sample (event trigger)

To specify the type of object sampling to use for an event, use the **sample** command in event trigger configuration mode. To disable teh configured settings, use the **no** form of this command.

sample {**absolute** | **delta** | **changed**}

no sample {**absolute** | **delta** | **changed**}

Syntax Description

absolute	Uses the present value of the MIB object while sampling.
delta	Uses the difference between the present value and the previous value sampled at the previous interval for sampling.
changed	Uses the Boolean condition to check if the present value is different from the previous value.

Command Default

The default sampling method is absolute.

Command Modes

Event trigger configuration (config-event-trigger)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

The **sample** command enables the specified sampling method for the object. You can specify the following sampling methods.

- Absolute
- Delta
- Changed

Absolute sampling uses the value of the MIB object during sampling. The default sampling method is absolute.

Delta sampling uses the last sampling value maintained in the application. This method requires applications to do continuous sampling.

The changed sampling method uses the changed value of the object since the last sample.

Examples

The following example shows how to specify the sampling method as absolute:

```
Router(config)# snmp mib event trigger owner owner1 name triggerA
Router(config-event-trigger)# sample absolute
```

Related Commands

Command	Description
snmp mib event trigger owner	Specifies owner for an event trigger.

sample (expression)

To specify the method of sampling the object, use the **sample** command in expression object configuration mode. To disable the specified method of object sampling, use the **no** form of this command.

sample {**absolute** | **delta** | **changed**}

no sample

Syntax Description

absolute	Uses the present value of the MIB object while sampling.
delta	Uses the difference between the present value and the previous value sampled at the previous interval for sampling.
changed	Uses a Boolean condition to check if the present value is different from the previous value.

Command Default

The default sampling method is absolute.

Command Modes

Expression object configuration (config-expression-object)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

The Expression MIB allows you to create expressions based on a combination of objects. The expressions are evaluated according to the sampling method. The Expression MIB supports the following types of object sampling:

- Absolute
- Delta
- Changed

The **sample** command enables the specified sampling method for the object. If there are no delta or changed values in an expression, the expression is evaluated when a requester attempts to read the value of the expression. In this case, all requesters get a newly calculated value.

For expressions with delta or change values, the evaluation is performed for every sampling. In this case, requesters get the value as of the last sample period.

Examples

The following example shows how to specify the sampling method as absolute:

```
Router(config)# snmp mib expression owner owner1 name expressionA
Router(config-expression)# object 32
Router(config-expression-object)# sample absolute
```

Related Commands

Command	Description
snmp mib expression owner	Specifies the owner for an expression.

scheduler heapcheck process

To perform a "sanity check" for corruption in memory blocks when a process switch occurs, use the **scheduler heapcheck process** command in global configuration mode. To disable this feature, use the **no** form of this command.

scheduler heapcheck process [**memory** [**fast**] [**io**] [**multibus**] [**pci**] [**processor**] [**checktype** {**all** | **data** | **magic** | **mlite-data** | **pointer** | **refcount** | **lite-chunks**}]]

no scheduler heapcheck process

Syntax Description

memory	(Optional) Specifies checking all memory blocks and memory pools.
fast	(Optional) Specifies checking the fast memory block.
io	(Optional) Specifies checking the I/O memory block.
multibus	(Optional) Specifies checking the multibus memory block.
pci	(Optional) Specifies checking the process control information (PCI) memory block.
processor	(Optional) Specifies checking the processor memory block.
checktype	(Optional) Specifies checking specific memory pools.
all	(Optional) Specifies checking the value of the block magic, red zone, size, refcount, and pointers (next and previous).
data	(Optional) Specifies checking the value of normal blocks.
magic	(Optional) Specifies checking the value of the block magic, red zone, and size.
mlite-data	(Optional) Specifies checking the value of memory allocation lite (malloc-lite) blocks.
pointer	(Optional) Specifies checking the value of the next and previous pointers.
refcount	(Optional) Specifies checking the value of the block magic and refcount.
lite-chunks	(Optional) Specifies checking the memory blocks allocated by the memory allocation lite (malloc_lite) feature.

Defaults

This command is disabled by default. If no keywords are specified, a sanity check will be performed on all the memory blocks and memory pools.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.3(11)T	The **lite-chunks** keyword was added.
12.4(20)T	The **data** and **mlite-data** keywords were added.

Usage Guidelines

When configuring this command, you can choose none or all memory block keywords (**fast**, **io**, **multibus**, **pci**, **processor**, and **checktype**).

Enabling this command has a significant impact on router performance.

Examples

The following example shows how to sanity check for corruption in the I/O memory block when a process switch occurs. In this example, the values of only the block magic, red zone, and size will be checked.

```
scheduler heapcheck process memory io checktype magic
```

The following example shows how to sanity check for corruption in the processor memory block when a process switch occurs. In this example, the values of only the next and previous pointers will be checked.

```
scheduler heapcheck process memory processor checktype pointer
```

Related Commands

Command	Description
memory lite	Enables the malloc_lite feature.
memory sanity	Performs a “sanity check” for corruption in buffers and queues.

schema

To specify the bulk statistics schema to be used in a specific bulk statistics transfer configuration, use the **schema** command in Bulk Statistics Transfer configuration mode. To remove a previously configured schema from a specific bulk statistics transfer configuration, use the **no** form of this command.

schema *schema-name*

no schema *schema-name*

Syntax Description

schema-name	Name of a previously configured bulk statistics schema.

Command Default

No bulk statistics schema is specified.

Command Modes

Bulk Statistics Transfer configuration (config-bulk-tr)

Command History

Release	Modification
12.0(24)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(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.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS Release XE 2.1.

Usage Guidelines

Repeat this command as desired for a specific bulk statistics transfer configuration. Multiple schemas can be associated with a single transfer configuration; all collected data will be in a single bulk statistics data file (VFile).

Examples

In the following example, the bulk statistics schemas ATM2/0-IFMIB and ATM2/0-CAR are associated with the bulk statistics transfer configuration called bulkstat1:

```
Router(config)# snmp mib bulkstat transfer bulkstat1
Router(config-bulk-tr)# schema ATM2/0-IFMIB
Router(config-bulk-tr)# schema ATM2/0-CAR
Router(config-bulk-tr)# url primary ftp://user:pswrd@host/folder/bulkstat1
Router(config-bulk-tr)# retry 2
Router(config-bulk-tr)# retain 10
Router(config-bulk-tr)# exit
```

Related Commands

Command	Description
snmp mib bulkstat transfer	Names a bulk statistics transfer configuration and enters Bulk Statistics Transfer configuration mode.

scripting tcl encdir

To specify the default location of external encoding files used by the Tool Command Language (Tcl) shell, use the **scripting tcl encdir** command in global configuration mode. To remove the default location, use the **no** form of this command.

scripting tcl encdir *location-url*

no scripting tcl encdir

Syntax Description

location-url	The URL used to access external encoding files used by Tcl.

Defaults

Tcl does not use external encoding files.

Command Modes

Global configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
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.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

Character strings in Tcl are encoded using 16-bit Unicode characters. Different operating system interfaces or applications can generate character strings using other encoding methods. Use the **scripting tcl encdir** command to configure a location URL for the external Tcl character encoding files to support the Tcl **encoding** command.

Tcl contains only a few character sets within the Tcl shell. Additional characters sets are loaded, as needed, from external files.

Examples

The following example shows how to specify a default location for external encoding files to be used by Tcl:

```
Router# configure terminal
Router(config)# scripting tcl encdir tftp://10.18.117.23/file2/
```

Related Commands

Command	Description
scripting tcl init	Specifies an initialization script for the Tcl shell.
tclsh	Enables the Tcl shell and enters Tcl configuration mode.

scripting tcl init

To specify an initialization script for the Tool Command Language (Tcl) shell, use the **scripting tcl init** command in global configuration mode. To remove the initialization script, use the **no** form of this command.

scripting tcl init *init-url*

no scripting tcl init

Syntax Description

init-url	The URL used to access the initialization script to be used by Tcl.

Defaults

Tcl does not run an initialization script.

Command Modes

Global configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
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.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

Use the **scripting tcl init** command when you want to predefine Tcl procedures to run in an initialization script. The initialization script runs when the Tcl shell is entered and saves manual sourcing of the individual scripts.

Examples

The following example shows how to specify an initialization script to run when the Tcl shell is enabled:

```
Router# configure terminal
Router(config)# scripting tcl init ftp://user:password@172.17.40.3/tclscript/initfile3.tcl
```

Related Commands

Command	Description
scripting tcl encdir	Specifies the default location of external encoding files used by the Tcl shell.
tclsh	Enables the Tcl shell and enters Tcl configuration mode.

scripting tcl low-memory

To set a low memory threshold for free memory for Tool Command Language (Tcl)-based applications, use the **scripting tcl low-memory** command in global configuration mode. To remove the specific low memory threshold and return to using the default value, use the **no** form of this command.

scripting tcl low-memory *bytes*

no scripting tcl low-memory

Syntax Description

bytes	Specifies the low memory threshold. The memory threshold can be set from 0 to 4294967295 bytes.

Defaults

The default value is 25 percent of the available free memory at start up when Tcl initializes.

Note The default is platform-specific. (It depends on how much memory is installed, and how much memory is free when Tcl initializes).

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
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.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

Use the **scripting tcl low-memory** command to set the threshold for free memory. If minimum free RAM drops below this threshold, Tcl aborts the current script. This prevents the Tcl interpreter from allocating too much RAM and crashing the router.

Examples

The following example shows how to set the threshold for free memory when the Tcl shell is initialized:

```
Router# configure terminal
Router(config)# scripting tcl low-memory 33117513
```

Related Commands

Command	Description
scripting tcl encdir	Specifies the default location of external encoding files used by the Tcl shell.
scripting tcl init	Specifies an initialization script for the Tcl shell.
tclsh	Enables the Tcl shell and enters Tcl configuration mode.

scripting tcl secure-mode

To enable signature verification of the interactive Tool Command Language (Tcl) scripts, use the **scripting tcl secure-mode** command in global configuration mode. To disable signature verification of the interactive Tcl scripts, use the **no** form of this command.

scripting tcl secure-mode

no scripting tcl secure-mode

Syntax Description

This command has no arguments or keywords.

Command Default

The signature verification of the interactive Tcl scripts is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(15)T	This command was introduced.

Usage Guidelines

Use the **scripting tcl secure-mode** command to enable signature verification of all Tcl scripts run on the router. By default, the signature verification of the interactive Tcl scripts is disabled. You must enable the signature verification in order to verify whether the Tcl scripts match their digital signature. That would indicate they have not been altered since the digital signature was generated. If the script does not contain the digital signature, the script may run in a limited mode for untrusted script (that is, a script that has failed signature verification) or may not run at all. After receiving the results from the signature verification, the scripts are executed.

