A through M Commands

absolute

To specify an absolute time for a time-range, use the **absolute** command in time-range configuration mode. To remove the time limitation, use the **no** form of this command.

absolute[**start** *time date*| **end** *time date*]

no absolute

Syntax Description

start *time date*	(Optional) Absolute time and date that the **permit** or **deny** statement of the associated access list starts going into effect. The *time* is expressed in 24-hour notation, in the form of *hours:minutes*. For example, 8:00 is 8:00 a.m. and 20:00 is 8:00 p.m. The *date* is expressed in the format *day month year*. The minimum start is 00:00 1 January 1993. If no start time and date are specified, the **permit** or **deny** statement is in effect immediately.
end *time date*	(Optional) Absolute time and date that the **permit** or **deny** statement of the associated access list is no longer in effect. Same time and date format as described for the **start** keyword. The end time and date must be after the start time and date. The maximum end time is 23:59 31 December 2035. If no end time and date are specified, the associated **permit** or **deny** statement is in effect indefinitely.

Command Default

There is no absolute time when the time range is in effect.

Command Modes

Time-range configuration

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Time ranges are used by IP and Internetwork Packet Exchange (IPX) extended access lists. Time ranges are applied to the **permit** or **deny** statements found in these access lists.

The **absolute** command is one way to specify when a time range is in effect. Another way is to specify a periodic length of time with the periodic command. Use either of these commands after the **time-range** command, which enables time-range configuration mode and specifies a name for the time range. Only one **absolute** entry is allowed per **time-range** command.

If a **time-range** command has both **absolute** and **periodic** values specified, then the **periodic** items are evaluated only after the **absolute start** time is reached, and are not further evaluated after the **absolute end** time is reached.

Note All time specifications are interpreted as local time. To ensure that the time range entries take effect at the desired times, the software clock should be synchronized using the Network Time Protocol (NTP), or some other authoritative time source. For more information, refer to the "Performing Basic System Management" document on Cisco.com.

Examples

In the following example, an access list named 'northeast' references a time range named 'xyz'. The access list and time range configuration permits traffic on Ethernet interface 0, starting at noon on January 1, 2005 and going forever.

```
time-range xyz
 absolute start 12:00 1 January 2005
!
ip access-list extended northeast
 permit ip any any time-range xyz
!
interface ethernet 0
 ip access-group northeast in
```

The configuration sample permits UDP traffic until noon on December 31, 2005. After that time, UDP traffic is no longer allowed out Ethernet interface 0.

```
time-range abc
 absolute end 12:00 31 December 2005
!
ip access-list extended northeast
 permit udp any any time-range abc
!
interface ethernet 0
 ip access-group northeast out
```

The configuration sample permits outgoing UDP traffic on Ethernet interface 0 on weekends only, from 8:00 a.m. on January 1, 2005, to 6:00 p.m. on December 31, 2006:

```
time-range weekend1
 absolute start 8:00 1 January 2005 end 18:00 31 December 2006
 periodic weekends 00:00 to 23:59
!
ip access-list extended northeast1
 permit udp any any time-range weekend1
!
interface ethernet 0
 ip access-group northeast1 out
```

Related Commands

Command	Description
deny	Sets conditions under which a packet does not pass a named access list.
periodic	Specifies a recurring (weekly) start and end time for a time range.
permit	Sets conditions under which a packet passes a named access list.
time-range	Enables time-range configuration mode and names a time range definition.

buffer-length

To specify the maximum length of the data stream to be forwarded, use the **buffer-length**command in line configuration mode. To restore the default setting, use the **no** form of this command.

buffer-length *bytes*

no buffer-length

Syntax Description

bytes	The length of the buffer in bytes. Valid values range from 1 to 1536. The default buffer length is 1536 bytes.

Command Default

1536 bytes

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.
15.1(1)T	This command was modified. The minimum allowed length was changed to 1 byte.

Usage Guidelines

The **buffer-length**command configures the length of the forwarded data stream. The higher the value used for the *byte*argument is, the longer the delay between data transmissions will be. Configuring a smaller buffer-length can prevent connections from timing out inappropriately.

A connection timeout with a high buffer-length value is a very rare occurrence and it depends on the CPU load. Configuring a lower buffer-length value can prevent connection timeouts. A lower buffer-length value is needed only when data transmission is time critical.

Caution A lower buffer-length value should be used with caution. If all the Network Management (NM) and WAN interface card (WIC) slots in the router are filled with async cards, and each of the tty async lines is configured with a buffer length of 1 byte, then the load on the CPU can be increased and the CPU can stall.

Examples

The following example configures a buffer length of 1 byte:

```
Router(config)# line 1
Router(config-line)# buffer-length 1
```

buffers

To make adjustments to initial public buffer pool settings and to the limits at which temporary buffers are created and destroyed, use the **buffers** command in global configuration mode. To return the buffer pool settings to their default sizes, use the **no** form of this command.

buffers {{**header**| **fastswitching**| *interface number*| **small**| **middle**| **big**| **verybig**| **large**| **huge** {**initial**| **max-free**| **min-free**| **permanent**} *buffers*}| **particle-clone** *particle-clones*| **element** {**minimum**| **permanent**} *elements*}

no buffers {{**header**| **fastswitching**| *interface number*| **small**| **middle**| **big**| **verybig**| **large**| **huge** {**initial**| **max-free**| **min-free**| **permanent**} *buffers*}| **particle-clone** *particle-clones*| **element** {**minimum**| **permanent**} *elements*}

Syntax Description

header	Number of particles in the header particle pool. The range is from 256 to 65535. The defaults are min:256, max:1024, and cache:256.
fastswitching	Number of particles in the fastswitching particle pool. The range is from 512 to 65535. The defaults are min:0, max:512, and cache:512.
type number	Interface *type* and *number* of the interface buffer pool. The *type* value cannot be **fddi**.
small	Buffer size of this public buffer pool is 104 bytes.
middle	Buffer size of this public buffer pool is 600 bytes.
big	Buffer size of this public buffer pool is 1524 bytes.
verybig	Buffer size of this public buffer pool is 4520 bytes.
large	Buffer size of this public buffer pool is 5024 bytes.
huge	Public buffer pool can be configured with the **buffers huge size** command. Default buffer size of this public buffer pool, in bytes, is 18024.
initial	Number of additional temporary buffers that are to be allocated when the system is reloaded. This keyword can be used to ensure that the system has necessary buffers immediately after reloading in a high-traffic environment.
max-free	Maximum number of free or unallocated buffers in a buffer pool. The maximum number of small buffers that can be constructed in the pool is 20480.

min-free	Minimum number of free or unallocated buffers in a buffer pool.
permanent	Number of permanent buffers that the system tries to create and keep. Permanent buffers are normally not trimmed by the system.
buffers	Number of buffers to be allocated. The range is 0 to 65536.
particle-clone *particle-clone*	Number of particle clones to grow. The range is from 1024 to 65535. The default is 1024.
element	Buffer elements. The required keywords for the **element** keyword are as follows: • **permanent** --Permanent buffer elements. • **minimum** --Minimum buffer elements.
elements	Number of buffer elements. For permanent buffer elements. The range is from 500 to 65535. The default is 500. For minimum buffer elements. The range is from 500 to 65535.

