC or privileged EXEC mode.

```
show x28 hunt-group [group-num]
```

<b>Syntax Description</b>	<i>group-num</i> (Optional) Identification number of a particular hunt group.
---------------------------	---

**Command Default** The members of all X.28 hunt groups in the router are displayed.

**Command Modes**  
User EXEC  
Privileged EXEC

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.3(11)YN	This command was introduced.
	12.4(4)T	This command was integrated into Cisco IOS Release 12.4(4)T.

### Examples

The following example displays the configuration of four hunt (“rotary”) groups and the current status of their member lines:

```
Router# show x28 hunt-group

ID Type  HG-Address  TTy      Address  Uses  status
=====
 1  RRA    23456   97      34567  2     INUSE
      98     12345   0       NXTUSE
      100    -      0     INUSEO
      102    456789  0       IDLE
 2  QBR,FIF -      99      -      0     UNAVL
 3  QUE,FIF -      101     -      0     NXTUSE
 4  FIF    56789   103    67890  0     UNAVL
      104    789012  0       UNAVL
```

**Table 45: show x28 hunt-group Field Descriptions**

<b>Field</b>	<b>Description</b>
ID	The identification number of the hunt group.

Field	Description
Type	<p>The line-selection mechanism used within the group:</p> <ul style="list-style-type: none"> <li>• <b>FIF</b> (First Idle First): Lines are searched in increasing order of their line (absolute) number, and the first idle line found is given the incoming call.</li> <li>• <b>RRA</b> (Round-Robin): The incoming call is given to the line whose line number is the next highest from the line that received the last call.</li> <li>• <b>QUE</b> (Queued): If all lines in the group are busy when a call request arrives, that call is queued and given to the first line that frees up. (Not implementable with Multi-PAD X.25 addressing.)</li> <li>• <b>QBR</b> (Queued By Role): Same as “Queued,” except that calls belonging to priority users are placed at the head of the queue. (Not implementable with Multi-PAD X.25 addressing.)</li> </ul>
HG-Address	X.28 address assigned to the hunt group.
TTy	Absolute number of the line.
Address	X.121 address assigned to that line.
Uses	How many calls have been placed on that line.
status	<p>Current status of the line:</p> <ul style="list-style-type: none"> <li>• <b>IDLE</b> : available</li> <li>• <b>NXTUSE</b> : idle and next to be used</li> <li>• <b>INUSE</b> : busy in a PAD call</li> <li>• <b>INUSEO</b> : busy in a non-PAD call</li> <li>• <b>UNAVL</b> : unavailable (either because of inactive modem control signals or because PAD transport is unavailable)</li> </ul>

## show x29 access-lists

To display X.29 access lists, use the **show x29 access-lists** command in user EXEC or privileged EXEC mode.

```
show x29 access-lists [access-list-number]
```

<b>Syntax Description</b>	<i>access-list-number</i> (Optional) Standard x29 access list number. The range is from 0 to 500.
---------------------------	---

**Command Default** If no argument is specified, information for all X.29 access lists is displayed.

**Command Modes**  
 User EXEC (>)  
 Privileged EXEC (#)

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.0	This command was introduced in a release earlier than Cisco IOS Release 12.0.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
	Cisco IOS XE Release 2.1	This command was implemented on the Cisco ASR 1000 series routers.

### Examples

The following is sample output from the **show x29 access-lists** command:

```
Router# show x29 access-lists

X29 access list 10
  permit 192.0.2.0
X29 access list 20
  deny 192.0.2.255
X29 access list 50
  permit 192.0.2.10
```

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

**Table 46: show x29 access-lists Field Descriptions**

<b>Field</b>	<b>Description</b>
X29 access list	Displays the access list number which is configured to be allowed or denied access.
permit	Displays the source IP address of the incoming packet which is permitted to have access to the protocol translator.
deny	Displays the source IP address of the incoming packet which is configured to deny access and clear call requests immediately.

---

**Related Commands**

Command	Description
x29 access-list	Limits access to the access server from certain X.25 hosts.

# show xconnect

To display information about xconnect attachment circuits and pseudowires, use the **show xconnect** command in user EXEC or privileged EXEC mode.

```
show xconnect {{all|interface type number} [detail]|peer ip-address {all|vcid vcid-value} [detail]
|pwmib [peer ip-address vcid-value]}
```

## Cisco IOS SR and S Trains

```
show xconnect {{all|interface type number|memory|rib} [detail] [checkpoint]|peer ip-address
{all|vcid vcid-value} [detail]|pwmib [peer ip-address vcid-value]}
monitor
```

## Cisco uBR10012 Router and Cisco uBR7200 Series Universal Broadband Routers

```
show xconnect {all|peer ip-address {all|vcid vcid-value}|pwmib [peer ip-address vcid-value]}
[detail]
```

### Syntax Description

<b>all</b>	Displays information about all xconnect attachment circuits and pseudowires.
<b>interface</b>	Displays information about xconnect attachment circuits and pseudowires on the specified interface.
<i>type</i>	Interface type. For more information, use the question mark (?) online help function. Valid values for the <i>type</i> argument are as follows: <ul style="list-style-type: none"> <li>• <b>atm number</b>—Displays xconnect information for a specific ATM interface or subinterface.</li> <li>• <b>atm number vp vpi-value</b>—Displays virtual path (VP) xconnect information for a specific ATM virtual path identifier (VPI). The <b>show xconnect atm number vp vpi-value</b> command will not display information about virtual circuit (VC) xconnects using the specified VPI.</li> <li>• <b>atm number vc vpi-value/vci-value</b>—Displays VC xconnect information for a specific ATM VPI and virtual circuit identifier (VCI) combination.</li> <li>• <b>ethernet number</b>—Displays port-mode xconnect information for a specific Ethernet interface or subinterface.</li> <li>• <b>fastethernet number</b>—Displays port-mode xconnect information for a specific Fast Ethernet interface or subinterface.</li> <li>• <b>serial number</b>—Displays xconnect information for a specific serial interface.</li> <li>• <b>serial number dlci-number</b>—Displays xconnect information for a specific Frame Relay data-link connection identifier (DLCI).</li> </ul>
<i>number</i>	Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.
<b>detail</b>	(Optional) Displays detailed information about the specified xconnect attachment circuits and pseudowires.

<b>peer</b>	Displays information about xconnect attachment circuits and pseudowires associated with the specified peer.
<i>ip-address</i>	The IP address of the peer.
<b>all</b>	Displays all xconnect information associated with the specified peer IP address.
<b>vcid</b>	Displays xconnect information associated with the specified peer IP address and the specified VC ID.
<i>vcid-value</i>	The VC ID value.
<b>pwmib</b>	Displays information about the pseudowire MIB.
<b>memory</b>	Displays information about the xconnect memory usage.
<b>rib</b>	Displays information about the pseudowire Routing Information Base (RIB).
<b>checkpoint</b>	(Optional) Displays the autodiscovered pseudowire information that is checkpointed to the standby Route Processor (RP).
<b>monitor</b>	Displays information about xconnect monitor usage for bidirectional forwarding detection (BFD).

### Command Modes

User EXEC (>)

Privileged EXEC (#)

### Command History

Release	Modification
12.0(31)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2(33)SRB	This command was modified. The <b>rib</b> keyword was added.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.4(24)T	This command was modified in a release earlier than Cisco IOS Release 12.4(24)T. The <b>pwmib</b> keyword was added.
12.2(33)SRC	This command was modified in a release earlier than Cisco IOS Release 12.2(33)SRC. The <b>memory</b> keyword was added.
12.2(33)SCC	This command was integrated into Cisco IOS Release 12.2(33)SCC.







### Sample Output for All Xconnect Attachment Circuits and Pseudowires on a Cisco uBR10012 Router in the Brief Display Format in Cisco IOS Release 12.2(33)SCF

The following is sample output from the **show xconnect** command in the brief (default) display format for all xconnect attachment circuits and pseudowires on a Cisco uBR10012 router in Cisco IOS Release 12.2(33)SCF:

```
Router# show xconnect all
```

```
Legend:   XC ST=Xconnect State   S1=Segment1 State   S2=Segment2 State
          UP=Up                 DN=Down             AD=Admin Down       IA=Inactive
          SB=Standby           RV=Recovering       NH=No Hardware
XC ST Segment 1                               S1 Segment 2                               S2
-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
DN   ac   Bu254:55 (DOCSIS)                    DN mpls 10.2.3.4:55                          DN
UP   ac   Bu254:1000 (DOCSIS)                   UP mpls 10.2.3.4:1000                        UP
UP   ac   Bu254:400 (DOCSIS)                    UP mpls 10.76.2.1:400                       UP
DN   ac   Bu254:600 (DOCSIS)                    DN mpls 10.76.2.1:600                       DN
UP   ac   Bu254:1800 (DOCSIS)                   UP mpls 10.76.2.1:1800                      UP
DN   ac   Bu254:45454 (DOCSIS)                  DN mpls 10.76.2.1:45454                     DN
```

### Sample Output for All Xconnect Attachment Circuits and Pseudowires on a Cisco uBR10012 Router in the Detailed Display Format