A Cisco IOS Crypto image software is required to enable this command and configure the Signed Tcl Scripts feature. The Crypto configuration commands enable the Cisco x.509 certificate storage. The **scripting tcl secure-mode** command can be enabled after the Crypto configuration trustpoint commands are enabled.

The **scripting tcl trustpoint name** command must be configured with the **scripting tcl secure-mode** command to verify the integrity of Tcl script signatures run on the router. Both commands must be configured to fully operate the feature; otherwise, a syslog message is generated:

```
*Jun 13 17:35:14.219: %SYS-6-SCRIPTING_TCL_INVALID_OR_MISSING_SIGNATURE: tcl signing
validation failed on script signed with trustpoint name mytrust, cannot run the signed TCL
script.
```

In addition, the **crypto pki trustpoint** *name* command provided should contain a certificate that matches the certificate that was originally used to generate the digital signature on the Tcl script.

Examples

The following example shows how to enable signature verification of the interactive Tcl scripts:

```
Router(config)# crypto pki trustpoint mytrust
Router(ca-trustpoint)# enrolment terminal
Router(ca-trustpoint)# exit
```

```
Router(config)# crypto pki authenticate mytrust
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
MIIEuDCCA6CgAwIBAgIBADANBgkqhkiG9w0BAQQFADCBnjELMAkGA1UEBhMCVVMx
EzARBgNVBAgTCkNhbGlmb3JuaWExETAPBgNVBAcTCFNhbiBKb3NlMRwwGgYDVQQK
ExNDaXNjbyBTeXN0ZW1zLCBJbmMuMQ4wDAYDVQQLEwVOU1NURzEWMBQGA1UEAxMN
Sm9obiBMYXV0bWFubjEhMB8GCSqGSIb3DQEJARYSamxhdXRtYW5AY2lzY28uY29t
MB4XDTA2MTExNzE3NTgwMVoXDTA5MTExNjE3NTgwMVowgZ4xCzAJBgNVBAYTAlVT
MRMwEQYDVQQIEwpDYWxpZm9ybmlhMREwDwYDVQQHEwhTYW4gSm9zZTEcMBoGA1UE
ChMTQ2lzY28gU3lzdGVtcywgSW5jLjEOMAwGA1UECxMFTlNTVEcxFjAUBgNVBAMT
DUpvaG4gTGF1dG1hbm4xITAfBgkqhkiG9w0BCQEWEmpsYXV0bWFuQGNpc2NvLmNv
bTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALxtqTMCirMb+CdyWLuH
oWAM8CEJDwQggL7MWBhoi3TSMd/ww2XBB9biBtdlH6jHsjCiOwAR5OorakwfPyf7
mvRJ2PqJALs+Vn93VBKIG6rZUl4+wdOx686BVddIZvEJQPbROiYTzfazWV70aLMV
bd7/B7vF1SG1YK9y1tX9p9nZyZ0x47OAXetwOaGinvlG7VNuTXaASBLUjCRZsIlz
SBrXXedBzZ6+BuoWm1FK45EYSlag5Rt9RGXXMBqzx91iyhrJ3zDDmkExa45yKJET
mAgDVMcpeteJtif47UDZJK30g4MbMyx/c8WGhmJ54qRL9BZEPmDxMQkNP10l8MAl
Q8sCAwEAAaOB/jCB+zAdBgNVHQ4EFgQU9/ToDvbMR3JfJ4xEa4X47oNFq5kwgcsG
A1UdIwSBwzCBwIAU9/ToDvbMR3JfJ4xEa4X47oNFq5mhgaSkgaEwgZ4xCzAJBgNV
BAYTAlVTMRMwEQYDVQQIEwpDYWxpZm9ybmlhMREwDwYDVQQHEwhTYW4gSm9zZTEc
MBoGA1UEChMTQ2lzY28gU3lzdGVtcywgSW5jLjEOMAwGA1UECxMFTlNTVEcxFjAU
BgNVBAMTDUpvaG4gTGF1dG1hbm4xITAfBgkqhkiG9w0BCQEWEmpsYXV0bWFuQGNp
c2NvLmNvbYIBADAMBgNVHRMEBTADAQH/MA0GCSqGSIb3DQEBBAUAA4IBAQBtEs/4
MQeN9pT+XPCPg2ObQU8y2AadI+I34YK+fDHsFOh68hZhpszTN2VpNEvkFXpADhgr
7DkNGtwTCla481v70iNFViQVL+inNrZwWMxoTnUNCK7Hc5kHkXt6cj0mvsefVUzx
Xl70mauhESRVlmYWrJxSsrEILerZYsuv5HbFdand+/rErmP2HVyfdntLnKdSzmXJ
5lwE/Et2QtYNGor0OBlLesowfslR3LhHi4wn+5is7mALgNw/NuTiUr1zH18OeB4m
wcpBIJsLaJu6ZUJQl7IqdswSa3fHd5qq0/k8P9z0YAYrf3+MFQr4ibvsYvHlO087
o2Js1gW4qz34pqNh

Certificate has the following attributes:
       Fingerprint MD5: 1E327DBB 330936EB 2FB8EACB 4FD1133E
      Fingerprint SHA1: EE7FF9F4 05148842 B9D50FAC D76FDC9C E0703246
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported

Router(config)# scripting tcl secure-mode
Router(config)# scripting tcl trustpoint name mytrust
```

Related Commands

Command	Description
scripting tcl trustpoint name	Associates an existing configured trustpoint name with a certificate to verify Tcl scripts.

scripting tcl trustpoint name

To associate an existing configured trustpoint name with a certificate to verify Tool Command Language (Tcl) scripts, use the **scripting tcl trustpoint name** command in global configuration mode. To remove an existing configured trustpoint name, use the **no** form of this command.

scripting tcl trustpoint name *name*

no scripting tcl trustpoint name *name*

Syntax Description

name	Name of the configured trustpoint name associated with a certificate. Only one name can be associated with one certificate.

Command Default

A trustpoint name is not associated with a certificate to verify the Tcl scripts.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(15)T	This command was introduced.

Usage Guidelines

Use the **scripting tcl trustpoint name** command to associate an existing configured trustpoint name with a certificate to verify Tcl scripts. This way, Tcl identifies which certificate is used for verifying the Tcl scripts. The name must match an existing configured trustpoint name, otherwise, the command is rejected with an error message on the console. You can enter the command multiple times and configure multiple trustpoint names. Once you enter the command, you cannot modify the trustpoint name. However, you can remove the trustpoint name using the **no** form of the command. You must individually remove each name. When the last name is removed, no signature checking is performed, and the untrusted script (that is, a script that has failed signature verification) action configured by the **scripting tcl trustpoint untrusted** command is also removed.

A Cisco IOS Crypto image software is required to enable this command and configure the Signed Tcl Scripts feature. The Crypto configuration commands enable the Cisco x.509 certificate storage. The **scripting tcl trustpoint name** command can be enabled after the Crypto configuration trustpoint commands are enabled.

The **scripting tcl secure-mode** command must be configured with the **scripting tcl trustpoint name** command to verify the integrity of Tcl script signatures run on the router. Both commands must be configured to fully operate this feature; otherwise, a syslog message is generated:

```
*Jun 13 17:53:31.659: %SYS-6-SCRIPTING_TCL_SECURE_TRUSTPOINT: scripting tcl secure-mode is
enabled, however no scripting tcl trustpoint names configured, cannot verify signed TCL
script.
```

In addition, the **crypto pki trustpoint** *name* command provided should contain a certificate that matches the certificate that was originally used to generate the digital signature on the Tcl script.

Examples

The following example shows how the **scripting tcl trustpoint name** command is used to associate existing trustpoint names. Different names can be used for different departments with certificates:

```
Router(config)# crypto pki trustpoint mytrust
Router(ca-trustpoint)# enrolment terminal
Router(ca-trustpoint)# exit
Router(config)# crypto pki authenticate mytrust
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
MIIEuDCCA6CgAwIBAgIBADANBgkqhkiG9w0BAQQFADCBnjELMAkGA1UEBhMCVVMx
EzARBgNVBAgTCkNhbGlmb3JuaWExETAPBgNVBAcTCFNhbiBKb3NlMRwwGgYDVQQK
ExNDaXNjbyBTeXN0ZW1zLCBJbmMuMQ4wDAYDVQQLEwVOU1NURzEWMBQGA1UEAxMN
Sm9obiBMYXV0bWFubjEhMB8GCSqGSIb3DQEJARYSamxhdXRtYW5AY2lzY28uY29t
MB4XDTA2MTExNzE3NTgwMVoXDTA5MTExNjE3NTgwMVowgZ4xCzAJBgNVBAYTAlVT
MRMwEQYDVQQIEwpDYWxpZm9ybmlhMREwDwYDVQQHEwhTYW4gSm9zZTEcMBoGA1UE
ChMTQ2lzY28gU3lzdGVtcywgSW5jLjEOMAwGA1UECxMFTlNTVEcxFjAUBgNVBAMT
DUpvaG4gTGF1dG1hbm4xITAfBgkqhkiG9w0BCQEWEmpsYXV0bWFuQGNpc2NvLmNv
bTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALxtqTMCirMb+CdyWLuH
oWAM8CEJDwQggL7MWBhoi3TSMd/ww2XBB9biBtdlH6jHsjCiOwAR5OorakwfPyf7
mvRJ2PqJALs+Vn93VBKIG6rZUl4+wdOx686BVddIZvEJQPbROiYTzfazWV70aLMV
bd7/B7vF1SG1YK9y1tX9p9nZyZ0x47OAXetwOaGinvlG7VNuTXaASBLUjCRZsIlz
SBrXXedBzZ6+BuoWm1FK45EYSlag5Rt9RGXXMBqzx91iyhrJ3zDDmkExa45yKJET
mAgDVMcpeteJtif47UDZJK30g4MbMyx/c8WGhmJ54qRL9BZEPmDxMQkNP10l8MAl
Q8sCAwEAAaOB/jCB+zAdBgNVHQ4EFgQU9/ToDvbMR3JfJ4xEa4X47oNFq5kwgcsG
A1UdIwSBwzCBwIAU9/ToDvbMR3JfJ4xEa4X47oNFq5mhgaSkgaEwgZ4xCzAJBgNV
BAYTAlVTMRMwEQYDVQQIEwpDYWxpZm9ybmlhMREwDwYDVQQHEwhTYW4gSm9zZTEc
MBoGA1UEChMTQ2lzY28gU3lzdGVtcywgSW5jLjEOMAwGA1UECxMFTlNTVEcxFjAU
BgNVBAMTDUpvaG4gTGF1dG1hbm4xITAfBgkqhkiG9w0BCQEWEmpsYXV0bWFuQGNp
c2NvLmNvbYIBADAMBgNVHRMEBTADAQH/MA0GCSqGSIb3DQEBBAUAA4IBAQBtEs/4
MQeN9pT+XPCPg2ObQU8y2AadI+I34YK+fDHsFOh68hZhpszTN2VpNEvkFXpADhgr
7DkNGtwTCla481v70iNFViQVL+inNrZwWMxoTnUNCK7Hc5kHkXt6cj0mvsefVUzx
Xl70mauhESRVlmYWrJxSsrEILerZYsuv5HbFdand+/rErmP2HVyfdntLnKdSzmXJ
5lwE/Et2QtYNGor0OBlLesowfslR3LhHi4wn+5is7mALgNw/NuTiUr1zH18OeB4m
wcpBIJsLaJu6ZUJQl7IqdswSa3fHd5qq0/k8P9z0YAYrf3+MFQr4ibvsYvHlO087
o2Js1gW4qz34pqNh

Certificate has the following attributes:
       Fingerprint MD5: 1E327DBB 330936EB 2FB8EACB 4FD1133E
      Fingerprint SHA1: EE7FF9F4 05148842 B9D50FAC D76FDC9C E0703246
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported

Router(config)# scripting tcl secure-mode
Router(config)# scripting tcl trustpoint name mytrust
Router(config)# scripting tcl trustpoint name dept_accounting
Router(config)# scripting tcl trustpoint name dept_hr
```

