major rising

To set major level threshold values for the buffer, CPU, and memory resource owners (ROs), use the **major rising** command in buffer owner configuration mode, CPU owner configuration mode, or memory owner configuration mode. To disable this function, use the **no** form of this command.

major rising *rising-threshold-value* [**interval** *interval-value*] [**falling** *falling-threshold-value* [**interval** *interval-value*]] [**global**]

no major rising

Syntax Description

rising-threshold-value	The rising threshold value as a percentage. Valid values are from 1 to 100.
interval	(Optional) Specifies the time, in seconds, during which the variation in rising or falling threshold values are not reported to the request/response unit (RU), resource group, or resource user types. For example, if the buffer usage count remains above the configured threshold value for the configured interval, a notification is sent to the RU, resource group, or resource user types.
interval-value	The time, in seconds, during which the variation in rising or falling threshold values is not reported to the RU, resource group, or resource user types. Valid values are from 0 to 86400. The default value is 0.
falling	(Optional) Specifies the falling threshold value as a percentage.
falling-threshold-value	(Optional) The falling threshold value. Valid values are from 1 to 100.
global	(Optional) Configures a global threshold. The **global** keyword is optional when you set major threshold values for public buffer, processor CPU, I/O memory, and processor memory. The **global** keyword is required when you set major threshold values for interrupt CPU and total CPU.

Command Default

Disabled

Command Modes

Buffer owner configuration
CPU owner configuration
Memory owner configuration

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.

Usage Guidelines

The interval is the dampening or observation interval time, in seconds, during which the variations in the rising and falling threshold values are not notified to the ROs or RUs. That is, the interval is the time the system waits to check whether the threshold value stabilizes. The interval is set to avoid unnecessary and unwanted threshold notifications. If not configured, the system defaults to 0 seconds.

This command allows you to configure three types of thresholding:

- System Global Thresholding
- User Local Thresholding
- Per User Global Thresholding

System Global Thresholding

System global thresholding is used when the entire resource reaches a specified value. That is, RUs are notified when the total resource utilization goes above or below a specified threshold value. The notification order is determined by the priority of the RU. The RUs with a lower priority are notified first, and are expected to reduce the resource utilization. This notification order prevents the high-priority RUs from being sent unwanted notifications.

You can set rising and falling threshold values. For example, if you have set a total CPU utilization threshold value of 70% as the rising major value and 15% as the falling major value, when the total CPU utilization crosses the 70% mark, a major Up notification is sent to all the RUs and when the total CPU utilization falls below 15%, a major Down notification is sent to all the RUs. The same criteria apply to buffer ROs and memory ROs.

User Local Thresholding

User local thresholding is used when a specified RU exceeds the configured limits. The user local thresholding method prevents a single RU from monopolizing resources. That is, the specified RU is notified when its resource utilization exceeds or falls below a configured threshold value. For example, if you set a CPU utilization threshold value of 70% as the rising major value and 15% as the falling major value, when the CPU utilization of the specified RU crosses the 70% mark, a major Up notification is sent to that RU only and when the CPU utilization of the specified RU falls below 15%, a major Down notification is sent to only that RU. The same method also applies to buffer and memory ROs.

Per User Global Thresholding

Per user global thresholding is used when the entire resource reaches a specified value. This value is unique for each RU and notification is sent only to the specified RU. User global thresholding is similar to user local thresholding, except that the global resource usage is compared against the thresholds. That is, only the specified RU is notified when the total resource utilization exceeds or falls below a configured threshold value. For example, if you set a CPU utilization threshold value of 70% as the rising major value and 15% as the falling major value, when the total CPU utilization crosses the 70% mark, a major Up notification is sent to only the specified RU and when the total CPU utilization falls below 15%, a major Down notification is sent to only the specified RU. The same method also applies to buffer and memory ROs.

Threshold Violations

The Cisco IOS device sends out error messages when a threshold is violated. The following examples help you understand the error message pattern when different threshold violations occur in buffer, CPU, and memory ROs:

System Global Threshold Violation in Buffer RO

The threshold violation in buffer RO for a system global threshold shows the following output:

```
System global threshold-Violation (keywords Critical, Major and Minor alone will vary
accordingly)
==========================================================================================
00:15:11: %SYS-4-GLOBALBUFEXCEED: Buffer usage has gone above global buffer Major
threshold
configured <value> Current usage :<value>
```

For example:

```
00:15:11: %SYS-4-GLOBALBUFEXCEED: Buffer usage has gone above global buffer Major
threshold
configured 100 Current usage :101

System global threshold- Recovery (keywords Critical, Major and Minor alone will vary
accordingly)
================================================================================================
00:17:10: %SYS-5-GLOBALBUFRECOVER: Buffer usage has gone below global buffer Major
threshold
configured <value> Current usage :<value>
```

For example:

```
00:17:10: %SYS-5-GLOBALBUFRECOVER: Buffer usage has gone below global buffer Critical
threshold
configured 70 Current usage :69
```

Per User Global Threshold Violation in Buffer RO

The threshold violation in buffer RO for a user global threshold shows the following output:

```
User global threshold - Violation (keywords Critical, Major and Minor alone will vary
accordingly)
================================================================================================
00:24:04: %SYS-4-RESGLOBALBUFEXCEED: Buffer usage has gone above buffer Major threshold
configured by resource user  <user-name>
 configured 100 Current usage :101

User global threshold - Recovery (keywords Critical, Major and Minor alone will vary
accordingly)
================================================================================================
00:25:08: %SYS-4-RESGLOBALBUFRECOVER: Buffer usage has gone below buffer Major threshold
configured by resource user  <user-name>
configured 76 Current usage :75
```

User Local Threshold Violation in Buffer RO

The threshold violation in buffer RO for a user local threshold shows the following output:

```
User local threshold - Violation (keywords Critical, Major and Minor alone will vary
accordingly)
================================================================================================
00:31:15: %SYS-4-RESBUFEXCEED: Resource user  user_1 has exceeded the buffer Major
threshold. configured 108 Current usage :109

User local threshold- Recovery (keywords Critical, Major and Minor alone will vary
accordingly)
================================================================================================
00:31:05: %SYS-5-RESBUFRECOVER: Resource user  user_1 has recovered after exceeding the
buffer Major threshold. configured 90 Current usage :89
```

System Global Threshold Violation in CPU RO

The threshold violation in CPU RO for a system global threshold shows the following output:

```
System global threshold- Violation
(1) keywords Critical, Major and Minor will vary accordingly
(2) keywords total, process and interrupt will vary accordingly )
================================================================================================
00:19:36: %SYS-4-CPURESRISING: System is seeing global cpu util 19% at total level more
than the configured major limit 11%
System global threshold - Recovery
(1) keywords Critical, Major and Minor will vary accordingly
(2) keywords total, process and interrupt will vary accordingly )
```

```
==========================================================================================
00:20:56: %SYS-6-CPURESFALLING: System is no longer seeing global high cpu at total level
for the configured major limit 10%, current value 4%
```

Per User Global Threshold Violation in CPU RO

The threshold violation in CPU RO for a user global threshold shows the following output:

```
User global threshold - Violation
(1) keywords Critical, Major and Minor will vary accordingly
(2) keywords total, process and interrupt will vary accordingly )
==========================================================================================
00:14:21: %SYS-4-CPURESRISING: Resource user <user-name> is seeing global cpu util 11% at
total level more than the configured major limit 6%
```

For example:

```
00:14:21: %SYS-4-CPURESRISING: Resource user Test-proc-14:99s:1w:100n is seeing global cpu
util 11% at total level more than the configured major limit 6%

User global threshold- Recovery
(1) keywords Critical, Major and Minor will vary accordingly
(2) keywords total, process and interrupt will vary accordingly )
==========================================================================================
00:14:46: %SYS-6-CPURESFALLING: Resource user <user-name> is no longer seeing global high
cpu at total level for the configured critical limit 9%, current value 4%
```

For example:

```
00:14:46: %SYS-6-CPURESFALLING: Resource user Test-proc-14:99s:1w:100n is no longer seeing
global high cpu at total level for the configured critical limit 9%, current value 4%
```

User Local Threshold Violation in CPU RO

The threshold violation in CPU RO for a user local threshold shows the following output:

```
User local threshold - Violation (keywords Critical, Major and Minor will vary accordingly
- only process level)
==========================================================================================
00:12:11: %SYS-4-CPURESRISING: Resource user <user-name> is seeing local cpu util 15% at
process level more than the configured minor limit 6 %
```

For example:

```
00:12:11: %SYS-4-CPURESRISING: Resource user Test-proc-9:85s:15w:100n is seeing local cpu
util 15% at process level more than the configured minor limit 6%

User local threshold- Recovery (keywords Critical, Major and Minor will vary accordingly
- only process level)
==========================================================================================
00:13:11: %SYS-6-CPURESFALLING: Resource user <user-name> is no longer seeing local high
cpu at process level for the configured critical limit 9%, current value 3%
```

System Global Threshold Violation in Memory RO

The threshold violation in memory RO for a system global threshold shows the following output:

```
System global threshold - Violation (keywords Critical, Major and Minor alone will vary
accordingly)
(If violation happens in IO memory pool will be : I/O)
==========================================================================================


13:53:22: %SYS-5-GLOBALMEMEXCEED: Global Memory has exceeded the Minor threshold
Pool: Processor  Used: 422703520  Threshold: 373885200
```

For example:

```
13:54:03: %SYS-5-GLOBALMEMEXCEED: Global Memory has exceeded the Critical threshold
Pool: Processor  Used: 622701556  Threshold: 467356500

System global threshold - Recovery (keywords Critical, Major and Minor alone will vary
accordingly)
(If recovery happens in IO memory pool will be : I/O)
==========================================================================================
%SYS-5-GLOBALMEMRECOVER: Global Memory has recovered  after exceeding Minor threshold
Pool: Processor  Used: 222473448  Threshold: 355190940
```

For example:

```
13:50:41: %SYS-5-GLOBALMEMRECOVER: Global Memory has recovered  after exceeding Critical
threshold
Pool: Processor  Used: 222473152  Threshold: 443988675
```

Per User Global Threshold Violation in Memory RO

The threshold violation in memory RO for a user global threshold shows the following output:

```
User global threshold - Violation (keywords Critical, Major and Minor alone will vary
accordingly)
(If violation happens in IO memory pool will be : I/O)
==========================================================================================
00:53:14: %SYS-4-RESGLOBALMEMEXCEED: Global Memory has exceeded the Minor threshold
configure by resource user <XYZ>
Pool: Processor  Used: 62273916  Threshold: 62246820

User global threshold - Recovery (keywords Critical, Major and Minor alone will vary
accordingly)
(If recovery happens in IO memory pool will be : I/O)
==========================================================================================
00:32:56: %SYS-4-RESGLOBALMEMRECOVER: Global Memory has recovered after exceeding the
Critical threshold configure by resource user <XYZ>
Pool: Processor  Used: 329999508  Threshold: 375865440
```

User Local Threshold Violation in Memory RO

The threshold violation in memory RO for a user local threshold shows the following output:

```
User local threshold- Violation (keywords Critical, Major and Minor alone will vary
accordingly)
==========================================================================================
01:05:42: %SYS-4-RESMEMEXCEED: Resource user <XYZ> has exceeded the Critical memory
threshold
Pool: Processor Used: 103754740 Threshold: 103744700

User local threshold - Recovery (keywords Critical, Major and Minor alone will vary
accordingly)
==========================================================================================
00:44:43: %SYS-5-RESMEMRECOVER: Resource user <XYZ> has recovered after exceeding the
Critical memory threshold
Pool: Processor Used: 328892280 Threshold :375865440
```

Examples

Configuring Major Rising Values for System Global Thresholding

The following example shows how to configure the major threshold values for system global thresholding with a major rising threshold of 70% at an interval of 12 seconds and a major falling threshold of 15% at an interval of 10 seconds:

```
Router(config-owner-cpu)# major rising 70 interval 12 falling 15 interval 10 global
Router(config-owner-buffer)# major rising 70 interval 12 falling 15 interval 10 global
Router(config-owner-memory)# major rising 70 interval 12 falling 15 interval 10 global
```

Configuring Major Rising Values for User Local Thresholding

The following example shows how to configure the major threshold values for user local thresholding with a major rising threshold of 70% at an interval of 12 seconds and a major falling threshold of 15% at an interval of 10 seconds:

```
Router(config-owner-cpu)# major rising 70 interval 12 falling 15 interval 10
Router(config-owner-buffer)# major rising 70 interval 12 falling 15 interval 10
Router(config-owner-memory)# major rising 70 interval 12 falling 15 interval 10
```

Configuring Major Rising Values for Per User Global Thresholding

The following example shows how to configure the major threshold values for per user global thresholding with a major rising threshold of 70% at an interval of 12 seconds and a major falling threshold of 15% at an interval of 10 seconds:

```
Router(config-owner-cpu)# major rising 70 interval 12 falling 15 interval 10 global
Router(config-owner-buffer)# major rising 70 interval 12 falling 15 interval 10 global
Router(config-owner-memory)# major rising 70 interval 12 falling 15 interval 10 global
```

Related Commands

Command	Description
buffer public	Enters the buffer owner configuration mode and sets threshold values for buffer usage.
cpu interrupt	Enters the CPU owner configuration mode and sets threshold values for interrupt level CPU utilization.
cpu process	Enters the CPU owner configuration mode and sets threshold values for processor level CPU utilization.
cpu total	Enters the CPU owner configuration mode and sets threshold values for total CPU utilization.
memory io	Enters the memory owner configuration mode and sets threshold values for I/O memory.
memory processor	Enters the memory owner configuration mode and sets threshold values for processor memory.
policy (ERM)	Configures an ERM resource policy.
resource policy	Enters ERM configuration mode.
show resource all	Displays all the resource details.
slot (ERM policy)	Configures line cards.
system (ERM policy)	Configures system level ROs.

max-message

To set the maximum size limit for incoming messages, use the **max-message** command in Web Services Management Agent (WSMA) listener configuration mode or WSMA initiator configuration mode. To disable the maximum message size limit, use the **no** form of this command.

max-message *message-size*

no max-message

Syntax Description

message-size	Defines the maximum size, in kilobytes (KB), for the incoming message. The range is from1 to 2000. The default is 50 KB.

Command Default

The maximum message size is set to 50KB.

Command Modes

WSMA listener configuration (config-wsma-listen)

WSMA initiator configuration (config-wsma-init)

Command History

Release	Modification
12.4(24)T	This command was introduced.
15.1(1)T	This command was modified. Support was added for the WSMA initiator configuration mode.

Usage Guidelines

Use this command in WSMA listener configuration mode or in WSMA initiator configuration mode. To enter the WSMA listener configuration mode, enter the **wsma profile listener** command in global configuration mode. To enter the WSMA initiator configuration mode, use the **wsma profile initiator** command in global configuration mode.

If an incoming message exceeds the maximum message size, it is counted as oversized and dropped. An error message is sent to indicate that the message is dropped

Examples

The following example shows how to set the maximum message size for an incoming message to 290 KB:

```
Router(config)# wsma profile listener prof1
Router(config-wsma-listen)# max-message 290
Router(config-wsma-listen)#
```

Related Commands

Command	Description
acl	Enables access control lists for restricting addresses that can connect to a WSMA profile.
encap	Configures an encapsulation for a WSMA profile.

Command	Description
idle-timeout	Sets a time for the WSMA profile to disconnect the session when there is no network traffic.
stealth	Disables WSMA from sending SOAP faults.
transport	Defines a transport configuration for a WSMA profile.
wsma profile listener	Configures and enables a WSMA listener profile.
wsse	Enables the WSSE for a WSMA profile.

memory io

To enter memory owner configuration mode to set threshold values for I/O memory, use the **memory io** command in resource policy node configuration mode. To exit memory owner configuration mode, use the **no** form of this command.

memory io

no memory io

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Resource policy node configuration

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.

Usage Guidelines

This command allows you to enter memory owner configuration mode to set rising and falling values for critical, major, and minor thresholds for I/O memory.

Examples

The following example shows how to enter memory owner configuration mode to set threshold values for I/O memory:

```
Router(config-res-policy-node)# memory io
```

Related Commands

Command	Description
critical rising	Sets the critical level threshold values for the buffer, CPU, and memory ROs.
major rising	Sets the major level threshold values for the buffer, CPU, and memory ROs.
minor rising	Sets the minor level threshold values for the buffer, CPU, and memory ROs.
policy (ERM)	Configures an ERM resource policy.
resource policy	Enters ERM configuration mode.
show resource all	Displays all the resource details.
slot (ERM policy)	Configures line cards.
system (ERM policy)	Configures system level ROs.

memory processor

To enter memory owner configuration mode to set the threshold values for the processor memory, use the **memory processor** command in resource policy node configuration mode. To exit memory owner configuration mode, use the **no** form of this command.

memory processor

no memory processor

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Resource policy node configuration

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.

Usage Guidelines

This command allows you to enter memory owner configuration mode to set rising and falling values for critical, major, and minor thresholds for the processor memory.

Examples

The following example shows how to enter memory owner configuration mode to set the threshold values for the processor memory:

```
Router(config-res-policy-node)# memory processor
```

Related Commands

Command	Description
critical rising	Sets the critical level threshold values for the buffer, CPU, and memory ROs.
major rising	Sets the major level threshold values for the buffer, CPU, and memory ROs.
minor rising	Sets the minor level threshold values for the buffer, CPU, and memory ROs.
policy (ERM)	Configures an ERM resource policy.
resource policy	Enters ERM configuration mode.
show resource all	Displays all the resource details.
slot (ERM policy)	Configures line cards.
system (ERM policy)	Configures system level ROs.

memory statistics history table

To change the number of hours for which the memory log is maintained, use the **memory statistics history table** command in global configuration mode. To return the logging to its default values, use the **no** form of this command.

memory statistics history table *number-of-hours*

no memory statistics history table *number-of-hours*

Syntax Description

number-of-hours	Number of hours of history for which the log is maintained. Valid values are from 12 to 72. The default value is 24.

