

exception core-file

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

exception core-file *filename*

no exception core-file

| | | |
|---------------------------|-----------------|---|
| Syntax Description | <i>filename</i> | Name of the core dump file saved on the server. |
|---------------------------|-----------------|---|

| | |
|-----------------|--|
| Defaults | The core file is named <i>hostname-core</i> , where <i>hostname</i> is the name of the router. |
|-----------------|--|

| | |
|----------------------|----------------------|
| Command Modes | Global configuration |
|----------------------|----------------------|

| | | |
|------------------------|----------------|------------------------------|
| Command History | Release | Modification |
| | 10.2 | This command was introduced. |

| | |
|-------------------------|--|
| 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. |
|-------------------------|--|



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 | In the following example, the router is configured to use FTP to dump a core file named <i>dumpfile</i> 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 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. |

| Command | Description |
|-------------------------------------|---|
| 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 buffersize, use the **no** form of this command.

exception crashinfo buffersize *kilobytes*

no exception crashinfo buffersize *kilobytes*

| | | |
|---------------------------|------------------|--|
| Syntax Description | <i>kilobytes</i> | Sets the size of the buffersize to the specified value within the range of 32 to 100 kilobytes. The default is 32KB. |
|---------------------------|------------------|--|

| | |
|-----------------|---------------------------|
| Defaults | Crashinfo buffer is 32KB. |
|-----------------|---------------------------|

| | |
|----------------------|----------------------|
| 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 (3620, 2640, and 3660 platforms). |
| 12.2(13)T | This command was implemented in 6400-NSP 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 switch 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). |
|-------------------------|--|

| | |
|-----------------|--|
| 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 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 | <i>device:filename</i> | Specifies the flash device and file name to be used for storing the diagnostic information. The colon is required. |
|---------------------------|------------------------|--|

| | |
|-----------------|---------|
| Defaults | Enabled |
|-----------------|---------|

| | |
|----------------------|----------------------|
| 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 6400-NSP 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 switch 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 <i>filename_yyyymmdd-hhmmss</i> , where <i>y</i> is year, <i>m</i> is month, <i>d</i> is date, <i>h</i> is hour, and <i>s</i> 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 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 | <i>ip-address</i> | IP address of the server that stores the core dump file. |
| Defaults | Disabled | |
| Command Modes | Global configuration | |
| Command History | Release | Modification |
| | 10.3 | This command was introduced. |

Usage Guidelines



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 <i>slot-number</i> | | 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 <i>filename</i> | | (Optional) Stores the crash information in the specified file in NVRAM. The default filename is <i>hostname-core-slot-number</i> (for example, <i>c12012-core-8</i>). |
| main-memory <i>size</i> | | (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 <i>size</i> | | (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 <i>size</i> | | (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. |
| tx-buffer <i>size</i> | | |
| sqe-register-rx | | (Optional) Stores crash information for the receive or transmit silicon queueing engine registers on the line card. |
| sqe-register-tx | | |
| k | | (Optional) The k option multiplies the specified <i>size</i> by 1K (1024), and the m option multiplies the specified <i>size</i> by 1M (1024*1024). |
| m | | |

Defaults

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). |

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 cause the router to create a core dump and reboot when certain memory size parameters are violated, use the **exception memory** command in global configuration mode. To disable the rebooting and core dump, use the **no** form of this command.

exception memory { *fragment size* | **minimum size** }

no exception memory { *fragment* | **minimum** }

| | | |
|--------------------|----------------------|--|
| Syntax Description | fragment size | The minimum contiguous block of memory in the free pool, in bytes. |
| | minimum size | The minimum size of the free memory pool, in bytes. |

Defaults Disabled

Command Modes Global configuration

| Command History | Release | Modification |
|-----------------|---------|------------------------------|
| | 10.3 | This command was introduced. |

Usage Guidelines This command is used to troubleshoot memory leaks. The size is checked every 60 seconds. If you enter a size that is greater than the free memory, a core dump and router reload is generated after 60 seconds.



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 dump** command must be configured in order to generate a core dump file. If the **exception dump** command is not configured, the router reloads without generating a core dump.

Examples In the following example, the user configures the router to monitor the free memory. If the amount of free memory falls below 250,000 bytes, the router will dump the core file and reload.

```
Router(config)# exception dump 131.108.92.2
Router(config)# exception core-file memory.overrun
Router(config)# exception memory minimum 250000
```

| Related Commands | Command | Description |
|------------------|------------------------------|---|
| | exception core-file | Specifies the name of the core dump 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 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 | Command | Description |
|--------------------|-------------|--|
| | ftp | Uses FTP for core dumps. |
| | rcp | Uses rcp for core dumps. |
| | tftp | Uses TFTP for core dumps. This is the default. |

Defaults TFTP

Command Modes Global configuration

| Command History | Release | Modification |
|-----------------|---------|------------------------------|
| | 10.3 | This command was introduced. |

Usage Guidelines



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 | <i>size</i> | The size of the region for the exception-time memory pool. |
|---------------------------|-------------|--|

| | |
|-----------------|--------------|
| Defaults | 16,384 bytes |
|-----------------|--------------|

| | |
|----------------------|----------------------|
| Command Modes | Global configuration |
|----------------------|----------------------|

| Command History | Release | Modification |
|------------------------|---------|------------------------------|
| | 10.3 | This command was introduced. |

Usage Guidelines



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. |
| | 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. |

| Command | Description |
|------------------------|--|
| 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 | <i>number</i> | (Optional) A number from 1 to 4294967295 that indicates the maximum number of spurious interrupts to include in the core dump before reloading. |
|---------------------------|---------------|---|

| | |
|-----------------|----------|
| Defaults | Disabled |
|-----------------|----------|

| | |
|----------------------|----------------------|
| Command Modes | Global configuration |
|----------------------|----------------------|

| | | |
|------------------------|----------------|------------------------------|
| Command History | Release | Modification |
| | 10.3 | This command was introduced. |

Usage Guidelines



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. |

exec

To allow an EXEC process on a line, use the **exec** command in line configuration mode. To turn off the EXEC process for the specified line, use the **no** form of this command.

exec

no exec

Syntax Description This command has no arguments or keywords.

Defaults The EXEC processes is enabled on all lines.