Command Default

Buffers are set at default sizes that vary by hardware configuration.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
12.4(10)	The **minimum** keyword was added to set the minimum number of buffer elements. The **particle-clone** keyword was added to set the number of particle clones in the buffer pool. The **header** keyword was added to set the number of particles in the header particle pool. The **fastswitching** keyword was added to set the number of particles in the fastswitching particle pool.
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.

Release	Modification
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The default number of buffers in a pool is determined by the hardware configuration and can be displayed with the **show buffers** command in user EXEC mode. Generally, buffer settings do not need to be adjusted. Consult with technical support personnel before making any changes.

Note Improper buffer settings can adversely impact system performance.

You cannot configure FDDI buffers.

Use the **element** keyword with the **permanent** *elements* keyword-argument combination to increase the number of permanent buffer elements to prevent packet loss. For example, in a multicasting environment, a higher number of buffer elements may be needed to accommodate bursts of traffic.

Use the **element** keyword with the **minimum** *elements* keyword-argument combinationto set the minimum number of buffer elements.

Note It is preferable to use the **element** keyword with the **permanent** *elements* keyword-argument combination during system initialization because a higher number of permanent buffer elements will then be ready for use in case a burst of traffic occurs.

Use the **show buffers** command to display statistics such as the following:

- Free list (the total number of unallocated buffer elements)
- Max allowed (the maximum number of buffer elements that are available for allocation)
- Hits (the count of successful attempts to allocate a buffer when needed)
- Misses (the count of buffer allocation attempts that resulted in growing the buffer pool to allocate a buffer)
- Created (the count of new buffers created to satisfy buffer allocation attempts when the available buffers in the pool have already been allocated)

Note If the requested number of permanent buffer elements is fewer than the current number of permanent buffer elements, the configuration will not take effect until the next reload. Resetting the number of permanent buffer elements to the default value using the **no** form of this command will not take effect until the next reload.

Cisco 10000 Series Router

The table below lists the buffer sizes to configure if your network uses a RADIUS server for authentication.

Table 1: Buffer Sizes for RADIUS Authentication

Buffer	Size (in Bytes)
Small	15000
Middle	12000
Big	8000

Examples

Examples

The following example shows how to keep at least 50 small buffers free in the system:

```
Router(config)# buffers small min-free 50
```

The following example shows how to increase the permanent buffer pool allocation for big buffers to 200:

```
Router(config)# buffers big permanent 200
```

Examples

A general guideline is to display buffers with the **show buffers**command and to increase the buffer pool that is depleted.

The following example shows how to increase the permanent Ethernet interface 0 buffer pool on a Cisco 4000 router to 96 when the Ethernet 0 buffer pool is depleted:

```
Router(config)# buffers ethernet 0 permanent 96
```

Examples

The following example shows how to configure the number of permanent buffer elements to 6,000:

```
Router(config)# buffers element permanent 6000
```

The following example shows how to configure the number of minimum buffer elements to 6,000:

```
Router(config)# buffers element minimum 6000
```

Related Commands

Command	Description
load-interval	Changes the length of time for which data is used to compute load statistics.
show buffers	Displays statistics for the buffer pools on the network server.

buffers huge size

To dyn amically resize all huge buffers to the value you specify, use the **buffers huge size** command in global configuration mode. To restore the default buffer values, use the **no** form of this command.

buffers huge size *number-of-bytes*

no buffers huge size *number-of-bytes*

Syntax Description

number-of-bytes	Huge buffer size (in bytes). Valid range is from 18024 to 100000 bytes.

Command Default

18,024 bytes

Command Modes

Global configuration

Command History

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

Usage Guidelines

Use this command only after consulting with technical support personnel. The buffer size cannot be lowered below the default.

Note Improper buffer settings can adversely impact system performance.

Examples

The following example resizes huge buffers to 20,000 bytes:

```
Router(config)# buffers huge size 20000
```

Related Commands

Command	Description
buffers	Adjusts the initial buffer pool settings and the limits at which temporary buffers are created and destroyed.
show buffers	Displays statistics for the buffer pools on the network server.

buffers tune automatic

To enable automatic tuning of buffers, use the **buffers tune automatic**command in global configuration mode. To disable automatic tuning of buffers, use the **no** form of this command.

buffers tune automatic

no buffers tune automatic

Syntax Description

This command has no arguments or keywords.

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.

Usage Guidelines

This command enables automatic tuning of buffers. Even when the command is not enabled, the parameters are computed. When you enable the command later, the buffer parameters change to the computed values.

Examples

The following example shows how to enable automatic tuning of buffers:

```
Router(config)# buffers tune automatic
```

Related Commands

Command	Description
show buffers tune	Displays the automatic buffer tune details.

calendar set

To manually set the hardware clock (calendar), use one of the formats of the **calendar set**command in EXEC mode.

calendar set *hh* **:***mm***:***ss day month year*

Syntax Description

hh **:** *mm* **:** *ss*	Current time in hours (using 24-hour notation), minutes, and seconds.
day	Current day (by date) in the month.
month	Current month (by name).
year	Current year (no abbreviation).

Command Modes

EXEC

Command History

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

Usage Guidelines

Some platforms have a hardware clock that is separate from the software clock. In Cisco IOS software syntax, the hardware clock is called the "calendar." The hardware clock is a battery-powered chip that runs continuously, even if the router is powered off or rebooted. After you set the hardware clock, the software clock will be automatically set from the hardware clock when the system is restarted or when the **clock read-calendar** EXEC command is issued. The time specified in this command is relative to the configured time zone.

Examples

The following example manually sets the hardware clock to 1:32 p.m. on May 19, 2003:

```
Router# calendar set 13:32:00 May 19 2003
```

Related Commands

Command	Description
clock read-calendar	Performs a one-time update of the software clock from the hardware clock (calendar).
clock set	Sets the software clock.
clock summer-time	Configures the system time to automatically switch to summer time (daylight saving time).
clock timezone	Sets the time zone for display purposes.
clock update-calendar	Performs a one-time update of the hardware clock from the software clock.

clear platform hardware capacity rewrite-engine counter

To clear the packet drop and performance counters of the central rewrite engine on supervisors and line cards, use the **clear platform hardware capacity rewrite-engine counter** command in privileged EXEC mode.

clear platform hardware capacity rewrite-engine counter [**slot** *number*]

Syntax Description

slot *number*	Clears the packet drop and performance counters on the module in the specified slot. If no slot is specified, the counters are cleared on all slots.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

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

Examples

This example shows how to clear the packet drop and performance counters for the module in slot 6:

```
Router#
clear platform hardware capacity rewrite-engine counter slot 6
Router#
```

Related Commands

Command	Description
show platform hardware capacity rewrite-engine	Displays the packet drop and performance counters of the central rewrite engine on supervisors and line cards.

clock calendar-valid

To configure a system as an authoritative time source for a network based on its hardware clock (calendar), use the **clock calendar-valid** command in global configuration mode. To specify that the hardware clock is not an authoritative time source, use the **no** form of this command.

clock calendar-valid

no clock calendar-valid

Syntax Description

This command has no arguments or keywords.