Command Default

The memory log is maintained for 24 hours.

Command Modes

Global configuration

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.

Usage Guidelines

This command allows you to change the number of hours for which the memory log is maintained. You cannot disable this command. The **no** form of the command only returns the logging to its default value.

Examples

The following example shows how to change the memory log time to 48 hours of history:

```
Router(config)# memory statistics history table 48
```

Related Commands

Command	Description
show memory statistics history table	Displays the history of memory consumption on the Cisco IOS router over a specified period of time.

minor rising

To set minor level threshold values for the buffer, CPU, and memory resource owners (ROs), use the **minor rising** command in buffer owner configuration mode, CPU owner configuration mode, or memory owner configuration mode. To disable this function, use the **no** form of this command.

minor rising *rising-threshold-value* [**interval** *interval-value*] [**falling** *falling-threshold-value* [**interval** *interval-value*]] [**global**]

no minor rising

Syntax Description

rising-threshold-value	The rising threshold value as a percentage. Valid values are from 1 to 100.
interval	(Optional) Specifies the time, in seconds, during which the variation in rising or falling threshold values are not reported to the request/response unit (RU), resource group, or resource user types. For example, if the buffer usage count has gone above the configured threshold value and if it remains longer than the configured interval, a notification is sent to the RU, resource group, or resource user types.
interval-value	(Optional) The time, in seconds, during which the variation in rising or falling threshold values are not reported to the RU, resource group, or resource user types. Valid values are from 0 to 86400. The default value is 0.
falling	(Optional) Specifies the falling threshold value as a percentage.
falling-threshold-value	(Optional) The falling threshold value as a percentage. Valid values are from 1 to 100.
global	(Optional) Configures a global threshold. The **global** keyword is optional when you set major threshold values for public buffer, processor CPU, I/O memory, and processor memory. The **global** keyword is required when you set major threshold values for interrupt CPU and total CPU.

Command Default

Disabled by default.

Command Modes

Buffer owner configuration
CPU owner configuration
Memory owner configuration

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.

Usage Guidelines

The interval is the dampening or observation interval time in seconds during which the variations in the rising and falling threshold values are not notified to the ROs or RUs. That is, the interval is the time the system waits to check whether the threshold value stabilizes or not. The interval is set to avoid unnecessary and unwanted threshold notifications. If not configured, the system defaults to 0 seconds.

This command allows you to configure three types of thresholding:

- System Global Thresholding
- User Local Thresholding
- Per User Global Thresholding

System Global Thresholding

System global thresholding is used when the entire resource reaches a specified value. That is, RUs are notified when the total resource utilization goes above or below a specified threshold value. The notification order is determined by the priority of the RU. The RUs with a lower priority will be notified first, so that these low-priority RUs are expected to reduce the resource utilization. This order prevents the high-priority RUs from getting affected with unwanted notifications.

You can set rising and falling threshold values. For example, if you have set a total CPU utilization threshold value of 60% as the rising minor value and 5% as falling minor value, then when the total CPU utilization crosses the 60% mark, a minor Up notification is sent to all the RUs and when the total CPU utilization falls below 5%, a minor Down notification is sent to all the RUs. The same criteria apply to buffer ROs and memory ROs.

User Local Thresholding

User local thresholding is used when a specified RU exceeds the configured limits. The user local thresholding method prevents a single RU from monopolizing the resources. That is, the specified RU is notified when the resource utilization of the specified RU goes above or below a configured threshold value. For example, if you have set a CPU utilization threshold value of 60% as the rising minor value and 5% as the falling minor value, when the CPU utilization of the specified RU crosses the 60% mark, a minor Up notification is sent to only that RU and when the CPU utilization of the specified RU falls below 5%, a minor Down notification is sent to only that RU. The same method also applies to buffer and memory ROs.

Per User Global Thresholding

Per user global thresholding is used when the entire resource reaches a specified value. This value is unique for each RU and notification is sent only to the specified RU. User global thresholding is similar to user local thresholding, except that the global resource usage is compared against the thresholds. That is, only the specified RU is notified when the total resource utilization exceeds or falls below a configured threshold value. For example, if you have set a CPU utilization threshold value of 60% as the rising minor value and 5% as the falling minor value, when the total CPU utilization crosses the 60% mark, a minor Up notification is sent to only the specified RU and when the total CPU utilization falls below 5%, a minor Down notification is sent to only the specified RU. The same criteria also apply to buffer and memory ROs.

Threshold Violations

The Cisco IOS device sends out error messages when a threshold is violated. The following examples help you understand the error message pattern when different threshold violations occur in buffer, CPU, and memory ROs:

System Global Threshold Violation in Buffer RO

The threshold violation in buffer RO for a system global threshold shows the following output:

```
System global threshold-Violation (keywords Critical, Major and Minor alone will vary
accordingly)
================================================================================================
00:15:11: %SYS-4-GLOBALBUFEXCEED: Buffer usage has gone above global buffer Critical
threshold
configured <value> Current usage :<value>
```

For example:

```
00:15:11: %SYS-4-GLOBALBUFEXCEED: Buffer usage has gone above global buffer Critical
threshold
configured 144 Current usage :145

System global threshold- Recovery (keywords Critical, Major and Minor alone will vary
accordingly)
================================================================================================
00:17:10: %SYS-5-GLOBALBUFRECOVER: Buffer usage has gone below global buffer Critical
threshold
configured <value> Current usage :<value>
```

For example:

```
00:17:10: %SYS-5-GLOBALBUFRECOVER: Buffer usage has gone below global buffer Critical
threshold
configured 90 Current usage :89
```

Per User Global Threshold Violation in Buffer RO

The threshold violation in buffer RO for a user global threshold shows the following output:

```
User global threshold - Violation (keywords Critical, Major and Minor alone will vary
accordingly)
================================================================================================
00:24:04: %SYS-4-RESGLOBALBUFEXCEED: Buffer usage has gone above buffer Critical threshold
configured by resource user  <user-name>
configured 144 Current usage :145

User global threshold - Recovery (keywords Critical, Major and Minor alone will vary
accordingly)
================================================================================================
00:25:08: %SYS-4-RESGLOBALBUFRECOVER: Buffer usage has gone below buffer Critical
threshold configured by resource user <user-name>
configured 126 Current usage :125
```

User Local Threshold Violation in Buffer RO

The threshold violation in buffer RO for a user local threshold shows the following output:

```
User local threshold - Violation (keywords Critical, Major and Minor alone will vary
accordingly)
================================================================================================
00:31:15: %SYS-4-RESBUFEXCEED: Resource user  user_1 has exceeded the buffer Critical
threshold. configured 108 Current usage :109

User local threshold- Recovery (keywords Critical, Major and Minor alone will vary
accordingly)
================================================================================================
00:31:05: %SYS-5-RESBUFRECOVER: Resource user  user_1 has recovered after exceeding the
buffer Critical threshold. configured 90 Current usage :89
```

System Global Threshold Violation in CPU RO

The threshold violation in CPU RO for a system global threshold shows the following output:

```
System global threshold- Violation
(1) keywords Critical, Major and Minor will vary accordingly
(2) keywords total, process and interrupt will vary accordingly
================================================================================
00:19:36: %SYS-4-CPURESRISING: System is seeing global cpu util 19% at total level more
than the configured minor limit 11%

System global threshold - Recovery
(1) keywords Critical, Major and Minor will vary accordingly
(2) keywords total, process and interrupt will vary accordingly
================================================================================
00:20:56: %SYS-6-CPURESFALLING: System is no longer seeing global high cpu at total level
for the configured minor limit 10%, current value 4%
```

Per User Global Threshold Violation in CPU RO

The threshold violation in CPU RO for a user global threshold shows the following output:

```
User global threshold - Violation
(1) keywords Critical, Major and Minor will vary accordingly
(2) keywords total, process and interrupt will vary accordingly
================================================================================
00:14:21: %SYS-4-CPURESRISING: Resource user <user-name> is seeing global cpu util 11% at
total level more than the configured minor limit 6 %
```

For example:

```
00:14:21: %SYS-4-CPURESRISING: Resource user Test-proc-14:99s:1w:100n is seeing global cpu
util 11% at total level more than the configured minor limit 6%

User global threshold- Recovery
(1) keywords Critical, Major and Minor will vary accordingly
(2) keywords total, process and interrupt will vary accordingly
================================================================================
00:14:46: %SYS-6-CPURESFALLING: Resource user <user-name> is no longer seeing global high
cpu at total level for the configured critical limit 9%, current value 4%
```

For example:

```
00:14:46: %SYS-6-CPURESFALLING: Resource user Test-proc-14:99s:1w:100n is no longer seeing
global high cpu at total level for the configured critical limit 9%, current value 4%
```

User Local Threshold Violation in CPU RO

The threshold violation in CPU RO for a user local threshold shows the following output:

```
User local threshold - Violation (keywords Critical, Major and Minor will vary accordingly
- only process level)
================================================================================
00:12:11: %SYS-4-CPURESRISING: Resource user <user-name> is seeing local cpu util 15% at
process level more than the configured minor limit 6%
```

For example:

```
00:12:11: %SYS-4-CPURESRISING: Resource user Test-proc-9:85s:15w:100n is seeing local cpu
util 15% at process level more than the configured minor limit 6%

User local threshold- Recovery (keywords Critical, Major and Minor will vary accordingly
- only process level)
================================================================================
00:13:11: %SYS-6-CPURESFALLING: Resource user <user-name> is no longer seeing local high
cpu at process level for the configured critical limit 9%, current value 3%
```

System Global Threshold Violation in Memory RO

The threshold violation in memory RO for a system global threshold shows the following output:

```
System global threshold - Violation (keywords Critical, Major and Minor alone will vary
accordingly)
(If violation happens in IO memory pool will be : I/O)
================================================================================
13:53:22: %SYS-5-GLOBALMEMEXCEED: Global Memory has exceeded the Minor threshold
Pool: Processor  Used: 422703520  Threshold: 373885200
```

For example:

```
13:54:03: %SYS-5-GLOBALMEMEXCEED: Global Memory has exceeded the Critical threshold
Pool: Processor  Used: 622701556  Threshold: 467356500

System global threshold - Recovery ( keywords Critical, Major and Minor alone will vary
accordingly )
(If recovery happens in IO memory pool will be : I/O)
================================================================================
%SYS-5-GLOBALMEMRECOVER: Global Memory has recovered after exceeding Minor threshold
Pool: Processor  Used: 222473448  Threshold: 355190940
```

For example:

```
13:50:41: %SYS-5-GLOBALMEMRECOVER: Global Memory has recovered after exceeding Critical
threshold
Pool: Processor  Used: 222473152  Threshold: 443988675
```

Per User Global Threshold Violation in Memory RO

The threshold violation in memory RO for a user global threshold shows the following output:

```
User global threshold - Violation (keywords Critical, Major and Minor alone will vary
accordingly)
(If violation happens in IO memory pool will be : I/O)
================================================================================
00:53:14: %SYS-4-RESGLOBALMEMEXCEED: Global Memory has exceeded the Minor threshold
configure by resource user <XYZ>
Pool: Processor  Used: 62273916  Threshold: 62246820

User global threshold - Recovery (keywords Critical, Major and Minor alone will vary
accordingly)
(If recovery happens in IO memory pool will be : I/O)
================================================================================
00:32:56: %SYS-4-RESGLOBALMEMRECOVER: Global Memory has recovered after exceeding the
Critical threshold configure by resource user <XYZ>
Pool: Processor  Used: 329999508  Threshold: 375865440
```

User Local Threshold Violation in Memory RO

The threshold violation in memory RO for a user local threshold shows the following output:

```
User local threshold- Violation (keywords Critical, Major and Minor alone will vary
accordingly)
================================================================================
01:05:42: %SYS-4-RESMEMEXCEED: Resource user <XYZ> has exceeded the Critical memory
threshold
Pool: Processor Used: 103754740 Threshold: 103744700

User local threshold - Recovery (keywords Critical, Major and Minor alone will vary
accordingly)
================================================================================
00:44:43: %SYS-5-RESMEMRECOVER: Resource user <XYZ> has recovered after exceeding the
Critical memory threshold
Pool: Processor Used: 328892280 Threshold :375865440
```

Examples

Configuring Minor Rising Values for System Global Thresholding

The following example shows how to configure the minor threshold values for the system global thresholding with a minor rising threshold of 60% at an interval of 12 seconds and a minor falling threshold of 5% at an interval of 10 seconds:

```
Router(config-owner-cpu)# minor rising 60 interval 12 falling 5 interval 10 global
Router(config-owner-buffer)# minor rising 60 interval 12 falling 5 interval 10 global
Router(config-owner-memory)# minor rising 60 interval 12 falling 5 interval 10 global
```

Configuring Minor Rising Values for User Local Thresholding

The following example shows how to configure the minor threshold values for user local thresholding with a minor rising threshold of 60% at an interval of 12 seconds and a minor falling threshold of 5% at an interval of 10 seconds:

```
Router(config-owner-cpu)# minor rising 60 interval 12 falling 5 interval 10
Router(config-owner-buffer)# minor rising 60 interval 12 falling 5 interval 10
Router(config-owner-memory)# minor rising 60 interval 12 falling 5 interval 10
```

Configuring Minor Rising Values for Per User Global Thresholding

The following example shows how to configure the minor threshold values for per user global thresholding with a minor rising threshold of 60% at an interval of 12 seconds and a minor falling threshold of 5% at an interval of 10 seconds:

```
Router(config-owner-cpu)# minor rising 60 interval 12 falling 5 interval 10 global
Router(config-owner-buffer)# minor rising 60 interval 12 falling 5 interval 10 global
Router(config-owner-memory)# minor rising 60 interval 12 falling 5 interval 10 global
```

Related Commands

Command	Description
buffer public	Enters the buffer owner configuration mode and sets threshold values for buffer usage.
cpu interrupt	Enters the CPU owner configuration mode and sets threshold values for interrupt level CPU utilization.
cpu process	Enters the CPU owner configuration mode and sets threshold values for processor level CPU utilization.
cpu total	Enters the CPU owner configuration mode and sets threshold values for total CPU utilization.
memory io	Enters the memory owner configuration mode and sets threshold values for I/O memory.
memory processor	Enters the memory owner configuration mode and sets threshold values for processor memory.
policy (ERM)	Configures an ERM resource policy.
resource policy	Enters ERM configuration mode.
show resource all	Displays all the resource details.
slot (ERM policy)	Configures line cards.
system (ERM policy)	Configures system level ROs.

monitor capture

To enable and configure monitor packet capturing, use the the **monitor capture** privileged EXEC mode command. To disable monitor packet capturing, use the **no** form of this command.

monitor capture [**buffer size** *size*] [**circular | linear**] [**dot1q**] [**filter** *acl-num | exp-acl-num | acl-name*] [**length** *bytes*] {**clear** [**filter**] | **export buffer** *location* | **schedule at** *hh***:***mm***:***ss* [*date* [*month year*]] | **start** [**for** *number* {**seconds | packets**}] | **stop**}

no monitor capture [**buffer size** *size*] [**circular | linear**] [**dot1q**] [**filter** *acl-num | exp-acl-num | acl-name*] [**length** *bytes*] [**clear** [**filter**] | **export buffer** *location* | **schedule at** *hh***:***mm***:***ss* [*date* [*month year*]]]

Syntax Description

buffer size *size*	Specifies the capture buffer size in kilobytes. Range: 32 to 65535. Default: 2048 Kb.
circular | linear	Specifies a circular or linear capture buffer. The default is linear.
clear	Clears the capture buffer and sets the number of captured packets to zero.
dot1q	Includes dot1q information in the monitor capturing.
export buffer	Exports to remote location.
filter	Specifies that packets from a specified ACLs only are sent to the capture buffer.
acl-num	IP access list (standard or extended). Range: 1 to 199.
exp-acl-num	IP expanded access list (standard or extended). Range: 1300 to 2699.
acl-name	ACL name.
length *size*	Specifies the capture length of each packet in bytes. Range: 0 to 9216. Default: 68.
location	Location to dump capture buffer. Valid values are as follows: • **dot1q** *location*—Specifies the dot1q capture buffer location. • **bootflash:**—Location to dump buffer. • **disk0:**—Location to dump buffer. • **ftp:**—Location to dump buffer. • **http:**—Location to dump buffer. • **https:**—Location to dump buffer. • **rcp:**—Location to dump buffer. • **scp:**—Location to dump buffer. • **sup-bootdisk:**—Location to dump buffer. • **tftp:**—Location to dump buffer.
schedule at	Schedules the capture at a specific time/date.
*hh***:***mm***:***ss*	Time in hours:minutes:seconds. Range: hours: 0 to 23; minutes: 0 to 59; seconds: 0 to 59.
date	(Optional) Date. Range: 1 to 31.
month	(Optional) Month. Range: 1 to 12.
start	Starts capturing the packets to the beginning of the buffer.

for	(Optional) Specifies the length of time in seconds or the number of packets.
number	Stops the capture after the specified number of seconds or packets. Range: 1 to 4294967295.
stop	Moves the capture to the OFF state.

Command Default

Capture buffer is disabled by default.

Command Modes

EXEC (>)

Command History

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

Usage Guidelines

The **buffer size** *size* keywords and argument defines the buffer size that is used to store the packet.

The **length** *size* keyword and argument copies the specified number of bytes of data from each packet. The default setting of 68 bytes is adequate for IP, ICMP, TCP, and UDP. If you set the length to 0, the whole packet is copied to the buffer.