Command Modes Line configuration

| Command History | Release | Modification |
|-----------------|---------|------------------------------|
| | 10.0 | This command was introduced. |

Usage Guidelines When you want to allow only an outgoing connection on a line, use the **no exec** command. The **no exec** command allows you to disable the EXEC process for connections which may attempt to send unsolicited data to the router. (For example, the control port of a rack of modems attached to an auxiliary port of router.) When certain types of data are sent to a line connection, an EXEC process can start, which makes the line unavailable.

When a user tries to Telnet to a line with the EXEC process disabled, the user will get no response when attempting to log on.

Examples The following example disables the EXEC process on line 7.

```
Router(config)# line 7
Router(config-line)# no exec
```

exec-banner

To reenable the display of EXEC and message-of-the-day (MOTD) banners on the specified line or lines, use the **exec-banner** command in line configuration mode. To suppress the banners on the specified line or lines, use the **no** form of this command.

exec-banner

no exec-banner

Syntax Description This command has no arguments or keywords.

Defaults Enabled on all lines

Command Modes Line configuration

| Command History | Release | Modification |
|-----------------|---------|------------------------------|
| | 10.0 | This command was introduced. |

Usage Guidelines This command determines whether the router will display the EXEC banner and the message-of-the-day (MOTD) banner when an EXEC session is created. These banners are defined with the **banner exec** and **banner motd** global configuration commands. By default, these banner are enabled on all lines. Disable the EXEC and MOTD banners using the **no exec-banner** command.

This command has no effect on the incoming banner, which is controlled by the **banner incoming** command.

The MOTD banners can also be disabled by the **no motd-banner** line configuration command, which disables MOTD banners on a line. If the **no exec-banner** command is configured on a line, the MOTD banner will be disabled regardless of whether the **motd-banner** command is enabled or disabled. [Table 24](#) summarizes the effects of the **exec-banner** command and the **motd-banner** command.

Table 24 Banners Displayed Based On exec-banner and motd-banner Combinations

| | exec-banner (default) | no exec-banner |
|------------------------------|-----------------------|----------------|
| | MOTD banner | None |
| motd-banner (default) | EXEC banner | |
| no motd-banner | EXEC banner | None |

For reverse Telnet connections, the EXEC banner is never displayed. Instead, the incoming banner is displayed. The MOTD banner is displayed by default, but it is disabled if either the **no exec-banner** command or **no motd-banner** command is configured. [Table 25](#) summarizes the effects of the **exec-banner** command and the **motd-banner** command for reverse Telnet connections.

Table 25 *Banners Displayed Based On exec-banner and motd-banner Combinations for Reverse Telnet Sessions to Async Lines*

| | exec-banner (default) | no exec-banner |
|------------------------------|-----------------------|-----------------|
| | MOTD banner | Incoming banner |
| motd-banner (default) | Incoming banner | |
| no motd-banner | Incoming banner | Incoming banner |

Examples

The following example suppresses the EXEC and MOTD banners on virtual terminal lines 0 to 4:

```
Router(config)# line vty 0 4
Router(config-line)# no exec-banner
```

Related Commands

| Command | Description |
|------------------------|--|
| banner exec | Defines and enables a customized banner to be displayed whenever the EXEC process is initiated. |
| banner incoming | Defines and enables a customized message to be displayed when there is an incoming connection to a terminal line from a host on the network. |
| banner motd | Defines and enables a customized message-of-the-day banner. |
| motd-banner | Controls (enables or disables) the display of message-of-the-day banners on a specified line or lines. |

exec-character-bits

To configure the character widths of EXEC and configuration command characters, use the **exec-character-bits** command in line configuration mode. To restore the default value, use the **no** form of this command.

exec-character-bits {7 | 8}

no exec-character-bits

Syntax Description

| | |
|----------|--|
| 7 | Selects the 7-bit character set. This is the default. |
| 8 | Selects the full 8-bit character set for use of international and graphical characters in banner messages, prompts, and so on. |

Defaults

7-bit ASCII character set

Command Modes

Line configuration

Command History

| Release | Modification |
|---------|------------------------------|
| 10.0 | This command was introduced. |

Usage Guidelines

Setting the EXEC character width to 8 allows you to use special graphical and international characters in banners, prompts, and so on. However, setting the EXEC character width to 8 bits can cause failures. If a user on a terminal that is sending parity enters the **help** command, an “unrecognized command” message appears because the system is reading all 8 bits, and the eighth bit is not needed for the **help** command.



Note

If you are using the **autoselect** function, set the activation character to the default (Return) and the value for **exec-character-bits** to 7. If you change these defaults, the application will not recognize the activation request.

Examples

The following example enables full 8-bit international character sets, except for the console, which is an ASCII terminal. It illustrates use of the **default-value exec-character-bits** global configuration command and the **exec-character-bits** line configuration command.

```
Router(config)# default-value exec-character-bits 8
Router(config)# line 0
Router(config-line)# exec-character-bits 7
```

Related Commands

| Command | Description |
|---|--|
| default-value exec-character-bits | Defines the EXEC character width for either 7 bits or 8 bits. |
| default-value special-character-bits | Configures the flow control default value from a 7-bit width to an 8-bit width. |
| length | Sets the terminal screen length. |
| terminal exec-character-bits | Locally changes the ASCII character set used in EXEC and configuration command characters for the current session. |
| terminal special-character-bits | Changes the ASCII character widths to accept special characters for the current terminal line and session. |

exec-timeout

To set the interval that the EXEC command interpreter waits until user input is detected, use the **exec-timeout** command in line configuration mode. To remove the timeout definition, use the **no** form of this command.

exec-timeout *minutes* [*seconds*]

no exec-timeout

| Syntax Description | <i>minutes</i> | Integer that specifies the number of minutes. The default is 10 minutes. |
|--------------------|----------------|--|
| | <i>seconds</i> | (Optional) Additional time intervals in seconds. |

| Defaults | 10 minutes |
|----------|------------|
|----------|------------|

| Command Modes | Line configuration |
|---------------|--------------------|
|---------------|--------------------|

| Command History | Release | Modification |
|-----------------|---------|------------------------------|
| | 10.0 | This command was introduced. |

| Usage Guidelines | If no input is detected during the interval, the EXEC facility resumes the current connection. If no connections exist, the EXEC facility returns the terminal to the idle state and disconnects the incoming session. |
|------------------|--|
|------------------|--|