Command Default

The router is not configured as a time source.

Command Modes

Global configuration

Command History

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

Usage Guidelines

Some platforms have a hardware clock that is separate from the software clock. The hardware clock runs continuously, even if the router is powered off or rebooted. If no outside time source is available on your network, use this command to make the hardware clock an authoritative time source.

Because the hardware clock is not as accurate as other time sources, you should configure this command only when a more accurate time source (such as NTP) is not available.

Examples

The following example configures a router as the time source for a network based on its hardware clock:

```
Router(config)# clock calendar-valid
```

Related Commands

Command	Description
ntp master	Configures the Cisco IOS software as an NTP master clock to which peers synchronize themselves when an external NTP source is not available.

Command	Description
vines time use-system	Sets VINES network time based on the system time.

clock read-calendar

To manually read the hardware clock (calendar) settings into the software clock, use the **clock read-calendar** command in EXEC mode.

clock read-calendar

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

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

Usage Guidelines

Some platforms have a hardware clock that is separate from the software clock. The hardware clock runs continuously, even if the router is powered off or rebooted. When the router is rebooted, the hardware clock is automatically read into the software clock. However, you may use this command to manually read the hardware clock setting into the software clock. This command is useful if the **calendar set** command has been used to change the setting of the hardware clock.

Examples

The following example configures the software clock to set its date and time by the hardware clock setting:

```
Router> clock read-calendar
```

Related Commands

Command	Description
calendar set	Sets the hardware clock.
clock set	Manually sets the software clock.
clock update-calendar	Performs a one-time update of the hardware clock from the software clock.
ntp update-calendar	Periodically updates the hardware clock from the software clock.

clock save interval

To preserve recent date and time information in NVRAM for when a Cisco IOS device without a battery-backed calendar is power-cycled or reloaded, use the **clock save interval**command in global configuration mode. To return to the default disabled state, use the **no** form of this command.

clock save interval *hours*

no clock save interval *hours*

Syntax Description

hours	Interval at which the time will be stored in NVRAM. Accepted intervals range from 8 to 24 hours.

Command Default

This function is disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The benefit of using this command is that upon returning from a system reload or power cycle, the system clock will be set to a time and date near the current time and date instead of being reset to the system default time and date. In the absence of better information, Cisco IOS devices will initially set their system clocks to *epoch start* , which will typically be midnight (UTC) March 1, 1993 or 2002.

When this command is entered, the date and time are saved to NVRAM at the interval specified by this command, and also during any shutdown process. When the system starts up, the system clock is set to the last time and date saved to NVRAM.

All Cisco IOS devices support Network Time Protocol (NTP) or Simple Network Time Protocol (SNTP) to learn the time from the network, and some Cisco IOS devices have built-in battery-backed clocks to maintain that time. The **clock save interval**command is for those Cisco IOS devices that do not have battery-backed clocks and need to know the time and date before they can start communicating with a network. Because the March 1 system default date will likely occur before the valid date of any recently issued certificate, communications attempted with almost any certificate will fail because it is not yet valid according to the local clock.

Saving the time at a 24-hour interval should work well for most networks, unless there is a certificate that maintains a shorter life span.

Being aware of the time and date is critical for networking devices, and it becomes an issue when communication to a network requires use of a time-based credential, such as a certificate that has start and end dates and times. NTP and SNTP are the proper ways to set the time of a network device. The **clock save interval**command is intended to complement use of NTP and SNTP, so this command is useful only when a certificate is required to initiate communication to an NTP server, and the Cisco IOS device does not have a battery-back hardware clock, but does have NVRAM.

The system time will only be saved to NVRAM when set by an authoritative source such as NTP or SNTP; the system will not save the time entered through the **set clock** command. Additionally, a clock is considered valid only when the following criteria apply:

- The clock was set by the user using the **set clock** command and declared authoritative by the **clock calendar-valid** command.
- The clock time was learned through NTP or SNTP.

Through a confluence of events, there is no means to authoritatively declare a user-entered time as valid unless the calendar (battery-backed date and time) is declared valid. Since there is no actual calendar in a system with this command, the **clock calendar-valid** command is unavailable, and therefore a user-entered time can never be considered authoritative on platforms without a battery-backed calendar. This state is intentional because a battery-backed clock continues to run, and an NVRAM clock will stay the same. And again, for these reasons the **clock save interval**command must complement the use of NTP and SNTP.

Examples

The following example shows how to configure a Cisco IOS device to save the time at 24-hour intervals:

```
Router(config)# clock save interval 24
```

clock set

To manually set the system software clock, use one of the following formats of the **clock set** command in privileged EXEC mode.

clock set *hh* **:** *mm* **:** *ss day month year*

clock set *hh* **:** *mm* **:** *ss month day year*

Syntax Description

hh **:** *mm* **:** *ss*	Current time in hours (24-hour format), minutes, and seconds.
day	Current day (by date) in the month.
month	Current month (by name).
year	Current year (no abbreviation).

Command Modes

Privileged EXEC mode

Command History

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

Usage Guidelines

Generally, if the system is synchronized by a valid outside timing mechanism, such as a Network Time Protocol (NTP) or VINES clock source, or if you have a router with a hardware clock, you need not set the software clock. Use this command if no other time sources are available. The time specified in this command is assumed to be in the time zone specified by the configuration of the **clock timezone** command.

Examples

The following example manually sets the software clock to 7:29 p.m. on May 13, 2003:

```
Router# clock set 19:29:00 13 May 2003
```

Related Commands

Command	Description
calendar set	Sets the hardware clock.
clock read-calendar	Performs a one-time update of the software clock from the hardware clock (calendar).
clock summer-time	Configures the system to automatically switch to summer time (daylight saving time).
clock timezone	Sets the time zone for display purposes.

clock summer-time

To configure the system to automatically switch to summer time (daylight saving time), use one of the formats of the **clock summer-time** command in global configuration mode. To configure the Cisco IOS software not to automatically switch to summer time, use the **no** form of this command.

clock summer-time *zone* {**date** *start-date start-month start-year hh* **:** *mm end-date end-month end-year hh* **:** *mm* [*offset*]| **recurring** [*week*| **first**| **last**] *start-date start-month hh* **:** *mm* {*end-week*| **first**| **last**} *end-day end-month hh* **:** *mm* [*offset*]}

no clock summer-time

Syntax Description

zone	Name of the time zone (for example, "PDT" for Pacific Daylight Time) to be displayed when summer time is in effect. The length of the *zone*argument *is limited to seven characters.*
date	Configures summer time based on the date.
start-date	Start day of the week (Sunday, Monday, and so on).
start-month	Start month of the year.
start-year	Start year.
hh **:** *mm*	(Optional) Time (military format) in hours and minutes. The colon is required.
end-date	End date of the month (1 to 31).
end-month	(Optional) End month (January, February, and so on) of the year.
end-year	End year (1993 to 2035).
offset	(Optional) Number of minutes to add during summer time (default is 60). The range is 1 to 1440.
recurring	Configures a recurring start and end of summer time.
week	(Optional) Week of the month (1 to 4). Use **first** to specify the first week and **last**to specify the last week
first	(Optional) Specifies the first week of the month
last	(Optional) Specifies the last week of the month

end-day	(Optional) End day of the week (Sunday, Monday, and so on).