The **linear** capture buffer mode specifies that capture stops when the end of the capture buffer is reached. In the **circular** capture buffer mode, the capture will begin to overwrite earlier entries when the capture buffer becomes full. Changing the buffer mode or the buffer length automatically stops the capture.

If the ACL specified is configured, it is used for applying the filter in the software. When you specify a capture filter ACL in the **start** command, the new ACL will not override any configured ACLs. The new ACL will execute in software.

If you configure the capture schedule, the capture schedule stops the capture start for the specified future time. This is the same as manually starting a capture at the specified time. If any capture is already running, that capture is stopped and the buffer is cleared.

The format for **time** and **date** is *hh:mm:ss dd mmm yyyy*. The time zone is GMT. The hour is specified in 24-hour notation, and the month is specified by a three-letter abbreviation. For example, to set a capture starting time of 7:30 pm on October 31, 2008, use the notation 19:30:00 31 oct 2008.

If you do not enter the **start** or **stop** keyword, the capture buffer is initialized and set in the OFF state.

If you enter the **no monitor capture** command without entering any keywords or arguments, capture is stopped and the capture buffer is deleted. After entering the **no** form of the monitor capture command, the capture buffer cannot be displayed or exported. If you specify the *length* or **buffer size** with the **no monitor capture** command, the capture is not deleted and the length or buffer size is set to the default values. The **start** and **stop** keywords are not valid with the **no monitor capture** command.

To clear the EXEC configurations or any capture schedules, enter the **clear** keyword. The **clear** keyword clears the capture buffer and sets the number of captured packets to zero.

Examples

This example shows how to configure the capture length initially before starting the capture:

```
Router# monitor capture length 128
Router# monitor capture start
Router# monitor capture stop
```

This example shows how to start a new capture with non-default values:

```
Router# monitor capture length 100 circular start
Router# monitor capture stop
```

Related Commands

Command	Description
show monitor capture	Displays the capture buffer contents.

monitor capture buffer

To configure a capture buffer to capture packet data, use the **monitor capture buffer** command in privileged EXEC mode. To stop capturing packet data into the buffer, use the **no** form of this command.

monitor capture buffer *buffer-name* [**circular** | **clear** | **export** *export-location* | **filter access-list** {*ip-access-list* | *ip-expanded-list* | *access-list-name*} | **limit** {**allow-nth-pak** *nth-packet* | **duration** *seconds* | **packet-count** *total-packets* | **packets-per-sec** *packets*} | **linear** | **max-size** *element-size* | **size** *buffer-size* [**max-size** *element-size*]]

no monitor capture buffer *buffer-name*

Syntax Description

buffer-name	Name of the capture buffer.
circular	(Optional) Specifies that the buffer is of circular type.
clear	(Optional) Clears contents of capture buffer.
export *export-location*	(Optional) Exports data from capture buffer in PCAP format to the export location specified: **ftp:**, **http:**, **https:**, **pram:**, **rcp:**, **scp:**, **tftp:.**
filter access-list	(Optional) Configures filters to filter the packets stored in the capture buffer using access control lists (ACLs). Name or type of access lists can be specified as criteria for configuring the filters.
ip-access-list	(Optional) The IP access list number. Range is from 1 to 199.
ip-expanded-list	(Optional) The IP expanded access list number. Range is from 1300 to 2699.
access-list-name	(Optional) Name of the access list.
limit	(Optional) Limits the packets captured based on the parameters specified.
allow-nth-pak *nth-packet*	(Optional) Allows every *n*th packet in the captured data through the buffer.
duration seconds	(Optional) Specifies the duration of capture measured, in seconds. Range is from 1 to 2147483647.
packet-count *total-packets*	(Optional) Specifies the total number of packets captured. Range is from 1 to 2147483647.
packets-per-sec *packets*	(Optional) Specifies the number of packets copied per second. Range is from 1 to 2147483647.
linear	(Optional) Specifies that the buffer is of linear type. By default, the capture buffer is of linear type.
max-size *element-size*	(Optional) Maximum size of element in the buffer, in bytes. Range is from 68 to 9500.
size *buffer-size*	(Optional) Size of the buffer. Range is from 256 kilo bytes (KB) to 100 mega bytes (MB). The default value is 1 MB.

Command Default

Data packets are not captured into a capture buffer.

Command Modes

Privileged EXEC (#)

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.

Usage Guidelines

Use this command to configure the capture buffer. You can configure two types of capture buffers: linear and circular. When the linear buffer is full, data capture stops automatically. When the circular buffer is full, data capture starts from the beginning.

Use the **limit** keyword to control the rate at which packets are captured.

Examples

The following example shows how to define a capture buffer named pktrace1 that is up to 256KB long and includes 256 bytes per packet:

```
Router# monitor capture buffer pktrace1 circular size 256 max-size 256
```

The following example shows how to export the data from the pktrace1 buffer for analysis:

```
Router# monitor capture buffer pktrace1 export tftp://88.1.88.9/pktrace1
```

Related Commands

Command	Description
debug packet-capture	Enables packet capture infra debugs.
monitor capture point	Defines a monitor capture point and associates it with a capture buffer.
show monitor capture	Displays the contents of a capture buffer or a capture point.

monitor capture point

To define a monitor capture point, use the **monitor capture point** command in privileged EXEC mode. To disable the monitor capture point, use the **no** form of this command.

monitor capture point {**ip** | **ipv6**}{**cef** *capture-point-name interface-name interface-type* {**both** | **in** | **out**} | **process-switched** *capture-point-name* {**both** | **from-us** | **in** | **out**}}

no monitor capture point {**ip** | **ipv6**} {**cef** *capture-point-name interface-name interface-type* | **process-switched** *capture-point-name*}

Syntax Description

ip	Configures an IPv4 capture point.
ipv6	Configures an IPv6 capture point.
cef	Specifies that the capture point contains Cisco Express Forwarding (CEF) packets.
capture-point-name	Name of the capture point.
interface-name interface-type	Specifies the interface name and type. For more information, use the question mark (?) online help function.
both	Specifies that the packets are captured in ingress and egress directions.
in	Specifies that the packets are captured in ingress direction.
out	Specifies that the packets are captured in egress direction.
process-switched	Specifies that the capture point contains process switched packets.
from-us	Specifies that the packets are originating locally.

Command Default

Monitor capture points are not defined.

Command Modes

Privileged EXEC (#)

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.

Usage Guidelines

Two types of capture points can be defined: IPv4 and IPv6. Once defined, use the **monitor capture point associate** command to associate the capture point with a capture buffer. Use the **monitor capture point start** command to start packet capture.

Multiple packet capture points can be activated on a given interface. For example, Border Gateway Protocol (BGP) packets can be captured into one capture buffer and Open Shortest Path First (OSPF) packets into another.

Examples

The following example shows how to define a capture point named ipceffa0/1 with CEF switching path and the Fast Ethernet interface 0/1:

```
Router# monitor capture point ip cef ipceffa0/1 fastEthernet 0/1 both
```

Related Commands

Command	Description
debug packet-capture	Enables packet capture infra debugs.
monitor capture buffer	Configures a capture buffer to capture packet data.
monitor capture point associate	Associates a monitor capture point with a capture buffer.
monitor capture point start	Enables a monitor capture point to start capturing packet data.
show monitor capture	Displays the contents of a capture buffer or a capture point.

monitor capture point associate

To associate a monitor capture point with a capture buffer, use the **monitor capture point associate** command in privileged EXEC mode.

monitor capture point associate *capture-point-name capture-buffer-name*

Syntax Description

capture-point-name	Name of the capture point to be associated with the capture buffer.
capture-buffer-name	Name of the capture buffer.

Command Default

Monitor capture points are not associated with capture buffers.

Command Modes

Privileged EXEC (#)

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.

Usage Guidelines

Use the **monitor capture point** command to define the capture points. Once the capture points are defined, use the **monitor capture point associate** command to associate a capture point with a capture buffer. This results in all packets captured from the specified capture point to be dumped into the associated capture buffer. A capture point can be associated with only one capture buffer.

Use the **monitor capture point disassociate** command to disassociate the specified capture point from the capture buffer.

Examples

The following example shows how to associate the ipceffa0/1 capture point to the pktrace1 capture buffer:

```
Router# monitor capture point associate ipceffa0/1 pktrace1
```

Related Commands

Command	Description
debug packet-capture	Enables packet capture infra debugs.
monitor capture buffer	Configures a capture buffer to capture packet data.
monitor capture point	Defines a monitor capture point.
monitor capture point disassociate	Disassociates a monitor capture point from the specified monitor capture buffer.
show monitor capture	Displays the contents of a capture buffer or a capture point.

monitor capture point disassociate

To disassociate a monitor capture point from its associations with a capture buffer, use the **monitor capture point disassociate** command in privileged EXEC mode.

monitor capture point disassociate *capture-point-name*

Syntax Description

capture-point-name	Specifies the name of the capture point to be disassociated from the capture buffer.

Command Default

Monitor capture points are not associated with capture buffers.

Command Modes

Privileged EXEC (#)

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.

Usage Guidelines

Use the **monitor capture point associate** command to associate a capture point with a capture buffer. This results in all packets captured from the specified capture point to be dumped into the associated capture buffer. A capture point can be associated with only one capture buffer.

Use the **monitor capture point disassociate** command to disassociate the specified capture point from the capture buffer.

Examples

The following example shows how to disassociate the ipceffa0/1 capture point from its capture buffer:

```
Router# monitor capture point disassociate ipceffa0/1
```

Related Commands

Command	Description
debug packet-capture	Enables packet capture infra debugs.
monitor capture buffer	Configures a capture buffer to capture packet data.
monitor capture point	Defines a monitor capture point.
monitor capture point associate	Associates a monitor capture point with a capture buffer.
show monitor capture	Displays the contents of a capture buffer or a capture point.

monitor capture point start

To enable a monitor capture point to start capturing packet data, use the **monitor capture point start** command in privileged EXEC mode.

monitor capture point start {*capture-point-name* | **all**}

Syntax Description

capture-point-name	Name of the capture point to start capturing packet data.
all	Configures all capture points to start capturing packet data.

Command Default

Data packets are not captured into a capture buffer.

Command Modes

Privileged EXEC (#)

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.

Usage Guidelines

Use this command to capture packet data at a traffic trace point into a buffer.

Once the capture point is defined, use the **monitor capture point start** command to enable the packet data capture. To stop capturing the packet data, use the **monitor capture point stop** command.

Examples

The following example shows how to start the packet capture:

```
Router# monitor capture point start ipceffa0/1

Mar 21 11:13:34.023: %BUFCAP-6-ENABLE: Capture Point ipceffa0/1 enabled.
```

Related Commands

Command	Description
debug packet-capture	Enables packet capture infra debugs.
monitor capture buffer	Configures a capture buffer to capture packet data.
monitor capture point	Defines a monitor capture point.
monitor capture point stop	Disables the packet capture.
show monitor capture	Displays the contents of a capture buffer or a capture point.

monitor capture point stop

To disable the packet capture, use the **monitor capture point stop** command in privileged EXEC mode.

monitor capture point stop {*capture-point-name* | **all**}

Syntax Description

capture-point-name	Name of the capture point to stop the packet capture.
all	Configures all capture points to stop the packet capture.

Command Default

Data packets are not captured into a capture buffer.

Command Modes

Privileged EXEC (#)

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.

Examples

```
Router# monitor capture point stop ipceffa0/1

Mar 21 11:14:20.152: %BUFCAP-6-DISABLE: Capture Point ipceffa0/1 disabled.
```

Related Commands

Command	Description
debug packet-capture	Enables packet capture infra debugs.
monitor capture buffer	Configures a capture buffer to capture packet data.
monitor capture point	Defines monitor capture points.
show monitor capture	Displays the contents of a capture buffer or a capture point.

monitor drop

To enable and configure the information flow violations counter, use the **monitor drop** privileged EXEC mode command. To disable the information flow violations counter, use the **no** form of this command.

monitor drop match {**ip** *acl-name* | **ipv6** *acl-name*} [**threshold-count** *num-pack*] [**interval** *interval-sec*]

no monitor drop match {**ip** *acl-name* | **ipv6** *acl-name*} [**threshold-count** *num-pack*] [**interval** *interval-sec*]

Syntax Description

match	(Optional) Matches the protocol types. Possible *match* values are: • *ip*—ipv4 protocol • *ipv6*—ipv6 protocol
acl-name	ACL name.
threshold-count	Specifies the threshold for the number of packets dropped. The range is from 1 to 4294967295.
interval	(Optional) Specifies the drop monitor interval, in seconds. Range: 1 to 255. Default: 60.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced on the Cisco ASR 1000 Series Routers.

Examples

The following example displays the number of information flow policy violations by an individual source network identifier within a specified time period:

```
Router# monitor drop match match ip myacl threshold-count 1 interval 60
Already monitor this ACL:myacl
```

monitor event-trace cpu-report (EXEC)

To monitor the event tracing of the CPU reports, use the **monitor event-trace cpu-report** command in user EXEC or privileged EXEC mode.

monitor event-trace cpu-report {**clear** | **continuous** [**cancel**] | **disable** | **dump** [**pretty**] | **enable** | **one-shot**}

Syntax Description

clear	Clears the event tracing.
continuous	Displays continuously the latest event trace entries.
cancel	(Optional) Cancels the continuous display of the latest event trace entries.
disable	Disables event tracing.
dump	Dumps the event buffer into a file.
pretty	(Optional) Dumps the event buffer into a file in ASCII format.
enable	Enables the event tracing.
one-shot	Indicates that first clears the event trace, sets running, and then disables at wrap point.

Command Default

Disabled

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 example shows how to enable event tracing of the CPU reports:

```
Router# monitor event-trace cpu-report enable
```

The following example shows how to enable continuous event tracing of the CPU reports:

```
Router# monitor event-trace cpu-report continuous
```

The following example shows how to dump the event tracing information into a file in ASCII format:

```
Router# monitor event-trace cpu-report dump pretty
```

The following example shows how to clear the event tracing information:

```
Router# monitor event-trace cpu-report clear
```

Related Commands

Command	Description
show monitor event-trace cpu-report	Displays the CPU report details for event tracing on a networking device.

monitor event-trace cpu-report (global)

To monitor the collection of CPU report traces, use the **monitor event-trace cpu-report** command in global configuration mode.

monitor event-trace cpu-report {**disable** | **dump-file** *location* | **enable** | **size** | **stacktrace**}

Syntax Description

disable	Disables event tracing.
dump-file	Dumps the event buffer into a file.
location	The URL at which the file is stored.
enable	Enables the event tracing.
size	Sets the size of event trace. Valid values are from 1 to 1000000.
stacktrace	Clears the trace buffer first and then traces the call stack at tracepoints. Valid values for the depth of stack traces stored are from 1 to 16.

Command Default

Disabled

Command Modes

Global configuration

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 example shows how to enable event tracing of the CPU reports:

```
Router(config)# monitor event-trace cpu-report enable
```

The following example shows how to dump the event tracing information into a file at http:\\www.cisco.com location:

```
Router# monitor event-trace cpu-report dump-file http:\\www.cisco.com
```

The following example shows how to disable the event tracing information:

```
Router# monitor event-trace cpu-report disable
```

The following example shows how to first clear the event tracing and then trace the call stacks at the tracepoints 4:

```
Router# monitor event-trace cpu-report stacktrace 4
```

Related Commands

Command	Description
show monitor event-trace cpu-report	Displays the CPU report details for event tracing on a networking device.

monitor platform command

To monitor the output of a **show** command by watching the output continually appear on the console, enter the **monitor platform command** command in priviliged EXEC or diagnostic mode.

monitor platform command show *show-command-option*

Syntax Description

show *show-command-option*	A **show** command option from an existing **show** command.

Command Modes

Diagnostic Mode (diag)

Privileged EXEC (#)

Command Default

No default behavior or values.

Command History

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

Usage Guidelines

When the **monitor platform command** command is entered, a monitor function that continually displays the output of the specified **show** *show-command-option* will appear on the console. Enter **Ctrl-C** or **q** at any time while the monitor is running to return to the command-line interface prompt.

Once the monitor is running, the following options, which can be seen at any time by entering **h** or **?**, are available:

- **d**—toggle continuous diff mode. In continuous diff mode, the monitor will display the changes that have occurred inbetween display intervals.
- **D**—toggle fixed diff mode. In fixed diff mode, the monitor will display all changes made after entering fixed diff mode in each line of output.
- **h**—help. Displays the menu options available while the monitor is running.
- **q**—quit. Quits the monitor and returns to the command-line interface prompt.
- **r**—set a refresh time. Takes user to a prompt where the refresh time can be specified in seconds.
- **s**—set a sort column. Takes user to a prompt where the sorting of tabular output can be set.
- **?**—help. Displays the menu options available while the monitor is running.

To see the *show-command-options* that can be used with this command, enter **monitor platform command show ?** and continue to navigate the CLI using the **?** help function.

The output of a **show** command specified using the **show** *show-command-option* within this command-line is identical to the output that would be displayed if the **show** command was entered once without using the **monitor platform command** function. For information on the output of a particular **show** command, see the command reference for that specified **show** command.