To specify no timeout, enter the **exec-timeout 0 0** command.

| Examples | The following example sets a time interval of 2 minutes, 30 seconds: |
|----------|--|
|----------|--|

```
Router(config)# line console
Router(config-line)# exec-timeout 2 30
```

The following example sets a time interval of 10 seconds:

```
Router(config)# line console
Router(config-line)# exec-timeout 0 10
```

execute-on

To execute commands on a line card, use the **execute-on** command in privileged EXEC mode.

execute-on {**slot** *slot-number* | **all** | **master**} *command*

| Syntax Description | | |
|--------------------------------|--|---|
| slot <i>slot-number</i> | Executes the command on the line card in the specified slot. Slot numbers can be chosen from the following ranges: | <ul style="list-style-type: none"> • Cisco 12012 router: 0 to 11 • Cisco 12008 access server: 0 to 7 • Cisco AS5800 access server: 0 to 13 |
| all | Executes the command on all line cards. | |
| master | (AS5800 only) Executes the designated command on a Dial Shelf Controller (DSC). Do not use this option; it is used for technical support troubleshooting only. | |
| <i>command</i> | Cisco IOS command to remotely execute on the line card. | |

Command Modes Privileged EXEC

| Command History | Release | Modification |
|-----------------|-----------|---|
| | 11.2 GS | This command was introduced to support Cisco 12000 series Gigabit Switch Routers. |
| | 11.3(2)AA | This command was implemented in images for the Cisco AS5800 series. |

Usage Guidelines Use this command to execute a command on one or all line cards to monitor and maintain information on one or more line cards (for example, a line card in a specified slot on a dial shelf). This allows you to issue commands remotely; that is, to issue commands without needing to log in to the line card directly. The **all** form of the command allows you to issue commands to all the line cards without having to log in to each in turn.

Though this command does not have a **no** form, note that it is possible to use the **no** form of the remotely executed commands used in this command.



Tips

This command is useful when used with **show EXEC** commands (such as **show version**), because you can verify and troubleshoot the features found only on a specific line card. Please note, however, that because not all statistics are maintained on the line cards, the output from some of the **show** commands might not be consistent.

Cisco 12000 GSR Guidelines and Restrictions

You can use the **execute-on** privileged EXEC command only from Cisco IOS software running on the GRP card.

**Timesaver**

Though you can use the **attach** privileged EXEC command to execute commands on a specific line card, using the **execute-on slot** command saves you some steps. For example, first you must use the **attach** command to connect to the Cisco IOS software running on the line card. Next you must issue the command. Finally you must disconnect from the line card to return to the Cisco IOS software running on the GRP card. With the **execute-on slot** command, you can perform three steps with one command. In addition, the **execute-on all** command allows you to perform the same command on all line cards simultaneously.

Cisco AS5800 Guidelines and Restrictions

The purpose of the command is to conveniently enable certain commands to be remotely executed on the dial shelf cards from the router without connecting to each line card. This is the recommended procedure, because it avoids the possibility of adversely affecting a good configuration of a line card in the process. The **execute-on** command does not give access to every Cisco IOS command available on the Cisco AS5800 access server. In general, the purpose of the **execute-on** command is to provide access to statistical reports from line cards without directly connecting to the dial shelf line cards.

**Caution**

Do not use this command to change configurations on dial shelf cards, because such changes will not be reflected in the router shelf.

Using this command makes it possible to accumulate inputs for inclusion in the **show tech-support** command.

The **master** form of the command can run a designated command remotely on the router from the DSC card. However, using the console on the DSC is *not* recommended. It is used for technical support troubleshooting only.

The **show tech-support** command for each dial shelf card is bundled into the router shelf's **show tech-support** command via the **execute-on** facility.

The **execute-on** command also support interactive commands such as the following:

```
router: execute-on slave slot slot ping
```

The **execute-on** command has the same limitations and restrictions as a **vty telnet** client has; that is, it cannot reload DSC using the following command:

```
router: execute-on slave slot slot reload
```

You can use the **execute-on** command to enable remote execution of the commands included in the following partial list:

- **debug dsc clock**
- **show context**
- **show diag**
- **show environment**
- **show dsc clock**
- **show dsi**
- **show dsip**
- **show tech-support**

Examples

In the following example, the user executes the **show controllers** command on the line card in slot 4 of a Cisco 12000 series GSR:

```
Router# execute-on slot 4 show controllers
```

```
===== Line Card (Slot 4) =====
```

```
Interface POS0
Hardware is BFLC POS
lcpos_instance struct    6033A6E0
RX POS ASIC addr space  12000000
TX POS ASIC addr space  12000100
SUNI framer addr space  12000400
SUNI rsop intr status   00
CRC16 enabled, HDLC enc, int clock
no loop
```

```
Interface POS1
Hardware is BFLC POS
lcpos_instance struct    6033CEC0
RX POS ASIC addr space  12000000
TX POS ASIC addr space  12000100
SUNI framer addr space  12000600
SUNI rsop intr status   00
CRC32 enabled, HDLC enc, int clock
no loop
```

```
Interface POS2
Hardware is BFLC POS
lcpos_instance struct    6033F6A0
RX POS ASIC addr space  12000000
TX POS ASIC addr space  12000100
SUNI framer addr space  12000800
SUNI rsop intr status   00
CRC32 enabled, HDLC enc, int clock
no loop
```

```
Interface POS3
Hardware is BFLC POS
lcpos_instance struct    60341E80
RX POS ASIC addr space  12000000
TX POS ASIC addr space  12000100
SUNI framer addr space  12000A00
SUNI rsop intr status   00
CRC32 enabled, HDLC enc, ext clock
no loop
Router#
```

Related Commands

| Command | Description |
|---------------|--|
| attach | Connects you to a specific line card for the purpose of executing commands using the Cisco IOS software image on that line card. |

exit (EXEC)

To close an active terminal session by logging off the router, use the **exit** command in EXEC mode.

exit

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes EXEC

| Command History | Release | Modification |
|-----------------|---------|------------------------------|
| | 10.0 | This command was introduced. |

Usage Guidelines Use the **exit** command in EXEC mode to exit the active session (log off the device). This command can be used in any EXEC mode (such as User EXEC mode or Privileged EXEC mode) to exit from the EXEC process.