Related Commands

Command	Description
scripting tcl secure-mode	Enables signature verification of the interactive Tcl scripts.

scripting tcl trustpoint untrusted

To allow the interactive Tool Command Language (Tcl) scripts to run regardless of the scripts failing the signature check, use the **scripting tcl trustpoint untrusted** command in global configuration mode. To disallow the interactive Tcl scripts to run regardless of the scripts failing the signature check, use the **no** form of this command.

scripting tcl trustpoint untrusted {**execute** | **safe-execut**e | **terminate**}

no scripting tcl trustpoint untrusted

Syntax Description

execute	Executes Tcl scripts even if the signature verification fails. If the **execute** keyword is configured, signature verification is not at all performed. **Caution** Use of this keyword is usually not recommended because the signature verification is not at all performed.
safe-execute	Executed the Tcl script in safe mode if the signature verification fails.
terminate	Does not run the Tcl script if the signature verification fails. The default keyword is **terminate**.

Command Default

No script that fails signature verification can run; the script immediately stops.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(15)T	This command was introduced.

Usage Guidelines

Use the **scripting tcl trustpoint untrusted** command to allow the interactive Tcl scripts to run regardless of the scripts failing the signature check or in untrusted mode. The untrusted script (that is, a script that has failed signature verification) is not safe to use.

Caution Use of the **execute** keyword is usually not recommended because the signature verification is not at all performed.

The **execute** keyword is provided for internal testing purposes and to provide flexibility. For example in a situation where a certificate has expired but the other configurations are valid and you want to work with the existing configuration, then you can use the **execute** keyword to work around the expired certificate.

The **safe-execute** keyword allows the script to run in safe mode. You can use the **tclsafe** command and also enter the interactive Tcl shell safe mode to explore the safe mode Tcl commands that are available. In order to get a better understanding of what is available in this limited safe mode, use the **tclsafe** Exec command to explore the options.

The **terminate** keyword stops any script from running and reverts to default behavior. The default policy is to terminate. When the last trustpoint name is removed, the untrusted action is also removed. The untrusted action cannot be entered until at least one trustpoint name is configured for Tcl.

Note This command only applies to the Tcl shell; it does not impact other components that make use of Tcl. For example, Embedded Event Manager (EEM) cannot perform any signature checking.

Examples

The following example shows how to execute the Tcl script in safe mode if the signature verification fails:

```
Router(config)# scripting tcl trustpoint untrusted safe-execute
```

Related Commands

Command	Description
scripting tcl trustpoint name	Associates an existing configured trustpoint name with a certificate to verify Tcl scripts.
tclsafe	Enables the interactive Tcl shell untrusted safe mode.

server (boomerang)

To configure the server address for a specified boomerang domain, use the **server** command in boomerang configuration mode. To remove this command from the configuration file and restore the system to its default condition with respect to this command, use the **no** form of this command.

server *server-ip-address*

no server *server-ip-address*

Syntax Description

server-ip-address	IP address of the specified server.

Command Default

No default behavior or values.

Command Modes

Boomerang configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

The **server** command can be used only on a Director Response Protocol (DRP) agent. The boomerang client is the Director Response Protocol (DRP) agent.

Use the **server** command to specify a server address that is to be associated with a given domain name. This configuration overrides the server-to-DRP agent association that is configured on DistributedDirector.

Examples

The following example configures the server for a domain named www.boom1.com. The server address for www.boom1.com is 172.16.101.101:

```
Router(config)# ip drp domain www.boom1.com
Router(config-boomerang)# server 172.16.101.101

Router# show running-config
.
.
.
ip drp domain www.boom1.com
content-server 172.16.101.101
```

Related Commands

Command	Description
alias (boomerang)	Configures an alias name for a specified domain.
ip drp domain	Adds a new domain to the DistributedDirector client or configures an existing domain and puts the client in boomerang configuration mode.

Command	Description
show ip drp	Displays DRP statistics on DistributedDirector or a DRP server agent.
show ip drp boomerang	Displays boomerang information on the DRP agent.
ttl dns	Configures the number of seconds for which an answer received from the boomerang client will be cached by the DNS client.
ttl ip	Configures the IP TTL value for the boomerang response packets sent from the boomerang client to the DNS client in number of hops.

set (EEM)

To set the value of a local Embedded Event Manager (EEM) applet variable, use the **set** command in applet configuration mode. To remove the value of an EEM applet variable, use the **no** form of this command.

set *label* **_exit_status** *exit-value*

no set *label* **_exit_status** *exit-value*

Syntax Description

label	Unique identifier that can be any string value. Actions are sorted and run in ascending alphanumeric key sequence using the label as the sort key. If the string contains embedded blanks, enclose it in double quotation marks.
_exit_status	Specifies the EEM applet variable name. Currently only the **_exit_status** variable is supported. • *exit-value*—Integer value that represents the exit status for the applet. Zero represents an exit status of success, and a nonzero value represents an exit status of failure.

Command Default

No EEM applet variable values are set.

Command Modes

Applet configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(18)SXF4	This command was integrated into Cisco IOS Release 12.2(18)SXF4 to support Software Modularity images only.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(18)SXF5	This command was integrated into Cisco IOS Release 12.2(18)SXF5.

Usage Guidelines

In EEM applet configuration mode, three types of configuration statements are supported. The **event** commands are used to specify the event criteria to trigger the applet to run, the **action** commands are used to specify an action to perform when the EEM applet is triggered, and the **set** command is used to set the value of an EEM applet variable. Currently only the **_exit_status** variable is supported for the **set** command.

Examples

The following example shows how to set the **_exit_status** variable to represent a successful status after an event has occurred three times and an action has been performed:

```
Router(config)# event manager applet cli-match
Router(config-applet)# event cli pattern {.*interface loopback*} sync yes occurs 3
```

```
Router(config-applet)# action 1.0 cli command "no shutdown"
Router(config-applet)# set 1.0 _exit_status 0
```

Related Commands

Command	Description
event manager applet	Registers an event applet with the Embedded Event Manager and enters applet configuration mode.

set platform software trace

To set the trace level for a specific module within a process, use the **set platform software trace** command privileged EXEC or diagnostic mode command.

set platform software trace *process hardware-module slot module trace-level*

Syntax Description

process	Specifies the process whose tracing level is being set. Options currently include: • **chassis-manager**—The Chassis Manager process. • **cpp-control-process**—The CPP Control process • **cpp-driver**—The CPP driver process • **cpp-ha-server**—The CPP HA server process • **cpp-service-process**—The CPP service process • **forwarding-manager**—The Forwarding Manager process. • **host-manager**—The Host Manager process. • **interface-manager**—The Interface Manager process. • **ios**—The IOS process. • **logger**—The logging manager process • **pluggable-services**—The pluggable services process. • **shell-manager**—The Shell Manager process.
hardware-module	Specifies the hardware module where the process in which the trace level is being set is running. Options include: • **carrier-card**—The process is on a SPA Interface Processor (SIP). • **forwarding-processor**—The process is on an Embedded Services Processor (ESP). • **route-processor**—The process is on an RP.
slot	Specifies the slot of the *hardware-module*. Options include: • *number*—The number of the SIP slot of the hardware module where the trace level is being set. For instance, if you want to specify the SIP in SIP slot 2 of the router, enter 2 as the *number*. *SIP-slot*/*SPA-bay*—The number of the SIP router slot and the number of the SPA bay of that SIP. For instance, if you want to specify the SPA in bay 2 of the SIP in router slot 3, enter 3/2. • **cpp active**—The Cisco Packet Processor (CPP) in the active ESP. • **cpp standby**—The CPP in the standby ESP. • **f0**—The ESP in ESP slot 0. • **f1**—The ESP in ESP slot 1 • **fp active**—The active ESP. • **fp standby**—The standby ESP.

- **r0**—The RP in RP slot 0.
- **r1**—The RP in RP slot 1.
- **rp active**—The active RP.
- **rp standby**—The standby RP.

module — Specifies the module within the process where the tracing level is being set. Options include:

- **acl**—access control list module.
- **all-modules**—all modules within the process
- **aom**—Asynchronous Object Manager module.
- **apdb**—Access Policies database module.
- **bipc**—BIPC process module, which is responsible for inter-process communication.
- **btrace**—Btrace tracing module.
- **cce**—CCE client process module, which is responsible for common classification.
- **cef**—Cisco Express Forwarding module.
- **chasfs**—Chassis Filesystem module.
- **cman_fp**—Chassis Manager module on the ESP.
- **cmand**—Chassis Manager module.
- **cmcc**—Chassis Manager module on the SIP.
- **cpp_cp**—CPP Client Control process
- **cpp-debug**—CPP debugging process module.
- **cpp_dr**—CPP Driver process
- **cpp_ha**— CPP HA process
- **cpp_sp**—CPP Services process
- **ec**—Etherchannel module.
- **erspan**—Encapsulated Remote Switch Port Analyzer module.
- **ess**—Edge Switch Services module.
- **evlib**—Event module.
- **evutil**—Event Utility module.
- **flash**—Flash module.
- **fman**—Forwarding Manager module.
- **fpm**—Flexible Packet Match module.
- **frag**—Fragmentation module.
- **fw**—Firewall module.
- **hman**—Host Manager module.
- **icmp**—ICMP module.