Examples

In the following example, the **monitor platform command** command is used to repeatedly show the output of the **show rom-monitor r0** command. Note that Ctrl-Z is used to stop the output display and return to the command-line prompt.

```
Router# monitor platform command show rom-monitor r0

System Bootstrap, Version 12.2(20070807:170946) [asr1000_rommon_rel_1_22 101], DEVELOPMENT
SOFTWARE
Copyright (c) 1994-2006 by cisco Systems, Inc.

System Bootstrap, Version 12.2(20070807:170946) [asr1000_rommon_rel_1_22 101], DEVELOPMENT
SOFTWARE
Copyright (c) 1994-2006 by cisco Systems, Inc.

System Bootstrap, Version 12.2(20070807:170946) [asr1000_rommon_rel_1_22 101], DEVELOPMENT
SOFTWARE
Copyright (c) 1994-2006 by cisco Systems, Inc.

System Bootstrap, Version 12.2(20070807:170946) [asr1000_rommon_rel_1_22 101], DEVELOPMENT
SOFTWARE
Copyright (c) 1994-2006 by cisco Systems, Inc.

System Bootstrap, Version 12.2(20070807:170946) [asr1000_rommon_rel_1_22 101], DEVELOPMENT
SOFTWARE
Copyright (c) 1994-2006 by cisco Systems, Inc.

System Bootstrap, Version 12.2(20070807:170946) [asr1000_rommon_rel_1_22 101], DEVELOPMENT
SOFTWARE
Copyright (c) 1994-2006 by cisco Systems, Inc.

System Bootstrap, Version 12.2(20070807:170946) [asr1000_rommon_rel_1_22 101], DEVELOPMENT
SOFTWARE
Copyright (c) 1994-2006 by cisco Systems, Inc.

q

Router#
```

monitor platform software process

To monitor software processes on the Cisco ASR 1000 Series Routers, enter the **monitor platform software process** command in priviliged EXEC or diagnostic mode.

monitor platform software process [*slot*]

Syntax Description

slot	Specifies the slot of the *hardware-module*. Options include: • *number*—the number of the SIP slot. For instance, if you wanted to specify the SIP in SIP slot 2 of the router, enter 2 as the *number*. • **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.

Command Modes

Diagnostic Mode (diag)

Privileged EXEC (#)

Command Default

No default behavior or values.

Command History

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

Usage Guidelines

When the **monitor platform software process** command is entered, a monitor function that shows memory-related data about the router by process will appear on the console. This monitor function will continue to update itself until **Ctrl-C** or **q** is entered to return to the command-line interface prompt.

Many options are available while the monitor is running. To view these options, enter **h** or **?** while the monitor is running.

If this command is entered without a *slot* specification, the output will reflect all processes on the active RP.

This command is particularly useful for monitoring cpu and memory usage by process.

Examples

In the following example, the **monitor platform software process** command is entered to monitor all processes on a Cisco ASR 1000 Series Router.

```
Router# monitor platform software process
top - 18:29:08 up 1 day,  1:36,  0 users,  load average: 0.00, 0.00, 0.00
Tasks: 138 total,   3 running, 135 sleeping,   0 stopped,   0 zombie
Cpu(s):  0.7% us,  0.0% sy,  0.0% ni, 99.3% id,  0.0% wa,  0.0% hi,  0.0% si
Mem:   3941456k total,  1076004k used,  2865452k free,    59904k buffers
Swap:        0k total,        0k used,        0k free,   673648k cached

 PID USER    PR NI VIRT RES  SHR S %CPU %MEM  TIME+ COMMAND
 9429 root   20  0 42224 21m 18m S  0.3  0.5  1:54.54 imand
10126 root   20  0 1886m 259m 79m R  0.3  6.7  4:02.15 ppc_linux_iosd-
27897 binos  20  0 2352 1212  932 R  0.3  0.0  0:00.02 top
  1 root    20  0 1928  576  500 S  0.0  0.0  0:11.48 init
  2 root    39 19   0   0   0 S  0.0  0.0  0:00.06 ksoftirqd/0
  3 root    15 -5   0   0   0 S  0.0  0.0  0:00.00 events/0
  4 root    15 -5   0   0   0 S  0.0  0.0  0:00.01 khelper
  5 root    15 -5   0   0   0 S  0.0  0.0  0:00.00 kthread
 26 root    15 -5   0   0   0 S  0.0  0.0  0:00.00 kblockd/0
 30 root    15 -5   0   0   0 S  0.0  0.0  0:00.23 khubd
 66 root    20  0   0   0   0 S  0.0  0.0  0:00.00 pdflush
 67 root    20  0   0   0   0 S  0.0  0.0  0:00.02 pdflush
 68 root    15 -5   0   0   0 S  0.0  0.0  0:00.01 kswapd0
 69 root    15 -5   0   0   0 S  0.0  0.0  0:00.00 aio/0
 70 root    15 -5   0   0   0 S  0.0  0.0  0:00.00 xfslogd/0
 71 root    15 -5   0   0   0 S  0.0  0.0  0:00.00 xfsdatad/0
677 root    20  0   0   0   0 S  0.0  0.0  0:00.11 mtdblockd
736 root    15 -5   0   0   0 S  0.0  0.0  0:00.00 scsi_eh_0
737 root    15 -5   0   0   0 S  0.0  0.0  0:00.00 usb-storage
740 root    15 -5   0   0   0 S  0.0  0.0  0:00.00 scsi_eh_1
741 root    15 -5   0   0   0 S  0.0  0.0  0:00.05 usb-storage
766 root    15 -5   0   0   0 S  0.0  0.0  0:00.00 scsi_eh_2
767 root    15 -5   0   0   0 S  0.0  0.0  0:00.00 scsi_eh_3
768 root    15 -5   0   0   0 S  0.0  0.0  0:00.00 scsi_eh_4
769 root    15 -5   0   0   0 S  0.0  0.0  0:00.00 scsi_eh_5
782 root    15 -5   0   0   0 S  0.0  0.0  0:00.00 mcp-rtc-wq
1617 root    0 -20   0   0   0 S  0.0  0.0  0:00.00 loop0
1708 bin    20  0 2028  628  524 S  0.0  0.0  0:00.00 portmap
1710 bin    20  0 2028  604  512 S  0.0  0.0  0:00.00 portmap
1764 root    0 -20   0   0   0 S  0.0  0.0  0:00.01 loop1
1798 root    0 -20   0   0   0 S  0.0  0.0  0:00.12 loop2
1832 root    0 -20   0   0   0 S  0.0  0.0  0:00.19 loop3
1866 root    0 -20   0   0   0 S  0.0  0.0  0:00.01 loop4
1956 root    0 -20   0   0   0 S  0.0  0.0  0:00.05 loop5
1990 root    0 -20   0   0   0 S  0.0  0.0  0:00.04 loop6
2031 root    0 -20   0   0   0 S  0.0  0.0  0:00.06 loop7
2898 root   16 -4 1928 456 344 S  0.0  0.0  0:00.23 udevd
3762 root   30 10   0   0   0 S  0.0  0.0  0:00.00 jffs2_gcd_mtd1
 4179 root      20   0  2924 1356 1148 S  0.0  0.0   0:00.00 auxinit.sh
q
Router#
```

monitor processes cpu extended

To configure a process or processes to be included in the extended load monitor report, use the **monitor processes cpu extended** command in user EXEC or privileged EXEC mode. To disable this function, use the **no** form of this command.

monitor processes cpu extended *process-id-list*

no monitor processes cpu extended *process-id-list*

Syntax Description

process-id-list	The list of process identifiers (PIDs). You can specify a maximum of eight processes. Valid values range from 1 to 2147483647.

Command Default

Disabled by default.

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.

Usage Guidelines

This command marks a process or processes to be monitored for extended CPU load. You can specify a maximum of eight processes to be monitored using this command. This command is used to forcibly put a process in the latency report generated by the extended load monitor.

Examples

The following example shows how to enable extended CPU load monitor for the process with PID 2:

```
Router# monitor processes cpu extended 2
```

Related Commands

Command	Description
show processes cpu extended	Displays an extended CPU load report.

monitor traffic-util backplane

To enable the backplane traffic utilization monitor or set the traffic monitor interval, use the **monitor traffic-util backplane** command in global configuration mode. To disable the backplane traffic utilization monitor, use the **no** form of this command. To return to the default settings, use the **default** form of this command.

monitor traffic-util backplane [**logging interval** *interval*] [**interval** *interval* | **threshold** *percentage*]

[**no | default**] **monitor traffic-util backplane**

Syntax Description

logging interval *interval*	(Optional) Specifies the traffic monitor backplane syslog interval in seconds when utilization is in the crossed state. Range: 300 to 14400. Default: 300.
interval *interval*	(Optional) Specifies the traffic monitor interval in seconds. Range: 1 to 255. Default: 60.
threshold *percentage*	(Optional) Specifies in percent the backplane traffic utilization threshold for the traffic monitor to generate a syslog message. Range: 1 to 100. Default: 80.
default	(Optional) Returns to the default settings.

Command Default

Backplane traffic utilization monitor is disabled by default.

Command Modes

Global configuration ((config)#)

Command History

Release	Modification
12.2(33)SXH4	Support for this command was introduced.
12.2(33)SXI	Support for this command was introduced.
12.2(33)SXF15	Support for this command was introduced.

Usage Guidelines

If you enable backplane traffic utilization monitoring, the **default** form of this command sets the command defaults to interval is **60** and percentage is **80**.

Examples

The following example shows how to enable backplane traffic utilization monitoring:

```
Router(config)# monitor traffic-util backplane
```

The following example shows how to disable backplane traffic utilization monitoring:

```
Router(config)# no monitor traffic-util backplane
```

The following example shows how to specify the traffic monitor interval in seconds:

```
Router(config)# monitor traffic-util backplane interval 50
```

The following example shows how to specify the traffic monitor backplane syslog interval in seconds when utilization is in the crossed state:

```
Router(config)# monitor traffic-util backplane logging interval 600
```

The following example shows how to specify the traffic monitor threshold:

```
Router(config)# monitor traffic-util backplane threshold 70
```

Related Commands

Command	Description
monitor traffic-util fpoe	Enables and configures the traffic utilization monitor for the fabric channel.
show catalyst6000 traffic-meter	Displays the percentage of the backplane (shared bus) utilization and traffic monitor status information.

monitor traffic-util fabric

To enable the traffic monitor for a fabric channel and set the interval and threshold values, use the **monitor traffic-util fabric** command in global configuration mode. To disable the fabric channel traffic utilization monitor, use the **no** form of this command.

monitor traffic-util fabric {*mod-num* | **all**} {**channel** {**0** | **1** | **both**}} {**direction** {**egress** | **ingress** | **both**}} [**interval** *interval* **threshold** *percentage*]

no monitor traffic-util fabric

Syntax Description

mod-num	Number of the module.
all	Specifies all module numbers.
channel	Specifies a fabric channel.
0	Specifies channel 0.
1	Specifies channel 1.
both	Specifies both channels.
direction	Specifies the traffic direction to monitor.
egress	Specifies egress traffic only.
ingress	Specifies ingress traffic only.
both	Specifies egress and ingress traffic.
interval *interval*	(Optional) Specifies the traffic monitor interval in seconds. Range: 1 to 255. Default: 60.
threshold *percentage*	Specifies the percentage of fabric channel traffic utilization monitor threshold before the traffic monitor generates a syslog message. Range: 1 to 100. Default: 80.

Command Default

The fabric channel traffic utilization monitor is disabled by default. If you enable traffic monitoring, the defaults are as follows:

- **all**.
- *interval* is 60.
- *percentage* is 80.

Command Modes

Global configuration ((config)#)

Command History

Release	Modification
12.2(33)SXI	Support for this command was introduced.

Examples

The following example shows how to specify the fabric channel traffic utilization monitor interval for a specific fabric channel:

```
Router(config)# monitor traffic-util fabric channel 1 interval 50
```

The following example shows how to specify the fabric channel traffic utilization monitor threshold for a specific fabric channel and for egress traffic only:

```
Router(config)# monitor traffic-util fabric channel 1 egress interval 100 threshold 80
```

Related Commands

Command	Description
monitor traffic-util backplane	Enables and configures the backplane traffic utilization monitor.
show catalyst6000 traffic-meter	Displays the percentage of the backplane (shared bus) utilization and traffic monitor status information.

monitor traffic-util fpoe

To set the fabric channel traffic utilization monitor to generate syslog messages, use the **monitor traffic-util fpoe** command in global configuration mode. To disable the fabric channel traffic utilization monitor, use the **no** form of this command.

monitor traffic-util fpoe {*fpoe-num* | **all**} {**egress** | **ingress** | **both**} [**interval** *interval* | **threshold** *percentage*]

no monitor traffic-util fpoe

Syntax Description

fpoe-num	Number of the fabric-port-of-exit (FPOE). Range: 0 to 19.
all	Specifies all FPOE numbers.
egress	Specifies egress traffic only.
ingress	Specifies ingress traffic only.
both	Specifies egress and ingress traffic.
interval *interval*	(Optional) Specifies the traffic monitor interval in seconds. Range: 1 to 255. Default: 60.
threshold *percentage*	(Optional) Specifies the percentage of fabric channel traffic utilization monitor threshold before the traffic monitor generates a syslog message. Range: 1 to 100. Default: 80.

Command Default

The fabric channel traffic utilization monitor is disabled by default. If you enable traffic monitoring, the defaults are as follows:

- **all**.
- *interval* is 60.
- *percentage* is 80.

Command Modes

Global configuration ((config)#)

Command History

Release	Modification
12.2(33)SXI	Support for this command was introduced.

Usage Guidelines

You can enter the *fpoe-num* as a list or a range. Separate each entry with a comma and each range with a hyphen (-). For example, 1,3,5-9,12.

The fabric supports a maximum of 18 fabric channels/ports. For this reason, the fabric header contains an 18-bit fabric-port-of-exit (FPOE) field only. Each of the 18 bits in the fabric header act as a port-select for a destination fabric channel in the crossbar.

Examples

The following example shows how to specify the fabric channel traffic utilization monitor interval for a specific fabric channel:

```
Router(config)# monitor traffic-util fpoe 8 interval 50
```

The following example shows how to specify the fabric channel traffic utilization monitor threshold for a specific fabric channel and for egress traffic only:

```
Router(config)# monitor traffic-util fpoe 6 egress threshold 80
```

Related Commands

Command	Description
monitor traffic-util backplane	Enables and configures the backplane traffic utilization monitor.
show catalyst6000 traffic-meter	Displays the percentage of the backplane (shared bus) utilization and traffic monitor status information.

netconf beep initiator

To configure Blocks Extensible Exchange Protocol (BEEP) as the transport protocol for Network Configuration Protocol (NETCONF) and to configure a peer as the BEEP initiator, use the **netconf beep initiator** command in global configuration mode. To disable the BEEP initiator, use the **no** form of this command.

netconf beep initiator {*hostname* | *ip-address*} *port-number* **user** *sasl-user* **password** *sasl-password* [**encrypt** *trustpoint*] [**reconnect-time** *seconds*]

no netconf beep initiator {*hostname* | *ip-address*} *port-number*

Syntax Description

hostname	Hostname of the remote device. Spaces and special characters cannot be used in hostnames. An error message is displayed if the syntax of the hostname is not appropriate.
ip-address	IP address of the remote device.
port-number	Specifies the BEEP port to use. The valid range is 1 to 65535.
user *sasl-user*	Specifies the Simple Authentication and Security Layer (SASL) user on the far end for this NETCONF session.
password *sasl-password*	Sets the password for the SASL user on the far end.
encrypt *trustpoint*	(Optional) Configures transport layer security (TLS) on this NETCONF session.
reconnect-time *seconds*	(Optional) Specifies the retry timeout, in seconds, for the NETCONF session. The range is from 3 to 3600.

Command Default

BEEP is not enabled as the transport protocol for NETCONF sessions.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(9)T	This command was introduced.
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.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

Use the **netconf beep initiator** command to specify BEEP as the transport protocol for NETCONF sessions and to specify a peer as the BEEP initiator.

BEEP is a peer-to-peer client-server protocol. Each peer is labeled in the context of the role it plays at a given time. When a BEEP session is established, the peer that awaits new connections is the BEEP listener. The other peer, which establishes a connection to the listener, is the BEEP initiator. The BEEP peer that starts an exchange is the client; similarly, the other BEEP peer is the server. Typically, a BEEP peer that acts in the server role also performs in the listening role. However, because BEEP is a peer-to-peer protocol, the BEEP peer that acts in the server role is not required to also perform in the listening role.

Use the optional **encrypt** keyword to configure BEEP to use TLS to provide simple security for NETCONF sessions.

If an invalid hostname is specified for the remote device, an error message is displayed.

Examples

The following example shows how to enable NETCONF over BEEP and to configure a BEEP peer as the BEEP initiator:

```
!
hostname myhost
ip domain-name mydomain.com

ntp server myntpserver.mydomain.com

!generate RSA key pair
crypto key generate rsa general-keys

!do this only once - 1024 bytes

!config a trust point
crypto pki trustpoint mytrustpoint
 enrollment url http://10.10.10.10
 subject-name CN=myhost.mydomain.com
 revocation-check none

!get self signed cert
 crypto pki authenticate mytrustpoint

!get own certificate
 crypto pki enroll mytrustpoint

 netconf beep initiator host1 23 user user1 password password1 encrypt mytrustpoint
reconnect-time 60
```

Related Commands

Command	Description
netconf beep listener	Configures BEEP as the transport protocol for NETCONF and configures a peer as the BEEP listener.

netconf beep listener

To configure Blocks Extensible Exchange Protocol (BEEP) as the transport protocol for Network Configuration Protocol (NETCONF) and to configure a peer as the BEEP listener, use the **netconf beep listener** command in global configuration mode. To disable the BEEP listener, use the **no** form of this command.

netconf beep listener [*port-number*] [**acl** *access-list-number*] [**sasl** *sasl-profile*] [**encrypt** *trustpoint*]

no netconf beep listener

Syntax Description

port-number	(Optional) Specifies which BEEP port on which to listen.
acl *access-list-number*	(Optional) Specifies the access control list to be applied to restrict incoming client connections.
sasl *sasl-profile*	(Optional) Configures a Simple Authentication and Security Layer (SASL) profile to use during session establishment.
encrypt *trustpoint*	(Optional) Configures transport layer security (TLS) on a NETCONF session.

Command Default

BEEP is not enabled as the transport protocol for NETCONF sessions.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(9)T	This command was introduced.
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.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS Cisco IOS XE Release 2.1.