Examples In the following example, the **exit** (global) command is used to move from global configuration mode to privileged EXEC mode, the **disable** command is used to move from privileged EXEC mode to user EXEC mode, and the **exit** (EXEC) command is used to log off (exit the active session):

```
Router(config)# exit
Router# disable
Router> exit
```

| Related Commands | Command | Description |
|------------------|----------------------|---|
| | disconnect | Disconnects a line. |
| | end | Ends your configuration session by exiting to EXEC mode. |
| | exit (global) | Exits from the current configuration mode to the next highest configuration mode. |
| | logout | Closes your connection to the device (equivalent to the exit command). |

exit (global)

To exit any configuration mode to the next highest mode in the CLI mode hierarchy, use the **exit** command in any configuration mode.

exit

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes All configuration modes

| Command History | Release | Modification |
|-----------------|---------|------------------------------|
| | 10.0 | This command was introduced. |

Usage Guidelines The **exit** command is used in the Cisco IOS CLI to exit from the current command mode to the next highest command mode in the CLI mode hierarchy.

For example, use the **exit** command in global configuration mode to return to privileged EXEC mode. Use the **exit** command in interface, line, or router configuration mode to return to global configuration mode. Use the **exit** command in subinterface configuration mode to return to interface configuration mode. At the highest level, EXEC mode, the **exit** command will exit the EXEC mode and disconnect from the router interface (see the description of the **exit (EXEC)** command for details).

Examples The following example shows how to exit from the subinterface configuration mode and to return to the interface configuration mode:

```
Router(config-subif)# exit
Router(config-if)#
```

The following example displays an exit from the interface configuration mode to return to the global configuration mode:

```
Router(config-if)# exit
Router(config)#
```

| Related Commands | Command | Description |
|------------------|--------------------|---|
| | disconnect | Disconnects a line. |
| | end | Ends your configuration session by exiting to privileged EXEC mode. |
| | exit (EXEC) | Closes the active terminal session by logging off the router. |

file prompt

To specify the level of prompting, use the **file prompt** command in global configuration mode.

file prompt [**alert** | **noisy** | **quiet**]

| Syntax Description | Parameter | Description |
|--------------------|--------------|---|
| | alert | (Optional) Prompts only for destructive file operations. This is the default. |
| | noisy | (Optional) Confirms all file operation parameters. |
| | quiet | (Optional) Seldom prompts for file operations. |

Defaults alert

Command Modes Global configuration

| Command History | Release | Modification |
|-----------------|---------|------------------------------|
| | 11.0 | This command was introduced. |

Usage Guidelines Use this command to change the amount of confirmation needed for different file operations. This command affects only prompts for confirmation of operations. The router will always prompt for missing information.

Examples The following example configures confirmation prompting for all file operations:

```
Router(config)# file prompt noisy
```

filter-for-history

To define the type of information kept in the history table for an Service Assurance Agent (SAA) operation, use the **filter-for-history** command in SAA RTR configuration mode. To return to the default value, use the **no** form of this command.

filter-for-history { **none** | **all** | **overThreshold** | **failures** }

no filter-for-history { **none** | **all** | **overThreshold** | **failures** }

Syntax Description

| | |
|----------------------|---|
| none | No history kept. This is the default. |
| all | All operation operations attempted are kept in the history table. |
| overThreshold | Only packets that are over the threshold are kept in the history table. |
| failures | Only packets that fail for any reason are kept in the history table. |

Defaults

No SAA history is kept for an operation.

Command Modes

SAA RTR configuration
 SAA DHCP Configuration (config-rtr-dhcp)
 SAA Echo configuration (config-rtr-echo)

Command History

| Release | Modification |
|---------|------------------------------|
| 11.2 | This command was introduced. |

Usage Guidelines

Use the **filter-for-history** command to control what gets stored in the history table for the SAA. To control how much history gets saved in the history table, use the **lives-of-history-kept**, **buckets-of-history-kept**, and the **samples-of-history-kept** SAA RTR configuration commands.

An operation can collect history and capture statistics. By default, history is not collected. When a problem arises where history is useful (for example, a large number of timeouts are occurring), you can configure the **lives-of-history-kept** command to collect history.



Note

Collecting history increases the RAM usage. Only collect history when you think there is a problem. For general network response time information, use statistics.

Examples

In the following example, only operation packets that fail are kept in the history table:

```
Router(config)# rtr 1
Router(config-rtr)# type echo protocol ipIcmpEcho 172.16.161.21
Router(config-rtr)# lives-of-history-kept 1
Router(config-rtr)# filter-for-history failures
```

| Related Commands | Command | Description |
|------------------|--------------------------------|--|
| | buckets-of-history-kept | Sets the number of history buckets that are kept during the lifetime of the SAA. |
| | lives-of-history-kept | Sets the number of lives maintained in the history table for the SAA operation. |
| | rtr | Specifies an SAA operation and enters SAA RTR configuration mode. |
| | samples-of-history-kept | Sets the number of entries kept in the history table per bucket for the SAA operation. |

format

To format a Class A or Class C Flash file system, use the **format** command in EXEC mode.

Class C Flash File System

format *filesystem1*:

Class A Flash File System

format [**spare** *spare-number*] *filesystem1*: [[*filesystem2*:][*monlib-filename*]]



Caution

Reserve a certain number of memory sectors as spares, so that if some sectors fail, most of the Flash memory card can still be used. Otherwise, you must reformat the Flash card when some of the sectors fail.

Syntax Description

| | |
|------------------------|---|
| spare | (Optional) Reserves spare sectors as specified by the <i>spare-number</i> argument when formatting Flash memory. |
| <i>spare-number</i> | (Optional) Number of the spare sectors to reserve on formatted Flash memory. Valid values are from 0 to 16. The default value is zero. |
| <i>filesystem1</i> : | Flash memory to format, followed by a colon. |
| <i>filesystem2</i> : | (Optional) File system containing the monlib file to use for formatting <i>filesystem1</i> followed by a colon. |
| <i>monlib-filename</i> | (Optional) Name of the ROM monitor library file (monlib file) to use for formatting the <i>filesystem1</i> argument. The default monlib file is the one bundled with the system software. When used with HSA and you do not specify the <i>monlib-filename</i> argument, the system takes ROM monitor library file from the slave image bundle. If you specify the <i>monlib-filename</i> argument, the system assumes that the files reside on the slave devices. |

Defaults

The default monlib file is the one bundled with the system software.