Command Default

Summer time is disabled. If the **clock summer-time** *zone* **recurring** command is specified without parameters, the summer time rules default to United States rules. Default of the *offset* argument is 60.

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 modified in a release earlier than Cisco IOS Release 15.0(1)M. The **first** and **last** keywords were added.

Usage Guidelines

Use this command if you want to automatically switch to summer time (for display purposes only). Use the **recurring** form of the command if the local summer time rules are of this form. Use the **date** keyword to specify a start and end date for summer time if you cannot use the **recurring** keyword.

In both the **date** and **recurring** forms of the command, the first part of the command specifies when summer time begins, and the second part specifies when it ends. All times are relative to the local time zone. The start time is relative to standard time. The end time is relative to summer time. If the starting month is chronologically after the ending month, the system assumes that you are in the southern hemisphere.

Examples

The following example specifies that summer time starts on the first Sunday in April at 2 a.m. and ends on the last Sunday in October at 2 a.m.:

```
Router(config)# clock summer-time PDT recurring 1 Sunday April 2:00 last Sunday October
2:00
```

If you live in a place where summer time does not follow the pattern in the first example, you can specify the exact date and times. In the following example, daylight saving time (summer time) is configured to start on October 12, 1997 at 2 a.m., and end on April 26, 1998 at 2 a.m.:

```
Router(config)# clock summer-time PDT date 12 October 1997 2:00 26 April 1998 2:00
```

Related Commands

Command	Description
calendar set	Sets the hardware clock.
clock timezone	Sets the time zone for display purposes.

clock timezone

To set the time zone for display purposes, use the **clock timezone** command in global configuration mode. To set the time to Coordinated Universal Time (UTC), use the **no**form of this command.

clock timezone *zone hours-offset* [*minutes-offset*]

no clock timezone

Syntax Description

zone	Name of the time zone to be displayed when standard time is in effect. The length of the *zone*argument *is limited to 7 characters.*
hours-offset	Hours difference from UTC.
minutes-offset	(Optional) Minutes difference from UTC.

Command Default

UTC

Command Modes

Global configuration

Command History

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

Usage Guidelines

The system internally keeps time in UTC, so this command is used only for display purposes and when the time is manually set.

The table below lists common time zone acronyms used for the *zone* argument.

Table 2: Common Time Zone Acronyms

Acronym	Time Zone Name and UTC Offset
Europe	

Acronym	Time Zone Name and UTC Offset
GMT	Greenwich Mean Time, as UTC
BST	British Summer Time, as UTC + 1 hour
IST	Irish Summer Time, as UTC + 1 hour
WET	Western Europe Time, as UTC
WEST	Western Europe Summer Time, as UTC + 1 hour
CET	Central Europe Time, as UTC + 1
CEST	Central Europe Summer Time, as UTC + 2
EET	Eastern Europe Time, as UTC + 2
EEST	Eastern Europe Summer Time, as UTC + 3
MSK	Moscow Time, as UTC + 3
MSD	Moscow Summer Time, as UTC + 4
United States and Canada	
AST	Atlantic Standard Time, as UTC -4 hours
ADT	Atlantic Daylight Time, as UTC -3 hours
ET	Eastern Time, either as EST or EDT, depending on place and time of year
EST	Eastern Standard Time, as UTC -5 hours
EDT	Eastern Daylight Saving Time, as UTC -4 hours
CT	Central Time, either as CST or CDT, depending on place and time of year
CST	Central Standard Time, as UTC -6 hours
CDT	Central Daylight Saving Time, as UTC -5 hours
MT	Mountain Time, either as MST or MDT, depending on place and time of year
MST	Mountain Standard Time, as UTC -7 hours
MDT	Mountain Daylight Saving Time, as UTC -6 hours

Acronym	Time Zone Name and UTC Offset
PT	Pacific Time, either as PST or PDT, depending on place and time of year
PST	Pacific Standard Time, as UTC -8 hours
PDT	Pacific Daylight Saving Time, as UTC -7 hours
AKST	Alaska Standard Time, as UTC -9 hours
AKDT	Alaska Standard Daylight Saving Time, as UTC -8 hours
HST	Hawaiian Standard Time, as UTC -10 hours
Australia	
WST	Western Standard Time, as UTC + 8 hours
CST	Central Standard Time, as UTC + 9.5 hours
EST	Eastern Standard/Summer Time, as UTC + 10 hours (+11 hours during summer time)

The table below lists an alternative method for referring to time zones, in which single letters are used to refer to the time zone difference from UTC. Using this method, the letter Z is used to indicate the zero meridian, equivalent to UTC, and the letter J (Juliet) is used to refer to the local time zone. Using this method, the International Date Line is between time zones M and Y.

Table 3: Single-Letter Time Zone Designators

Letter Designator	Word Designator	Difference from UTC
Y	Yankee	UTC -12 hours
X	Xray	UTC -11 hours
W	Whiskey	UTC -10 hours
V	Victor	UTC -9 hours
U	Uniform	UTC -8 hours
T	Tango	UTC -7 hours
S	Sierra	UTC -6 hours
R	Romeo	UTC -5 hours

Letter Designator	Word Designator	Difference from UTC
Q	Quebec	UTC -4 hours
P	Papa	UTC -3 hours
O	Oscar	UTC -2 hours
N	November	UTC -1 hour
Z	Zulu	Same as UTC
A	Alpha	UTC +1 hour
B	Bravo	UTC +2 hours
C	Charlie	UTC +3 hours
D	Delta	UTC +4 hours
E	Echo	UTC +5 hours
F	Foxtrot	UTC +6 hours
G	Golf	UTC +7 hours
H	Hotel	UTC +8 hours
I	India	UTC +9 hours
K	Kilo	UTC +10 hours
L	Lima	UTC +11 hours
M	Mike	UTC +12 hours

The following example sets the time zone to Pacific Standard Time (PST), which is 8 hours behind UTC:

```
Router(config)# clock timezone PST -8
```

The following example sets the time zone to Atlantic Time (AT) for Newfoundland, Canada, which is 3.5 hours behind UTC:

```
Router(config)# clock timezone AT -3 30
```

Related Commands

Command	Description
calendar set	Sets the hardware clock.