Usage Guidelines

Use the **netconf beep listener** command to specify BEEP as the transport protocol for NETCONF sessions and to specify a peer as the BEEP listener.

BEEP is a peer-to-peer client-server protocol. Each peer is labeled in the context of the role it plays at a given time. When a BEEP session is established, the peer that awaits new connections is the BEEP listener. The other peer, which establishes a connection to the listener, is the BEEP initiator. The BEEP peer that starts an exchange is the client; similarly, the other BEEP peer is the server. Typically, a BEEP peer that acts in the server role also performs in the listening role. However, because BEEP is a peer-to-peer protocol, the BEEP peer that acts in the server role is not required to also perform in the listening role.

You must configure an SASL profile before you can configure NETCONF over BEEP to use SASL during session establishment.

Examples

The following example shows how to configure NETCONF over BEEP and to specify a peer as the BEEP listener:

```
Router(config)# sasl profile beep
 mechanism digest-md5
 server user user1 password password1
 exit
Router(config)# netconf beep listener 23 acl 1 sasl beep encrypt 25
```

Related Commands

Command	Description
netconf beep initiator	Configures BEEP as the transport protocol for NETCONF and configures a peer as the BEEP initiator.

netconf format

To associate Network Configuration Protocol (NETCONF) with an Operational Data Model (ODM) spec file for Extensible Markup Language (XML) formatted requests, use the **netconf format** command in global configuration mode. To remove the association, use the **no** form of this command.

netconf format *location*:*local-filename*

no netconf format

Syntax Description

location:*local-filename*	Command ODM file location and filename. Valid locations are **bootflash:**, **flash:**, **nvram:**, and any valid disk or slot number (such as **disk0:** or **slot1:**). ODM spec files have a .odm suffix.

Command Default

The spec file defined by the **format global** command is used.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(54)SG	This command was integrated into Cisco IOS Release 12.2(54)SG.

Usage Guidelines

Use the **netconf format** command to make an association with NETCONF to use the specified ODM spec file for all XML-formatted requests coming from NETCONF operations.

The ODM spec file must exist on the filesystem before NETCONF can be configured to use it. If the file does not exist, the **netconf format** command is rejected.

Examples

The following example shows how to associate a file named spec3.3.odm with NETCONF:

```
netconf format disk0:spec3.3.odm
```

Related Commands

Command	Description
netconf lock-time	Limits the amount of time NETCONF can lock a configuration.
netconf max-sessions	Limits the total number of NETCONF sessions.
netconf ssh	Enables NETCONF over SSHv2.

netconf lock-time

To specify the maximum time a network configuration protocol (NETCONF) configuration lock is in place without an intermediate operation, use the **netconf lock-time** command in global configuration mode. To set the NETCONF configuration lock time to the default value, use the **no** form of this command.

netconf lock-time *seconds*

no netconf lock-time

Syntax Description

seconds	Maximum NETCONF session time in seconds. The valid range is 1 to 300 seconds. The default is 10 seconds.

Command Default

The maximum lock time for a NETCONF session is 10 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.2(33)SRA	This command was introduced.
12.4(9)T	This command was integrated into Cisco IOS Release 12.4(9)T.
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

NETCONF enables you to set a configuration lock. Setting a configuration lock allows you to have exclusive rights to the configuration in order to apply configuration changes. Other users will not have access to the console during the lock time. If the user who has enabled the configuration lock is inactive, the lock timer expires and the session is ejected, preventing the configuration from being locked out if the user loses network connectivity while they have the configuration locked.

Examples

The following example shows how to limit a NETCONF configuration lock to 60 seconds:

```
Router(config)# netconf lock-time 60
```

Related Commands

Command	Description
clear netconf	Clears NETCONF statistics counters, NETCONF sessions, and frees associated resources and locks.
debug netconf	Enables debugging of NETCONF sessions.
netconf max-sessions	Specifies the maximum number of concurrent NETCONF sessions allowed.

Command	Description
netconf ssh	Enables NETCONF over SSHv2.
show netconf	Displays NETCONF statistics counters and session information.

netconf max-message

To specify the maximum size of messages received in a network configuration protocol (NETCONF) session, use the **netconf max-message** command in global configuration mode. To set an infinite message size for the messages received, use the **no** form of this command.

netconf max-message *size*

no netconf max-message

Syntax Description

size	Specifies the maximum message size, in kilobytes (kB), for the messages received. The valid range in is from 1 to 2147483.

Command Default

The maximum message size is set to infinite.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

The **netconf max-message** command specifies the maximum amount of memory required to be allocated to messages received in a NETCONF session. To protect the device against denial-of-service (DOS) attacks (that is, cases where the device runs out of memory for routing tasks) ensure the maximum size is not set to be very big. The **no netconf max-message** command sets the maximum message size to an infinite value.

Examples

The following example shows how to configure a maximum size of 37283 KB for messages received in a NETCONF session:

```
Router# configure terminal
Router(config)# netconf max-message 37283
```

Related Commands

Command	Description
netconf beep initiator	Configures BEEP as the transport protocol for NETCONF and configures a peer as the BEEP initiator.
netconf beep listener	Configures BEEP as the transport protocol for NETCONF and configures a peer as the BEEP listener.
netconf format	Associates NETCONF with an ODM spec file for XML-formatted requests.
netconf lock-time	Specifies the maximum time a NETCONF configuration lock is in place without an intermediate operation.

Command	Description
netconf max-sessions	Specifies the maximum number of concurrent NETCONF sessions allowed.
netconf ssh	Enables NETCONF over SSHv2.

netconf max-sessions

To specify the maximum number of concurrent network configuration protocol (NETCONF) sessions allowed, use the **netconf max-sessions** command in global configuration mode. To reset the number of concurrent NETCONF sessions allowed to the default value of four sessions, use the **no** form of this command.

netconf max-sessions *session*

no netconf max-sessions

Syntax Description

session	Specifies the total number of concurrent NETCONF sessions allowed. The default is 4. The range is 4 to 16.

Command Default

Four concurrent NETCONF sessions are allowed.

Command Modes

Global configuration

Command History

Release	Modification
12.2(33)SRA	This command was introduced.
12.4(9)T	This command was integrated into Cisco IOS Release 12.4(9)T.
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

You can have multiple NETCONF Network Managers concurrently connected. The **netconf max-sessions** command allows the maximum number of concurrent NETCONF sessions. The number of NETCONF sessions is also limited by the amount of available of vty line configured.

Note There must be at least as many vty lines configured as there are concurrent NETCONF sessions.

Extra NETCONF sessions beyond the maximum are not accepted.

Examples

The following example allows a maximum of five concurrent NETCONF sessions:

```
Router(config)# netconf max-sessions 5
```

Related Commands

Command	Description
clear netconf	Clears NETCONF statistics counters, NETCONF sessions, and frees associated resources and locks.
debug netconf	Enables debugging of NETCONF sessions.

Command	Description
netconf lock-time	Specifies the maximum time a NETCONF configuration lock is in place without an intermediate operation.
netconf ssh	Enables NETCONF over SSHv2.
show netconf	Displays NETCONF statistics counters and session information.

netconf ssh

To enable Network Configuration Protocol (NETCONF) over Secure Shell Version 2 (SSHv2), use the **netconf ssh** command in global configuration mode. To disable NETCONF over SSHv2, use the **no** form of this command.

netconf ssh [**acl** *access-list-number*]

no netconf ssh

Syntax Description

acl	(Optional) Specifies an access list to use during NETCONF sessions.
access-list-number	Number of the access list to use during NETCONF sessions.

Command Default

NETCONF over SSHv2 is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(33)SRA	This command was introduced.
12.4(9)T	This command was integrated into Cisco IOS Release 12.4(9)T.
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

NETCONF is supported only on SSHv2.

Examples

The following example shows how to enable NETCONF over SSHv2 and apply access list 1 to NETCONF sessions:

```
Router(config)# netconf ssh acl 1
```

Related Commands

Command	Description
clear netconf	Clears NETCONF statistics counters, NETCONF sessions, and frees associated resources and locks.
debug netconf	Enables debugging of NETCONF sessions.
netconf lock-time	Specifies the maximum time a NETCONF configuration lock is in place without an intermediate operation.
netconf max-sessions	Specifies the maximum number of concurrent NETCONF sessions allowed.
show netconf	Displays NETCONF statistics counters and session information.

no snmp-server

To disable Simple Network Management Protocol (SNMP) agent operation, use the **no snmp-server** command in global configuration mode.

no snmp-server

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

This command disables all running versions of SNMP (SNMPv1, SNMPv2C, and SNMPv3) on the device.

Examples

The following example disables the current running version of SNMP:

```
Router(config)# no snmp-server
```

ntp access-group

To control access to the Network Time Protocol (NTP) services on the system, use the **ntp access-group** command in global configuration mode. To remove access control to the NTP services, use the **no** form of this command.

ntp access-group {**peer** | **query-only** | **serve** | **serve-only**} {*access-list-number* | *access-list-number-expanded* | *access-list-name*} [**kod**]

no ntp [**access-group** {**peer** | **query-only** | **serve** | **serve-only**} {*access-list-number* | *access-list-number-expanded* | *access-list-name*}]

Syntax Description

peer	Allows time requests and NTP control queries and allows the system to synchronize to the remote system.
query-only	Allows only NTP control queries. See RFC 1305 (NTP version 3).
serve	Allows time requests and NTP control queries, but does not allow the system to synchronize to the remote system.
serve-only	Allows only time requests. **Note** You must configure the **ntp server** *ip-address* command before using the **serve-only** keyword.
access-list-number	Number (from 1 to 99) of a standard IPv4 access list.
access-list-number-expanded	Number (from 1300 to 1999) of an expanded range IPv4 access list.
access-list-name	Name of an access list.
kod	(Optional) Sends the "Kiss-o-Death" (KOD) packet to any host that tries to send a packet that is not compliant with the access-group policy.

Command Default

By default, there is no access control. Full access is granted to all systems.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
12.4(15)T	This command was modified in a release earlier than Cisco IOS Release 12.4(15)T. The *access-list-number-expanded* argument was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	This command was modified. The *access-list-name* argument and **kod** keyword were added. Support for IPv6 was added.

Release	Modification
12.2(33)SXJ	This command was modified. The *access-list-name* argument and **kod** keyword were added. Support for IPv6 was added.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S. Support for IPv6 was added.
15.1(4)M	This command was integrated into Cisco IOS Release 15.1(4)M.

Usage Guidelines

The access group options are scanned in the following order from the least restrictive to most restrictive:

1. **peer**
2. **query-only**
3. **serve**
4. **serve-only**

Access is granted for the first match that is found. If no access groups are specified, all access is granted to all sources. If you specify any access groups, only the specified access is granted. This facility provides minimal security for the time services of the system. However, it can be circumvented by a determined programmer. If tighter security is desired, use the NTP authentication facility.

The NTP service can be activated by entering any **ntp** command. When you use the **ntp access-group** command, the NTP service is activated (if it has not already been activated) and access control to NTP services is configured simultaneously.

When you enter the **no ntp access-group** command, only access control to NTP services is removed. The NTP service itself remains active, along with any other previously configured NTP functions.

To disable the NTP service on a device, use the **no ntp** command without any keywords in global configuration mode. For example, if you want to remove not only the access control to NTP services, but also all NTP functions from the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also disabled.

Examples

The following example shows how to configure a system to allow itself to be synchronized by a peer from access list 99. However, the system restricts access to allow only time requests from access list 42.

```
Router(config)# ntp access-group peer 99
Router(config)# ntp access-group serve-only 42
```

In the following IPv6 example, a KOD packet is sent to any host that tries to send a packet that is not compliant with the access-group policy:

```
Router(config)# ntp access-group serve acl1 kod
```

The following example shows how to remove all the configured NTP options and disable the NTP server:

```
Router(config)# no ntp
```

Related Commands

Command	Description
access-list	Configures the access list mechanism for filtering frames by protocol type or vendor code.
ntp server	Allows the software clock to be synchronized by a time server.

ntp allow mode private

Note Effective with Cisco IOS Release 12.2(33)SXJ, the **ntp allow mode private** command is not available in Cisco IOS software.

To allow the processing of private mode Network Time Protocol (NTP) packets, use the **ntp allow mode private** command in global configuration mode. To disable the processing of private mode NTP packets, use the **no** form of this command.

ntp allow mode private

no ntp allow mode private

Syntax Description

This command has no arguments or keywords.

Command Default

By default, the private mode NTP packets are not processed.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SXH7	This command was introduced.
12.2(33)SXJ	This command was removed.

Usage Guidelines

The private mode NTP packets will be blocked if this command is not enabled. If you are using NTP version 4 (NTPv4), you need not configure this command. NTP private mode packet processing is enabled by default in NTPv4.

Examples

The following example shows how to enable the processing of private mode NTP packets:

```
Router(config)# ntp allow mode private
```

Related Commands

Command	Description
ntp	Activates the NTP service.

ntp authenticate

To enable Network Time Protocol (NTP) authentication, use the **ntp authenticate** command in global configuration mode. To disable the function, use the **no** form of this command.

ntp authenticate

no ntp [**authenticate**]

Syntax Description

This command has no arguments or keywords.

Command Default

By default, NTP authentication is not enabled.

Command Modes

Global configuration (config)

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	This command was modified. Support for NTPv4 and IPv6 was added.
12.2(33)SXJ	This command was modified. Support for NTPv4 and IPv6 was added.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S. Support for IPv6 was added.
15.1(4)M	This command was integrated into Cisco IOS Release 15.1(4)M.

Usage Guidelines

Use this command if you want to authenticate NTP. If this command is specified, the system will not synchronize to another system unless it carries one of the authentication keys specified in the **ntp trusted-key** global configuration command.

The NTP service can be activated by entering any **ntp** command. When you use the **ntp authenticate** command, the NTP service is activated (if it has not already been activated) and NTP authentication is enabled simultaneously.

In the **no** form of any **ntp** command, all the keywords are optional. When you enter the **no ntp authenticate** command, only the NTP authentication is removed from the NTP service. The NTP service itself remains active, along with any other functions you that previously configured.

To disable the NTP service on a device, you must enter the **no ntp** command without any keywords in global configuration mode. For example, if you previously issued the **ntp authenticate** command and you now want to disable not only the authentication, but also all NTP functions from the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also disabled.

Examples

The following example shows how to configure the system to synchronize only to systems that provide the authentication key 42 in their NTP packets:

```
Router(config)# ntp authenticate
Router(config)# ntp authentication-key 42 md5 aNiceKey
Router(config)# ntp trusted-key 42
```

The following example shows how to remove all the configured NTP options and disable the NTP server:

```
Router(config)# no ntp
```

Related Commands

Command	Description
ntp authentication-key	Defines an authentication key for NTP.
ntp trusted-key	Authenticates the identity of a system to which NTP will synchronize.

ntp authentication-key

To define an authentication key for Network Time Protocol (NTP), use the **ntp authentication-key** command in global configuration mode. To remove the authentication key for NTP, use the **no** form of this command.

ntp authentication-key *number* **md5** *key* [*encryption-type*]

no ntp [**authentication-key** *number*]

Syntax Description

number	Key number from 1 to 4294967295.
md5	Specifies the authentication key. Message authentication support is provided using the message digest 5 (MD5) algorithm. The key type **md5** is the only key type supported.
key	Character string of up to 32 characters that is the value of the MD5 key. **Note** In auto secure mode, an error is displayed on the console and the authentication key is not configured if the character string length exceeds 32.
encryption-type	(Optional) Authentication key encryption type. Range: 0 to 4294967295.

Command Default

No authentication key is defined for NTP.

Command Modes

Global configuration (config)

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	This command was modified. Support for NTPv4 and IPv6 was added.
12.2(33)SXJ	This command was modified. Support for NTPv4 and IPv6 was added.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S. Support for IPv6 was added.
15.1(4)M	This command was integrated into Cisco IOS Release 15.1(4)M.

Usage Guidelines

Use this command to define authentication keys for use with other NTP commands in order to provide a higher degree of security.

Note When this command is written to NVRAM, the key is encrypted so that it is not displayed in the configuration.

When you configure the authentication key using the **ntp authentication-key** command or using the **auto secure ntp** command, if the length of the MD5 key exceeds 32 characters, an error message is displayed.

The NTP service can be activated by entering any **ntp** command. When you use the **ntp authentication-key** command, the NTP service is activated (if it has not already been activated) and the NTP authentication key is defined simultaneously.

When you enter the **no ntp authentication-key** command, only the NTP authentication key is removed from the NTP service. The NTP service itself remains active, along with any other previously configured NTP functions.

Note If a specific authentication key configuration is removed, the NTP process is not stopped until all the authentication key configurations are removed.

To disable the NTP service on a device, use the **no ntp** command without any keywords in global configuration mode. For example, if you want to remove not only the access control to NTP services, but also all NTP functions from the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also disabled.