The default number of spare sectors is zero (0).

Command Modes

EXEC

Command History

| Release | Modification |
|---------|------------------------------|
| 11.0 | This command was introduced. |

Usage Guidelines

Use this command to format Class A or C Flash memory file systems.

In some cases, you might need to insert a new PCMCIA Flash memory card and load images or backup configuration files onto it. Before you can use a new Flash memory card, you must format it.

Sectors in Flash memory cards can fail. Reserve certain Flash memory sectors as “spares” by using the optional *spare* argument on the **format** command to specify 0 to 16 sectors as spares. If you reserve a small number of spare sectors for emergencies, you can still use most of the Flash memory card. If you specify 0 spare sectors and some sectors fail, you must reformat the Flash memory card, thereby erasing all existing data.

The monlib file is the ROM monitor library. The ROM monitor uses this file to access files in the Flash file system. The Cisco IOS system software contains a monlib file.

In the command syntax, *filesystem1*: specifies the device to format and *filesystem2*: specifies the optional device containing the monlib file used to format *filesystem1*:. If you omit the optional *filesystem2*: and *monlib-filename* arguments, the system formats *filesystem1*: using the monlib file already bundled with the system software. If you omit only *the optional filesystem2*: argument, the system formats *filesystem1*: using the monlib file from the device you specified with the **cd** command. If you omit only the optional *monlib-filename* argument, the system formats *filesystem1*: using the *filesystem2*: monlib file. When you specify both arguments—*filesystem2*: and *monlib-filename*—the system formats *filesystem1*: using the monlib file from the specified device. You can specify *filesystem1*:’s own monlib file in this argument. If the system cannot find a monlib file, it terminates its formatting.



Note

You can read from or write to Flash memory cards formatted for Cisco 7000 series Route Processor (RP) cards in your Cisco 7200 and 7500 series routers, but you cannot boot the Cisco 7200 and 7500 series routers from a Flash memory card formatted for the Cisco 7000 series routers. Similarly, you can read from or write to Flash memory cards formatted for the Cisco 7200 and 7500 series routers in your Cisco 7000 series routers, but you cannot boot the Cisco 7000 series routers from a Flash memory card formatted for the Cisco 7200 and 7500 series routers.

Examples

The following example formats a Flash memory card inserted in slot 0:

```
Router# format slot0:

Running config file on this device, proceed? [confirm]y
All sectors will be erased, proceed? [confirm]y
Enter volume id (up to 31 characters): <Return>
Formatting sector 1 (erasing)
Format device slot0 completed
```

When the console returns to the EXEC prompt, the new Flash memory card is formatted and ready for use.

Related Commands

| Command | Description |
|--------------------------|---|
| cd | Changes the default directory or file system. |
| copy | Copies any file from a source to a destination. |
| delete | Deletes a file on a Flash memory device. |
| show file systems | Lists available file systems. |
| squeeze | Permanently deletes Flash files by squeezing a Class A Flash file system. |
| undelete | Recovers a file marked “deleted” on a Class A or Class B Flash file system. |

frequency

To set the rate at which a specified SAA operation is sent into the network, use the **frequency** command in SAA RTR configuration mode. To return to the default value, use the **no** form of this command.

frequency *seconds*

no frequency

| Syntax Description | <i>seconds</i> | Number of seconds between the SAA probe operations. |
|--------------------|----------------|---|
|--------------------|----------------|---|

| Defaults | 60 seconds |
|----------|------------|
|----------|------------|

| Command Modes | SAA RTR configuration |
|---------------|-----------------------|
|---------------|-----------------------|

| Command History | Release | Modification |
|-----------------|---------|------------------------------|
| | 11.2 | This command was introduced. |

Usage Guidelines If an individual SAA operational probe takes longer to execute than the specified frequency value, a statistics counter called “busy” is incremented rather than sending a second probe.



Note

We recommend that you do not set the frequency value to less than 60 seconds for the following reasons: It is not needed when keeping statistics (the default), and it can slow down the WAN because of the potential overhead that numerous operations can cause.

The value specified for the **frequency** command cannot be less than the value specified for the **timeout** SAA RTR configuration command.

Examples The following example configures SAA IP/ICMP Echo operation 1 to send a probe every 90 seconds:

```
Router(config)# rtr 1
Router(config-rtr)# type echo protocol ipIcmpEcho 172.16.1.176
Router(config-rtr)# frequency 90
```

| Related Commands | Command | Description |
|------------------|----------------|---|
| | rtr | Specifies an SAA operation and enters SAA RTR configuration mode. |
| | timeout | Sets the amount of time the SAA operation waits for a response from its request packet. |

fsck

To check a File Allocation Table (FAT)-based disk or Class C filesystem for damage and to repair any problems, use the **fsck** command in privileged EXEC mode.

fsck [**/nocrc**] *filesystem:* [**/automatic**]

| Syntax Description | | |
|--------------------|---|--|
| /nocrc | (Optional. This keyword is available for Class C Flash file systems only.) Omits cyclic redundancy checks (CRCs). | |
| <i>filesystem:</i> | The filesystem prefix indicating the disk to be checked. The colon (:) is required. Typically, the filesystem prefix will be disk0: or disk1: . | |
| /automatic | (Optional. This keyword is available for ATA FAT-based disks only.) Specifies that the check and repair actions should proceed automatically. This option can be used to skip the prompts for each check and repair action. | |

Defaults If the **/automatic** keyword is not used, CLI prompts for actions are issued.

Command Modes Privileged EXEC

| Command History | Release | Modification |
|-----------------|----------------------|--|
| | 11.3 AA | This command was introduced. |
| | 12.2(13)T, 12.0(22)S | This command was implemented on the Cisco 7000 family of routers and on the Cisco 10000 and 12000 series to support ATA disks. |

Usage Guidelines This command will perform all of the steps necessary to remove corrupted files and reclaim unused disk space. Changes include checking for incorrect file sizes, cluster loops, and so on. The default form of this command will issue multiple prompts to confirm each of the changes. However, you can skip these prompts by using the **/automatic** keyword when issuing the command.

When the **/automatic** keyword is used you will be prompted to confirm that you want the automatic option. Prompts for actions will be skipped, but all actions performed will be displayed to the terminal (see the example below).