The following is sample output from the **show xconnect** command in the detailed display format for all xconnect attachment circuits and pseudowires on a Cisco uBR10012 router:

```
Router# show xconnect all detail
```

```
Legend:   XC ST=Xconnect State   S1=Segment1 State   S2=Segment2 State
          UP=Up                 DN=Down             AD=Admin Down       IA=Inactive
          SB=Standby           RV=Recovering       NH=No Hardware
XC ST Segment 1                               S1 Segment 2                               S2
-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
UP   ac   Bu254:2001 (DOCSIS)                    UP mpls 10.76.1.1:2001                          UP
          Interworking: ethernet
          Local VC label 40
          Remote VC label 110
          pw-class:
UP   ac   Bu254:2002 (DOCSIS)                    UP mpls 10.76.1.1:2002                          UP
          Interworking: ethernet
          Local VC label 41
          Remote VC label 88
          pw-class:
UP   ac   Bu254:2004 (DOCSIS)                    UP mpls 10.76.1.1:2004                          UP
          Interworking: ethernet
          Local VC label 42
          Remote VC label 111
          pw-class:
DN   ac   Bu254:22 (DOCSIS)                       UP mpls 101.1.0.2:22                            DN
          Interworking: ethernet
          Local VC label 39
          Remote VC label unassigned
          pw-class:
```



Field	Description
Segment1 or Segment2	Information about the type of xconnect, the interface type, and the IP address the segment is using. The types of xconnects are as follows: <ul style="list-style-type: none"> <li>• ac—Attachment circuit</li> <li>• l2tp—Layer 2 Tunnel Protocol</li> <li>• mpls—Multiprotocol Label Switching</li> <li>• pri ac—Primary attachment circuit</li> <li>• sec ac—Secondary attachment circuit</li> </ul>
S1 or S2	State of the segment. The valid states are: <ul style="list-style-type: none"> <li>• AD—The segment is administratively down.</li> <li>• DN—The segment is down.</li> <li>• HS—The segment is in hot standby mode.</li> <li>• RV—The segment is recovering from a graceful restart.</li> <li>• SB—The segment is in a standby state.</li> <li>• UP—The segment is up.</li> </ul>

The additional fields displayed in the detailed output are self-explanatory.

### VPLS Autodiscovery Feature Example

For the VPLS Autodiscovery feature, issuing the **show xconnect rib** command provides RIB details, as shown in the following example:

```
Router# show xconnect rib

Local Router ID: 10.0.0.0
+- Origin of entry (I=iBGP/e=eBGP)
| +- Imported without a matching route target (Yes/No)?
| | +- Provisioned (Yes/No)?
| | | +- Stale entry (Yes/No)?
| | | |
| | | |
v v v v
O I P S      VPLS-ID      Target ID      Next-Hop      Route-Target
-----+-----+-----+-----+-----
I Y N N      66:66      10.0.0.1      10.1.1.2      66:66
I Y N N      66:66      10.1.1.2      10.1.1.3      66:66
I N Y N      1:1       10.1.1.1      10.1.1.1      2:2
I N Y N      1:1       10.1.1.1      10.1.1.3      2:2
I N Y N
```

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

Table 48: show xconnect rib Field Descriptions

Field	Description
Local Router ID	A unique router identifier. Virtual Private LAN Service (VPLS) Autodiscovery automatically generates a router ID using the MPLS global router ID.
Origin of entry	Origin of the entry. The origin can be “I” for internal Border Gateway Protocol (BGP) or “e” for external BGP.
Imported without a matching route target	Specifies whether the route was imported prior to configuring a route target.
Provisioned	Specifies whether the pseudowire has been provisioned using a learned route.
VPLS/WPWS-ID	Virtual Private LAN Service (VPLS) domain. VPLS Autodiscovery automatically generates a VPLS ID using the BGP autonomous system number and the configured VFI VPN ID.
Target ID	Target ID. The IP address of the destination router.
Next-Hop	IP address of the next hop router.
Route-Target	Route target (RT). VPLS Autodiscovery automatically generates a route target using the lower 6 bytes of the route distinguisher (RD) and VPN ID.

For VPLS Autodiscovery, issuing the **show xconnect rib detail** command provides more information about the routing information base, as shown in the following example:

```
Router# show xconnect rib detail
```

```
Local Router ID: 10.9.9.9
VPLS-ID 10:123, TID 10.7.7.7
  Next-Hop: 10.7.7.7
  Hello-Source: 10.9.9.9
  Route-Target: 10:123
  Incoming RD: 10:10
  Forwarder: vfi VPLS1
  Origin: BGP
  Provisioned: Yes
VPLS-ID 10:123, TID 10.7.7.8
  Next-Hop: 10.7.7.8
  Hello-Source: 10.9.9.9
  Route-Target: 10:123
  Incoming RD: 10:11
  Forwarder: vfi VPLS1
  Origin: BGP
  Provisioned: No
VPLS-ID 10.100.100.100:1234, TID 0.0.0.2
  Next-Hop: 10.2.2.2, 10.3.3.3, 10.4.4.4
  Hello-Source: 10.9.9.9
  Route-Target: 10.111.111.111:12345, 10.8.8.8:345
  Incoming RD: 10:12
  Forwarder: vfi VPLS2
  Origin: BGP
```

```

Provisioned: Yes
VPLS-ID 10.100.100.100:1234, TID 10.13.1.1
Next-Hop: 10.1.1.1
Hello-Source: 10.9.9.9
Route-Target: 10.111.111.111:12345
Incoming RD: 10:13
Forwarder: vfi VPLS2
Origin: BGP
Provisioned: Yes
    
```

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

**Table 49: show xconnect rib detail Field Descriptions**

Field	Description
Hello-Source	Source IP address used when Label Distribution Protocol (LDP) hello messages are sent to the LDP peer for the autodiscovered pseudowire.
Incoming RD	Route distinguisher for the autodiscovered pseudowire.
Forwarder	VFI to which the autodiscovered pseudowire is attached.

### L2VPN VPLS Inter-AS Option B Examples

The following is sample output from the **show xconnect rib** command when used in a Layer 2 Virtual Private Network (L2VPN) VPLS Inter-AS Option B configuration:

```

Router# show xconnect rib

Local Router ID: 10.9.9.9
+- Origin of entry (I=iBGP/e=eBGP)
| +- Provisioned (Yes/No)?
| | +- Stale entry (Yes/No)?
| | |
| | |
v v v
O P S      VPLS-ID      Target ID      Next-Hop      Route-Target
-+-+-----+-----+-----+-----+-----+
I Y N      1:1          10.11.11.11   10.11.11.11   1:1
I Y N      1:1          10.12.12.12   10.12.12.12   1:1
    
```

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

**Table 50: show xconnect rib Field Descriptions**

Field	Description
Local Router ID	A unique router identifier. Virtual Private LAN Service (VPLS) Autodiscovery automatically generates a router ID using the MPLS global router ID.
Origin of entry	Origin of the entry. The origin can be “I” for internal BGP or “e” for external BGP.
Provisioned	Specifies whether the pseudowire has been provisioned using a learned route; Yes or No.
Stale entry	Specifies whether it is a stale entry; Yes or No.

Field	Description
VPLS-ID	VPLS domain. VPLS Autodiscovery automatically generates a VPLS ID using the BGP autonomous system number and the configured VFI VPN ID.
Target ID	IP address of the destination router.
Next-Hop	IP address of the next hop router.
Route-Target	VPLS Autodiscovery automatically generates a route target using the lower 6 bytes of the route distinguisher (RD) and VPN ID.

The following is sample output from the **show xconnect rib detail** command when used in an ASBR configuration. On an ASBR, the **show xconnect rib detail** command displays the Layer 2 VPN BGP network layer reachability information (NLRI) received from the BGP peers. The display also shows the signaling messages received from the targeted LDP sessions for a given target attachment individual identifier (TAII).

```
Router# show xconnect rib detail
```

```
Local Router ID: 10.1.1.3
VPLS-ID: 1:1, Target ID: 10.1.1.1
  Next-Hop: 10.1.1.1
  Hello-Source: 10.1.1.3
  Route-Target: 2:2
  Incoming RD: 10.0.0.0:1
  Forwarder:
  Origin: BGP
  Provisioned: Yes
  SAI1: 10.0.0.1, LDP Peer Id: 10.255.255.255, VC Id: 1001 ***
  SAI2: 10.1.0.1, LDP Peer Id: 10.255.255.255, VC Id: 1002 ***
```

After the passive TPE router receives the BGP information (and before the passive TPE router receives the LDP label), the peer information will be displayed in the output of the **show xconnect rib** command. The peer information will not be displayed in the **show mpls l2transport vc** command because the VFI ATOM xconnect has not yet been provisioned.

Therefore, for passive TPEs, the entry “Passive : Yes” is added to the output from the **show xconnect rib detail** command. In addition, the entry “Provisioned: Yes” is displayed after the neighbor xconnect is successfully created (without any retry attempts).

In the sample output, the two lines beginning with “SAI” show that this ASBR is stitching two provider PE routers (10.0.0.1 and 10.1.0.1) to the TAI 10.1.1.1.