Examples

The following example shows how to configure the system to synchronize only to systems providing the authentication key 42 in their NTP packets:

```
Router(config)# ntp authenticate
Router(config)# ntp authentication-key 42 md5 aNiceKey
Router(config)# ntp trusted-key 42
```

The following example shows how to remove all the configured NTP options and disable the NTP server:

```
Router(config)# no ntp
```

The following example shows the error message displayed when the authentication key character string length exceeds 32:

```
Router(config)# ntp authentication-key 23 md5 11111111111111111111111111111111
%NTP: Key too long
```

Related Commands

Command	Description
auto secure	Secures the management and forwarding planes of the router.
ntp authenticate	Enables NTP authentication.
ntp peer	Configures the software clock to synchronize a peer or to be synchronized by a peer.
ntp server	Allows the software clock to be synchronized by a time server.
ntp trusted-key	Authenticates the identity of a system to which NTP will synchronize.

ntp broadcast

To configure the options for broadcasting Network Time Protocol (NTP) traffic, use the **ntp broadcast** command in interface configuration mode. To disable this capability, use the **no** form of this command.

ntp broadcast [**client** | [**destination** {*ip-address* | *hostname*}] [**key** [*broadcast-key*]] [**version** *number*]]

no ntp [**broadcast** [**client** | [**destination** {*ip-address* | *hostname*}] [**key** [*broadcast-key*]] [**version** *number*]]]

Syntax Description

client	(Optional) Configures a device to listen to NTP broadcast messages.
destination	(Optional) Configures a device to receive broadcast messages.
ip-address | *hostname*	(Optional) IP address or hostname of the device to send NTP broadcast messages to.
key	(Optional) Configures a broadcast authentication key.
broadcast-key	(Optional) Integer from 1 to 4294967295 that is the key number. In the Cisco IOS Release 12.2SX train, the range is from 0 to 4294967295.
version	(Optional) Indicates that an NTP version is configured.
number	(Optional) Integer from 2 to 4 indicating the NTP version. In the Cisco IOS Release 12.2SX train, the range is from 1 to 4.

Defaults

NTP broadcasting is disabled.

Command Modes

Interface configuration (config-if)

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(20T	This command was modified. Support for NTPv4 and IPv6 was added.
12.2(33)SXJ	This command was modified. Support for NTPv4 and IPv6 was added.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S. Support for IPv6 was added.
15.1(4)M	This command was integrated into Cisco IOS Release 15.1(4)M.

Usage Guidelines

The NTP service can be activated by entering any **ntp** command. When you use the **ntp broadcast** command, the NTP service is activated (if it has not already been activated) and the options are configured for sending NTP traffic simultaneously.

In the **no** form of any **ntp** command, all the keywords are optional. When you enter the **no ntp broadcast** command, only the configuration to send NTP broadcast packets on a specified interface is removed from the NTP service. The NTP service itself remains active, along with any other functions that you previously configured.

To disable the NTP service on a device, you must enter the **no ntp** command without keywords. For example, if you previously issued the **ntp broadcast** command and you now want to remove not only the broadcast capability, but also all NTP functions from the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also disabled.

Examples

The following example shows how to configures Ethernet interface 0 to send NTP version 2 broadcasts:

```
Router(config)# interface ethernet 0
Router(config-if)# ntp broadcast version 2
```

The following example shows how to remove all the configured NTP options and disable the NTP server:

```
Router(config)# no ntp
```

Related Commands

Command	Description
ntp broadcast client	Allows the system to receive NTP broadcast packets on an interface.
ntp broadcastdelay	Sets the estimated round-trip delay between the Cisco IOS software and an NTP broadcast server.

ntp broadcast client

To configure a device to receive Network Time Protocol (NTP) broadcast messages on a specified interface, use the **ntp broadcast client** command in interface configuration mode. To disable this capability, use the **no** form of this command.

ntp broadcast client [**novolley**]

no ntp [**broadcast** [**client**]]

Syntax Description

novolley	(Optional) Disables any messages sent to the broadcast server. Avoids the propagation delay measurement phase and directly uses a preconfigured value instead when used in conjunction with the **ntp broadcastdelay** command. **Note** Public key authentication does not work without the volley.

Command Default

By default, an interface is not configured to receive NTP broadcast messages.

Command Modes

Interface configuration (config-if)

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	This command was modified. Support for NTPv4 and IPv6 was added. The **novolley** keyword was added.
12.2(33)SXJ	This command was modified. Support for NTPv4 and IPv6 was added.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S. Support for IPv6 was added.
15.1(4)M	This command was integrated into Cisco IOS Release 15.1(4)M.

Usage Guidelines

Use this command to allow the system to listen to broadcast packets on an interface-by-interface basis.

The NTP service can be activated by entering any **ntp** command. When you use the **ntp broadcast client** command, the NTP service is activated (if it has not already been activated) and the device is configured to receive NTP broadcast packets on a specified interface simultaneously.

In the **no** form of any **ntp** command, all the keywords are optional. When you enter the **no ntp broadcast client** command, only the broadcast client configuration is removed from the NTP service. The NTP service itself remains active, along with any other functions that you previously configured.

To disable the NTP service on a device, you must enter the **no ntp** command without any keywords. For example, if you previously issued the **ntp broadcast client** command and you now want to remove not only the broadcast client capability, but also all NTP functions from the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also disabled.

In IPv6 configuration, the **ntp broadcastdelay** command is used when the **ntp broadcast client** or **ntp multicast client** command is configured with the **novolley** keyword.

Examples

In the following example, the system is configured to receive (listen to) NTP broadcasts on Ethernet interface 1:

```
Router(config)# interface ethernet 1
Router(config-if)# ntp broadcast client
```

The following example shows how to remove all the configured NTP options and disable the NTP server:

```
Router(config)# no ntp
```

Related Commands

Command	Description
ntp broadcastdelay	Sets the estimated round-trip delay between the system and an NTP broadcast server.
ntp multicast client	Configures the system to receive NTP multicast packets on a specified interface.

ntp broadcastdelay

To set the estimated round-trip delay between the Cisco IOS software and a Network Time Protocol (NTP) broadcast server, use the **ntp broadcastdelay** command in global configuration mode. To revert to the default value, use the **no** form of this command.

ntp broadcastdelay *microseconds*

no ntp [**broadcastdelay**]

Syntax Description

microseconds	Estimated round-trip time (in microseconds) for NTP broadcasts. The range is from 1 to 999999.

Command Default

By default, the round-trip delay between the Cisco IOS software and an NTP broadcast server is 3000 microseconds.

Command Modes

Global configuration (config)

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	This command was modified. Support for NTPv4 and IPv6 was added.
12.2(33)SXJ	This command was modified. Support for NTPv4 and IPv6 was added.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S. Support for IPv6 was added.
15.1(4)M	This command was integrated into Cisco IOS Release 15.1(4)M.

Usage Guidelines

Use the **ntp broadcastdelay** command when the router is configured as a broadcast client and the round-trip delay on the network is other than 3000 microseconds. In IPv6, the value set by this command should be used only when the **ntp broadcast client** and **ntp multicast client** commands have the **novolley** keyword enabled.

The NTP service can be activated by entering any **ntp** command. When you use the **ntp broadcastdelay** command, the NTP service is activated (if it has not already been activated) and the estimated round-trip delay between the Cisco IOS software and an NTP broadcast server is set simultaneously.

In the **no** form of any **ntp** command, all the keywords are optional. When you enter the **no ntp broadcastdelay** command, only the estimated round-trip delay between the Cisco IOS software and an NTP broadcast server is removed from the NTP service. The NTP service itself remains active, along with any other functions you previously configured.

To disable the NTP service on a device, you must enter the **no ntp** command without any keywords in global configuration mode. For example, if you previously issued the **ntp broadcastdelay** command and you now want to remove not only the delay setting, but also all NTP functions from the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also disabled.

Examples

The following example shows how to set the estimated round-trip delay between a router and the broadcast client to 5000 microseconds:

```
Router(config)# ntp broadcastdelay 5000
```

The following example shows how to remove all the configured NTP options and disable the NTP server:

```
Router(config)# no ntp
```

Related Commands

Command	Description
ntp broadcast client	Configures the specified interface to receive NTP broadcast packets.
ntp multicast client	Configures the system to receive NTP multicast packets on a specified interface.

ntp clear drift

To reset the drift value stored in the persistent data file, use the **ntp clear drift** command in privileged EXEC mode.

ntp clear drift

Syntax Description

This command has no arguments or keywords.

Command Default

The drift value stored in the persistent data file is not reset.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SXJ	This command was integrated into Cisco IOS Release 12.2(33)SXJ.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.
15.1(4)M	This command was integrated into Cisco IOS Release 15.1(4)M.

Usage Guidelines

The **ntp clear drift** command is used to reset the local clock drift value in the persistent data file. The drift is the frequency offset between the local clock hardware and the authoritative time from the Network Time Protocol version 4 (NTPv4) servers. NTPv4 automatically computes this drift and uses it to compensate permanently for local clock imperfections.

This command is available only when the NTP service is activated using any **ntp** command in global configuration mode.

Examples

The following example shows how to reset the drift value in the persistent data file:

```
Router# ntp clear drift
```

Related Commands

Command	Description
ntp	Activates the NTP service.

ntp clock-period

Caution Do not use this command; it is documented for informational purposes only. The system automatically generates this command as Network Time Protocol (NTP) determines the clock error and compensates.

Note Effective with Cisco IOS Release 15.0(1)M, the **ntp clock-period** command is not available in Cisco IOS software.

As NTP compensates for the error in the software clock, it keeps track of the correction factor for this error. When the value for the clock period needs to be adjusted, the system automatically enters the correct value into the running configuration. To remove the automatically generated value for the clock period, use the **no** form of this command.

ntp clock-period *value*

no ntp [**clock-period**]

Syntax Description

value	Amount of time to add to the software clock for each clock hardware tick (this value is multiplied by 2^{-32}). The default value is 17179869 2^{-32} seconds (4 milliseconds).

Defaults

The clock period value is automatically generated.

Command Modes

Global configuration (config)

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.
15.0(1)M	This command was removed.

Usage Guidelines

Do not manually set a value for the NTP clock period.

If the system has automatically entered a value for the clock period into the running configuration, NTP synchronizes faster after the system is restarted when the **copy running-config startup-config** command has been entered to save the configuration to NVRAM.

The NTP service can be activated by entering any **ntp** command. In the **no** form of any **ntp** command, all the keywords are optional. When you enter the **no ntp clock-period** command, only the automatically generated value is removed. You should remove this command line when copying configuration files to other devices.The NTP service itself remains active, along with any other functions you previously configured.

To disable the NTP service on a device, you must enter the **no ntp** command without keywords in global configuration mode. For example, if you want to remove not only the clock period, but all NTP functions from the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also disabled.

Examples

If the system has automatically entered a value for the clock period into the running configuration, NTP synchronizes faster after the system is restarted when the **copy running-config startup-config** command has been entered to save the configuration to NVRAM. The following example shows a typical difference between the values of the NTP clock-period setting in the running configuration and in the startup configuration:

```
Router# show startup-config | include clock-period

ntp clock-period 17180239

Router# show running-config | include clock-period

ntp clock-period 17180255
```

The following example shows how to remove the automatically generated value for the clock period from the running configuration:

```
Router(config)# no ntp clock-period
```

The following example shows how to remove all the configured NTP options and disable the NTP server:

```
Router(config)# no ntp
```

ntp disable

To prevent an interface from receiving Network Time Protocol (NTP) packets, use the **ntp disable** command in interface configuration mode. To enable the receipt of NTP packets on an interface, use the **no** form of this command.

ntp disable [**ip** | **ipv6**]

no ntp disable [**ip** | **ipv6**]

Syntax Description

ip	(Optional) Disables IP-based NTP traffic.
ipv6	(Optional) Disables IPv6-based NTP traffic.

Command Default

By default, interfaces receive NTP packets.

Command Modes

Interface configuration (config-if)

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	This command was modified. Support for IPv6 was added. The optional **ip** and **ipv6** keywords were added.
12.2(33)SXJ	This command was modified. Support for IPv6 was added. The optional **ip** and **ipv6** keywords were added.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S. Support for IPv6 was added.
15.1(4)M	This command was integrated into Cisco IOS Release 15.1(4)M.

Usage Guidelines

This command provides a simple method of access control.

Use the **ntp disable** command in interface configuration mode to configure an interface to reject NTP packets. If the **ntp disable** command is configured on an interface that does not have any NTP service running, the interface remains disabled even after the NTP service is started by another NTP configuration. When you use the **ntp disable** command without the **ip** or **ipv6** keyword, NTP is disabled on the interface for all the address families.

When you enter the **no ntp disable** command in interface configuration mode, the interface that was configured to reject NTP packets is enabled to receive NTP packets.

Note Remove all NTP commands from an interface before entering the **ntp disable** command on that interface.

Configuring the **ntp disable** command on an interface does not stop the NTP service. To disable the NTP service on a device, use the **no ntp** command without keywords in global configuration mode. For example, if you had previously issued the **ntp disable** command and you now want to remove not only this restriction, but also all NTP functions from the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also disabled.

Examples

The following example shows how to prevent Ethernet interface 0 from receiving NTP packets:

```
Router(config)# interface ethernet 0
Router(config-if)# ntp disable
```

The following example shows the message displayed when you try to execute the **ntp disable** command on an interface that has other NTP commands configured on it:

```
Router(config-if)# ntp disable

%NTP: Unconfigure other NTP commands on this interface before executing 'ntp disable'
```

If you had previously issued the **ntp disable** command and you now want to remove not only this restriction, but also all NTP functions from the device, use the **no ntp** command without keywords in global configuration mode. The following example shows how to disable the NTP service on a device:

```
Router(config)# no ntp
```

Related Commands

Command	Description
ntp	Activates the NTP service.

ntp logging

To enable Network Time Protocol (NTP) message logging, use the **ntp logging** command in global configuration mode. To disable NTP logging, use the **no** form of this command.

ntp logging

no ntp [**logging**]

Syntax Description

This command has no arguments or keywords.

Command Default

NTP message logging is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(7)T	This command was introduced.
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	This command was modified. Support for IPv6 was added.
12.2(33)SXJ	This command was modified. Support for IPv6 was added.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S. Support for IPv6 was added.
15.1(4)M	This command was integrated into Cisco IOS Release 15.1(4)M.

Usage Guidelines

Use the **ntp logging** command to control the display of NTP logging messages.

The NTP service can be activated by entering any **ntp** command. When you use the **ntp logging** command, the NTP service is activated (if it has not already been activated) and message logging is enabled simultaneously.

In the **no** form of any **ntp** command, all the keywords are optional. When you enter the **no ntp logging** command, only message logging is disabled in the NTP service. The NTP service itself remains active, along with any other functions that you previously configured.

To disable the NTP service on a device, you must enter the **no ntp** command without keywords. For example, if you previously issued the **ntp logging** command and you now want to disable not only the message logging, but also all NTP functions from the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also disabled.

Examples

The following example shows how to enable NTP message logging and verify that it is enabled:

```
Router# configure terminal
```

```
Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)# ntp logging
Router(config)# end

Router# show running-config | include ntp
ntp logging
ntp clock-period 17180152
ntp peer 10.0.0.1
ntp server 192.168.166.3
```

The following example shows how to disable NTP message logging and verify to that it is disabled:

```
Router# configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)# no ntp logging
Router# end
Router(config)# show running-config | include ntp

ntp clock-period 17180152
ntp peer 10.0.0.1
ntp server 192.168.166.3
```

The following example shows how to remove all the configured NTP options and disable the NTP server:

```
Router(config)# no ntp
```

Related Commands

Command	Description
ntp peer	Configures the software clock to synchronize a peer or to be synchronized by a peer.
ntp server	Allows the software clock to be synchronized by an NTP time server.

ntp master

To configure the Cisco IOS software as a Network Time Protocol (NTP) master clock to which peers synchronize themselves when an external NTP source is not available, use the **ntp master** command in global configuration mode. To disable the master clock function, use the **no** form of this command.

ntp master [*stratum*]

no ntp [**master**]

Caution Use this command with caution. Valid time sources can be easily overridden using this command, especially if a low stratum number is configured. Configuring multiple devices in the same network with the **ntp master** command can cause instability in keeping time if the devices do not agree on the time.

Syntax Description

stratum	(Optional) Number from 1 to 15. Indicates the NTP stratum number that the system will claim.

Command Default

By default, the master clock function is disabled. When enabled, the default stratum is 8.

Command Modes

Global configuration (config)

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	This command was modified. Support for IPv6 was added.
12.2(33)SXJ	This command was modified. Support for IPv6 was added.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S. Support for IPv6 was added.
15.1(4)M	This command was integrated into Cisco IOS Release 15.1(4)M.

Usage Guidelines

Because the Cisco implementation of NTP does not support directly attached radio or atomic clocks, the router is normally synchronized, directly or indirectly, to an external system that has such a clock. In a network without Internet connectivity, such a time source may not be available. The **ntp master** command is used in such cases.

A system with the **ntp master** command configured that cannot reach any clock with a lower stratum number will claim to be synchronized at the configured stratum number, and other systems will be willing to synchronize to it via NTP.

Note The software clock must have been set from some source, including manual setting, before the **ntp master** command will have any effect. This protects against distributing erroneous time after the system is restarted.

The NTP service can be activated by entering any **ntp** command. When you use the **ntp master** command, the NTP service is activated (if it has not already been activated) and the Cisco IOS software is configured as an NTP master clock simultaneously. When you enter the **no ntp master** command, only the NTP master clock configuration is removed from the NTP service. The NTP service itself remains active, along with any other functions that you previously configured.

To disable the NTP service on a device, you must enter the **no ntp** command without any keywords in global configuration mode. For example, if you had previously issued the **ntp master** command and you now want to remove not only the master clock function, but also all NTP functions from the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also disabled.

Examples

The following example shows how to configure a router as an NTP master clock to which peers may synchronize:

```
Router(config)# ntp master 10
```

The following example shows how to remove all the configured NTP options and disable the NTP server:

```
Router(config)# no ntp
```

Related Commands

Command	Description
clock calendar-valid	Configures the system hardware clock that is an authoritative time source for the network.

ntp max-associations

To configure the maximum number of Network Time Protocol (NTP) peers and clients for a routing device, use the **ntp max-associations** command in global configuration mode. To return the maximum associations value to the default, use the **no** form of this command.

ntp max-associations *number*

no ntp [**max-associations**]

Syntax Description

number	Number of NTP associations. The range is from 1 to 4294967295. The default is 100. In the Cisco IOS Release 12.2SX train, the range is from 0 to 4294967295.