This command works with ATA PCMCIA cards formatted in DOS, or for Class C Flash file systems.



Note

Only one partition (the active partition) will be checked in the ATA disk.

Examples The following example shows sample output from using the **fsck** command in automatic mode:

```
Router# fsck /automatic disk1:
Proceed with the automatic mode? [yes] y
Checking the boot sector and partition table...
Checking FAT, Files and Directories...
```

```
Start cluster of file disk1:/file1 is invalid, removing file
File disk1:/file2 has a free/bad cluster, truncating...
File disk1:/file2 truncated.
File disk1:/file3 has a free/bad cluster, truncating...
File disk1:/file3 truncated.
File disk1:/file4 has a invalid cluster, truncating...
File disk1:/file4 truncated.
File disk1:/file5 has a invalid cluster, truncating...
File disk1:/file5 truncated.
File disk1:/file6 has a invalid cluster, truncating...
File disk1:/file6 truncated.
File size of disk1:/file7 is not correct, correcting it
File disk1:/file8 cluster chain has a loop, truncating it
File disk1:/file8 truncated.
File disk1:/file9 cluster chain has a loop, truncating it
File disk1:/file9 truncated.
File disk1:/file16 has a free/bad cluster, truncating...
File disk1:/file16 truncated.
File disk1:/file20 has a free/bad cluster, truncating...
File disk1:/file20 truncated.
Reclaiming unused space...
Created file disk1:/fsck-4 for an unused cluster chain
Created file disk1:/fsck-41 for an unused cluster chain
Created file disk1:/fsck-73 for an unused cluster chain
Created file disk1:/fsck-106 for an unused cluster chain
Created file disk1:/fsck-121 for an unused cluster chain
Created file disk1:/fsck-132 for an unused cluster chain
Created file disk1:/fsck-140 for an unused cluster chain
Created file disk1:/fsck-156 for an unused cluster chain
Created file disk1:/fsck-171 for an unused cluster chain
Created file disk1:/fsck-186 for an unused cluster chain
Created file disk1:/fsck-196 for an unused cluster chain
Created file disk1:/fsck-235 for an unused cluster chain
Created file disk1:/fsck-239 for an unused cluster chain
Updating FAT...
fsck of disk1: complete
```

full-help

To get help for the full set of user-level commands, use the **full-help** command in line configuration mode.

full-help

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes Line configuration

| Command History | Release | Modification |
|-----------------|---------|------------------------------|
| | 10.0 | This command was introduced. |

Usage Guidelines The **full-help** command enables (or disables) an unprivileged user to see all of the help messages available. It is used with the **show ?** command.

Examples In the following example, the **show ?** command is used first with full-help disabled. Then **full-help** is enabled for the line, and the **show ?** command is used again to demonstrate the additional help output that is displayed.

```
Router> show ?

bootflash  Boot Flash information
calendar   Display the hardware calendar
clock      Display the system clock
context    Show context information
dialer     Dialer parameters and statistics
history    Display the session command history
hosts      IP domain-name, lookup style, nameservers, and host table
isdn       ISDN information
kerberos   Show Kerberos Values
modemcap   Show Modem Capabilities database
ppp        PPP parameters and statistics
rmon       rmon statistics
sessions   Information about Telnet connections
snmp       snmp statistics
terminal   Display terminal configuration parameters
users      Display information about terminal lines
version    System hardware and software status

Router> enable
Password:<letmein>

Router# configure terminal
```

```

Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# line console 0
Router(config-line)# full-help
Router(config-line)# exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router# disable
Router> show ?

  access-expression  List access expression
  access-lists       List access lists
  aliases            Display alias commands
  apollo             Apollo network information
  appletalk          AppleTalk information
  arp                ARP table
  async              Information on terminal lines used as router interfaces
  bootflash          Boot Flash information
  bridge             Bridge Forwarding/Filtering Database [verbose]
  bsc                BSC interface information
  bstun              BSTUN interface information
  buffers            Buffer pool statistics
  calendar           Display the hardware calendar
  .
  .
  .
  translate          Protocol translation information
  ttycap             Terminal capability tables
  users              Display information about terminal lines
  version            System hardware and software status
  vines              VINES information
  vlans              Virtual LANs Information
  whoami             Info on current tty line
  x25                X.25 information
  xns                XNS information
  xremote            XRemote statistics

```

Related Commands

| Command | Description |
|-------------|--|
| help | Displays a brief description of the help system. |

help

To display a brief description of the help system, use the **help** command in any command mode.

help

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

Command Modes User EXEC
Privileged EXEC
All configuration modes

| Command History | Release | Modification |
|-----------------|---------|------------------------------|
| | 10.0 | This command was introduced. |

Usage Guidelines The **help** command provides a brief description of the context-sensitive help system, which functions as follows:

- To list all commands available for a particular command mode, enter a question mark (?) at the system prompt.
- To obtain a list of commands that begin with a particular character string, enter the abbreviated command entry immediately followed by a question mark (?). This form of help is called *word help*, because it lists only the keywords or arguments that begin with the abbreviation you entered.
- To list the keywords and arguments associated with a command, enter a question mark (?) in place of a keyword or argument on the command line. This form of help is called *command syntax help*, because it lists the keywords or arguments that apply based on the command, keywords, and arguments you have already entered.

Examples In the following example, the **help** command is used to display a brief description of the help system:

```
Router# help
```

```
Help may be requested at any point in a command by entering
a question mark '?'. If nothing matches, the help list will
be empty and you must backup until entering a '?' shows the
available options.
```

```
Two styles of help are provided:
```

1. Full help is available when you are ready to enter a command argument (e.g. 'show ?') and describes each possible argument.
2. Partial help is provided when an abbreviated argument is entered and you want to know what arguments match the input (e.g. 'show pr?'.)

The following example shows how to use word help to display all the privileged EXEC commands that begin with the letters “co.” The letters entered before the question mark are reprinted on the next command line to allow the user to continue entering the command.

```
Router# co?
configure connect copy
Router# co
```

The following example shows how to use command syntax help to display the next argument of a partially complete **access-list** command. One option is to add a wildcard mask. The <cr> symbol indicates that the other option is to press Enter to execute the command without adding any more keywords or arguments. The characters entered before the question mark are reprinted on the next command line to allow the user to continue entering the command or to execute that command as it is.

```
Router(config)# access-list 99 deny 131.108.134.234 ?
A.B.C.D Mask of bits to ignore
<cr>
Router(config)# access-list 99 deny 131.108.134.234
```

Related Commands

| Command | Description |
|------------------|--|
| full-help | Enables help for the full set of user-level commands for a line. |

history

To enable the command history function, use the **history** command in line configuration mode. To disable the command history function, use the **no** form of this command.

history

no history

Syntax Description This command has no arguments or keywords.