Command	Description
clock set	Manually set the software clock.
clock summer-time	Configures the system to automatically switch to summer time (daylight saving time).
show clock	Displays the software clock.

clock update-calendar

To perform a one-time update of the hardware clock (calendar) from the software clock, use the **clock update-calendar** command in user EXEC or privileged EXEC mode.

clock update-calendar

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC

Privileged EXEC

Command History

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

Usage Guidelines

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

If the software clock and hardware clock are not synchronized, and the software clock is more accurate, use this command to update the hardware clock to the correct date and time.

Examples

The following example copies the current date and time from the software clock to the hardware clock:

```
Router> clock update-calendar
```

Related Commands

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

exception core-file

To specify the name of the core dump file in Cisco IOS or Cisco IOS Software Modularity software, use the **exception core-file** command in global configuration mode. To return to the default core filename, use the **no**form of this command.

Cisco IOS Software

exception core-file *filename*

no exception core-file

Cisco IOS Software Modularity

exception core-file [*filename*] [**limit** *upper-limit*] **[compress] [timestamp]**

no exception core-file

Syntax Description

filename	Name of the core dump file saved on the server. (Optional) In Software Modularity images, if this argument is not specified, the default core file is named using the name of the process that is being dumped. For example, if the raw_ip.proc is the process that is being dumped, then the default core file is named raw_ip.proc.
limit	(Optional) For Cisco IOS Software Modularity images only. Specifies an upper limit of a range so that core dumps of more than one process can be created without overwriting the previous core dump.
upper-limit	(Optional) For Cisco IOS Software Modularity images only. Number, in the range from 1 to 64, that represents the upper limit.
compress	(Optional) For Cisco IOS Software Modularity images only. Turns on dump file compression. By default, compression is turned off.
timestamp	(Optional) For Cisco IOS Software Modularity images only. Adds a time stamp to the core dump file.

Command Default

Cisco IOS Software: The core file is named *hostname* -core, where *hostname* is the name of the router. Cisco IOS Software Modularity: The core file is named using the name of the process that is being dumped.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.2	This command was introduced.
12.2(18)SXF4	The **limit**, **compress**, and **timestamp** keywords were added to support Software Modularity images.

Usage Guidelines

If you use TFTP to dump the core file to a server, the router will only dump the first 16 MB of the core file. If the router's memory is larger than 16 MB, the whole core file will not be copied to the server. Therefore, use rcp or FTP to dump the core file. The network dump is not supported in Software Modularity images.

Caution This command is of use only to Cisco technical support representatives in analyzing system failures in the field. Under normal circumstances, there should be no reason to change the default core filename. For that reason, this command should be used only by Cisco Certified Internetwork Experts (CCIEs) or under the direction of Cisco Technical Assistance Center (TAC) personnel.

Examples

Examples

In the following example, the router is configured to use FTP to dump a core file named dumpfile to the FTP server at 172.17.92.2 when the router crashes:

```
ip ftp username red
ip ftp password blue
exception protocol ftp
exception dump 172.17.92.2
exception core-file dumpfile
```

Examples

In the following example, the router is configured to dump the main memory used by the TCP process to a file named dump-tcp when the TCP process crashes. The dump file is configured with an upper limit of 20, to be compressed, and to have a time stamp applied.

```
exception core tcp.proc mainmem
exception core-file dump-tcp limit 20 compress timestamp
```

Note The **exception protocol**and **exception dump**commands are not supported in Software Modularity images.

Related Commands

Command	Description
exception core	Sets or changes the core dump options for a Cisco IOS Software Modularity process.

Command	Description
exception dump	Causes the router to dump a core file to a particular server when the router crashes.
exception memory	Causes the router to create a core dump and reboot when certain memory size parameters are violated.
exception protocol	Configures the protocol used for core dumps.
exception spurious-interrupt	Causes the router to create a core dump and reload after a specified number of spurious interrupts.
ip ftp password	Specifies the password to be used for FTP connections.
ip ftp username	Configures the username for FTP connections.

exception crashinfo buffersize

To change the size of the buffer used for crashinfo files, use the **exception crashinfo buffersize**command in global configuration mode. To revert to the default buffer size, use the **no**form of this command.

exception crashinfo buffersize *kilobytes*

no exception crashinfo buffersize *kilobytes*

Syntax Description

kilobytes	Buffer size, in kilobytes (KB). Range is 32 to 256. Default is 32.

Command Default

Crashinfo buffer is 32 KB.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(4)T, 12.2(11)	This command was introduced for the Cisco 3600 series only (3620, 3640, and 3660 platforms).
12.2(13)T	This command was implemented in Cisco 6400-NSP images.
12.2(15)JA	This command was integrated into Cisco IOS Release 12.2(15)JA.
12.2(18)SXF4	This command was integrated into Release 12.2(18)SXF4 to support Software Modularity images.

Usage Guidelines

The crashinfo file saves information that helps Cisco technical support representatives to debug problems that caused the Cisco IOS image to fail (crash). The device writes the crash information to the console at the time of the failure, and the file is created the next time you boot the Cisco IOS image after the failure (instead of while the system is failing).

Note If you are running a Software Modularity image, setting the crashinfo buffer size to the default of 32 KB does not limit the crashinfo buffer size. The crashinfo file size is limited to the value set if the value is set to anything other than the default 32 KB.

Examples

In the following example, the crashinfo buffer is set to 100 KB:

```
Router(config)# exception crashinfo buffersize 100
```

Related Commands

Command	Description
exception crashinfo file	Enables the creation of a diagnostic file at the time of unexpected system shutdowns.

exception crashinfo dump

To specify the type of output information to be written to the crashinfo file, use the **exception crashinfo dump** command in global configuration mode. To remove this information from the crashinfo file, use the **no** form of this command.

exception crashinfo dump {**command** *cli*| **garbage-detector**}

no exception crashinfo dump {**command** *cli*| **garbage-detector**}

Syntax Description

command *cli*	Indicates the Cisco IOS command for which you want the output information written to the crashinfo file.
garbage-detector	If a router crashes due to low memory, specifies that the output from the **show memory debug leaks summary** command should be written to the crashinfo file.

Command Default

This command is disabled by default.

If a router crashes due to low memory, the output from the following Cisco IOS commands is written to the crashinfo file by default:

- **show process memory**
- **show processes cpu**
- **show memory summary**
- **show buffers**

If the **exception crashinfo dump garbage-detector** command is enabled, the output from the **show memory debug leaks summary** command is also written to the crashinfo file by default.

Command Modes

Global configuration

Command History

Release	Modification
12.3(11)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

A benefit for using the **exception crashinfo dump** command is that it allows users to customize the crashinfo file to contain information that is relevant to their troubleshooting situation.