- **imand**—Interface Manager module.
- **imccd**—Interface Manager module on the SIP.
- **interfaces**—interface module.
- **IOSCC**—IOS module on the SIP.
- **IOSRP**—IOS module on the RP.
- **iosd**—IOS module.
- **ipc**—Inter-Process Communication module.
- **iphc**—IP Header Compression module.
- **ipsec**—IPSEC module.
- **mlp**—Multilink PPP module.
- **mqipc**—Message queue module.
- **nat**—Network Address Translation module.
- **netflow**—Netflow module.
- **om**—Object Manager module.
- **pam_updb**—User database module.
- **peer**—Peer information modules.
- **psdui**—Export module.
- **punt**—Punt information module.
- **qos**—Quality of Service modules.
- **route-map**—Route map modules.
- **services**—Services.
- **stile**—STILE modules.
- **tdllib**—Type management modules.
- **tppiosrp**—The utility library module.
- **ttymon**—The console monitoring module.
- **uihandler**—CLI command handler modules.
- **uiparse**—User interface parsing modules.
- **uipeer**—User interface peer modules.
- **uistatus**—User interface status modules.
- **urpf**—Unicast Reverse Path Forwarding modules.
- **usernames**—User module.

trace-level	Specifies the trace level. Options include: • **emergency**—Emergency level tracing. An emergency-level trace message is a message indicating the system is unusable. • **error**—Error level tracing. An error-level tracing message is a message indicating a system error. • **warning**—Warning level tracing. A warning-level tracing message is a message indicating a warning about the system. • **info**—Information level tracing. An information-level tracing message is a non-urgent message providing information about the system. • **debug**—Debug level tracing. A debug-level trace message is a non-urgent message providing a large amount of detail about the module. • **verbose**—Verbose level tracing. All possible tracing messages are sent when the trace level is set to verbose. • **noise**—Noise level tracing. The noise level is always equal to the highest tracing level possible and always generates every possible tracing message. The noise level is always equal to the highest-level tracing message possible for a module, even if future enhancements to this command introduce options that allow users to set higher tracing levels.

Command Modes

Privileged EXEC (#)
Diagnostic (diag)

Defaults

The default tracing level for all modules on the Cisco ASR 1000 series routers is critical.

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced.

Usage Guidelines

The *module* options vary by process and by *hardware-module*. Use the **?** option when entering this command to see which *module* options are available with each keyword sequence.

Use the **show platform software trace message** command to view trace messages.

Trace files are stored in the tracelogs directory in the harddisk: file system. These files can be deleted without doing any harm to your router operation.

Trace file output is used for debugging. The trace level is a setting that determines how much information about a module should be stored in trace files. The levels are documented in Table 35.

Table 35 Tracing Levels and Descriptions

Trace Level	Level Number	Description
Emergency	0	The message is regarding an issue that makes the system unusable.
Alert	1	The message is regarding an action that must be taken immediately.
Critical	2	The message is regarding a critical condition. This is the default setting for every module on the Cisco ASR 1000 Series Routers.
Error	3	The message is regarding a system error.
Warning	4	The message is regarding a system warning
Notice	5	The message is regarding a significant issue, but the router is still working normally.
Informational	6	The message is useful for informational purposes only.
Debug	7	The message provides debug-level output.
Verbose	8	All possible tracing messages are sent.
Noise	-	All possible trace messages for the module. The noise level is always equal to the highest possible tracing level. Even if a future enhancement to tracing introduces a higher tracing level, the noise level will become equal to the level of that new enhancement.

Trace level settings are leveled, meaning that every setting will contain all messages from the lower setting plus the messages from its own setting. For instance, setting the trace level to 3(error) ensures that the trace file will contain all output for the 0 (emergencies), 1 (alerts), 2 (critical), and 3 (error) settings. Setting the trace level to 4 (verbose) will ensure that all trace output for the specific module will be included in that trace file.

All trace levels are not user-configurable. Specifically, the alert, critical, and notice tracing levels cannot be set by users. If you wish to trace these messages, set the trace level to a higher level that will collect these messages.

Caution Setting tracing of a module to the debug level or higher can have a negative performance impact. Setting tracing to this level or higher should be done with discretion.

Caution Setting a large number of modules to a high tracing levels can severely degrade performance. If a high level of tracing is needed in a specific context, it is almost always preferable to set a single module on a higher tracing level rather than setting multiple modules to high tracing levels.

Examples

In the following example, the trace level for the ACL module in the Forwarding Manager of the ESP processor in slot 0 is set to the informational tracing level (info).

```
set platform software trace forwarding-manager F0 acl info
```

Related Commands

Command	Description
show platform software trace level	Displays trace levels for specified modules.
show platform software trace message	Displays trace messages.

shell environment load

To download Cisco IOS Shell (IOS.sh) environment from a specified file to the current TTY, use the **shell environment load** command in privileged EXEC mode.

shell environment load *filename:URL* {**merge** | **replace**}

Syntax Description

filename:URL	The URL of the shell environment file.
merge	Merge into the current shell environment.
replace	Replace the current shell environment

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(4)M	This command was introduced.
15.1(2)S	This command was integrated into Cisco IOS Release 15.1(2)S.

Usage Guidelines

Use the **shell environment load** command to download the Cisco IOS.sh environment from a specified file to the current terminal. Use the **shell environment save** command to save this specific file prior to loading the file using the **shell environment load** command.

Examples

This example shows how to save and then load a Cisco IOS.sh environment file and merge it into the current shell environment:

```
Router> enable
Router# configure terminal
Router(config)#
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# shell processing full
Router# exit
Router# shell environment save disk0:URL
Router# shell environment load disk0:URL merge
```

Related Commands

Command	Description
shell environment save	Saves a Cisco IOS.sh environment functions to a specific file.
show shell environment	Displays a Cisco IOS.sh environment information.

shell environment save

To save all current Cisco IOS Shell (IOS.sh) environment functions to a specific file, use the **shell environment save** command in privileged EXEC mode.

shell environment save *filename***:***URL*

Syntax Description

filename:URL	The URL of the shell environment file.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(4)M	This command was introduced.
15.1(2)S	This command was integrated into Cisco IOS Release 15.1(2)S.

Usage Guidelines

Use the **shell environment save** command to save all current shell environment, except built-in shell functions, to a specified file. Then only you can use the **shell environment load** command to load the Cisco IOS.sh environment in the specific file on the current terminal.

Examples

This example shows how to save a Cisco IOS.sh environment file:

```
Router> enable
Router# configure terminal
Router(config)#
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# shell processing full
Router# exit
Router# shell environment save disk0:URL
```

Related Commands

Command	Description
shell environment load	Downloads a Cisco IOS.sh environment from a specified file to the current TTY.
show shell environment	Displays a Cisco IOS.sh environment information.

shell init

To enable Cisco IOS Shell (IOS.sh) initialization options, use the **shell init** command in global configuration mode. To disable the Cisco IOS.sh initialization options, use the **no** form of this command.

shell init {*filename:URL* **no-exec**}

no shell init

Syntax Description

filename:URL	The URL of the shell environment file.
no-exec	Stores the initialization filename and loads the saved environment from that file at the next rebooting of the router.

Defaults

Cisco IOS.sh initialization is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(4)M	This command was introduced.
15.1(2)S	This command was integrated into Cisco IOS Release 15.1(2)S.

Usage Guidelines

Use the **shell init** command to provide Cisco IOS.sh environment access to everyone who logs on to the router. If this command is configured, during system boot up, the router automatically reads and loads the content of the shell configuration from the given file which includes the user-defined variables and functions created previously. It copies the saved files into the Cisco IOS.sh environment. When you use the **no-exec** keyword, it allows you to store the initialization filename and loads the saved environment from that file at the next rebooting of the router.

Note This command is similar to the **show environment load** command which allows you to download the Cisco IOS.sh environment operations.

Examples

This example shows how to enable Cisco IOS.sh processing in all IOS modes:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# shell processing full
Router(config)# shell init disk0:URL
```

Related Commands

Command	Description
show environment load	Downloads a Cisco IOS.sh environment operations.

shell processing

To restore the default behavior of Cisco IOS Shell (IOS.sh) processing, use the **shell processing** command in global configuration mode. To disable the Cisco IOS.sh functions, use the **no** form of this command.

shell processing {**full**}

no shell processing

Syntax Description

full	Enables shell processing.

Defaults

Cisco IOS.sh processing is enabled for other applications to use the shell functions.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(4)M	This command was introduced.
15.1(2)S	This command was integrated into Cisco IOS Release 15.1(2)S.

Usage Guidelines

To enable shell processing and access all its functions, it is recommended that you use the **shell processing full** command. This allows you the ability to use shell processing in the configuration level without entering the **terminal shell** command on your terminal at the EXEC level. Use the **no shell processing** command to disable Cisco IOS.sh processing on the router. To restore the default Cisco IOS.sh processing, use the **shell processing** command. To reenable shell processing and access all its functions, it is recommended that you use the **shell processing full** command.

You can turn shell processing on the terminal by using the **terminal shell** EXEC command. However shell processing feature is only on while the terminal is running. Once the terminal is turned off, shell processing is off. When the **terminal shell** command is used, shell processing is not visible in the running configuration because it is only on the terminal level and is not in the configuration level. It is convenient to use the **terminal shell** command at the terminal level to quickly access the Cisco IOS.sh man commands.

To enable shell processing and access all its functions in the configuration, it is recommended that you use the **shell processing full** command.

Examples

This example shows how to enable Cisco IOS.sh processing in all Cisco IOS configuration modes:

```
Router> enable
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# shell processing full
```

show buffers leak

Command	Description
terminal shell	Enables Cisco IOS.sh functions on the router.

To display the details of all the buffers that are older than one minute in the system, use the **show buffers leak** command in user EXEC or privileged EXEC mode.

show buffers leak [**resource user**]

Syntax Description

resource user	(Optional) Displays the resource user information to which the leaked buffers belong to.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Examples

The following is sample output from the **show buffers leak** command:

```
Router# show buffers leak

Header   DataArea Pool    Size  Link Enc    Flags      Input     Output   User

6488F464  E000084 Small    74    0    0       10       None       None EEM ED Sy
6488FB5C  E000304 Small    74    0    0       10       None       None EEM ED Sy
648905D0  E0006C4 Small    61    0    0        0       None       None EEM ED Sy
648913C0  E000BC4 Small    74    0    0       10       None       None EEM ED Sy
6489173C  E000D04 Small    74    0    0       10       None       None EEM ED Sy
648921B0  E0010C4 Small    60    0    0        0       None       None Init
6489252C  E001204 Small   103    0    0       10       None       None EEM ED Sy
64892C24  E001484 Small    74    0    0       10       None       None EEM ED Sy
64892FA0  E0015C4 Small    74    0    0       10       None       None EEM ED Sy
64893A14  E001984 Small    74    0    0       10       None       None EEM ED Sy
64893D90  E001AC4 Small    61    0    0        0       None       None EEM ED Sy
64894804  E001E84 Small    61    0    0        0       None       None EEM ED Sy
6517CB64  E32F944 Small    74    0    0       10       None       None EEM ED Sy
6517D25C  E176D44 Small    74    0    0       10       None       None EEM ED Sy
6517D5D8  E176E84 Small    74    0    0       10       None       None EEM ED Sy
6517D954  E209A84 Small    74    0    0       10       None       None EEM ED Sy
6517E744  E209D04 Small    61    0    0        0       None       None EEM ED Sy
6517EE3C  E29CBC4 Small    61    0    0        0       None       None EEM ED Sy
65180324  E177844 Small    74    0    0       10       None       None EEM ED Sy
65180D98  E177C04 Small    61    0    0        0       None       None EEM ED Sy
65E1F3A0  E4431A4 Small   102    0    0        0       None       None EEM ED Sy
64895278  E002644 Middl   191    0    0       10       None       None EEM ED Sy
64895CEC  E003004 Middl   173    0    0       10       None       None EEM ED Sy
64896068  E003344 Middl   176    0    0       10       None       None EEM ED Sy
648963E4  E003684 Middl   191    0    0       10       None       None EEM ED Sy
64896E58  E004044 Middl   109    0    0       10       None       None EEM ED Sy
```

```
64897C48  E004D44 Middl   194     0     0        10        None       None EEM ED Sy
65181F04  E330844 Middl   173     0     0        10        None       None EEM ED Sy
65183070  E3C3644 Middl   105     0     0        10        None       None EEM ED Sy
65DF9558  E4746E4 Middl   107     0     0         0        None       None EEM ED Sy
65DFA6C4  E475724 Middl   116     0     0         0        None       None EEM ED Sy
65DFADBC  E475DA4 Middl   115     0     0         0        None       None EEM ED Sy
65DFC620  E477464 Middl   110     0     0         0        None       None EEM ED Sy
64C64AE0        0 FS He     0     0     3         0        None       None Init
64C64E5C        0 FS He     0     0     3         0        None       None Init
64C651D8        0 FS He     0     0     3         0        None       None Init
64C65554        0 FS He     0     0     0         0        None       None Init
64C658D0        0 FS He     0     0     0         0        None       None Init
64C65C4C        0 FS He     0     0     0         0        None       None Init
64C65FC8        0 FS He     0     0     0         0        None       None Init
64C66344        0 FS He     0     0     0         0        None       None Init
64D6164C        0 FS He     0     0     0         0        None       None Init
64EB9D10        0 FS He     0     0     0         0        None       None Init
6523EE14        0 FS He     0     0     0         0        None       None Init
65413648        0 FS He     0     0     0         0        None       None Init
```

The following is sample output from the **show buffers leak resource user** command:

```
Router# show buffers leak resource user

Resource User:  EEM ED Syslog count:       32
Resource User:           Init count:        2
Resource User:         *Dead* count:        2
Resource User: IPC Seat Manag count:       11
Resource User:      XDR mcast count:        2
```

Table 36 describes the significant fields shown in the display.

Table 36 show buffers leak Field Descriptions

Field	Description
Header	Buffer header.
DataArea	The area where the data is available.
Pool	The different buffer pools such as ipc, header, fs header, small, middle, big, very big, large, or huge buffers.
Size	Size of the buffer pool. For example, small buffers are less than or equal to 104 bytes long. Middle buffers are in the range of 105 to 600 bytes long.
Flags	Flags of a packet. The flag indicates whether a particular packet is an incoming packet or is generated by the router.
User	The resource user name.

Related Commands

Command	Description
buffer public	Enters the buffer owner configuration mode and sets thresholds for buffer usage.
buffer tune automatic	Enables automatic buffer tuning.

show buffers tune

To display the details of automatic tuning of buffers, use the **show buffers tune** command in user EXEC or privileged EXEC mode.

show buffers tune

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Examples

The following is sample output from the **show buffers tune** command:

```
Router# show buffers tune

Tuning happened for the pool Small
Tuning happened at 20:47:25
Oldvalues
permanent:50  minfree:20  maxfree:150
Newvalues
permanent:61  minfree:15  maxfree:76
Tuning happened for the pool Middle
Tuning happened at 20:47:25
Oldvalues
permanent:25  minfree:10  maxfree:150
Newvalues
permanet:36  minfree:9  maxfree:45
```

Table 37 describes the significant fields shown in the display.

Table 37 show buffers tune Field Descriptions

Field	Description
Oldvalues	The minimum and maximum free buffers before automatic tuning was enabled.
Newvalues	The minimum and maximum free buffers after automatic tuning was enabled.

Related Commands

Command	Description
buffer tune automatic	Enables automatic tuning of buffers.

show buffers usage

To display the details of the buffer usage pattern in a specified buffer pool, use the **show buffers usage** command in user EXEC or privileged EXEC mode.

show buffers usage [**pool** *pool-name*]

Syntax Description

pool	(Optional) Displays the details of a specified pool.
pool-name	(Optional) Specified pool. If a pool is not specified, details of all the pools are displayed. Valid values are ipc, header, fs header, small, middle, big, verybig, large, and huge.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Examples

The following is sample output from the **show buffers usage** command:

```
Router# show buffers usage

Statistics for the Small pool
Caller pc    : 0x626BA9E0 count:       20
Resource User: EEM ED Sys count:       20
Caller pc    : 0x60C71F8C count:        1
Resource User:       Init count:        1
Number of Buffers used by packets generated by system:   62
Number of Buffers used by incoming packets:               0

Statistics for the Middle pool
Caller pc    : 0x626BA9E0 count:       12
Resource User: EEM ED Sys count:       12
Number of Buffers used by packets generated by system:   41
Number of Buffers used by incoming packets:               0

Statistics for the Big pool
Number of Buffers used by packets generated by system:   50
Number of Buffers used by incoming packets:               0

Statistics for the VeryBig pool
Number of Buffers used by packets generated by system:   10
Number of Buffers used by incoming packets:               0

Statistics for the Large pool
Number of Buffers used by packets generated by system:    0
Number of Buffers used by incoming packets:               0

Statistics for the Huge pool
Number of Buffers used by packets generated by system:    0
```

```
Number of Buffers used by incoming packets:               0

Statistics for the IPC pool
Number of Buffers used by packets generated by system:    2
Number of Buffers used by incoming packets:               0

Statistics for the Header pool
Number of Buffers used by packets generated by system:  511
Number of Buffers used by incoming packets:               0

Statistics for the FS Header pool
Caller pc    : 0x608F68FC count:        9
Resource User:       Init count:       12
Caller pc    : 0x61A21D3C count:        1
Caller pc    : 0x60643FF8 count:        1
Caller pc    : 0x61C526C4 count:        1
Number of Buffers used by packets generated by system:   28
Number of Buffers used by incoming packets:               0
```

The following is sample output from the **show buffers usage pool** command for the pool named small:

```
Router# show buffers usage pool small

Statistics for the Small pool
Caller pc    : 0x626BA9E0 count:       20
Resource User: EEM ED Sys count:       20
Caller pc    : 0x60C71F8C count:        1
Resource User:       Init count:        1
Number of Buffers used by packets generated by system:   62
Number of Buffers used by incoming packets:               0
```

Related Commands

Command	Description
buffer public	Enters buffer owner configuration mode and sets thresholds for buffer usage.
show buffers leak	Displays details of the buffers that have leaked.

show calendar

To display the current time and date setting for the hardware clock, use the **show calendar** command in EXEC mode:

show calendar

Syntax Description

This command has no arguments or keywords.

Command Modes

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.

Usage Guidelines

Some platforms have a hardware clock (calendar) which is separate from the software clock. The hardware clock is battery operated, and runs continuously, even if the router is powered off or rebooted.

You can compare the time and date shown with this command with the time and date listed via the **show clock** EXEC command to verify that the hardware clock and software clock are synchronized with each other. The time displayed is relative to the configured time zone.

Examples

In the following sample display, the hardware clock indicates the time stamp of 12:13:44 p.m. on Friday, July 19, 1996:

```
Router> show calendar

12:13:44 PST Fri Jul 19 1996
```

Related Commands

Command	Description
show clock	Displays the time and date from the system software clock.

show cdp

To display global Cisco Discovery Protocol (CDP) information, including timer and hold-time information, use the **show cdp** command in privileged EXEC mode.

show cdp [**vlan** *vlan*]

Syntax Description

vlan *vlan*	(Optional) Specifies a VLAN. Limits the display of switch port information to the specified VLAN. Range: 1 to 4094.

Command Default

No default behavior or values.

Command Modes

EXEC (#)
Privileged EXEC (>)

Command History

Release	Modification
10.3	This command was introduced.
12.0(3)T	The output of this command was modified to include CDP Version 2 information.
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.
12.2(33)SXI	This command was changed to add the optional **vlan** *vlan* keyword and argument.

Usage Guidelines

Cisco IOS Release 12.2(33)SXI and later releases allow you to limit the display of switch port information to the specified VLAN.

Examples

The following example shows that the current router is sending CDP advertisements every 1 minute (the default setting for the **cdp timer** global configuration command). Also shown is that the current router directs its neighbors to hold its CDP advertisements for 3 minutes (the default for the **cdp holdtime** global configuration command), and that the router is enabled to send CDP Version 2 advertisements:

```
Router# show cdp

Global CDP information:
Sending CDP packets every 60 seconds
Sending a holdtime value of 180 seconds
Sending CDPv2 advertisements is enabled
```

The following example shows how to limit the displayed CDP information to a specific VLAN:

```
Router# show cdp vlan 11
Global CDP information:
        Sending CDP packets every 60 seconds
        Sending a holdtime value of 180 seconds
        Sending CDPv2 advertisements is  enabled
```

Table 38 describes the significant fields shown in the display.

Table 38 show cdp Field Descriptions

Field	Definition
Sending CDP packets every XX seconds	The interval (in seconds) between transmissions of CDP advertisements. This field is controlled by the **cdp timer** command.
Sending a holdtime value of XX seconds	The amount of time (in seconds) the device directs the neighbor to hold a CDP advertisement before discarding it. This field is controlled by the **cdp holdtime** command.
Sending CDPv2 advertisements is XX	The state of whether CDP Version-2 type advertisements are enabled to be sent. Possible states are enabled or disabled. This field is controlled by the **cdp advertise v2** global configuration command.

Related Commands

Command	Description
cdp advertise-v2	Enables CDP Version 2 advertising functionality on a device.
cdp holdtime	Specifies the amount of time the receiving device should hold a CDP packet from your router before discarding it.
cdp timer	Specifies how often the Cisco IOS software sends CDP updates.
show cdp entry	Displays information about a specific neighbor device listed in the CDP table.
show cdp interface	Displays information about the interfaces on which CDP is enabled.
show cdp neighbors	Displays detailed information about neighboring devices discovered using CDP.
show cdp traffic	Displays information about traffic between devices gathered using CDP.

show cdp entry

To display information about a specific neighboring device discovered using Cisco Discovery Protocol (CDP), use the **show cdp entry** command in privileged EXEC mode.

show cdp entry {***** | *device-name*[*****]} [**version**] [**protocol**]

Syntax Description

*****	Displays all of the CDP neighbors.
device-name[*****]	Name of the neighbor about which you want information. You can enter an optional asterisk (*) at the end of a *device-name* as a wildcard. For example, entering **show cdp entry dev*** will match all device names that begin with **dev**.
version	(Optional) Limits the display to information about the version of software running on the router.
protocol	(Optional) Limits the display to information about the protocols enabled on a router.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.3	This command was introduced.
12.2(8)T	Support for IPv6 address and address type information was added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
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.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Examples

The following is sample output from the **show cdp entry** command. Information about the neighbor *device.cisco.com* is displayed, including device ID, protocols and addresses, platform, interface, hold time, and version.

```
Router# show cdp entry device.cisco.com

Device ID: device.cisco.com
Entry address(es):
  IP address: 10.1.17.24
  IPv6 address: FE80::203:E3FF:FE6A:BF81  (link-local)
  IPv6 address: 4000::BC:0:0:C0A8:BC06  (global unicast)
  CLNS address: 490001.1111.1111.1111.00
Platform: cisco 3640,  Capabilities: Router
Interface: Ethernet0/1,  Port ID (outgoing port): Ethernet0/1
Holdtime : 160 sec

Version :
Cisco Internetwork Operating System Software
IOS (tm) 3600 Software (C3640-A2IS-M), Experimental Version 12.2
Copyright (c) 1986-2001 by cisco Systems, Inc.
Compiled Wed 08-Aug-01 12:39 by joeuser
```

The following is sample output from the **show cdp entry version** command. Only information about the version of software running on *device.cisco.com* is displayed.

```
Router# show cdp entry device.cisco.com version

Version information for device.cisco.com:
 Cisco Internetwork Operating System Software
IOS (tm) 3600 Software (C3640-A2IS-M), Experimental Version 12.2
Copyright (c) 1986-2001 by cisco Systems, Inc.
Compiled Wed 08-Aug-01 12:39 by joeuser
```

The following is sample output from the **show cdp entry protocol** command. Only information about the protocols enabled on *device.cisco.com* is displayed.

```
Router# show cdp entry device.cisco.com protocol

Protocol information for device.cisco.com:
  IP address: 10.1.17.24
  IPv6 address: FE80::203:E3FF:FE6A:BF81  (link-local)
  IPv6 address: 4000::BC:0:0:C0A8:BC06  (global unicast)
  CLNS address: 490001.1111.1111.1111.00
```

Related Commands

Command	Description
show cdp	Displays global CDP information, including timer and hold-time information.
show cdp interface	Displays information about the interfaces on which CDP is enabled.
show cdp neighbors	Displays detailed information about neighboring devices discovered using CDP.
show cdp traffic	Displays traffic information from the CDP table.

show cdp interface

To display information about the interfaces on which Cisco Discovery Protocol (CDP) is enabled, use the **show cdp interface** command in privileged EXEC mode.

show cdp interface [*type number*]

Syntax Description

type	(Optional) Type of interface about which you want information.
number	(Optional) Number of the interface about which you want information.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.3	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 cdp interface** command. Status information and information about CDP timer and hold-time settings is displayed for all interfaces on which CDP is enabled.

```
Router# show cdp interface

Serial0 is up, line protocol is up, encapsulation is SMDS
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
Ethernet0 is up, line protocol is up, encapsulation is ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
```

The following is sample output from the **show cdp interface** command with an interface specified. Status information and information about CDP timer and hold-time settings is displayed for Ethernet interface 0 only.

```
Router# show cdp interface ethernet 0

Ethernet0 is up, line protocol is up, encapsulation is ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
```

Related Commands

Command	Description
show cdp	Displays global CDP information, including timer and hold-time information.
show cdp entry	Displays information about a specific neighbor device or all neighboring devices discovered using CDP.
show cdp neighbors	Displays detailed information about neighboring devices discovered using CDP.
show cdp traffic	Displays traffic information from the CDP table.

show cdp neighbors

To display detailed information about neighboring devices discovered using Cisco Discovery Protocol, use the **show cdp neighbors** command in privileged EXEC mode.

show cdp neighbors [*type number*] [**detail**]

Syntax Description

type	(Optional) Interface type that is connected to the neighbors about which you want information; possible valid values are **ethernet**, **fastethernet**, **gigabitethernet**, **tengigabitethernet**, **port-channel**, and **vlan**.
number	(Optional) Number of the interface connected to the neighbors about which you want information.
detail	(Optional) Displays detailed information about a neighbor (or neighbors) including network address, enabled protocols, hold time, and software version.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
10.3	This command was introduced.
12.0(3)T	The output of this command using the **detail** keyword was expanded to include Cisco Discovery Protocol Version 2 information.
12.2(8)T	Support for IPv6 address and address type information was added.
12.2(14)S	Support for IPv6 address and address type information was added.
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command was introduced on the Supervisor Engine 2.
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.
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 **vlan** keyword is supported in Catalyst 6500 series switches that are configured with a Supervisor Engine 2.

The **port-channel** values are from 0 to 282; values from 257 to 282 are supported on the call switching module (CSM) and the firewall services module (FWSM) only.

Examples

The following is sample output from the **show cdp neighbors** command:

```
Router# show cdp neighbors

Capability Codes:R - Router, T - Trans Bridge, B - Source Route Bridge S - Switch,
```

```
H - Host, I - IGMP, r - Repeater
Device ID  Local Intrfce  Holdtme  Capability  Platform  Port ID
joe        Eth 0          133      R           4500      Eth 0
sam        Eth 0          152      R           AS5200    Eth 0
terri      Eth 0          144      R           3640      Eth0/0
maine      Eth 0          141                  RP1       Eth 0/0
sancho     Eth 0          164                  7206      Eth 1/0
```

Table 39 describes the fields shown in the display.

Table 39 show cdp neighbors Field Descriptions

Field	Definition
Capability Codes	The type of device that can be discovered.
Device ID	The name of the neighbor device and either the MAC address or the serial number of this device.
Local Intrfce	The local interface through which this neighbor is connected.
Holdtme	The remaining amount of time (in seconds) the current device will hold the Cisco Discovery Protocol advertisement from a sending router before discarding it.
Capability	The type of the device listed in the CDP Neighbors table. Possible values are as follows: • R—Router • T—Transparent bridge • B—Source-routing bridge • S—Switch • H—Host • I—IGMP device • r—Repeater
Platform	The product number of the device.
Port ID	The interface and port number of the neighboring device.

The following is sample output for one neighbor from the **show cdp neighbors detail** command. Additional detail is shown about neighbors, including network addresses, enabled protocols, and software version.

```
Router# show cdp neighbors detail

Device ID: device.cisco.com
Entry address(es):
  IPv6 address: FE80::203:E3FF:FE6A:BF81  (link-local)
  IPv6 address: 4000::BC:0:0:C0A8:BC06  (global unicast)
Platform: cisco 3640,  Capabilities: Router
Interface: Ethernet0/1,  Port ID (outgoing port): Ethernet0/1
Holdtime : 160 sec

Version :
Cisco Internetwork Operating System Software
IOS (tm) 3600 Software (C3640-A2IS-M), Version 12.2(25)SEB4, RELE)
Duplex Mode: half
Native VLAN: 42
VTP Management Domain: 'Accounting Group'
```

Table 40 describes the fields shown in the display.

Table 40 show cdp neighbors detail Field Descriptions

Field	Definition
Device ID	The name of the neighbor device and either the MAC address or the serial number of this device.
Entry address(es)	A list of network addresses of neighbor devices.
IPv6 address: FE80::203:E3FF:FE6A:BF81 (link-local)	The network address of the neighbor device. The address can be in IP, IPv6, IPX, AppleTalk, DECnet, or Connectionless Network Service (CLNS) protocol conventions. IPv6 addresses are followed by one of the following IPv6 address types: • global unicast • link-local • multicast • site-local • V4 compatible **Note** For Cisco IOS Releases12.2(33)SXH3, Release 12.2(33)SXI and later releases, the command will not display the AppleTalk address.
Platform	The product name and number of the neighbor device.
Capabilities	The device type of the neighbor. This device can be a router, a bridge, a transparent bridge, a source-routing bridge, a switch, a host, an IGMP device, or a repeater.
Interface	The local interface through which this neighbor is connected.
Port ID	The interface and port number of the neighboring device.
Holdtime	The remaining amount of time (in seconds) the current device will hold the CDP advertisement from a sending router before discarding it.
Version	The software version of the neighbor device.
advertisement version:	Version of CDP that is being used for CDP advertisements.
Duplex Mode	The duplex state of connection between the current device and the neighbor device.
Native VLAN	The ID number of the VLAN on the neighbor device.
VTP Management Domain	A string that is the name of the collective group of VLANs associated with the neighbor device.

Related Commands

Command	Description
show cdp	Displays global CDP information, including timer and hold-time information.
show cdp entry	Displays information about a specific neighbor device listed in the CDP table.

Command	Description
show cdp interface	Displays information about the interfaces on which CDP is enabled.
show cdp traffic	Displays information about traffic between devices gathered using CDP.

show cdp tlv

To display information about Cisco Discovery Protocol (CDP) Type-Length-Values (TLVs), use the **show cdp tlv** command in privileged EXEC mode.

show cdp tlv {**app interface** *type number* | **location** [**all** | **civic** | **elin**] [**interface** *type number*] | **location-server** [**interface** *type number*]}

Syntax Description

app	Displays application TLVs stored in CDP messages.
interface *type number*	Specifies the interface type and number.
location	Displays location information for TLVs.
all	(Optional) Displays location information for all TLVs.
civic	(Optional) Displays civic location information.
elin	(Optional) Displays emergency location identifier number (ELIN) location information.
location-server	Displays location-server information stored in CDP for one interface or for all interfaces.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(55)SE	This command was introduced.

Usage Guidelines

You can use the **show cdp tlv** command to verify the TLVs configured on CDP. The **show cdp tlv** command displays location-specific information for an interface, if an interface is specified; otherwise, it displays location-specific information for all interfaces. You can also choose to display location-specific information for civic, ELIN, or all TLVs.

Examples

The following example shows how to display location-specific information for all TLVs:

```
Router# show cdp tlv location civic interface gigabitEthernet 3/0/2

No CIVIC Location received from neighbor(switch1)
Interface (GigabitEthernet3/0/2), Civic country code: US
    CA type: 3, Len: 9, Value: bangalore
    CA type: 24, Len: 6, Value: 560087
    CA type: 25, Len: 18, Value: CessnaBusinessPark
    CA type: 34, Len: 13, Value: OuterRingRoad
```

Table 41 describes the significant fields shown in the display.

Table 41 show cdp tlv Field Descriptions

Field	Description
Interface	Displays the interface on which location support is configured.
CA type	Displays the civic address (CA) type.
Len	Displays the variable length of the civic address.
Value	Displays the application TLV value information.

Related Commands

Command	Description
cdp tlv	Configures location support in CDP.

show cdp traffic

To display information about traffic between devices gathered using Cisco Discovery Protocol (CDP), use the **show cdp traffic** command in privileged EXEC mode.

show cdp traffic

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.3	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 cdp traffic** command:

```
Router# show cdp traffic

Total packets output: 543, Input: 333
Hdr syntax: 0, Chksum error: 0, Encaps failed: 0
No memory: 0, Invalid: 0, Fragmented: 0
CDP version 1 advertisements output: 191, Input: 187
CDP version 2 advertisements output: 352, Input: 146
```

Table 42 describes the significant fields shown in the display.

Table 42 show cdp traffic Field Descriptions

Field	Definition
Total packets output	The number of CDP advertisements sent by the local device. Note that this value is the sum of the CDP Version 1 advertisements output and CDP Version 2 advertisements output fields.
Input	The number of CDP advertisements received by the local device. Note that this value is the sum of the CDP Version 1 advertisements input and CDP Version 2 advertisements input fields.
Hdr syntax	The number of CDP advertisements with bad headers, received by the local device.
Chksum error	The number of times the checksum (verifying) operation failed on incoming CDP advertisements.

Table 42 show cdp traffic Field Descriptions (continued)

Field	Definition
Encaps failed	The number of times CDP failed to send advertisements on an interface because of a failure caused by the bridge port of the local device.
No memory	The number of times the local device did not have enough memory to store the CDP advertisements in the advertisement cache table when the device was attempting to assemble advertisement packets for transmission and parse them when receiving them.
Invalid	The number of invalid CDP advertisements received and sent by the local device.
Fragmented	The number of times fragments or portions of a single CDP advertisement were received by the local device instead of the complete advertisement.
CDP version 1 advertisements output	The number of CDP Version 1 advertisements sent by the local device.
Input	The number of CDP Version 1 advertisements received by the local device.
CDP version 2 advertisements output	The number of CDP Version 2 advertisements sent by the local device.
Input	The number of CDP Version 2 advertisements received by the local device.

Related Commands

Command	Description
show cdp	Displays global CDP information, including timer and hold-time information.
show cdp entry	Displays information about a specific neighbor device listed in the CDP table.
show cdp interface	Displays information about the interfaces on which CDP is enabled.
show cdp neighbors	Displays detailed information about neighboring devices discovered using CDP.

show clock

To display the time and date from the system software clock, use the **show clock** command in user EXEC or privileged EXEC mode.

show clock [**detail**]

Syntax Description

detail	(Optional) Indicates the clock source (NTP, VINES, hardware clock, and so on) and the current summer-time setting (if any).

Command Modes

User EXEC
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.
12.4(20)T	Support for IPv6 was added.

Usage Guidelines

The software clock keeps an "authoritative" flag that indicates whether the time is authoritative (believed to be accurate). If the software clock has been set by a timing source (for example, via NTP), the flag is set. If the time is not authoritative, it will be used only for display purposes. Until the clock is authoritative and the "authoritative" flag is set, the flag prevents peers from synchronizing to the software clock.

The symbol that precedes the **show clock** display indicates the following:

Symbol	Description	Example
*	Time is not authoritative: the software clock is not in sync or has never been set.	*15:29:03.158 UTC Tue Feb 25 2003:
(blank)	Time is authoritative: the software clock is in sync or has just been set manually	15:29:03.158 UTC Tue Feb 25 2003:
.	Time is authoritative, but NTP is not synchronized: the software clock was in sync, but has since lost contact with all configured NTP servers	.15:29:03.158 UTC Tue Feb 25 2003:

These symbols are also used in NTP-based timestamping, such as for syslog (SEM) messages.

Note In general, NTP synchronization takes approximately 15 to 20 minutes.

Examples

The following sample output shows that the current clock is authoritative and that the time source is NTP:

```
Router> show clock detail

15:29:03.158 PST Tue Feb 25 2003
Time source is NTP
```

The following example shows the current clock is authoritative, but NTP is not yet synchronized:

```
Router> show clock

.16:42:35.597 UTC Tue Feb 25 2003
```

Related Commands

Command	Description
clock set	Manually sets the software clock.
show calendar	Displays the current time and date setting of the system hardware clock.

show cns config connections

To display the status of the Cisco Networking Services (CNS) event agent connection, use the **show cns config connections** command in privileged EXEC mode.

show cns config connections

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(8)T	This command was introduced. This command replaces the **show cns config status** command.

Usage Guidelines

Use the **show cns config connections** command to determine whether the CNS event agent is connecting to the gateway, connected, or active, and to display the gateway used by the event agent and its IP address and port number.

Examples

The following is sample output from the **show cns config connections** command:

```
Router# show cns config connections

The partial configuration agent is enabled.

Configuration server:  10.1.1.1
Port number:           80
Encryption:            disabled
Config id:             test1
Connection Status:     Connection not active.
```

Related Commands

Command	Description
show cns config outstanding	Displays information about incremental CNS configurations that have started but not yet completed.
show cns config stats	Displays statistics about the CNS configuration agent.
show cns config status	Displays the status of the CNS Configuration Agent.

show cns config outstanding

To display information about incremental (partial) Cisco Networking Services (CNS) configurations that have started but not yet completed, use the **show cns config outstanding** command in privileged EXEC mode.

show cns config outstanding

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.2(8)T	This command was implemented on Cisco 2600 series and Cisco 3600 series routers.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

Use the **show cns config outstanding** command to display information about outstanding incremental (partial) configurations that have started but not yet completed, including the following:

- Queue ID (location of configuration in the config queue)
- Identifier (group ID)
- Config ID (identity of configuration within the group)

Examples

The following is sample output from the **show cns config outstanding** command:

```
Router# show cns config outstanding

The outstanding configuration information:
queue id   identifier       config-id
1          identifierREAD   config_idREAD
```

Related Commands

Command	Description
cns config cancel	Cancels an incremental two-phase synchronization configuration.
config-cli	Displays the status of the CNS event agent connection.
show cns config stats	Displays statistics about the CNS configuration agent.

show cns config stats

To display statistics about the Cisco Networking Services (CNS) configuration agent, use the **show cns config stats** command in privileged EXEC mode.

show cns config stats

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.2(8)T	This command was implemented on Cisco 2600 series and Cisco 3600 series routers.
12.3(1)	Additional output fields were added.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

This command displays the following statistics on the CNS configuration agent:

- The number of configurations requests received
- The number of configurations completed
- The number of configurations failed
- The number of configurations pending
- The number of configurations cancelled
- The time stamp of the last configuration received
- The time stamp of the initial configuration received

Examples

The following is sample output from the **show cns config stats** command:

```
Router# show cns config stats

6 configuration requests received.
4 configurations completed.
1 configurations failed.
1 configurations pending.
0 configurations cancelled.
The time of last received configuration is *May 5 2003 10:42:15 UTC.
Initial Config received *May 5 2003 10:45:15 UTC.
```

Related Commands

Command	Description
clear cns config stats	Clears all the statistics about the CNS configuration agent.
show cns config outstanding	Displays information about incremental CNS configurations that have started but not yet completed.

show cns config status

Note Effective with Cisco IOS Release 12.2(8)T, the **show cns config status** command is replaced by the **show cns config connections** command. See the **show cns config connections** command for more information.

To display the status of the Cisco Networking Services (CNS) Configuration Agent, use the **show cns config status** command in EXEC mode.

show cns config status

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC (>)

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.2(8)T	This command was replaced by the **show cns config connections** command.
12.0(18)ST	This command was integrated into Cisco IOS Release 12.0(18)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0 (22)S.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

This command displays the status of the Configuration Agent. Use this option to display the following information about the Configuration Agent:

- Status of the Configuration Agent, for example, whether it has been configured properly.
- IP address and port number of the trusted server that the Configuration Agent is using.
- Config ID (identity of configuration within the configuration group).

Related Commands

Command	Description
cns config cancel	Cancels a CNS configuration.
cns config initial	Starts the initial CNS Configuration Agent.
cns config partial	Starts the partial CNS Configuration Agent.
cns config retrieve	Gets the configuration of a routing device using CNS.
show cns config connections	Displays the status of the CNS event agent connection.

show cns event connections

To display the status of the Cisco Networking Services (CNS) event agent connection, use the **show cns event connections** command in privileged EXEC mode.

show cns event connections

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

Use the **show cns event connections** command to display the status of the event agent connection—such as whether it is connecting to the gateway, connected, or active—and to display the gateway used by the event agent and its IP address and port number.

Examples

The following example displays the IP address and port number of the primary and backup gateways:

```
Router# show cns event connections

The currently configured primary event gateway:
        hostname is 10.1.1.1.
        port number is 11011.
Event-Id is Internal test1
Keepalive setting:
        none.
Connection status:
        Connection Established.
The currently configured backup event gateway:
        none.
The currently connected event gateway:
        hostname is 10.1.1.1.
        port number is 11011.
```

Related Commands

Command	Description
show cns event stats	Displays statistics about the CNS event agent connection.
show cns event subject	Displays a list of subjects about the CNS event agent connection.

show cns event gateway

To display information about the Cisco Networking Services (CNS) Event Agent, use the **show cns event gateway** command in EXEC mode.

show cns event gateway

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(18)ST	This command was integrated into Cisco IOS Release 12.0 (18)ST

Usage Guidelines

Use this command to display the following information about CNS gateways:

- Primary gateway:
  - IP address
  - Port number
- Backup gateways:
  - IP address
  - Port number
- Currently connected gateway:
  - IP address
  - Port number

Related Commands

Command	Description
cns event	Configures the CNS Event Gateway.

show cns event stats

To display statistics about the Cisco Networking Services (CNS) event agent connection, use the **show cns event stats** command in privileged EXEC mode.

show cns event stats

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(18)ST	This command was integrated into Cisco IOS Release 12.0(18)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(8)T	This command was implemented on the Cisco 2600 series and the Cisco 3600 series routers.
12.3(1)	Output was changed to display statistics generated since last cleared.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

Use this command to display the following statistics for the CNS event agent:

- Number of events received
- Number of events sent
- Number of events not processed successfully
- Number of events in the queue
- Time stamp showing when statistics were last cleared (time stamp is router time)
- Number of events received since the statistics were cleared
- Time stamp of latest event received (time stamp is router time)
- Time stamp of latest event sent
- Number of applications using the Event Agent
- Number of subjects subscribed

Examples

The following example displays statistics for the CNS event agent:

```
Router# show cns event stats
```

```
0 events received.
1 events sent.
0 events not processed.
0 events in the queue.
0 events sent to other IOS applications.
Event agent stats last cleared at Apr 4 2003 00:55:25 UTC
No events received since stats cleared
The time stamp of the last received event is *Mar 30 2003 11:04:08 UTC
The time stamp of the last sent event is *Apr 11 2003 22:21:23 UTC
3 applications are using the event agent.
0 subjects subscribed.
1 subjects produced.
0 subjects replied.
```

Related Commands

Command	Description
clear cns event stats	Clears all the statistics about the CNS event agent.
cns event	Enables and configures CNS event agent services.
show cns event connections	Displays the status of the CNS event agent connection.
show cns event subject	Displays a list of subjects about the CNS event agent connection.

show cns event status

To display information about the Cisco Networking Services (CNS) Event Agent, use the **show cns event status** command in EXEC mode.

show cns event status

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(18)ST	This command was integrated into Cisco IOS Release 12.0 (18)ST.

Usage Guidelines

Use this command to display the following information about the CNS Event Agent:

- Status of Event Agent:
  - Connected
  - Active
- Gateway used by the Event Agent:
  - IP address
  - Port number
- Device ID

Related Commands

Command	Description
cns event	Configures the CNS Event Gateway.

show cns event subject

To display a list of subjects about the Cisco Networking Services (CNS) event agent connection, use the **show cns event subject** command in privileged EXEC mode.

show cns event subject [*name*]

Syntax Description

name	(Optional) Displays a list of applications that are subscribing to this specific subject name.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(18)ST	This command was integrated into Cisco IOS Release 12.0(18)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(8)T	This command was implemented on the Cisco 2600 series and the Cisco 3600 series.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

Use the **show cns event subject** command to display a list of subjects of the event agent that are subscribed to by applications.

Examples

The following example displays the IP address and port number of the primary and backup gateways:

```
Router# show cns event subject

The list of subjects subscribed by applications.
   cisco.cns.mibaccess:request
   cisco.cns.config.load
   cisco.cns.config.reboot
   cisco.cns.exec.cmd
```

Related Commands

Command	Description
show cns event connections	Displays the status of the CNS event agent connection.
show cns event stats	Displays statistics about the CNS event agent connection.

show cns image connections

To display the status of the Cisco Networking Services (CNS) image management server HTTP connections, use the **show cns image connections** command in privileged EXEC mode.

show cns image connections

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(1)	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

Use the **show cns image connections** command when troubleshooting HTTP connection problems with the CNS image server. The output displays the following information:

- Number of connection attempts
- Number of connections that were never connected and those that were abruptly disconnected
- Date and time of last successful connection

Examples

The following is sample output from the **show cns image connections** command:

```
Router# show cns image connections

CNS Image Agent:  HTTP connections
Connection attempts 1
never connected:0   Abrupt disconnect:0
Last successful connection at 11:45:02.000 UTC Mon May 6 2003
```

Related Commands

Command	Description
show cns image inventory	Displays inventory information about the CNS image agent.
show cns image status	Displays status information about the CNS image agent.

show cns image inventory

To provide a dump of Cisco Networking Services (CNS) image inventory information in extensible markup language (XML) format, use the **show cns image inventory** command in privileged EXEC mode.

show cns image inventory

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(1)	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

To view the XML output in a better format, paste the content into a text file and use an XML viewing tool.

Examples

The following is sample output from the **show cns image inventory** command:

```
Router# show cns image inventory

Inventory Report
<imageInventoryReport><deviceName><imageID>Router</imageID><hostName>Router</ho
IOS (tm) C2600 Software (C2600-I-M), Experimental Version 12.3(20030414:081500)]
Copyright (c) 1986-2003 by cisco Systems, Inc.
Compiled Mon 14-Apr-03 02:03 by engineer</versionString><imageFile>tftp://10.25>
```

Related Commands

Command	Description
show cns image connections	Displays connection information for the CNS image agent.
show cns image status	Displays status information about the CNS image agent.

show cns image status

To display status information about the Cisco Networking Services (CNS) image agent, use the **show cns image status** command in privileged EXEC mode.

show cns image status

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(1)	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

Use this command to display the following status information about the CNS image agent:

- Start date and time of last upgrade
- End date and time of last upgrade
- End date and time of last successful upgrade
- End date and time of last failed upgrade
- Number of failed upgrades
- Number of successful upgrades with number of received messages and errors
- Transmit status with number of attempts, successes, and failures

Examples

The following is sample output from the **show cns image status** command:

```
Router# show cns image status

Last upgrade started at 11:45:02.000 UTC Mon May 6 2003
Last upgrade ended at 11:56:04.000 UTC Mon May 6 2003 status SUCCESS

Last successful upgrade ended at 00:00:00.000 UTC Mon May 6 2003
Last failed upgrade ended at 00:00:00.000 UTC Wed Apr 16 2003
Number of failed upgrades: 2
Number of successful upgrades: 6
 messages received: 12
 receive errors: 5
Transmit Status
  TX Attempts:4
    Successes:3         Failures 2
```

Related Commands

Command	Description
show cns image connections	Displays connection information for the CNS image agent.
show cns image inventory	Displays image inventory information in XML format.

show ethernet oam status

To display Ethernet operations, maintenance, and administration (OAM) configurations for all interfaces or for a specific interface, use the **show ethernet oam status** command in privileged EXEC mode.

show ethernet oam status [**interface** *type slot*/[*subslot*/]*port* | **vlan** *vlan*]

Syntax Description

interface	(Optional) Specifies an interface.
type	(Optional) Type of Ethernet interface. Valid values are: FastEthernet, GigabitEthernet, TenGigabitEthernet.
slot/[*subslot*/]*port*	(Optional) Chassis slot number and port number where the Ethernet interface is located. If the Ethernet interface is located on a shared port adapter (SPA), the subslot number may also be required. The subslot is the secondary slot number on the SPA Interface Processor (SIP) where the SPA is installed.
vlan *vlan*	(Optional) Limits the display to interfaces on the specified VLAN. Range: 1 to 4094

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRA	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SXI	This command was changed to add the optional **vlan** *vlan* keyword and argument. The *subslot* field was added to support Ethernet interfaces located on a SPA.

Usage Guidelines

Use this command to display the runtime settings of link-monitoring and general OAM operations for all interfaces or for a specific interface.

OAM must be operational on the interface or interfaces before you issue this command.

Cisco IOS Release 12.2(33)SXI and later releases allow you to limit the display of switch port information to the specified VLAN.

Examples

The following example shows output from a **show ethernet oam status** command for interface GigabitEthernet 6/11:

```
Router# show ethernet oam status interface gigabitethernet 6/11

GigabitEthernet6/11
General
-------
  Mode:                 active
```

```
  PDU max rate:           10 packets per second
  PDU min rate:           1 packet per 1 second
  Link timeout:           5 seconds
  High threshold action: no action

Link Monitoring
---------------
  Status: supported (on)

  Symbol Period Error
    Window:               1 million symbols
    Low threshold:        1 error symbol(s)
    High threshold:       none

  Frame Error
    Window:               10 x 100 milliseconds
    Low threshold:        1 error frame(s)
    High threshold:       none

  Frame Period Error
    Window:               1 x 100,000 frames
    Low threshold:        1 error frame(s)
    High threshold:       none

  Frame Seconds Error
    Window:               600 x 100 milliseconds
    Low threshold:        1 error second(s)
    High threshold:       none
```

Table 43 describes the significant fields shown in the display.

Table 43 show ethernet oam status Field Descriptions

Field	Description
General	
Mode	Active or passive mode of the interface.
PDU max rate	Maximum number of protocol data units (PDUs) transmitted per second.
PDU min rate	Minimum number of PDUs transmitted per second.
Link timeout	Amount of time with inactivity before the link is dropped.
High threshold action	Action that occurs when the high threshold for an error is exceeded.
Link Monitoring	
Status	Operational state of the port.
Symbol Period Error	
Window	Specified number of error symbols.
Low threshold	Minimum number of error symbols.
High threshold	Maximum number of error symbols.
Frame Error	
Window	Specified amount of time in milleseconds.
Low threshold	Minimum number of error frames.
High threshold	Maximum number of error frames.

Table 43 show ethernet oam status Field Descriptions (continued)

Field	Description
Frame Period Error	
Window	Frequency at which the measurement is taken, in milliseconds.
Low threshold	Minimum number of error frames.
High threshold	Maximum number of error frames.
Frame Seconds Error	
Window	Frequency at which the measurement is taken, in milliseconds.
Low threshold	Lowest value at which an event will be triggered.
High threshold	Highest value at which an event will be triggered.

Related Commands

Command	Description
show ethernet oam discovery	Displays discovery information for all Ethernet OAM interfaces or for a specific interface.
show ethernet oam statistics	Displays detailed information about Ethernet OAM packets.
show ethernet oam summary	Displays active Ethernet OAM sessions.