Command Default

The maximum association value of NTP peers and clients is 100.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0	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	This command was modified. Support for IPv6 was added.
12.2(33)SXJ	This command was modified. Support for IPv6 was added.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S. Support for IPv6 was added.
15.1(4)M	This command was integrated into Cisco IOS Release 15.1(4)M.

Usage Guidelines

The router can be configured to define the maximum number of NTP peer and client associations that the router will serve. Use the **ntp max-associations** command to set the maximum number of NTP peer and client associations that the router will serve.

The **ntp max-associations** command is useful for ensuring that the router is not overwhelmed by NTP synchronization requests. For an NTP master server, this command is useful for allowing numerous devices to synchronize to a router.

The NTP service can be activated by entering any **ntp** command. When you use the **ntp max-associations** command, the NTP service is activated (if it has not already been activated) and the maximum number of NTP peers and clients is configured simultaneously.

In the **no** form of any **ntp** command, all the keywords are optional. When you enter the **no ntp max-associations** command, only the maximum number value is removed from the NTP service. The NTP service itself remains active, along with any other functions that you previously configured.

To disable the NTP service on a device, you must enter the **no ntp** command without any keywords in global configuration mode. For example, if you previously issued the **ntp max-associations** command and you now want to remove not only that maximum value, but also all NTP functions from the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also disabled.

Note By default, the previous configuration values are retained when the last valid configuration (configuration for which the NTP service needs to run) is removed. Only the configuration values related to the maximum number of NTP peer and client associations are reset to the default value when the NTP process is disabled.

Examples

In the following example, the router is configured to act as an NTP server to 200 clients:

```
Router(config)# ntp max-associations 200
```

The following example shows how to remove all the configured NTP options and disable the NTP server:

```
Router(config)# no ntp
```

Related Commands

Command	Description
show ntp associations	Displays all current NTP associations for the device.

ntp maxdistance

To configure a maximum distance (maxdistance) threshold value to govern the number of packets required for synchronization for Network Time Protocol version 4 (NTPv4), use the **ntp maxdistance** command in global configuration mode. To set the maxdistance threshold to the default value, use the **no** form of this command.

ntp maxdistance *threshold-value*

no ntp [**maxdistance**]

Syntax Description

threshold-value	Maxdistance threshold value. Range: 1 to 16. Default: 1.

Command Default

By default, a maxdistance threshold of 1 is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SXJ	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S. Support for IPv6 was added.
15.1(4)M	This command was integrated into Cisco IOS Release 15.1(4)M.

Usage Guidelines

Use the **ntp maxdistance** command to configure the maxdistance threshold for NTPv4. The maxdistance is a selection threshold that is configured for determining the number of packets required for synchronization.

The number of packets is determined by the synchronization distance for each association and a limit called the distance threshold. The synchronization distance starts at 16, then drops by a factor of about 2 when each packet is received. The default distance threshold is 1. Use the **ntp maxdistance** command to change the number of packets required.

When you enter the **no ntp maxdistance** command, only the NTP maxdistance configuration is removed from the NTP service. The NTP service itself remains active, along with any other previously configured NTP functions.

To disable the NTP service on a device, use the **no ntp** command without keywords in global configuration mode. For example, if you had previously issued the **ntp maxdistance** command and you now want to remove not only this restriction, but also all NTP functions from the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also disabled.

Examples

The following example shows how to set the maxdistance threshold value to 10:

```
Router(config)# ntp maxdistance 10
```

The following example shows the default setting of the maxdistance threshold:

```
Router# show running-config | include ntp

ntp max-associations 100
ntp maxdistance 1
Router#
```

Related Commands

Command	Description
ntp	Activates the NTP service.

ntp multicast

To configure a system to send Network Time Protocol (NTP) multicast packets on a specified interface, use the **ntp multicast** command in interface configuration mode. To disable this capability, use the **no** form of this command.

ntp multicast [*ip-address* | *ipv6-address*] [**key** *key-id*] [**ttl** *value*] [**version** *number*]

no ntp [**multicast** [*ip-address* | *ipv6-address*] [**key** *key-id*] [**ttl** *value*] [**version** *number*]]

Syntax Description

ip-address	(Optional) IPv4 address of the multicast group. Default address is 224.0.1.1.
ipv6-address	(Optional) IPv6 address of the multicast group. The address can be the all-nodes IPv6 address (FF02::1) or any other IPv6 multicast address.
key	(Optional) Defines a multicast authentication key.
key-id	(Optional) Authentication key number in the range from 1 to 4294967295. In the Cisco IOS Release 12.2SX train, the range is from 0 to 4294967295.
ttl	(Optional) Defines the time-to-live (TTL) value of a multicast NTP packet.
value	(Optional) TTL value in the range from 1 to 255. Default TTL value is 16.
version	(Optional) Defines the NTP version number.
number	(Optional) NTP version number in the range from 2 to 4. Default version number for IPv4 is 3, and default number for IPv6 is 4. In the Cisco IOS Release 12.2SX train, the range is from 1 to 4.

Command Default

NTP multicast capability is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	This command was modified. Support for NTPv4 and IPv6 was added. The *ipv6-address* argument was added.
12.2(33)SXJ	This command was modified. Support for NTPv4 and IPv6 was added. The *ipv6-address* argument was added.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S. Support for IPv6 was added.
15.1(4)M	This command was integrated into Cisco IOS Release 15.1(4)M.

Usage Guidelines

The TTL value is used to limit the scope of an audience for multicast routing.

The NTP service can be activated by entering any **ntp** command. When you use the **ntp multicast** command, the NTP service is activated (if it has not already been activated) and the interface on which to send multicast packets is configured simultaneously.

In the **no** form of any **ntp** command, all the keywords are optional. When you enter the **no ntp multicast** command, only the multicast capability is removed from the NTP service. The NTP service itself remains active, along with any other functions that you previously configured.

To disable the NTP service on a device, you must enter the **no ntp** command in global configuration mode without keywords. For example, if you had previously issued the **ntp multicast** command and you now want to remove not only the multicast capability, but also all NTP functions from the device, use the **no ntp** command in global configuration mode without any keywords. This ensures that all NTP functions are removed and that the NTP service is also disabled.

Examples

The following example shows how to configure Ethernet interface 0 to send NTP version 2 broadcasts:

```
Router(config)# interface ethernet 0
Router(config-if)# ntp multicast version 2
```

If you had previously issued the **ntp multicast** command and you now want to remove not only the multicast capability, but also all NTP functions from the device, use the **no ntp** command in global configuration mode without any keywords. The following example shows how to remove the **ntp multicast** command along with all the other configured NTP options and to disable the NTP server:

```
Router(config)# no ntp
```

Related Commands

Command	Description
ntp authentication-key	Defines an authentication key for NTP.
ntp multicast client	Allows the system to receive NTP multicast packets on an interface.

ntp multicast client

To configure the system to receive Network Time Protocol (NTP) multicast packets on a specified interface, use the **ntp multicast client** command in interface configuration mode. To disable this capability, use the **no** form of this command.

ntp multicast client [*ip-address* | *ipv6-address*] [**novolley**]

no ntp [**multicast client** [*ip-address* | *ipv6-address*]]

Syntax Description

ip-address	(Optional) IPv4 address of the multicast group. Default address is 224.0.1.1.
ipv6-address	(Optional) IPv6 address of the multicast group. The address can be the all-nodes IPv6 address (FF02::1) or any other IPv6 multicast address.
novolley	(Optional) Disables any messages sent to the broadcast server. Avoids propagation delay by using the value configured by the **ntp broadcastdelay** command.

Command Default

NTP multicast client capability is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	This command was modified. Support for IPv6 was added. The *ipv6-address* argument and **novolley** keyword were added.
12.2(33)SXJ	This command was modified. Support for IPv6 was added. The *ipv6-address* argument and **novolley** keyword were added.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S. Support for IPv6 was added.
15.1(4)M	This command was integrated into Cisco IOS Release 15.1(4)M.

Usage Guidelines

Use the **ntp multicast client** command to allow the system to listen to multicast packets on an interface-by-interface basis.

This command enables the multicast client mode on the local NTP host. In this mode, the host is ready to receive mode 5 (broadcast) NTP messages sent to the specified multicast address. After receiving the first packet, the client measures the nominal propagation delay using a brief client/server association with the server. After this initial phase, the client enters the broadcast client mode, in which it synchronizes its clock to the received multicast messages.

The NTP service can be activated by entering any **ntp** command. When you use the **ntp multicast client** command, the NTP service is activated (if it has not already been activated) and the interface on which to receive multicast packets is configured simultaneously.

In the **no** form of any **ntp** command, all the keywords are optional. When you enter the **no ntp multicast client** command, only the multicast client capability is removed from the NTP service. The NTP service itself remains active, along with any other functions that you previously configured.

To disable the NTP service on a device, you must enter the **no ntp** command without any keywords in global configuration mode. For example, if you had previously issued the **ntp multicast client** command and you now want to remove not only the multicast client capability, but also all NTP functions from the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also disabled.

In IPv6 configuration, the **ntp broadcastdelay** command is used when the **ntp broadcast client** or **ntp multicast client** command is configured with the **novolley** keyword.

Examples

In the following example, the system is configured to receive (listen to) NTP multicast packets on Ethernet interface 1:

```
Router(config)# interface ethernet 1
Router(config-if)# ntp multicast client
```

If you had previously issued the **ntp multicast client** command and you now want to remove not only the multicast client capability, but also all NTP functions from the device, use the **no ntp** command without any keywords. The following example shows how to remove the **ntp multicast client** command along with all the other configured NTP options and to disable the NTP server:

```
Router(config)# no ntp
```

Related Commands

Command	Description
ntp broadcast client	Configures the specified interface to receive NTP broadcast packets.
ntp broadcastdelay	Sets the estimated round-trip delay between the Cisco IOS software and an NTP broadcast server.

ntp panic update

To configure Network Time Protocol (NTP) to reject time updates greater than the panic threshold of 1000 seconds, use the **ntp panic update** command in global configuration mode. To disable the configuration, use the **no** form of this command.

ntp panic update

no ntp panic update

Syntax Description

This command has no arguments or keywords.

Command Default

NTP is not configured to reject time updates greater than the panic threshold value.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(1)T3	This command was introduced.

Usage Guidelines

If the **ntp panic update** command is configured and the received time updates are greater than the panic threshold of 1000 seconds, the time update is ignored and the following console message is displayed:

```
NTP Core (ERROR): time correction of -22842. seconds exceeds sanity limit 1000. seconds;
set clock manually to the correct UTC time.
```

Examples

The following example shows how to configure NTP to reject time updates greater than the panic threshold:

```
Router(config)# ntp panic update
```

Related Commands

Command	Description
ntp	Activates the NTP service.

ntp passive

To configure passive Network Time Protocol (NTP) associations, use the **ntp passive** command in global configuration mode. To disable the passive NTP associations, use the **no** form of this command.

ntp passive

no ntp [**passive**]

Syntax Description

This command has no arguments or keywords.

Command Default

By default, passive NTP associations are not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SXJ	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S. Support for IPv6 was added.
15.1(4)M	This command was integrated into Cisco IOS Release 15.1(4)M.

Usage Guidelines

Use the **ntp passive** command to configure passive NTP associations. By default, passive NTP associations are accepted only when configured using the **ntp passive** command. Use the **no ntp passive** command to change the configuration to the default, that is, not to accept passive associations.

The NTP service can be activated by entering any **ntp** command. When you use the **ntp passive** command, the NTP service is activated (if it has not already been activated) and the passive NTP associations are configured simultaneously.

When you enter the **no ntp passive** command, only the passive NTP association configuration is removed from the NTP service. The NTP service itself remains active, along with any other previously configured NTP functions.

To disable the NTP service on a device, use the **no ntp** command without keywords in global configuration mode. For example, if you had previously issued the **ntp passive** command and you now want to remove not only this restriction, but also all NTP functions from the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also disabled.

Examples

The following example shows how to configure passive NTP associations:

```
Router> enable
Router# configure terminal
Router(config)# ntp passive
```

The following example shows how to remove all the configured NTP options and disable the NTP server:

```
Router(config)# no ntp
```

Related Commands

Command	Description
ntp	Activates the NTP service.

ntp peer

To configure the software clock to synchronize an NTP peer or to be synchronized by an NTP peer, use the **ntp peer** command in global configuration mode. To disable this capability, use the **no** form of this command.

ntp peer [**vrf** *vrf-name*] {*ip-address* | *ipv6-address* | [**ip** | **ipv6**] *hostname*} [**normal-sync**] [**version** *number*] [**key** *key-id*] [**source** *interface-type interface-number*] [**prefer**] [**maxpoll** *number*] [**minpoll** *number*] [**burst**] [**iburst**]

no ntp [**vrf** *vrf-name*] {*ip-address* | *ipv6-address* | [**ip** | **ipv6**] *hostname*}

Syntax Description

vrf *vrf-name*	(Optional) Specifies that the peer should use a named VPN routing and forwarding (VRF) instance for routing to the destination instead of to the global routing table.
ip-address	IPv4 address of the peer providing or being provided the clock synchronization.
ipv6-address	IPv6 address of the peer providing or being provided the clock synchronization.
ip	(Optional) Forces Domain Name System (DNS) resolution to be performed in the IPv4 address space.
ipv6	(Optional) Forces DNS resolution to be performed in the IPv6 address space.
hostname	Hostname of the peer that is providing or being provided the clock synchronization.
normal-sync	(Optional) Disables the rapid synchronization at startup.
version	(Optional) Defines the Network Time Protocol (NTP) version number.
number	(Optional) NTP version number (2 to 4). In the Cisco IOS Release 12.2(33)SX train, the range is from 1 to 4.
key	(Optional) Defines the authentication key.
key-id	(Optional) Authentication key to use when sending packets to this peer.
source	(Optional) Specifies that the source address must be taken from the specified interface.
interface-type	(Optional) Name of the interface from which to pick the IPv4 or IPv6 source address. For more information, use the question mark (?) online help function.
interface-number	(Optional) Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.
prefer	(Optional) Makes this peer the preferred peer that provides synchronization.
maxpoll *number*	(Optional) Configures the maximum timing intervals, in seconds, between client requests sent to the server. The *number* argument ranges from 4 to 17, with 10 as the default.
minpoll *number*	(Optional) Configures the minimum timing intervals, in seconds, between client requests sent to the server. The *number* argument ranges from 4 to 17, with 6 as the default.

burst	(Optional) Enables burst mode. Burst mode allows the exchange of eight NTP messages (instead of two) during each poll interval in order to reduce the effects of network jitter.
iburst	(Optional) Enables initial burst (iburst) mode. Iburst mode triggers the immediate exchange of eight NTP messages (instead of two) when an association is first initialized. This feature allows rapid time setting at system startup or when an association is configured.

Command Default

No peers are configured.
The default **maxpoll** *number* is 10 seconds.
The default **minpoll** *number* is 6 seconds.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
12.3(14)T	This command was modified. The **normal-sync** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into 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	This command was modified. Support for IPv6 and NTPv4 was added. The **ip**, **ipv6**, **maxpoll**, **minpoll**, **burst**, and **iburst** keywords and the *ipv6-address* and *number* arguments were added.
12.2(33)SXJ	This command was modified. Support for IPv6 and NTPv4 was added. The **ip**, **ipv6**, **maxpoll**, **minpoll**, **burst**, and **iburst** keywords and the *ipv6-address* and *number* arguments were added. The command behavior was modified to display a message after selection of an unsupported NTP version.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S. Support for IPv6 was added.
15.1(4)M	This command was integrated into Cisco IOS Release 15.1(4)M.

Usage Guidelines

When a peer is configured, the default NTP version number is 3, no authentication key is used, and the source address is taken from the outgoing interface.

Use this command to allow a device to synchronize with a peer, or vice versa. Use the **prefer** keyword to reduce switching between peers.

If you are using the default version of 3 and NTP synchronization does not occur, try using NTP version 2 (NTPv2). For IPv6, use NTP version 4.

If you select an NTP version that is not supported, a message is displayed.

If you are using NTPv4, the NTP synchronization takes more time to complete (unlike NTPv3, which synchronizes in seconds or a maximum of 1 to 2 minutes). The acceptable time for synchronization in NTPv4 is 15 to 20 minutes. To achieve faster NTP synchronization, enable the burst or iburst mode by using the **burst** or **iburst** keyword. With the burst or iburst mode configured, NTP synchronization takes about 1 to 2 minutes.

The exact time span required for the NTP synchronization while using NTPv4 cannot be derived accurately. It depends on the network topology and complexity.

Multiple configurations are not allowed for the same peer or server. If a configuration exists for a peer and you use the **ntp peer** command to configure the same peer, the new configuration will replace the old one.

The NTP service can be activated by entering any **ntp** command. When you use the **ntp peer** command, the NTP service is activated (if it has not already been activated) and the peer is configured simultaneously.

When you enter the **no ntp peer** command, only the NTP peer configuration is removed from the NTP service. The NTP service itself remains active, along with any other previously configured NTP functions.

To disable the NTP service on a device, use the **no ntp** command without keywords in global configuration mode. For example, if you had previously issued the **ntp peer** command and you now want to remove not only this restriction, but also all NTP functions from the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also disabled.