Examples

The following example shows how to specify that the output from the **show interfaces** command should be written to the crashinfo file:

```
exception crashinfo dump command show interfaces
```

Related Commands

Command	Description
exception memory	Sets free memory and memory block size threshold parameters.
show interfaces	Displays statistics for all interfaces configured on the router or access server.

exception crashinfo file

To enable the creation of a diagnostic file at the time of unexpected system shutdowns, use the **exception crashinfo file**command in global configuration mode. To disable the creation of crashinfo files, use the **no**form of this command.

exception crashinfo file *device* **:** *filename*

no exception crashinfo file *device* **:** *filename*

Syntax Description

device:filename	Specifies the flash device and file name to be used for storing the diagnostic information. The file name can be up to 38 characters. The colon is required.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)T, 12.2(11)	This command was introduced for the Cisco 3600 series only.
12.2(13)T	This command was implemented in Cisco 6400-NSP images.
12.2(15)JA	This command was integrated into Cisco IOS Release 12.2(15)JA.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The crashinfo file saves information that helps Cisco technical support representatives to debug problems that caused the Cisco IOS image to fail (crash). The device writes the crash information to the console at the time of the failure, and the file is created the next time you boot the IOS image after the failure (instead of while the system is failing). The filename will be *filename_yyyymmdd-hhmmss* , where *y* is year, *m* is month, *d* is date, *h* is hour, and *s* is seconds.

Examples

In the following example, a crashinfo file called “crashdata” will be created in the default flash memory device if a system crash occurs:

```
Router(config)# exception crashinfo file flash:crashinfo
```

Related Commands

Command	Description
exception crashinfo buffersize	Changes the size of the crashinfo buffer.

exception crashinfo maximum files

To enable a Cisco device to automatically delete old crashinfo files to help create space for writing the new crashinfo files when a system crashes, use the **exception crashinfo maximum files** command in global configuration mode. To disable automatic deletion of crashinfo files, use the **no** form of this command.

exception crashinfo maximum files *file-numbers*

no exception crashinfo maximum files *file-numbers*

Syntax Description

file-numbers	Number of the most recent crashinfo files across all file systems in the device to be saved when crashinfo files are deleted automatically. • The range is from 1 to 32.

Command Default

Crashinfo files are not automatically deleted.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(11)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.2(3)T	This command was modified. The minimum value for the *file-numbers* argument was changed from 0 to 1.

Usage Guidelines

This command is effective only when a device crashes.

While booting a device, the default file location is bootflash.

If the file system does not have free space equivalent to or more than 250 KB, the system displays a warning. You can verify the available disk space and create free space for writing the crashinfo files.

Examples

The following example shows how to enable a Cisco device to automatically delete old crashinfo files if the device needs space for writing new crashinfo files when a system crashes. In this example, the device is configured to preserve the 22 latest crashinfo files from previous crashinfo collections.

```
configure terminal
```

```
!
exception crashinfo maximum files 22
```

Related Commands

Command	Description
exception crashinfo buffersize	Changes the size of the crashinfo buffer.
exception crashinfo file	Creates a diagnostic file at the time of unexpected system shutdown.

exception data-corruption

To manage data error exceptions, use the **exception data-corruption**command in global configuration mode. To disable the management of data error exceptions, use the **no** form of this command.

exception data-corruption {**buffer** {**log**| **truncate**}| **reload**}

no exception data-corruption {**buffer** {**log**| **truncate**}| **reload**}

Syntax Description

buffer	Sets buffer corruption behavior.
log	Logs the number of attempts to overwrite the buffer.
truncate	Truncates the number of times the buffer is overwritten.
reload	Immediately reloads the data when a problem is detected.

Command Default

Data error exceptions are not managed.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
12.2(33)SXI	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.

Examples

The following example shows how to enable the handling of data error exceptions:

```
Router(config)# exception data corruption buffer log
```

Related Commands

Command	Description
exception crashinfo	Facilitates the collection of crashinfo.

exception delay-dump

To pause or delay the dump of data error exceptions to the host, use the **exception delay-dump**command in global configuration mode. To disable the delay in the dump of data error exceptions to the host, use the **no** form of this command.

exception delay-dump *seconds*

no exception delay-dump

Syntax Description

seconds	Delay or pause time in seconds in the range 30 to 300. The default value is 30.

Command Default

The dump of data error exceptions is not delayed.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
12.2(33)SXI	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.

Examples

The following example shows how to enable the handling of data error exceptions:

```
Router> enable
Router# configure terminal
Router(config)# exception delay-dump 32
```

Related Commands

Command	Description
exception crashinfo	Facilitates the collection of crashinfo.

exception dump

To configure the router to dump a core file to a particular server when the router crashes, use the **exception dump** command in global configuration mode. To disable core dumps, use the **no**form of this command.

exception dump *ip-address*

no exception dump

Syntax Description

ip-address	IP address of the server that stores the core dump file.

Command Default

Disabled

Command Modes

Global configuration

Command History

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

Usage Guidelin

Caution Use the **exception dump** command only under the direction of a technical support representative. Creating a core dump while the router is functioning in a network can disrupt network operation. The resulting binary file, which is very large, must be transferred to a TFTP, FTP, or rcp server and subsequently interpreted by technical personnel that have access to source code and detailed memory maps.

If you use TFTP to dump the core file to a server, the router will only dump the first 16 MB of the core file. If the router's memory is larger than 16 MB, the whole core file will not be copied to the server. Therefore, use rcp or FTP to dump the core file.

The core dump is written to a file named *hostname* -core on your server, where *hostname* is the name of the router. You can change the name of the core file by configuring the **exception core-file** command.

This procedure can fail for certain types of system crashes. However, if successful, the core dump file will be the size of the memory available on the processor (for example, 16 MB for a CSC/4).

Examples

In the following example, a user configures a router to use FTP to dump a core file to the FTP server at 172.17.92.2 when it crashes:

```
Router(config)# ip ftp username red
```

```
Router(config)# ip ftp password blue
Router(config)# exception protocol ftp
Router(config)# exception dump 172.17.92.2
Router(config)# exception core-file dumpfile
```

Related Commands

Command	Description
exception core-file	Specifies the name of the core dump file.
exception memory	Causes the router to create a core dump and reboot when certain memory size parameters are violated.
exception protocol	Configures the protocol used for core dumps.
exception spurious-interrupt	Causes the router to create a core dump and reload after a specified number of spurious interrupts.
ip ftp password	Specifies the password to be used for FTP connections.
ip ftp username	Configures the username for FTP connections.
ip rcmd remote-username	Configures the remote username to be used when requesting a remote copy using rcp.

exception linecard

To enable storing of crash information for a line card and optionally specify the type and amount of information stored, use the **exception linecard** command in global configuration mode . To disable the storing of crash information for the line card, use the **no** form of this command.