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

**Table 51: show xconnect rib detail (for the ASBR) Field Descriptions**

Field	Description
VPLS-ID	VPLS identifier.
Target ID	IP address of the destination router.
Next-Hop	IP address of the next hop router.



Field	Description
Hello-Source	The source IP address used when LDP hello messages are sent to the LDP peer for the autodiscovered pseudowire.
Route-Target	VPLS Autodiscovery automatically generates a route target using the lower 6 bytes of the route distinguisher (RD) and VPN ID.
Incoming RD	Specifies the route distinguisher for the autodiscovered pseudowire.
Forwarder	The VFI to which the autodiscovered pseudowire is attached.
Origin	Origin of the entry.
Provisioned	Indicates whether the neighbor xconnect was successfully created (without any retry attempts).
SAII	Specifies the source attachment individual identifier.

The following is sample output from the **show xconnect rib checkpoint** command. Autodiscovered pseudowire information is checkpointed to the standby Route Processor (RP). The **show xconnect rib checkpoint** command displays that pseudowire information.

```
Router# show xconnect rib checkpoint
```

```
Xconnect RIB Active RP:
Checkpointing      : Allowed
Checkpointing epoch: 1
ISSU Client id: 2102, Session id: 108, Compatible with peer
Add entries send ok      :      14
Add entries send fail   :        0
Delete entries send ok   :        2
Delete entries send fail:        0
+- Checkpointed to standby          (Yes/No)?
| +- Origin of entry                (I=iBGP/e=eBGP)
| | +- Imported without a matching route target (Yes/No)?
| | |
v v v
C O I      VPLS-ID      Target ID      Next-Hop      Route-Target
-----+-----+-----+-----+-----
N I Y 66:66      10.1.1.1      10.1.1.3      66:66
N I Y 66:66      10.1.1.2      10.1.1.3      66:66
Y I N 1:1        10.1.1.1      10.1.1.1      2:2
Y I N 1:1        10.1.1.1      10.1.1.3      2:2
Y I N 1:1        10.1.1.2      10.1.1.3      2:2
```

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

**Table 52: show xconnect rib checkpoint Field Descriptions**

Field	Description
Checkpointing	Indicates whether checkpointing is allowed.
Checkpointing epoch	Indicates the checkpointing epoch number.
Checkpointed to standby	Indicates whether the autodiscovered pseudowire information is checkpointed to the standby RP.

Field	Description
Origin of entry	Origin of the entry. The origin can be "I" for internal BGP or "e" for external BGP.
Imported without a matching route target	Specifies whether the route was imported prior to configuring a route target.
VPLS-ID	The VPLS identifier.
Target ID	IP address of the destination router.
Next-Hop	IP address of the next hop router.

The following is sample output from the **show xconnect monitor** command.

```
Router# show xconnect monitor
```

```
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0% Time source is hardware calendar,
*21:00:39.098 GMT Fri May 6 2011
```

```
Peer IP          Local IP          State VC Refs
-----
10.1.1.2         10.1.1.1         Up    1
10.1.1.3         10.1.1.1         Up    1
```

**Table 53: show xconnect monitor Field Descriptions**

Field	Description
Peer IP	IP address of the peer. The peer IP address and the Local IP address are the loopback addresses to which a multihop session is associated.
Local IP	Local IP address. The peer IP address and the Local IP address are the loopback addresses to which a multihop session is associated.
State	State of the session.
VC Refs	Number of virtual circuits (VCs) that are tied to the multihop session represented by the peer IP address and the local IP address.



**Note** The following is the expected output for the **show xconnect monitor** command in different scenarios:

- When you remove a Bidirectional Forwarding Detection (BFD) map that associates timers and authentication with multihop templates using the **no bfd map** command, the session state is Down.
- When you unbind a single hop BFD template from an interface using the **no bfd template** command, the session state is Down.
- When you shut down the AC circuit, the session state is Up.
- When you disable pseudowire fast-failure detection using the **no monitor peer bfd** command, the VC entry associated with the pseudowire class in the **show xconnect monitor** command output is removed. If multiple VCs are present for a session, the VC Refs field of the command output shows the decrement in the number of VCs. The session state is Down for that VC.

#### Related Commands

Command	Description
<b>show atm pvc</b>	Displays all ATM PVCs and traffic information.
<b>show atm vc</b>	Displays all ATM PVCs and SVCs and traffic information.
<b>show atm vp</b>	Displays the statistics for all VPs on an interface or for a specific VP.
<b>show connect</b>	Displays configuration information about drop-and-insert connections that have been configured on a router.
<b>show frame-relay pvc</b>	Displays statistics about PVCs for Frame Relay interfaces.
<b>show interfaces</b>	Displays statistics for all interfaces configured on the router or access server.
<b>show l2tun session</b>	Displays the current state of Layer 2 sessions and protocol information about L2TP control channels.
<b>show mpls l2transport binding</b>	Displays VC label binding information.
<b>show mpls l2transport vc</b>	Displays information about AToM VCs that have been enabled to route Layer 2 packets on a router.

# shutdown (FR-ATM)

To shut down a Frame Relay-ATM Network Interworking (FRF.5) connection or a Frame Relay-ATM Service Interworking (FRF.8) connection, use the **shutdown** command in FRF.5 or FRF.8 connect configuration mode. To disable disconnection, use the **no** form of this command.

**shutdown**

**no shutdown**

## Syntax Description

This command has no arguments or keywords.

## Command Default

No default behavior or values

## Command Modes

FRF.5 connect configuration  
FRF.8 connect configuration

## Command History

Release	Modification
12.1(2)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 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

An FRF.5 or FRF.8 connection must be manually shut down once the interworking connection is created by use of the **shutdown** command.

## Examples

### FRF.5 Shutdown: Example

The following example shows how to shut down an FRF.5 connection:

```
Router(config)# connect network-2 interface serial10/1 16 atm3/0 0/32 network-interworking
.
.
Router(config-frf5)# shutdown
```

### FRF.8 Shutdown: Example

The following example shows how to shut down an FRF.8 connection:

```
Router(config)# connect serial10 100 atm3/0 1/35 service-interworking
.
.
Router(config-frf8)# shutdown
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>connect (FRF.5)</b>	Connects a Frame Relay DLCI or VC group to an ATM PVC.

## skeptical interval (OTV)

To configure a Cisco nonstop forwarding (NSF) helper functionality with an adjacency, use the **skeptical interval** command in OTV IS-IS instance configuration mode. To return to the default NSF helper setting, use the **no** form of this command.

**skeptical interval** *minutes*

**no skeptical interval**

### Syntax Description

<i>minutes</i>	Interval (in minutes) during which the hold time for an adjacency with a recently restarted router is not refreshed based on the hold time in the Intermediate System-to-Intermediate System (IS-IS) Hello (IIH) protocol data unit (PDU) with Request Restart (RR) set. Because the hold time is not updated during this interval, adjacency need not be kept up for a router that continuously restarts.  The range is from 0 to 1440.
----------------	--

### Command Default

The default skeptical interval is 5 minutes.

### Command Modes

OTV IS-IS instance configuration (config-otv-isis)

### Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was introduced.

### Usage Guidelines

NSF is not supported with the neighbor when you configure the **skeptical interval** command with a value other than 0. If you configure the **skeptical interval 0** command, NSF is always supported with the neighbor.

### Examples

The following example configures the skeptical interval to 30 minutes:

```
Router# configure terminal
Router(config)# otv isis overlay 1
Router(config-otv-isis)# skeptical interval 30
Router(config-otv-isis)# end
```

### Related Commands

Command	Description
<b>otv isis overlay</b>	Creates an OTV overlay interface.
<b>show otv isis</b>	Displays the IS-IS status and configuration.

## smds address

To specify the Switched Multimegabit Data Service (SMDS) individual address for a particular interface, use the **smds address** command in interface configuration mode. To remove the address from the configuration file, use the **no** form of this command.

**smds address** *smds-address*

**no smds address** *smds-address*

<b>Syntax Description</b>	<i>smds-address</i>	Individual address provided by the SMDS service provider. It is protocol independent.
<b>Command Default</b>	No address is specified.	
<b>Command Modes</b>	Interface configuration	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	10.0	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 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** All addresses for SMDS service are assigned by the service provider, and can be assigned to individuals and groups.

Addresses are entered in the Cisco SMDS configuration software using an E prefix for *multicast* addresses and a C prefix for *unicast* addresses. Cisco IOS software expects the addresses to be entered in E.164 format, which is 64 bits. The first 4 bits are the address type, and the remaining 60 bits are the address. If the first 4 bits are 1100 (0xC), the address is a unicast SMDS address, which is the address of an individual SMDS host. If the first 4 bits are 1110 (0xE), the address is a multicast SMDS address, which is used to broadcast a packet to multiple end points. The 60 bits of the address are in binary-coded decimal (BCD) format. Each 4 bits of the address field presents a single telephone number digit, allowing for up to 15 digits. At a minimum, you must specify at least 11 digits (44 bits). Unused bits at the end of this field are filled with ones.



**Note** If bridging is enabled on any interface, the SMDS address is erased and must be reentered.

### Examples

The following example specifies an individual address in Ethernet-style notation:

```
interface serial 0
  smds address c141.5797.1313.FFFF
```

## smds dxi

To enable the Data Exchange Interface (DXI) version 3.2 support, use the **smds dxi** command in interface configuration mode. To disable the DXI 3.2 support, use the **no** form of this command.

**smds dxi**  
**no smds dxi**

**Syntax Description** This command has no arguments or keywords.

**Command Default** Enabled

**Command Modes** Interface configuration

### Command History

Release	Modification
10.0	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 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

Adding this command to the configuration enables the DXI version 3.2 mechanism and encapsulates SMDS packets in a DXI frame before they are transmitted. DXI 3.2 adds an additional 4 bytes to the SMDS packet header to communicate with the SMDS data service unit (SDSU). These bytes specify the frame type. The interface expects all packets to arrive with DXI encapsulation.

The DXI 3.2 support also includes the heartbeat process as specified in the SIG-TS-001/1991 standard, revision 3.2. The heartbeat (active process) is enabled when both DXI and keepalives are enabled on the interface. The echo (passive process) is enabled when DXI is enabled on the interface. The heartbeat mechanism automatically generates a heartbeat poll frame every 10 seconds. This default value can be changed with the **keepalive** (LMI) command.

Fast switching of DXI frames is supported, but Interim Local Management Interface (ILMI) is not.



**Note** If you are running serial lines back-to-back, disable keepalive on SMDS interfaces. Otherwise, DXI declares the link down.



**Note** Switching in or out of DXI mode causes the IP cache to be cleared. This clearing process is necessary to remove all cached IP entries for the serial line being used. Stale entries must be removed to allow the new MAC header with or without DXI framing to be installed in the cache. This clearing process is not frequently done and is not considered to be a major performance penalty.



---

**Examples**

The following example enables DXI 3.2 on interface HSSI 0:

```
interface hssi 0
 encapsulation smds
 smds dxi
 smds address C120.1111.2222.FFFF
 ip address 172.20.1.30 255.255.255.0
 smds multicast ip E180.0999.9999
 smds enable-arp
```

---

**Related Commands**

Command	Description
<b>keepalive (LMI)</b>	Enables the LMI mechanism for serial lines using Frame Relay encapsulation.

## smds enable-arp

To enable dynamic Address Resolution Protocol (ARP), use the **smds enable-arp** interface configuration command. The multicast address for ARP must be set before this command is issued. To disable the interface once ARP has been enabled, use the **no** form of this command.

**smds enable-arp**  
**no smds enable-arp**

**Syntax Description** This command has no arguments or keywords.

**Command Default** Disabled

**Command Modes** Interface configuration

### Command History

Release	Modification
10.0	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 Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

### Examples

The following example enables the dynamic ARP routing table:

```
interface serial 0
ip address 172.20.1.30 255.255.255.0
smds multicast IP E180.0999.9999.2222
smds enable-arp
```

### Related Commands

Command	Description
<b>arp</b>	Enables ARP entries for static routing over the SMDS network.

## smds glean

To enable dynamic address mapping for Internet Packet Exchange (IPX) over Switched Multimegabit Data Service (SMDS), use the **smds glean** interface configuration command. To disable dynamic address mapping for IPX over SMDS, use the **no** form of this command.

```
smds glean protocol [timeout-value] [broadcast]
no smds glean protocol
```

Syntax Description		
<i>protocol</i>		Protocol type. Only IPX is supported.
<i>timeout-value</i>		(Optional) Time to live (TTL) value. Value can be from 1 to 65535 minutes. The default is 5 minutes. This value indicates how long a gleaned dynamic map is stored in the SMDS map table.
<b>broadcast</b>		(Optional) Marks the gleaned protocol address as a candidate for broadcast packets. All broadcast requests are sent to the unicast SMDS address.

**Command Default** Disabled

**Command Modes** Interface configuration

Command History	Release	Modification
	11.1	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 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** The **smds glean** command uses incoming packets to dynamically map SMDS addresses to higher-level protocol addresses. Therefore the need for static map configuration for the IPX protocol is optional rather than mandatory. However, any static map configuration overrides the dynamic maps.

If a map is gleaned and it already exists as a dynamic map, the timer for the dynamic map is reset to the default value or the user-specified value.

### Examples

The following example enables dynamic address mapping for IPX on interface serial 0 and sets the time to live (TTL) to 14 minutes:

```
interface serial 0
 encapsulation smds
 smds address c141.5797.1313.FFFF
 smds multicast ipx e1800.0999.9999.FFFF
 smds glean ipx 14
```

## smds multicast

To assign a multicast Switched Multimegabit Data Service (SMDS) E.164 address to a higher-level protocol, use the **smds multicast** command in interface configuration mode. To remove an assigned multicast address, use the **no** form of this command.

**smds multicast** *protocol smds-address*  
**no smds multicast** *protocol smds-address*

### Syntax Description

<i>protocol</i>	Protocol type. See the table below for a list of supported protocols and their keywords.
<i>smds-address</i>	SMDS address. Because SMDS does not incorporate broadcast addressing, a group address for a particular protocol must be defined to serve the broadcast function.

### Command Default

No mapping is defined.

### Command Modes

Interface configuration

### Command History

Release	Modification
10.0	This command was introduced.
12.2(13)T	The <b>vines</b> and <b>xns</b> arguments were removed because Banyan VINES and Xerox Network Systems are no longer available in the Cisco IOS software.
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

When configuring DECnet, you must enter all four DEC keywords (**decnet**, **decnet\_router-L1**, **decnet\_router-L2**, and **decnet\_node**) in the configuration.

The table below lists the high-level protocols supported by the **smds multicast** command.

**Table 54: smds multicast Supported Protocols**

Keyword	Protocol
<b>aarp</b>	AppleTalk Address Resolution Protocol
<b>appletalk</b>	AppleTalk
<b>arp</b>	Address Resolution Protocol
<b>bridge</b>	Transparent bridging
<b>clns</b>	International Organization for Standardization (ISO) Connectionless Network Service (CLNS)

Keyword	Protocol
<b>clns_es</b>	Multicast address for all CLNS end systems
<b>clns_is</b>	Multicast address for all CLNS intermediate systems
<b>decnet</b>	DECnet
<b>decnet_node</b>	DECnet multicast address for all end systems
<b>decnet_router-L1</b>	DECnet multicast address for all Level 1 (intra-area) routers
<b>decnet_router-L2</b>	DECnet multicast address for all Level 2 (interarea) routers
<b>ip</b>	Internet Protocol (IP)
<b>ipx</b>	Novell IPX

For IP, the IP NETWORK and MASK fields are no longer required. The Cisco IOS software accepts these arguments, but ignores the values. These were required commands for the previous multiple logical IP subnetworks configuration. The software continues to accept the arguments to allow for backward compatibility, but ignores the contents.

### Examples

The following example maps the IP broadcast address to the SMDS group address E180.0999.9999:

```
interface serial 0
  smds multicast IP E180.0999.9999.FFFF
```

## smds multicast arp

To map the Switched Multimegabit Data Service (SMDS) address to a multicast address, use the **smds multicast arp** interface configuration command. To disable this feature, use the **no** form of this command.

**smds multicast arp** *smds-address* [*ip-address mask*]  
**no smds multicast arp** *smds-address* [*ip-address mask*]

### Syntax Description

<i>smds-address</i>	SMDS address in E.164 format.
<i>ip-address</i>	(Optional) IP address.
<i>mask</i>	(Optional) Subnet mask for the IP address.

### Command Default

No mapping is defined.

### Command Modes

Interface configuration

### Command History

Release	Modification
10.0	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 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

This command is used only when an Address Resolution Protocol (ARP) server is present on a network. When broadcast ARPs are sent, SMDS first attempts to send the packet to all multicast ARP SMDS addresses. If none exist in the configuration, broadcast ARPs are sent to all multicast IP SMDS multicast addresses. If the optional ARP multicast address is missing, each entered IP multicast command is used for broadcasting.

### Examples

The following example configures broadcast ARP messages:

```
interface serial 0
  smds multicast arp E180.0999.9999.2222
```

### Related Commands

Command	Description
<b>smds multicast ip</b>	Maps an SMDS group address to a secondary IP address.

# smds multicast bridge

To enable spanning-tree updates, use the **smds multicast bridge** interface configuration command. To disable this function, use the **no** form of this command.

**smds multicast bridge** *smds-address*  
**no smds multicast bridge** *smds-address*

## Syntax Description

<i>smds-address</i>	SMDS multicast address in E.164 format.
---------------------	---

## Command Default

No multicast SMDS address is defined. Spanning tree updates are disabled for transparent bridging across SMDS networks.

## Command Modes

Interface configuration

## Command History

Release	Modification
10.0	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 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

To allow transparent bridging of packets across serial and High-Speed Serial Interface (HSSI) interfaces in an SMDS network, the SMDS interface must be added to an active bridge group. Also, standard bridging commands are necessary to enable bridging on an SMDS interface.

When the **smds multicast bridge** command is added to the configuration, broadcast packets are encapsulated with the specified SMDS multicast address configured for bridging. Two broadcast Address Resolution Protocol (ARP) packets are sent to the multicast address. One is sent with a standard (SMDS) ARP encapsulation, while the other is sent with the ARP packet encapsulated in an 802.3 MAC header. The native ARP is sent as a regular ARP broadcast.

Cisco's implementation of IEEE 802.6i transparent bridging for SMDS supports 802.3, 802.5, and FDDI frame formats. The router can accept frames with or without frame check sequence (FCS). Fast-switched transparent bridging is the default and is not configurable. If a packet cannot be fast switched, it is process switched.

In Cisco IOS Release 10.2 software (or earlier), bridging over multiple logical IP subnetworks is not supported. Bridging of IP packets in a multiple logical IP subnetworks environment is unpredictable.

## Examples

In the following example, all broadcast bridge packets are sent to the configured SMDS multicast address:

```
interface hssi 0
 encapsulation smds
 smds address C120.1111.2222.FFFF
 ip address 172.16.0.0 255.255.255.0
```

```
smds multicast bridge E180.0999.9999.FFFF  
bridge-group 5
```

**Related Commands**

Command	Description
<b>bridge-group</b>	Assigns each network interface to a bridge group.



## smds multicast ip

To map a Switched Multimegabit Data Service (SMDS) group address to a secondary IP address, use the **smds multicast ip** interface configuration command. To remove the address map, use the **no** form of this command.

```
smds multicast ip smds-address [ip-address mask]  
no smds multicast ip smds-address [ip-address mask]
```

Syntax Description	
<i>smds-address</i>	SMDS address in E.164 format.
<i>ip-address</i>	(Optional) IP address.
<i>mask</i>	(Optional) Subnet mask for the IP address.

**Command Default** The IP address and mask default to the primary address of the interface if they are left out of the configuration.

**Command Modes** Interface configuration

Command History	Release	Modification
	10.0	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 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** This command allows a single SMDS interface to be treated as multiple logical IP subnetworks. If taking advantage of the multiple logical IP subnetworks support in SMDS, you can use more than one multicast address on the SMDS interface (by entering multiple commands). However, each **smds multicast ip** command entry must be associated with a different IP address on the SMDS interface.

Broadcasts can be sent on the SMDS interface by means of the multicast address. By sending broadcasts in this manner, the router is not required to replicate broadcasts messages to every remote host.

In addition, the higher-level protocols such as Open Shortest Path First (OSPF) and Intermediate System-to-Intermediate System (IS-IS) can use the multicast capability by sending one update packet or routing packet to the multicast address.

If the optional IP address and mask arguments are not present, the SMDS address and multicast address are associated with the primary IP address of the interface. This association allows the command to be backward compatible with earlier versions of the software.

If an Address Resolution Protocol (ARP) multicast address is missing, each entered IP multicast command is used for broadcasting. The ARP multicast command has the same format as the IP multicast command and is typically used only when an ARP server is present in the network.



**Note** All routers at the other end of the SMDS cloud must have the multiple logical IP subnetworks capability enabled. If you allocate a different SMDS subinterface for each logical IP subnetwork on the SMDS interface, you do not have to configure secondary IP addresses.

### Examples

The following example configures an interface with two subinterfaces to support two different IP subnets with different multicast addresses to each network:

```
interface serial 2/0
 encapsulation smds
 smds address C120.1111.2222.4444
interface serial 2/0.1 multipoint
 smds addr c111.3333.3333.3333
 ip address 2.2.2.1 255.0.0.0
 smds multicast ip e222.2222.2222.2222
 smds enable-arp
interface serial 2/0.2 multipoint
 smds addr c111.2222.3333.3333.3333
 ip address 2.3.3.3 255.0.0.0
 smds multicast ip E180.0999.9999.FFFF
 smds enable-arp
```

### Related Commands

Command	Description
<b>smds multicast arp</b>	Maps the SMDS address to a multicast address.

## smds static-map

To configure a static map between an individual Switched Multimegabit Data Service (SMDS) address and a higher-level protocol address, use the **smds static-map** command in interface configuration mode. To remove the map, use the **no** form of this command with the appropriate arguments.

**smds static-map** *protocol protocol-address smds-address* [**broadcast**]  
**no smds static-map** *protocol protocol-address smds-address* [**broadcast**]

Syntax Description		
	<i>protocol</i>	Higher-level protocol. It can be one of the following values: <b>appletalk</b> , <b>clns</b> , <b>decnet</b> , <b>ip</b> , or <b>ipx</b> .
	<i>protocol-address</i>	Address of the higher-level protocol.
	<i>smds-address</i>	SMDS address, to complete the mapping.
	<b>broadcast</b>	(Optional) Marks the specified protocol address as a candidate for broadcast packets. All broadcast requests are sent to the unicast SMDS address.

**Command Default** No mapping is defined.

**Command Modes** Interface configuration

Command History	Release	Modification
	10.0	This command was introduced.
	12.2(13)T	The <b>vines</b> and <b>xns</b> arguments were removed because Banyan VINES and Xerox Network Systems are no longer available in the Cisco IOS software.
	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** The **smds static-map** command provides *pseudobroadcasting* by allowing the use of broadcasts on those hosts that cannot support SMDS multicast addresses.

### Examples

The following example illustrates how to enable pseudobroadcasting. The router at address C120.4444.9999 will receive a copy of the broadcast request because the broadcast keyword is specified with the **smds static-map** command. The host at address 172.16.1.15 is incapable of receiving multicast packets. The multicasting is simulated with this feature.

```
interface hssi 0
 encapsulation smds
 smds address C120.1111.2222.FFFF
 ip address 172.16.1.30 255.255.255.0
 smds static-map ip 172.16.1.15 C120.4444.9999.FFFF broadcast
 smds enable-arp
```

The following example illustrates how to enable multicasting. In addition to IP and ARP requests to E100.0999.9999, the router at address C120.4444.9999 will also receive a copy of the multicast request. The host at address 172.16.1.15 is incapable of receiving broadcast packets.

```
interface hssi 0
  encapsulation smps
  smps address C120.1111.2222.FFFF
  ip address 172.16.1.30 255.255.255.0
  smps multicast ip E100.0999.999.FFFF
  smps static-map ip 172.16.1.15 C120.4444.9999.FFFF
  smps enable-arp
```

## snmp-server enable traps waas

To enable Simple Network Management Protocol (SNMP) traps for WAAS Express, use the **snmp-server enable traps waas** command in global configuration mode. To disable the SNMP traps for WAAS Express, use the **no** form of this command.

```
snmp-server enable traps waas [cpu-throttle-on] [cpu-throttle-off] [license-deleted] [license-expired]
[license-revoked] [peer-overload] [tfo-conn-overload]
no snmp-server enable traps waas [cpu-throttle-on] [cpu-throttle-off] [license-deleted]
[license-expired] [license-revoked] [peer-overload] [tfo-conn-overload]
```

### Syntax Description

<b>cpu-throttle-on</b>	(Optional) Enables traps for WAAS Express CPU throttling on.
<b>cpu-throttle-off</b>	(Optional) Enables traps for WAAS Express CPU throttling off.
<b>license-deleted</b>	(Optional) Enables traps for deletion of WAAS Express licenses.
<b>license-expired</b>	(Optional) Enables traps for WAAS Express license expiry.
<b>license-revoked</b>	(Optional) Enables traps for revoked WAAS Express licenses.
<b>peer-overload</b>	(Optional) Enables traps for WAAS Express peer overload.
<b>tfo-conn-overload</b>	(Optional) Enables traps for WAAS Express Transport Flow Optimization (TFO) overload.

### Command Default

SNMP traps for WAAS Express are disabled.

### Command Modes

Global configuration (config)

### Command History

Release	Modification
15.2(3)T	This command was introduced.

### Examples

The following example shows how to enable traps to delete WAAS Express licenses and TFO overload:

```
Device# enable
Device# configure terminal
Device(config)# snmp-server enable traps waas license-deleted tfo-conn-overload
```

### Related Commands

Command	Description
<b>debug snmp detail</b>	Displays the SNMP debug messages.
<b>debug snmp packet</b>	Displays information about every SNMP packet sent or received by a device.
<b>show snmp mib</b>	Displays a list of MIB module instance identifiers registered on your device.

<b>Command</b>	<b>Description</b>
<b>snmp-server community</b>	Sets up the community access string to permit access to SNMP.
<b>snmp-server enable traps</b>	Enables all SNMP notification types that are available on your system.
<b>snmp-server host</b>	Specifies the recipient of an SNMP notification.
<b>snmp-server source-interface</b>	Specifies the interface from which an SNMP trap originates the notifications or traps.

# source-interface loopback

To assign a previously created loopback interface to an NVE interface, use the `source-interface loopback` command in NVE interface configuration mode. To remove the loopback interface from the NVE interface, use the `no` form of this command.

**source-interface loopback** *number*

---

**Syntax Description**

*number* The loopback interface assigned to the NVE interface.

---

---

**Command Modes**

NVE interface configuration (config-if)

---

---

**Command History****Release****Modification**

---

Cisco IOS XE Release 3.11S This command was introduced on the Cisco CSR 1000V.

---

The following example maps a loopback interface to an NVE interface:

```
Router(config)# interface nve 1
Router(config-if)# source-interface loopback 0
```

## spf-interval (OTV)

To configure the minimum interval between shortest path first (SPF) computations, use the **spf-interval** command in OTV IS-IS instance configuration mode. To remove the configuration for the SPF interval, use the **no** form of this command.

**spf-interval** *spf-max-wait* [*spf-initial-wait* *spf-second-wait* ]  
**no spf-interval**

### Syntax Description

<i>spf-max-wait</i>	Interval in seconds. The range is from 1 to 120.
<i>spf-initial-wait</i>	(Optional) Initial wait interval in milliseconds. The range is from 1 to 120000.
<i>spf-second-wait</i>	(Optional) Interval in milliseconds between the first and second SPF computations. The range is from 1 to 120000.

### Command Default

Layer 2 is configured, by default, with SPF intervals of 5 seconds, 50 milliseconds, and 200 milliseconds for the *spf-max-wait*, *spf-initial-wait*, and *spf-second-wait* arguments, respectively.

### Command Modes

OTV IS-IS instance configuration (config-otv-isis)

### Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was introduced.

### Examples

The following example shows how to configure the SPF interval:

```
Router# configure terminal
Router(config)# otv isis overlay 1
Router(config-otv-isis)# spf-interval 2 3 4
Router(config-otv-isis)# end
```

### Related Commands

Command	Description
<b>otv isis overlay</b>	Creates an OTV overlay interface.
<b>show otv isis</b>	Displays the IS-IS status and configuration.



## status admin-down disconnect

To configure Layer 2 tunneling (L2TUN) sessions to disconnect upon attachment circuit (AC) shutdown, use the **status admin-down disconnect** command in pseudowire class configuration mode. To disable disconnection of L2TUN sessions upon AC shutdown, use the **no** form of this command.

```
status admin-down disconnect
no status admin-down disconnect
```

### Syntax Description

This command has no arguments or keywords.

### Command Default

Layer 2 tunneling sessions do not disconnect upon attachment circuit (AC) shutdown.

### Command Modes

Pseudowire class configuration (config-pw)

### Command History

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

### Usage Guidelines

Use the **show l2tp session** command to determine whether the sessions are disconnected.

### Examples

The following example shows how to enter pseudowire class configuration mode to configure a pseudowire configuration template named ether-pw and configure L2TUN sessions to disconnect on AC shutdown.

```
Router> enable
Password:
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# pseudowire-class ether-pw
  Router(config-pw)# status admin-down disconnect
  Router(config-pw)# end
```

### Related Commands

Command	Description
<b>pseudowire-class</b>	Specifies the name of a Layer 2 pseudowire class and enter pseudowire class configuration mode.
<b>show l2tp session</b>	Displays information about L2TP sessions.
<b>show l2tun tunnel</b>	Displays the current state of Layer 2 Tunneling Protocol (L2TP) tunnels and information about configured tunnels, including local and remote hostnames, aggregate packet counts, and control channel information.

## suppress-server-encoding enable

To suppress server side encoding, use the **suppress-server-encoding enable** command in WAAS HTTP configuration mode. To enable server side encoding, use the **no** form of this command.

**suppress-server-encoding enable**  
**no suppress-server-encoding enable**

**Syntax Description** This command has no arguments or keywords.

**Command Default** Server encoding is not suppressed.

**Command Modes** WAAS HTTP configuration (config-waas-http)

Command History	Release	Modification
	15.2(3)T	This command was introduced.

**Usage Guidelines** A client uses the Accept-Encoding header in the HTTP request it sends to indicate the types of compressions it supports. The values usually sent by the client include identity, gzip, deflate and compress. When server side encoding is suppressed, the client side WAAS Express removes the values of this header, and the server does not compress the data it sends. WAAS Express uses the suppression of server side encoding mechanism to provide better compression on HTTP response from the server and also frees the server from the additional computation required to compress responses.

Before you can enable the **suppress-server-encoding enable** command, use the following commands:

- Use the **parameter-map type waas** command in global configuration mode to enter parameter map configuration mode.
- Use the **accelerator http-express** command in parameter map configuration mode to enter WAAS HTTP configuration mode.

### Examples

The following example shows how to suppress server side encoding:

```
Device(config)# parameter-map type waas waas_global
Device(config-profile)# accelerator http-express
Device(config-waas-http)# enable
Device(config-waas-http)# suppress-server-encoding enable
```

### Related Commands

Command	Description
<b>accelerator</b>	Enters a specific WAAS Express accelerator configuration mode based on the accelerator being configured.
<b>parameter-map type waas</b>	Configures WAAS Express global parameters.
<b>show waas accelerator</b>	Displays information about WAAS Express accelerators.

## tfo auto-discovery blacklist

To configure a blocked list with autodiscovery for WAAS Express, use the **tfo auto-discovery blacklist** command in parameter-map configuration mode. To remove the configuration, use the **no** form of this command.

```
tfo auto-discovery blacklist {enable | hold-time minutes}
no tfo auto-discovery blacklist {enable | hold-time minutes}
```

Syntax Description	enable	hold-time minutes
	Enables a blocked list.	Configures a blocked list hold time, in minutes. The range is 1 to 10080.

**Command Default** Blocked list with autodiscovery is not enabled.

**Command Modes** Parameter-map configuration (config-profile)

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

**Usage Guidelines** A server is block listed by WAAS Express if the server is not able to receive TCP packets with options because of the TCP packets with options being blocked by network devices such as firewalls. WAAS Express learns not to send TCP packets with options to these blocked listed servers.

Use this command to enable, configure, and integrate a blocked list with autodiscovery and specify the hold time for a blocked list in WAAS Express. Blocked lists enable you to get the benefit of WAAS Express if there are devices in your network that discard TCP packets with options.

Autodiscovery allows a WAAS Express device to automatically discover and connect to a new file server when a Common Internet File System (CIFS) request is received. The autodiscovery of peer WAAS Express devices is achieved using TCP options. These TCP options are recognized and understood only by WAAS Express devices and are ignored by non-WAAS Express devices.

### Examples

The following example configures autodiscovery by enabling the blocked list and setting the hold time for 100 minutes:

```
Router(config)# parameter-map type waas waas_global
Router(config-profile)# tfo auto-discovery blacklist enable
Router(config-profile)# tfo auto-discovery blacklist hold-time 100
```

Related Commands	Command	Description
	<b>cpu-threshold</b>	Sets the CPU threshold limit.
	<b>lz entropy</b>	Enables entropy checking to turn on Lempel-Ziv (LZ) compression.
	<b>parameter-map type waas</b>	Defines a WAAS Express parameter map.

<b>Command</b>	<b>Description</b>
<b>policy-map type waas</b>	Configures WAAS Express policy map.
<b>tfo optimize</b>	Configures compression for WAAS Express.

## tfo optimize

To configure the compression for WAAS Express, use the **tfo optimize** command in parameter-map configuration mode. To remove the compression, use the **no** form of this command.

```
tfo optimize {full | dre {yes | no compression {lz | none}}}
no tfo optimize [ {full | dre {yes | no compression {lz | none}}} ]
```

Syntax Description	full	Turns on Data Redundancy Elimination (DRE) and compression.
	dre	Enables DRE.
	yes	Turns on DRE.
	no	Turns off DRE.
	compression	Turns on compression.
	lz	Turns on Lempel-Ziv (LZ) compression.
	none	Turns off LZ compression.

**Command Default** Compression is not configured.

**Command Modes** Parameter-map configuration (config-profile)

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

**Usage Guidelines** Use this command to specify a compression technology to reduce the size of data. WAAS Express uses the following compression technologies to help you transmit data over your WAN:

- DRE
- LZ

These compression technologies reduce the size of transmitted data by removing redundant information before sending the shortened data stream over the WAN. By reducing the amount of transferred data, WAAS compression can reduce network utilization and application response times.

LZ compression operates on smaller data streams and keeps limited compression history. DRE operates on significantly larger streams (typically tens to hundreds of bytes or more) and maintains a much larger compression history. Large chunks of redundant data is common in file system operations when files are incrementally changed from one version to another or when certain elements are common to many files, such as file headers and logos.

**Examples** The following example turns off the DRE compression and turns on the LZ compression:

```
Router(config)# parameter-map type waas waas_global
Router(config-profile)# tfo optimize dre no compression lz
```

**Related Commands**

Command	Description
<b>cpu-threshold</b>	Sets the CPU threshold limit.
<b>lz entropy-check</b>	Enables entropy checking to turn on LZ compression.
<b>parameter-map type waas</b>	Defines a WAAS Express parameter map.
<b>policy-map type waas</b>	Configures WAAS Express policy map.
<b>tfo auto-discovery blacklist</b>	Configures black list with autodiscovery for WAAS Express.

# threshold de

To configure the threshold at which discard eligible (DE)-marked packets will be discarded from switched permanent virtual circuits (PVCs) on the output interface, use the **threshold de** command in Frame Relay congestion management configuration mode. To remove the threshold configuration, use the **no** form of this command.

**threshold de** *percentage*  
**no threshold de** *percentage*

<b>Syntax Description</b>	<i>percentage</i>	Threshold at which DE-marked packets will be discarded, specified as a percentage of maximum queue size.
---------------------------	-------------------	--

**Command Default** 100%

**Command Modes** Frame Relay congestion management configuration

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.1(2)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 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** You must enable Frame Relay congestion management on the interface before congestion management parameters will be effective. To enable Frame Relay congestion management and to enter Frame Relay congestion management configuration mode, use the **frame-relay congestion-management** interface command.

You must enable Frame Relay switching, using the **frame-relay switching** global command, before the **threshold de** command will be effective on switched PVCs.

## Examples

The following example shows how to configure a DE threshold of 40% on serial interface 1.