Examples

The following example shows how to configure a router to allow its software clock to be synchronized with the clock of the peer (or vice versa) at the IPv4 address 192.168.22.33 using NTPv2. The source IPv4 address is the address of Ethernet 0:

```
Router(config)# ntp peer 192.168.22.33 version 2 source ethernet 0
```

The following example shows how to configure a router to allow its software clock to be synchronized with the clock of the peer (or vice versa) at IPv6 address 2001:0DB8:0:0:8:800:200C:417A using NTPv4:

```
Router(config)# ntp peer 2001:0DB8:0:0:8:800:200C:417A version 4
```

The following example shows how to disable rapid synchronization at startup:

```
Router(config)# ntp peer 192.168.22.33 normal-sync
```

The following example shows the message displayed when you try to configure an unsupported NTP version:

```
Router(config)# ntp peer 192.168.22.33 version 1

NTP version 4 supports backward compatibility to only version 2 and 3
 Please re-enter version[2-4]
 Setting NTP version 4 as default
```

The following example shows how to remove all the configured NTP options and disable the NTP server:

```
Router(config)# no ntp
```

Related Commands

Command	Description
ntp authentication-key	Defines an authentication key for NTP.
ntp server	Allows the software clock to be synchronized by a time server.
ntp source	Uses a particular source address in NTP packets.

ntp refclock

To configure an external clock source for use with Network Time Protocol (NTP) services, use the **ntp refclock** command in line configuration mode. To disable support of the external time source, use the **no** form of this command.

ntp refclock {**trimble** | **telecom-solutions**} **pps** {**cts** | **ri** | **none**} [**inverted**] [**pps-offset** *milliseconds*] [**stratum** *number*] [**timestamp-offset** *number*]

no ntp [**refclock**]

Syntax Description

trimble	Enables the reference clock driver for the Trimble Palisade NTP Synchronization Kit (Cisco 7200 series routers only).
telecom-solutions	Enables the reference clock driver for a Telecom Solutions Global Positioning System (GPS) device.
pps	Enables a pulse per second (PPS) signal line. Indicates PPS pulse reference clock support. The options are **cts**, **ri**, or **none**.
cts	Enables PPS on the Clear To Send (CTS) line.
ri	Enables PPS on the Ring Indicator (RI) line.
none	Specifies that no PPS signal is available.
inverted	(Optional) Specifies that the PPS signal is inverted.
pps-offset *milliseconds*	(Optional) Specifies the offset of the PPS pulse. The number is the offset (in milliseconds).
stratum *number*	(Optional) Indicates the NTP stratum number that the system will claim. Number is from 0 to 14.
timestamp-offset *number*	(Optional) Specifies the offset of time stamp. The number is the offset (in milliseconds).

Command Default

By default, an external clock source for use with NTP services is not configured.

Command Modes

Line configuration (config-line)

Command History

Release	Modification
12.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	This command was modified. Support for IPv6 was added.
12.2(33)SXJ	This command was modified. Support for IPv6 was added.

Release	Modification
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S. Support for IPv6 was added.
15.1(4)M	This command was integrated into Cisco IOS Release 15.1(4)M.

Usage Guidelines

To configure a PPS signal as the source for NTP synchronization, use the following form of the **ntp refclock** command:

ntp refclock trimble pps {**cts** | **ri**} [**inverted**] [**pps-offset** *milliseconds*] [**stratum** *number*] [**timestamp-offset** *number*]

To configure a Trimble Palisade NTP Synchronization Kit as the GPS clock source connected to the auxiliary port of a Cisco 7200 router, use the following form of the **ntp refclock** command:

ntp refclock trimble pps none [**stratum** *number*]

To configure a Telecom Solutions product as the GPS clock source, use the **ntp refclock telecom-solutions** form of the command:

ntp refclock telecom-solutions pps cts [**stratum** *number*]

When two or more servers are configured with the same stratum number, the client will never synchronize with any of the servers. This is because the client is not able to identify the device with which to synchronize. When two or more servers are configured with the same stratum number, and if the client was in synchronization with one of the servers, the synchronization is lost if the settings on one server are changed.

The NTP service can be activated by entering any **ntp** command. When you use the **ntp refclock** command, the NTP service is activated (if it has not already been activated) and the external clock source is configured simultaneously.

In the **no** form of any **ntp** command, all the keywords are optional. When you enter the **no ntp refclock** command, only the external clock source is removed from the NTP service. The NTP service itself remains active, along with any other functions that you previously configured.

To terminate the NTP service on a device, you must enter the **no ntp** command without keywords in global configuration mode. For example, if you had previously issued the **ntp refclock** command and you now want to remove not only the external clock source, but also all NTP functions from the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also terminated.

Examples

The following example shows the configuration of a Trimble Palisade GPS time source on a Cisco 7200 router:

```
Router(config)# ntp master
Router(config)# ntp update-calendar
Router(config)# line aux 0
Router(config-line)# ntp refclock trimble pps none
```

The following example shows the configuration of a Telecom Solutions GPS time source on a Catalyst switch platform:

```
Router(config)# ntp master
Router(config)# ntp update-calendar
Router(config)# line aux 0
Router(config-line)# ntp refclock telecom-solutions pps cts stratum 1
```

If you had previously issued the **ntp refclock** command and you now want to remove not only the external clock source, but also all NTP functions from the device, use the **no ntp** command without any keywords in global configuration mode. The following example shows how to remove the **ntp refclock** command along with all the configured NTP options and how to disable the NTP server:

```
Router(config)# no ntp
```

Related Commands

Command	Description
show ntp associations	Displays the status of NTP associations configured for your system.

ntp server

To allow the software clock to be synchronized by a Network Time Protocol (NTP) time server, use the **ntp server** command in global configuration mode. To disable this capability, use the **no** form of this command.

ntp server [**vrf** *vrf-name*] {*ip-address* | *ipv6-address* | [**ip** | **ipv6**] *hostname*} [**normal-sync**] [**version** *number*] [**key** *key-id*] [**source** *interface-type interface-number*] [**prefer**] [**maxpoll** *number*] [**minpoll** *number*] [**burst**] [**iburst**]

no ntp server [**vrf** *vrf-name*] {*ip-address* | *ipv6-address* | [**ip** | **ipv6**] *hostname*}

Syntax Description

vrf *vrf-name*	(Optional) Specifies that the peer should use a named VPN routing forwarding (VRF) instance for routing to the destination instead of to the global routing table.
ip-address	IPv4 address of the peer providing or being provided the clock synchronization.
ipv6-address	IPv6 address of the peer providing or being provided the clock synchronization.
ip	(Optional) Forces domain name server (DNS) resolution to be performed in the IPv4 address space.
ipv6	(Optional) Forces DNS resolution to be performed in the IPv6 address space.
hostname	Hostname of the peer providing or being provided the clock synchronization.
normal-sync	(Optional) Disables the rapid synchronization at startup.
version	(Optional) Defines the NTP version number.
number	(Optional) NTP version number (2 to 4). In the Cisco IOS Release 12.2SX train, the range is from 1 to 4.
key	(Optional) Defines the authentication key.
key-id	(Optional) Authentication key to use when sending packets to this peer.
source	(Optional) Specifies that the source address must be taken from the specified interface.
interface-type	(Optional) Name of the interface from which to pick the IPv4 or IPv6 source address. For more information, use the question mark (?) online help function.
interface-number	(Optional) Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.
prefer	(Optional) Makes this peer the preferred peer that provides synchronization.
maxpoll *number*	(Optional) Configures the maximum timing intervals, in seconds, between client requests sent to the server. The *number* argument ranges from 4 to 17, with 10 as the default.
minpoll *number*	(Optional) Configures the minimum timing intervals, in seconds, between client requests sent to the server. The *number* argument ranges from 4 to 17, with 6 as the default.

burst	(Optional) Enables burst mode. Burst mode allows the exchange of eight NTP messages (instead of two) during each poll interval in order to reduce the effects of network jitter.
iburst	(Optional) Enables initial burst (iburst) mode. Iburst mode triggers the immediate exchange of eight NTP messages (instead of two) when an association is first initialized. This feature allows rapid time setting at system startup or when an association is configured.

Command Default

No servers are configured by default. If a server is configured, the default NTP version number is 3, an authentication key is not used, and the source IPv4 or IPv6 address is taken from the outgoing interface.

Command Modes

Global configuration (config)

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 was integrated into 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	This command was modified. Support for IPv6 was added to NTP version 4. The **ip**, **ipv6**, **maxpoll**, **minpoll**, **burst**, and **iburst** keywords and the *number* and *ipv6-address* arguments were added.
12.2(33)SXJ	This command was modified. Support for IPv6 was added to NTP version 4. The **ip**, **ipv6**, **maxpoll**, **minpoll**, **burst**, and **iburst** keywords and the *number* and *ipv6-address* arguments were added.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S. Support for IPv6 was added.
15.1(4)M	This command was integrated into Cisco IOS Release 15.1(4)M.

Usage Guidelines

Use this command if you want to allow the system to synchronize with the specified server.

When you use the *hostname* option, the router does a DNS lookup on that name, and stores the IPv4 or IPv6 address in the configuration. For example, if you enter the **ntp server** *hostname* command and then check the running configuration, the output shows "ntp server *a.b.c.d*," where *a.b.c.d* is the IP address of the host, assuming that the router is correctly configured as a DNS client.

Use the **prefer** keyword if you need to use this command multiple times, and you want to set a preferred server. Using the **prefer** keyword reduces switching between servers.

If you are using the default NTP version 3 and NTP synchronization does not occur, try NTPv2. Some NTP servers on the Internet run version 2. For IPv6, use NTP version 4.

If you are using NTPv4, the NTP synchronization takes more time to complete (unlike NTPv3, which synchronizes in seconds or a maximum of 1 to 2 minutes). The acceptable time for synchronization in NTPv4 is 15 to 20 minutes. To achieve faster NTP synchronization, enable the burst or iburst mode by using the **burst** or **iburst** keyword. With the burst or iburst mode configured, NTP synchronization takes about 1 to 2 minutes.

The exact time span required for the NTP synchronization while using NTPv4 cannot be derived accurately. It depends on the network topology and complexity.

The NTP service can be activated by entering any **ntp** command. When you use the **ntp server** command, the NTP service is activated (if it has not already been activated) and software clock synchronization is configured simultaneously.

When you enter the **no ntp server** command, only the server synchronization capability is removed from the NTP service. The NTP service itself remains active, along with any other previously configured NTP functions.

To disable the NTP service on a device, enter the **no ntp** command without keywords. For example, if you had previously issued the **ntp server** command and you now want to remove not only the server synchronization capability, but also all NTP functions from the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also disabled.

If you want to unconfigure an NTP server or a peer configured with a particular source interface, you must specify the interface type and number in the **no** form of the command.

Examples

The following example shows how to configure a router to allow its software clock to be synchronized with the clock by using the device at the IPv4 address 172.16.22.44 using NTPv2:

```
Router(config)# ntp server 172.16.22.44 version 2
```

The following example shows how to configure a router to allow its software clock to be synchronized with the clock by using the device at the IPv6 address 2001:0DB8:0:0:8:800:200C:417A using NTPv4:

```
Router(config)# ntp server 2001:0DB8:0:0:8:800:200C:417A version 4
```

The following example shows how to configure an NTP peer with a particular source interface:

```
Router(config)# ntp server 209.165.200.231 source ethernet 0/1
```

Related Commands

Command	Description
ntp authentication-key	Defines an authentication key for NTP.
ntp peer	Configures the software clock to synchronize a peer or to be synchronized by a peer.
ntp source	Uses a particular source address in NTP packets.

ntp source

To use a particular source address in Network Time Protocol (NTP) packets, use the **ntp source** command in global configuration mode. To remove the specified source address, use the **no** form of this command.

ntp source *interface-type interface-number*

no ntp [**source**]

Syntax Description

interface-type	Type of interface.
interface-number	Number of the interface.

Command Default

Source address is determined by the outgoing interface.

Command Modes

Global configuration (config)

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	This command was modified. Support was added to allow a specified interface to be configured with IPv6 addresses.
12.2(33)SXJ	This command was modified. Support was added to allow a specified interface to be configured with IPv6 addresses.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S. Support for IPv6 was added.
15.1(4)M	This command was integrated into Cisco IOS Release 15.1(4)M.

Usage Guidelines

Use this command when you want to use a particular source IPv4 or IPv6 address for all NTP packets. The address is taken from the named interface. This command is useful if the address on an interface cannot be used as the destination for reply packets. If the **source** keyword is present on an **ntp server** or **ntp peer** global configuration command, that value overrides the global value set by this command.

The NTP service can be activated by entering any **ntp** command. When you use the **ntp source** command, the NTP service is activated (if it has not already been activated) and the source address is configured simultaneously.

In the **no** form of any **ntp** command, all the keywords are optional. When you enter the **no ntp source** command, only the source address is removed from the NTP service. The NTP service itself remains active, along with any other functions that you previously configured.

To disable the NTP service on a device, you must enter the **no ntp** command without any keywords in global configuration mode. For example, if you had previously issued the **ntp source** command and you now want to remove not only the configured source address, but also all NTP functions from the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also disabled.

If the NTP source is not set explicitly, and a link fails or an interface state changes, the NTP packets are sourced from the next best interface and the momentarily lost synchronization is regained.

Examples

The following example shows how to configure a router to use the IPv4 or IPv6 address of Ethernet interface 0 as the source address of all outgoing NTP packets:

```
Router(config)# ntp source ethernet 0
```

The following example shows how to remove all the configured NTP options and disable the NTP server:

```
Router(config)# no ntp
```

Related Commands

Command	Description
ntp peer	Configures the software clock to synchronize a peer or to be synchronized by a peer.
ntp server	Allows the software clock to be synchronized by a time server.

ntp trusted-key

To authenticate the identity of a system to which Network Time Protocol (NTP) will synchronize, use the **ntp trusted-key** command in global configuration mode. To disable the authentication of the identity of the system, use the **no** form of this command.

ntp trusted-key *key-number*

no ntp [**trusted-key** *key-number*]

Syntax Description

key-number	Key number of the authentication key to be trusted.

Command Default

Authentication of the identity of the system is disabled.

Command Modes

Global configuration (config)

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	This command was modified. Support for IPv6 was added.
12.2(33)SXJ	This command was modified. Support for IPv6 was added.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S. Support for IPv6 was added.
15.1(4)M	This command was integrated into Cisco IOS Release 15.1(4)M.

Usage Guidelines

If authentication is enabled, use this command to define one or more key numbers (corresponding to the keys defined with the **ntp authentication-key** command) that a peer NTP system must provide in its NTP packets for synchronization. This function provides protection against accidentally synchronizing the system to a system that is not trusted, because the other system must know the correct authentication key.

The NTP service can be activated by entering any **ntp** command. When you use the **ntp trusted-key** command, the NTP service is activated (if it has not already been activated) and the system to which NTP will synchronize is authenticated simultaneously.

In the **no** form of any **ntp** command, all the keywords are optional. When you enter the **no ntp trusted-key** command, only the authentication is disabled in the NTP service. The NTP service itself remains active, along with any other functions that you previously configured.

To disable the NTP service on a device, you must enter the **no ntp** command without any keywords in global configuration mode. For example, if you had previously issued the **ntp trusted-key** command and you now want to remove not only the authentication, but also all NTP functions from the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also disabled.

Examples

The following example shows how to configure the system to synchronize only to systems providing authentication key 42 in its NTP packets:

```
Router(config)# ntp authenticate
Router(config)# ntp authentication-key 42 md5 aNiceKey
Router(config)# ntp trusted-key 42
```

The following example shows how to remove all the configured NTP options and disable the NTP server:

```
Router(config)# no ntp
```

Related Commands

Command	Description
ntp authenticate	Enables NTP authentication.
ntp authentication-key	Defines an authentication key for NTP.

ntp update-calendar

To periodically update the hardware clock (calendar) from a Network Time Protocol (NTP) time source, use the **ntp update-calendar** command in global configuration mode. To disable the periodic updates, use the **no** form of this command.

ntp update-calendar

no ntp [**update-calendar**]

Syntax Description

This command has no arguments or keywords.

Command Default

The hardware clock (calendar) is not updated.

Command Modes

Global configuration (config)

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	This command was modified. Support for IPv6 was added.
12.2(33)SXJ	This command was modified. Support for IPv6 was added.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S. Support for IPv6 was added.
15.1(4)M	This command was integrated into Cisco IOS Release 15.1(4)M.

Usage Guidelines

Some platforms have a battery-powered hardware clock, referred to in the CLI as the calendar, in addition to the software-based system clock. The hardware clock runs continuously, even if the router is powered off or rebooted.

If the software clock is synchronized to an outside time source via NTP, it is a good practice to periodically update the hardware clock with the time learned from NTP. Otherwise, the hardware clock will tend to gradually lose or gain time (drift), and the software clock and hardware clock may lose synchronization with each other. The **ntp update-calendar** command will enable the hardware clock to be periodically updated with the time specified by the NTP source. The hardware clock will be updated only if NTP has synchronized to an authoritative time server.

Many lower-end routers (for example, the Cisco 2500 series or the Cisco 2600 series) do not have hardware clocks, so this command is not available on those platforms.

To force a single update of the hardware clock from the software clock, use the **clock update-calendar** command in user EXEC mode.

The NTP service can be activated by entering any **ntp** command. When you use the **ntp update-calendar** command, the NTP service is activated (if it has not already been activated) and the hardware clock is updated simultaneously.

In the **no** form of any **ntp** command, all the keywords are optional. When you enter the **no ntp update-calendar** command, only the clock updates are stopped in the NTP service. The NTP service itself remains active, along with any other functions that you previously configured.

To disable the NTP service on a device, you must enter the **no ntp** command without any keywords in global configuration mode. For example, if you had previously issued the **ntp update-calendar** command and you now want to disable not only the periodic updates, but also all NTP functions running on the device, use the **no ntp** command without any keywords. This ensures that all NTP functions are removed and that the NTP service is also disabled.

Examples

The following example shows how to configure the system to periodically update the hardware clock from the NTP time source:

```
Router(config)# ntp update-calendar
```

The following example shows how to remove all the configured NTP options and disable the NTP server:

```
Router(config)# no ntp
```

Related Commands

Command	Description
clock read-calendar	Performs a one-time update of the software clock from the hardware clock (calendar).
clock update-calendar	Performs a one-time update of the hardware clock (calendar) from the software clock.