exception linecard {**all**| **slot** *slot-number*} [**corefile** *filename*| **main-memory** *size* [**k**| **m**]| **queue-ram** *size* [**k**| **m**]| **rx-buffer** *size* [**k**| **m**]| **sqe-register-rx**| **sqe-register-tx**| **tx-buffer** *size* [**k**| **m**]]

no exception linecard

Syntax Description

all	Stores crash information for all line cards.
slot *slot-number*	Stores crash information for the line card in the specified slot. Slot numbers range from 0 to 11 for the Cisco 12012 and 0 to 7 for the Cisco 12008 router.
corefile *filename*	(Optional) Stores the crash information in the specified file in NVRAM. The default filename is *hostname* **-core-** *slot-number* (for example, c12012-core-8).
main-memory *size*	(Optional) Stores the crash information for the main memory on the line card and specifies the size of the crash information. Size of the memory to store is 0 to 268435456.
queue-ram *size*	(Optional) Stores the crash information for the queue RAM memory on the line card and specifies the size of the crash information. Size of the memory to store can be from 0 to 1048576.
rx-buffer *size* **tx-buffer** *size*	(Optional) Stores the crash information for the receive and transmit buffer on the line card and specifies the size of the crash information. Size of the memory to store can be from 0 to 67108864.
sqe-register-rx **sqe-register-tx**	(Optional) Stores crash information for the receive or transmit silicon queueing engine registers on the line card.
k **m**	(Optional) The **k** option multiplies the specified *size* by 1K (1024), and the **m** option multiplies the specified *size* by 1M (1024*1024).

Command Default

No crash information is stored for the line card.

If enabled with no options, the default is to store 256 MB of main memory.

Command Modes

Global configuration

Command History

Release	Modification
11.2 GS	This command was introduced for Cisco 12000 series Gigabit Switch Routers (GSRs).
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use caution when enabling the **exception linecard** global configuration command. Enabling all options could cause a large amount (150 to 250 MB) of crash information to be sent to the server.

Caution Use the **exception linecard** global configuration command only when directed by a technical support representative. Only enable options that the technical support representative requests you to enable. Technical support representatives need to be able to look at the crash information from the line card to troubleshoot serious problems on the line card. The crash information contains all the line card memory information including the main memory and transmit and receive buffer information. .

Examples

In the following example, the user enables the storing of crash information for line card 8. By default, 256 MB of main memory is stored.

```
Router(config)# exception linecard slot 8
```

exception memory

To set free memory and memory block size threshold parameters, use the **exception memory** command in global configuration mode. To disable this functionality, use the **no**form of this command.

exception memory {**fragment**| **minimum**} [**processor**| **io**] *size* [**interval 1**] **[reboot]** [**data overflow** {**fast**| **iomem**| **pcimem**| **processor**| **transient**}]

no exception memory {**fragment**| **minimum**} [**processor**| **io**] *size* [**interval 1**] **[reboot]** [**data overflow** {**fast**| **iomem**| **pcimem**| **processor**| **transient**}]

Syntax Description

fragment *size*	Sets the minimum contiguous block of memory in the free pool, in bytes.
minimum *size*	Sets the minimum size of the free memory pool, in bytes. The range is from 1 to 4090445040.
processor	(Optional) Specifies processor memory.
io	(Optional) Specifies I/O memory.
interval 1	(Optional) Checks the largest memory block size every 1 second. If the **interval 1** keyword is not configured, the memory block size is checked every 60 seconds (1 minute) by default.
reboot	(Optional) Reloads the router when a memory size threshold is violated. If the **reboot** keyword is not configured, the router will not reload when a memory size threshold is violated.
data overflow	(Optional) Enables data overflow detection for the following memory types: • **fast** • **iomem** • **pcimem** • **processor** • **transient**

Command Default

This command is disabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.3	This command was introduced.
12.3(11)T	This command was modified. The **processor**, **io**, **interval 1**, and **reboot**keywords were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was modified. The **data overflow** keyword was added.

Usage Guidelines

This command is used to troubleshoot memory leaks and memory fragmentation issues.

The free memory size is checked for every memory allocation. The largest memory block size is checked every 60 seconds by default. If the **interval 1** keyword is configured, the largest memory block size is checked every 1 second.

When a memory size threshold is violated, the router will display an error message and create a crashinfo file. A core dump file will also be created if the **exception dump**command is configured. The router will not reload unless the **reboot** keyword is configured.

Caution Use the **exception** commands only under the direction of a technical support representative. Creating a core dump while the router is functioning in a network can disrupt network operation. The resulting binary file, which is very large, must be transferred to a TFTP, FTP, or rcp server and subsequently interpreted by technical personnel that have access to source code and detailed memory maps.

Examples

The following example shows how to configure the router to monitor the free memory. If the amount of free memory falls below 250,000 bytes, the router will create a crashinfo file and core dump file and reload.

```
configure terminal
!
exception dump 10.0.0.2
exception core-file memory.overrun
exception memory minimum 250000 reboot
```

Related Commands

Command	Description
exception core-file	Specifies the name of the core dump file.

Command	Description
exception crashinfo dump	Specifies the type of output information to be written to the crashinfo file.
exception dump	Configures the router to dump a core file to a particular server when the router crashes.
exception protocol	Configures the protocol used for core dumps.
exception region-size	Specifies the size of the region for the exception-time memory pool.
ip ftp password	Specifies the password to be used for FTP connections.
ip ftp username	Configures the username for FTP connections.

exception memory ignore overflow

To configure the Cisco IOS software to correct corruption in memory block headers and allow a router to continue its normal operation, use the **exception memory ignore overflow** command in global configuration mode. To disable memory overflow correction, use the **no** form of this command.

exception memory ignore overflow {**io**| **processor**} [**frequency** *seconds*] [**maxcount** *corrections*]

no exception memory ignore overflow {**io**| **processor**} [**frequency** *seconds*] [**maxcount** *corrections*]

Syntax Description

io	Selects input/output (also called packet) memory.
processor	Selects processor memory.
frequency *seconds*	(Optional) Specifies the minimum time gap between two memory block header corrections, in the range from 1 to 600 seconds. The default is once every 10 seconds.
maxcount *corrections*	(Optional) Specifies the maximum number of memory block header corrections allowed, in the range from 1 to 1000. The default is 0, which sets an unlimited number of corrections.

Command Default

The default is to allow the memory overflow correction once every 10 seconds, and for memory overflow corrections to happen an unlimited number of times.

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use this command to improve device availability when software faults are detected in the network. You can configure the frequency and the maximum number of memory overflow corrections. If overflow correction

is required more often than the configured value, a software forced reload is triggered because a severe system problem is indicated.

Examples

The following example shows how to set a maximum of five processor memory block header corruption corrections to occur every 30 seconds:

```
configure terminal
!
exception memory ignore overflow processor frequency 30 maxcount 5
end
```

Related Commands

Command	Description
show memory overflow	Displays the details of a memory block header corruption correction.

exception protocol

To configure the protocol used for core dumps, use the **exception protocol** command in global configuration mode. To configure the router to use the default protocol, use the **no**form of this command.

exception protocol {**ftp**| **rcp**| **tftp**}

no exception protocol

Syntax Description

ftp	Uses FTP for core dumps.
rcp	Uses rcp for core dumps.
tftp	Uses TFTP for core dumps. This is the default.