```
interface serial1
 encapsulation frame-relay
 frame-relay congestion-management
 threshold de 40
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>frame-relay congestion-management</b>	Enables Frame Relay congestion management functions on all switched PVCs on an interface, and enters congestion management configuration mode.
	<b>frame-relay congestion threshold de</b>	Configures the threshold at which DE-marked packets will be discarded from the traffic-shaping queue of a switched PVC.

<b>Command</b>	<b>Description</b>
<b>frame-relay congestion threshold ecn</b>	Configures the threshold at which ECN bits will be set on packets in the traffic-shaping queue of a switched PVC.
<b>frame-relay switching</b>	Enables PVC switching on a Frame Relay DCE or NNI.
<b>threshold ecn</b>	Configures the threshold at which ECN bits will be set on packets in switched PVCs on the output interface.



# threshold ecn

To configure the threshold at which explicit congestion notification (ECN) bits will be set on packets in switched permanent virtual circuits (PVCs) on the output interface, use the **threshold ecn** command in Frame Relay congestion management configuration mode. To remove the threshold configuration, use the **no** form of this command.

## For Frame Relay Switching

**threshold ecn** {bc | be} *percentage*

**no threshold ecn** {bc | be} *percentage*

## For Frame Relay over MPLS

**threshold ecn** *percentage*

**no threshold ecn** *percentage*

Syntax Description		
	<b>bc</b>	Specifies threshold for committed traffic. This keyword is not available for Frame Relay over MPLS.
	<b>be</b>	Specifies threshold for excess traffic. This keyword is not available for Frame Relay over MPLS.
	<i>percentage</i>	Threshold at which ECN bits will be set on packets, specified as a percentage of maximum queue size. Default is 100 percent.

**Command Default** An ECN threshold is not configured.

**Command Modes** Frame Relay congestion management configuration

Command History	Release	Modification
	12.1(2)T	This command was introduced.
	12.0(26)S	This command was modified for Frame Relay over MPLS.
	12.2(27)SXA	This command was integrated into Cisco IOS Release 12.2(27)SXA.
	12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

**Usage Guidelines** You must enable Frame Relay congestion management on the interface before congestion management parameters will be effective. To enable Frame Relay congestion management and to enter Frame Relay congestion management configuration mode, use the **frame-relay congestion-management** interface command.

### Frame Relay Switching Guidelines

- You must enable Frame Relay switching, using the **frame-relay switching** global command, before the **threshold ecn** command will be effective on switched PVCs.
- You can configure separate queue thresholds for committed and excess traffic.

- Configure the BECN threshold so that it is greater than or equal to zero and less than or equal to the BECN threshold. Configure the BECN threshold so that it is less than or equal to 100.

## Examples

### Frame Relay Switching: Example

The following example shows how to configure a Be threshold of 0 and a Bc threshold of 20 percent on serial interface 1.

```
interface serial1
encapsulation frame-relay
frame-relay congestion-management
threshold ecn be 0
threshold ecn bc 20
```

### Frame Relay over MPLS: Example

The following example shows a configuration of interface serial2/1 for a threshold of 50 percent.

```
interface Serial2/1
bandwidth 50000
service-policy output output-policy
frame-relay congestion-management
threshold ecn 50
```

## Related Commands

Command	Description
<b>frame-relay congestion-management</b>	Enables Frame Relay congestion management functions on all switched PVCs on an interface, and enters congestion management configuration mode.
<b>frame-relay switching</b>	Enables PVC switching on a Frame Relay DCE or NNI.

## timeout setup

To configure the amount of time allowed to set up a control channel with a remote provider edge (PE) router at the other end of a Layer 2 pseudowire, use the **timeout setup** command in L2TP class configuration mode. To disable the configured value, use the **no** form of this command.

**timeout setup** *seconds*  
**no timeout setup** *seconds*

<b>Syntax Description</b>	<i>seconds</i>	The number of seconds allowed to set up a Layer 2 control channel. The valid values range from 60 to 6000. The default value is 300 seconds.
---------------------------	----------------	--

**Command Default** The default number of seconds allowed to set up a control channel is 300.

**Command Modes** L2TP class configuration

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.0(23)S	This command was introduced.
	12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.
	12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
	12.2(27)SBC	Support for this command was integrated into Cisco IOS Release 12.2(27)SBC.

**Usage Guidelines** Use this command to configure the amount of time that can be spent attempting to establish a control channel.

### Examples

The following example sets a timeout period of 200 seconds to establish a control channel with a remote peer in Layer 2 pseudowires that have been configured with the L2TP class named "l2tp-class1":

```
Router(config)
# l2tp-class l2tp-class1
Router(config-l2tp-class)
# timeout setup 200
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>l2tp-class</b>	Creates a template of L2TP control plane configuration settings that can be inherited by different pseudowire classes and enters L2TP class configuration mode.

## vc-group

To assign multiple Frame Relay data-link connection identifiers (DLCIs) to a virtual circuit (VC) group for Frame Relay-to-ATM Network Interworking (FRF.5), use the **vc-group** command in global configuration mode. To disable the VC group assignments, use the **no** form of this command.

**vc-group** *group-name*

**no vc-group** *group-name*

### Syntax Description

<i>group-name</i>	A VC group name entered as an 11-character maximum string.
-------------------	--

The following syntax description applies to the VC-group entries:

<i>fr-interface-name</i>	Frame Relay interface; for example, serial0/0.
<i>fr-dlci</i>	Frame Relay DLCI number, in the range 16 to 1007.
<i>fr-sscs-dlci</i>	(Optional) Frame Relay SSSC DLCI number, in the range of 16 to 991. Default is 1022.

### Command Default

No default behavior or values

### Command Modes

Global configuration (config)

VC-group configuration (config-vc-group)

### Command History

Release	Modification
12.1(2)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 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

This command specifies the Frame Relay DLCIs in the VC group and maps them to the Frame Relay-SSCS DLCIs. If the optional FR-SSCS DLCI value is not specified, its value is the same as the Frame Relay DLCI.

The **vc-group** command requires that you enter the following arguments in VC-group configuration mode to provide a map between Frame Relay DLCIs and Frame Relay-SSCS DLCIs:

*fr-interface-name fr-dlci [fr-sscs-dlci]*

### Examples

The following example shows how to configure an FRF.5 many-to-one connection. The **vc-group** command maps Frame Relay DLCI 16, 17, 18, and 19 to a VC group named “friends”:

```
Router(config)# vc-group friends
Router(config-vc-group)# serial0 16 1
6
Router(config-vc-group)# serial0 17 17
Router(config-vc-group)# serial0 18 18
Router(config-vc-group)# serial0 19 19
```

**Related Commands**

Command	Description
<b>show vc-group</b>	Displays the names of all VC groups.

# vpls-id

To assign an identifier to the Virtual Private LAN Services (VPLS) domain, use the **vpls-id** command in L2 VFI configuration or VFI autodiscovery configuration mode. To revert to the default VPLS ID, use the **no** form of this command.

**vpls-id** {*autonomous-system-number:nn* | *ip-address:nn*}

**no vpls-id** {*autonomous-system-number:nn* | *ip-address:nn*}

## Syntax Description

<i>autonomous-system-number:nn</i>	Specifies a 16-bit autonomous system number (ASN) and 32-bit arbitrary number. The ASN need not match the local ASN.
<i>ip-address:nn</i>	Specifies a 32-bit IP address and a 16-bit arbitrary number. Only IPv4 addresses are supported.

## Command Default

The VPLS ID is generated automatically by VPLS autodiscovery.

## Command Modes

L2 VFI configuration (config-vfi)

VFI autodiscovery configuration (config-vfi-autodiscovery)

## Command History

Release	Modification
12.2(33)SRB	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into a release prior to Cisco IOS XE Release 3.6S.
Cisco IOS XE Release 3.7S	This command was modified as part of the Multiprotocol Label Switching (MPLS)-based Layer 2 VPN (L2VPN) command modifications for cross-OS support. This command was made available in VFI autodiscovery configuration mode.

## Usage Guidelines

VPLS autodiscovery automatically generates a VPLS ID using the Border Gateway Protocol (BGP) ASN and the configured virtual forwarding instance (VFI) VPN ID. You can use the **vpls-id** command to change the automatically generated VPLS ID.

The Label Distribution Protocol (LDP) uses the VPLS ID when signaling VPLS autodiscovered neighbors. The VPLS ID identifies the VPLS domain.

Only one VPLS ID can be configured per VFI. The same VPLS ID cannot be configured in multiple VFIs on the same provider edge (PE) router.

The manually configured VPLS ID replaces the internally generated VPLS ID. The manually configured VPLS ID also changes the automatically generated route target (RT).

The **vpls-id** command defines the attachment group identifier (AGI) for the VPLS domain. Therefore, all PE routers in the same VPLS domain must use the same VPLS ID.

For interautonomous system configurations, you must manually configure the VPLS ID instead of using the automatically generated VPLS ID, because all PE routers do not share the same autonomous system number.

**Examples**

The following example shows how to set a VPLS ID to the autonomous system and network number 5:300:

```
Device(config)# l2 vfi SP2 autodiscovery
Device(config-vfi)# vpn id 200
Device(config-vfi)# vpls-id 5:300
```

The following example shows how to set the VPLS ID to IP address and network number 10.4.4.4:70

```
Device(config)# l2vpn vfi context vfi1
Device(config-vfi)# vpn id 200
Device(config-vfi)# autodiscovery bgp signaling ldp
Device(config-vfi-autodiscovery)# rd 2:3
Device(config-vfi-autodiscovery)# vpls-id 10.4.4.4:70
```

**Related Commands**

Command	Description
<b>autodiscovery (l2vpn vfi)</b>	Designates a VFI as having BGP autodiscovered pseudowire members.
<b>rd</b>	Creates routing and forwarding tables for a VRF.

## waas cm-register url

To register a device with the WAAS Central Manager, use the **waas cm-register url** command in privileged EXEC mode.

**waas cm-register url** *url port-number*

### Syntax Description

<b>url</b> <i>url</i>	URL of the device to be registered.
<i>port-number</i>	The port number.

### Command Default

No devices are registered with the WAAS Central Manager.

### Command Modes

Privileged EXEC (#)

### Command History

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

### Usage Guidelines

Use this command to register a device with the WAAS Central Manager. Before enabling this command, the WCM certificate must be installed on the router.



#### Note

The registration may fail if the port number is not specified.

The values for the *url* argument can be one of the following:

- **archive**
- **cns**
- **flash**
- **ftp**
- **http**
- **https**
- **null**
- **nvram**
- **rcp**
- **scp**
- **system**
- **tar**
- **tftp**



- **tmsys**
- **xmodem**
- **ymodem**

## Examples

The following example shows how to register a device with the WAAS Central Manager:

```
Router> enable
Router# waas cm-register url https://192.0.2.1:8443/wcm/register
```

## Related Commands

Command	Description
<b>clear waas</b>	Clears WAAS Express statistics and closed connections information.
<b>debug waas</b>	Displays debugging information for different WAAS Express modules.
<b>show waas alarms</b>	Displays WAAS Express status and alarms.
<b>show waas auto-discovery</b>	Displays information about WAAS Express autodiscovery.
<b>show waas connection</b>	Displays information about WAAS Express connections.
<b>show waas statistics aoim</b>	Displays WAAS Express peer information and negotiated capabilities.
<b>show waas statistics application</b>	Displays WAAS Express policy application statistics.
<b>show waas statistics auto-discovery</b>	Displays WAAS Express autodiscovery statistics.
<b>show waas statistics class</b>	Displays statistics for the WAAS Express class map.
<b>show waas statistics dre</b>	Displays WAAS Express DRE statistics.
<b>show waas statistics errors</b>	Displays WAAS Express error statistics.
<b>show waas statistics global</b>	Displays global WAAS Express statistics.
<b>show waas statistics lz</b>	Displays WAAS Express LZ statistics.
<b>show waas statistics pass-through</b>	Displays WAAS Express connections placed in a pass-through mode.
<b>show waas statistics peer</b>	Displays inbound and outbound statistics for peer WAAS Express devices.
<b>show waas status</b>	Displays the status of WAAS Express.
<b>show waas token</b>	Displays the value of the configuration token used by the WAAS Central Manager.

## waas config

To restore or remove WAAS Express default configurations, use the **waas config** command in privileged EXEC mode.

**waas config** {**restore-default** | **remove-all**}

### Syntax Description

<b>restore-default</b>	Restores the default configuration.
<b>remove-all</b>	Removes all configurations.

### Command Default

WAAS Express default configurations are not modified.

### Command Modes

Privileged EXEC (#)

### Command History

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

### Usage Guidelines

Use this command to either restore the default configurations or remove the configurations. This command works only if WAAS Express is not enabled on any interface.

### Examples

The following example shows how to restore the WAAS Express default configuration:

```
Router> enable
Router# waas config restore-default
```

### Related Commands

Command	Description
<b>class-map type waas</b>	Configures a WAAS Express class map.
<b>parameter-map type waas</b>	Configures WAAS Express global parameters.
<b>policy-map type waas</b>	Configures a WAAS Express policy map.
<b>waas enable</b>	Enables WAAS Express on a network interface of a router.
<b>waas export</b>	Associates a NetFlow exporter with WAAS Express.

## waas enable

To enable Wide-Area Application Services (WAAS) Express on a WAN interface, use the **waas enable** command in interface configuration mode. To disable WAAS Express on a WAN interface, use the **no** form of this command.

**waas enable**  
**no waas enable** [ **forced** | **remove-config** ]

Syntax Description	forced	(Optional) Stops all WAAS Express optimization flows.
	remove-config	(Optional) Removes all WAAS Express-related configurations.

**Command Default** WAAS Express is disabled.

**Command Modes** Interface configuration (config-if)

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

**Usage Guidelines** The **waas enable** command must be explicitly applied on each WAN interface. You can enable WAAS Express by using either the default class and policy maps created automatically or the class and policy maps that you define.



**Note** WAAS Express does not support the selection of a user-defined policy map to associate with the **waas enable** command. The default `waas_global` policy is used on the WAAS Express-enabled interface. You can modify the default `waas_global` policy. The default WAAS Express policy is extracted from the default WAAS policy.

### Examples

The following example shows how to enable WAAS Express on an Ethernet interface:

```
Device> enable
Device# configure terminal
Device(config)# interface ethernet 0/0
Device(config-if)# waas enable
Device(config-if)# exit
```

Related Commands	Command	Description
	<b>class-map type waas</b>	Configures a WAAS Express class map.
	<b>parameter-map type waas</b>	Configures WAAS Express global parameters.
	<b>policy-map type waas</b>	Configures a WAAS Express policy map.

## waas-ssl-trustpoint

To associate a trustpoint with Secure Sockets Layer (SSL)-Express accelerator, use the **waas-ssl-trustpoint** command in WAAS SSL configuration mode. To associate SSL-Express accelerator with a self-enrolled trustpoint, use the **no** form of this command.

**waas-ssl-trustpoint** *label*  
**no waas-ssl-trustpoint**

### Syntax Description

<i>label</i>	Label of the trustpoint.
--------------	--------------------------

### Command Default

SSL-Express accelerator is associated with a self-enrolled trustpoint.

### Command Modes

WAAS SSL configuration (config-waas-ssl)

### Command History

Release	Modification
15.2(3)T	This command was introduced.

### Usage Guidelines

The trustpoint associated with SSL-Express accelerator should already exist. You can create a trustpoint by using the **crypto pki trustpoint** command. An identity certificate should be enrolled under this trustpoint for WAAS Express to accept this configuration. This identity certificate is then used for the peering session established by the SSL-Express accelerator between WAAS Express devices.

SSL-Express accelerator, if enabled, generates a self-enrolled trustpoint and configures the trustpoint name using the **waas-ssl-trustpoint** command in the following situations:

- SSL-Express accelerator is enabled without any trustpoint configured and no self-signed certificate exists on the device.
- The trustpoint configured using the **waas-ssl-trustpoint** command is deleted.
- You use the **no** form of this command.



### Note

Using a trustpoint with certificate revocation check and configuring the **peer-cert-verify enable** command can result in an increase in the latency.

Before you can enable the **waas-ssl-trustpoint** command, use the following commands:

- Use the **parameter-map type waas** command in global configuration mode to enter parameter map configuration mode.
- Use the **accelerator ssl-express** command in parameter map configuration mode to enter WAAS SSL configuration mode.

### Examples

The following example shows how to associate a trustpoint with SSL-Express accelerator:

```

Device(config)# parameter-map type waas waas_global
Device(config-profile)# accelerator ssl-express
Device(config-waas-ssl)# enable
Device(config-waas-ssl)# waas-ssl-trustpoint ssl-tp

```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>accelerator</b>	Enters a specific WAAS Express accelerator configuration mode based on the accelerator being configured.
<b>crypto pki trustpoint</b>	Declares the trustpoint that your router should use.
<b>parameter-map type waas</b>	Configures WAAS Express global parameters.
<b>services host-service peering</b>	Configures the SSL-Express accelerator host peering service.
<b>show waas accelerator</b>	Displays information about WAAS Express accelerators.
<b>show waas statistics accelerator</b>	Displays statistical information about WAAS Express accelerators.