Defaults Enabled with ten command lines in the buffer.

Command Modes Line configuration

| Command History | Release | Modification |
|-----------------|---------|------------------------------|
| | 10.0 | This command was introduced. |

Usage Guidelines

The command history function provides a record of EXEC commands that you have entered. This function is particularly useful for recalling long or complex commands or entries, including access lists.

To change the number of command lines that the system will record in its history buffer, use the **history size** line configuration command.

The **history** command enables the history function with the last buffer size specified or, if there was not a prior setting, with the default of ten lines. The **no history** command disables the history function.

The **show history** EXEC command will list the commands you have entered, but you can also use your keyboard to display individual commands. [Table 26](#) lists the keys you can use to recall commands from the command history buffer.

Table 26 History Keys

| Key(s) | Functions |
|-----------------------------------|--|
| Ctrl-P or Up Arrow ¹ | Recalls commands in the history buffer in a backward sequence, beginning with the most recent command. Repeat the key sequence to recall successively older commands. |
| Ctrl-N or Down Arrow ¹ | Returns to more recent commands in the history buffer after recalling commands with Ctrl-P or the Up Arrow. Repeat the key sequence to recall successively more recent commands. |

1. The arrow keys function only with ANSI-compatible terminals.

Examples

In the following example, the command history function is disabled on line 4:

```
Router(config)# line 4
Router(config-line)# no history
```

Related Commands

| Command | Description |
|-------------------------|---|
| history size | Sets the command history buffer size for a particular line. |
| show history | Lists the commands you have entered in the current EXEC session. |
| terminal history | Enables the command history function for the current terminal session or changes the size of the command history buffer for the current terminal session. |

history size

To change the command history buffer size for a particular line, use the **history size** command in line configuration mode. To reset the command history buffer size to ten lines, use the **no** form of this command.

history size *number-of-lines*

no history size

| | | |
|---------------------------|------------------------|---|
| Syntax Description | <i>number-of-lines</i> | Specifies the number of command lines that the system will record in its history buffer. The range is from 0 to 256. The default is 10. |
|---------------------------|------------------------|---|

| | |
|-----------------|------------------|
| Defaults | 10 command lines |
|-----------------|------------------|

| | |
|----------------------|--------------------|
| Command Modes | Line configuration |
|----------------------|--------------------|

| | | |
|------------------------|----------------|------------------------------|
| Command History | Release | Modification |
| | 10.0 | This command was introduced. |

Usage Guidelines The **history size** command should be used in conjunction with the **history** and **show history** commands. The **history** command enables or disables the command history function. The **show history** command lists the commands you have entered in the current EXEC session. The number of commands that the history buffer will show is set by the **history size** command.



Note

The **history size** command only sets the size of the buffer; it does not reenables the history function. If the **no history** command is used, the **history** command must be used to reenables this function.

Examples The following example displays line 4 configured with a history buffer size of 35 lines:

```
Router(config)# line 4
Router(config-line)# history size 35
```

| | | |
|-------------------------|------------------------------|---|
| Related Commands | Command | Description |
| | history | Enables or disables the command history function. |
| | show history | Lists the commands you have entered in the current EXEC session. |
| | terminal history size | Enables the command history function for the current terminal session or changes the size of the command history buffer for the current terminal session. |

hold-character

To define the local hold character used to pause output to the terminal screen, use the **hold-character** command in line configuration mode. To restore the default, use the **no** form of this command.

hold-character *ascii-number*

no hold-character

| | | |
|---------------------------|---------------------|--|
| Syntax Description | <i>ascii-number</i> | ASCII decimal representation of a character or control sequence (for example, Ctrl-P). |
|---------------------------|---------------------|--|

| | |
|-----------------|-------------------------------|
| Defaults | No hold character is defined. |
|-----------------|-------------------------------|

| | |
|----------------------|--------------------|
| Command Modes | Line configuration |
|----------------------|--------------------|

| | | |
|------------------------|----------------|------------------------------|
| Command History | Release | Modification |
| | 10.0 | This command was introduced. |

| | |
|-------------------------|--|
| Usage Guidelines | The Break character is represented by zero; NULL cannot be represented. To continue the output, enter any character after the hold character. To use the hold character in normal communications, precede it with the escape character. See the “ASCII Character Set” appendix for a list of ASCII characters. |
|-------------------------|--|

| | |
|-----------------|---|
| Examples | The following example sets the hold character to Ctrl-S, which is ASCII decimal character 19: |
|-----------------|---|

```
Router(config)# line 8
Router(config-line)# hold-character 19
```

| | | |
|-------------------------|--------------------------------|---|
| Related Commands | Command | Description |
| | terminal hold-character | Sets or changes the hold character for the current session. |

hops-of-statistics-kept

To set the number of hops for which statistics are maintained per path for the SAA operation, use the **hops-of-statistics-kept** command in SAA RTR configuration mode. To return to the default value, use the **no** form of this command.

hops-of-statistics-kept *size*

no hops-of-statistics-kept

| | | |
|---------------------------|-------------|---|
| Syntax Description | <i>size</i> | Number of hops for which statistics are maintained per path. The default is 16 hops for type pathEcho and 1 hop for type echo . |
|---------------------------|-------------|---|

| | |
|-----------------|--|
| Defaults | 16 hops for type pathEcho 1 hop for type echo |
|-----------------|--|

| | |
|----------------------|-----------------------|
| Command Modes | SAA RTR configuration |
|----------------------|-----------------------|

| | | |
|------------------------|----------------|------------------------------|
| Command History | Release | Modification |
| | 11.2 | This command was introduced. |

| | |
|-------------------------|--|
| Usage Guidelines | One hop is the passage of a timed packet from this router to another network device. The other network device is assumed to be a device along the path to the destination (including the destination) when the operation type is pathEcho , or just the destination when the type is echo . When the number of hops reaches the size specified, no further hop information is stored. |
|-------------------------|--|