Command Default

TFTP

Command Modes

Global configuration

Command History

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

Usage Guidelin

Caution Use the **exception** commands only under the direction of a technical support representative. Creating a core dump while the router is functioning in a network can disrupt network operation. The resulting binary file, which is very large, must be transferred to a TFTP, FTP, or rcp server and subsequently interpreted by technical personnel that have access to source code and detailed memory maps.

If you use TFTP to dump the core file to a server, the router will only dump the first 16 MB of the core file. If the router's memory is larger than 16 MB, the whole core file will not be copied to the server. Therefore, use rcp or FTP to dump the core file.

Examples

In the following example, the user configures a router to use FTP to dump a core file to the FTP server at 172.17.92.2 when it crashes:

```
Router(config)# ip ftp username red
Router(config)# ip ftp password blue
```

```
Router(config)# exception protocol ftp
Router(config)# exception dump 172.17.92.2
```

Related Commands

Command	Description
exception core-file	Specifies the name of the core dump file.
exception dump	Causes the router to dump a core file to a particular server when the router crashes.
exception memory	Causes the router to create a core dump and reboot when certain memory size parameters are violated.
exception spurious-interrupt	Causes the router to create a core dump and reload after a specified number of spurious interrupts.
ip ftp password	Specifies the password to be used for FTP connections.
ip ftp username	Configures the username for FTP connections.

exception region-size

To specify the size of the region for the exception-time memory pool, use the **exception region-size**command in global configuration mode . To use the default region size, use the **no**form of this command.

exception region-size *size*

no exception region-size

Syntax Description

size	The size of the region for the exception-time memory pool.

Command Default

16,384 bytes

Command Modes

Global configuration

Command History

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

Usage Guidelin

Caution Use the **exception** commands only under the direction of a technical support representative. Creating a core dump while the router is functioning in a network can disrupt network operation. The resulting binary file, which is very large, must be transferred to a TFTP, FTP, or rcp server and subsequently interpreted by technical personnel that have access to source code and detailed memory maps.

The exception region-size command is used to define a small amount of memory to serve as a fallback pool when the processor memory pool is marked corrupt. The exception memory command must be used to allocate memory to perform a core dump.

Examples

In the following example, the region size is set at 1024:

```
Router(config)# exception region-size 1024
```

Related Commands

Command	Description
exception core-file	Specifies the name of the core dump file.

Command	Description
exception dump	Configures the router to dump a core file to a particular server when the router crashes.
exception memory	Causes the router to create a core dump and reboot when certain memory size parameters are violated.
exception protocol	Configures the protocol used for core dumps.
ip ftp password	Specifies the password to be used for FTP connections.
ip ftp username	Configures the username for FTP connections.

exception spurious-interrupt

To configure the router to create a core dump and reload after a specified number of spurious interrupts, use the exception spurious-interrupt command in global configuration mode . To disable the core dump and reload, use the no form of this command.

exception spurious-interrupt [*number*]

no exception spurious-interrupt

Syntax Description

number	(Optional) A number from 1 to 4294967295 that indicates the maximum number of spurious interrupts to include in the core dump before reloading.

Command Default

Disabled

Command Modes

Global configuration

Command History

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

Usage Guidelin

Caution Use the **exception** commands only under the direction of a technical support representative. Creating a core dump while the router is functioning in a network can disrupt network operation. The resulting binary file, which is very large, must be transferred to a TFTP, FTP, or rcp server and subsequently interpreted by technical personnel that have access to source code and detailed memory maps.

If you use TFTP to dump the core dump file to a server, the router will only dump the first 16 MB of the file. If the router's memory is larger than 16 MB, the whole core file will not be copied to the server. Therefore, use rcp or FTP to dump the core file.

Examples

In the following example, the user configures a router to create a core dump with a limit of two spurious interrupts:

```
Router(config)# exception spurious-interrupt 2
```

Related Commands

Command	Description
exception core-file	Specifies the name of the core dump file.
ip ftp password	Specifies the password to be used for FTP connections.
ip ftp username	Configures the user name for FTP connections.

guest ip address

To configure the remote-management IP address for the management virtual services container vNIC gateway interface, use the **guest ip address** command in virtual services container interface configuration mode. To remove the remote-managment IP address from the vNIC gateway interface, use the **no** form of this command.

guest ip address *remote-mgmt-ipv4-addr*

no guest ip address *remote-mgmt-ipv4-addr*

Syntax Description

remote-mgmt-ipv4-addr	Configures the remote-management IP address for the vNIC gateway interface for the management virtual services container.

Command Default

No default.

Command Modes

Virtual services container interface configuration

Command History

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

Usage Guidelines

This command is required when configuring the Cisco CSR 1000V to be remotely managed using the REST API or by Prime Network Services Controller.

Beginning with Cisco IOS XE Release 3.13S, if configuring the shared management interface, this command is not used for REST API support. However, it is still required if configuring REST API support using the dual management interface, or for remote management using Cisco Prime Network Services Controller.

Examples

The following example configures the IP guest address on a vNIC gateway interface:

```
router(config)# virtual-service csr_mgmt
router(config-virt-serv)# vnic gateway virtualportgroup 0vnic gateway virtualportgroup 0
router(config-virt-serv-intf) ip guest address 60.60.60.60
```

Related Commands

Command	Description
vnic gateway	Creates a virtual network interface card (vNIC) gateway interface fo the virtual services container.

Command	Description
virtual-service csr_mgmt	Configures the management virtual services container on the Cisco CSR 1000V and enters virtual services container configuration mode.

ip shared host-interface

To configure the shared management interface for REST API support on the Cisco CSR 1000V, use the **ip shared host-interface** command in virtual services configuration mode. To remove the shared management interface, use the **no** form of this command.

ip shared host-interface *mgmt-interface*

no ip shared host-interface *mgmt-interface*

Syntax Description

mgmt-interface	Enters the management IP interface.

Command Default

No default

Command Modes

Virtual Services configuration

Command History

Release	Modification
IOS XE 3.13S	This command was introduced on the Cisco CSR 1000V.

Usage Guidelines

This command is used when configuring REST API support on the Cisco CSR 1000V using the shared management interface. Using this command, you map the virtual services container to the management interface.

Examples

The following example maps the virtual services container to the shared Gigabit Ethernet 1 management interface and activates the virtual services container.

```
router(config)# virtual-service csr_mgmt
router(config-virt-serv)# no activate
router(config-virt-serv)# ip shared host-interface gigabitethernet 1
router(config-virt-serv)# activate
```

Related Commands

Command	Description
virtual-service csr_mgmt	Configures the management virtual services container on the Cisco CSR 1000V and enters virtual services container configuration mode.

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.