Examples The following example monitors the statistics of operation 2 for only 10 hops:

```
Router(config)# rtr 2
Router(config-rtr)# type pathecho protocol ipIcmpEcho 172.16.1.177
Router(config-rtr)# hops-of-statistics-kept 10
```

| | | |
|-------------------------|---|--|
| Related Commands | Command | Description |
| | distributions-of-statistics-kept | Sets the number of statistic distributions kept per hop during the lifetime of the SAA. |
| | hours-of-statistics-kept | Sets the number of hours for which statistics are maintained for the SAA operation. |
| | paths-of-statistics-kept | Sets the number of paths for which statistics are maintained per hour for the SAA operation. |

| Command | Description |
|---|---|
| rtr | Specifies an SAA operation and enters SAA RTR configuration mode. |
| statistics-distribution-interval | Sets the time interval for each statistics distribution kept for the SAA. |

hostname

To specify or modify the host name for the network server, use the **hostname** command in global configuration mode.

hostname *name*

Syntax Description

| | |
|-------------|---------------------------------------|
| <i>name</i> | New host name for the network server. |
|-------------|---------------------------------------|

Defaults

The default host name is Router.

Command Modes

Global configuration

Command History

| Release | Modification |
|---------|------------------------------|
| 10.0 | This command was introduced. |

Usage Guidelines

The host name is used in prompts and default configuration filenames.

Do not expect case to be preserved. Uppercase and lowercase characters look the same to many internet software applications. It may seem appropriate to capitalize a name the same way you might do in English, but conventions dictate that computer names appear all lowercase. For more information, refer to RFC 1178, *Choosing a Name for Your Computer*.

The name must also follow the rules for ARPANET host names. They must start with a letter, end with a letter or digit, and have as interior characters only letters, digits, and hyphens. Names must be 63 characters or fewer. A host name of less than 10 characters is recommended. For more information, refer to RFC 1035, *Domain Names—Implementation and Specification*.

On most systems, a field of 30 characters is used for the host name and the prompt in the CLI. Note that the length of your host name may cause longer configuration mode prompts to be truncated. For example, the full prompt for service profile configuration mode is:

```
(config-service-profile)#
```

However, if you are using the host-name of "Router", you will only see the following prompt (on most systems):

```
Router(config-service-profil)#
```

If the hostname is longer, you will see even less of the prompt:

```
Basement-rtr2(config-service)#
```

Keep this behavior in mind when assigning a name to your system (using the **hostname** global configuration command). If you expect that users will be relying on mode prompts as a CLI navigation aid, you should assign host names of no more than nine characters.

Examples

The following example changes the host name to “sandbox”:

```
Router(config)# hostname sandbox
sandbox(config)#
```

Related Commands

| Command | Description |
|--------------|---|
| setup | Enables you to make major changes to your configurations, for example, adding a protocol suit, making major addressing scheme changes, or configuring newly installed interfaces. |

hours-of-statistics-kept

To set the number of hours for which statistics are maintained for the Service Assurance Agent (SAA) operation, use the **hours-of-statistics-kept** command in SAA RTR configuration mode. To return to the default value, use the **no** form of this command.

hours-of-statistics-kept *hours*

no hours-of-statistics-kept

| | | |
|---------------------------|--------------|---|
| Syntax Description | <i>hours</i> | Number of hours that the router maintains statistics. The default is 2 hours. |
|---------------------------|--------------|---|

| | |
|-----------------|---------|
| Defaults | 2 hours |
|-----------------|---------|

| | |
|----------------------|-----------------------|
| Command Modes | SAA RTR configuration |
|----------------------|-----------------------|

| | | |
|------------------------|----------------|------------------------------|
| Command History | Release | Modification |
| | 11.2 | This command was introduced. |

Usage Guidelines

When the number of hours exceeds the specified value, the statistics table wraps (that is, the oldest information is replaced by newer information).

This command sets the amount of time statistics are kept for use by the **show rtr collection-statistics** command and **show rtr distribution** command.

Examples

The following example maintains 3 hours of statistics for SAA operation 2:

```
Router(config)# rtr 2
Router(config-rtr)# type pathecho protocol ipIcmpEcho 172.16.1.177
Router(config-rtr)# hours-of-statistics-kept 3
```

| | | |
|-------------------------|---|--|
| Related Commands | Command | Description |
| | distributions-of-statistics-kept | Sets the number of statistic distributions kept per hop during the lifetime of the SAA. |
| | hops-of-statistics-kept | Sets the number of hops for which statistics are maintained per path for the SAA operation. |
| | paths-of-statistics-kept | Sets the number of paths for which statistics are maintained per hour for the SAA operation. |
| | rtr | Specifies an SAA operation and enters SAA RTR configuration mode. |
| | statistics-distribution-interval | Sets the time interval for each statistic distribution kept for the SA Agent. |

http-raw-request

To explicitly specify the options for a GET request for an Service Assurance Agent (SAA) HTTP operation, use the **http-raw-request** command in SAA RTR configuration mode.

http-raw-request

Syntax Description This command has no arguments or keywords.

Defaults No options are specified for a GET request.

Command Modes SAA RTR configuration

| Command History | Release | Modification |
|-----------------|----------|------------------------------|
| | 12.0(5)T | This command was introduced. |

Usage Guidelines Using the **http-raw-request** command puts the CLI in HTTP Raw Request configuration mode, indicated by the (config-rtr-http) router prompt.

The **http-raw-request** command should follow the **type http operation raw** command. Use the raw-request command when you wish to explicitly specify the content of an HTTP request. Use HTTP 1.0 commands in HTTP Raw Request configuration mode.

The SAA will specify the content of an HTTP request for you if you use the **type http operation get** command. The SAA will send the HTTP request, receive the reply, and report Round-trip Time (RTT) statistics (including the size of the page returned).

Examples In the following example, SAA operation 6 is created and configured as an HTTP operation. The HTTP **GET** command is explicitly specified:

```
Router(config)# rtr 6
Router(config-rtr)# type http operation raw url http://www.cisco.com
Router(config-rtr)# http-raw-request
Router(config-rtr-http)# GET /index.html HTTP/1.0\r\n
Router(config-rtr-http)# \r\n
Router(config-rtr-http)# exit
Router(config)# rtr schedule 6 start-time now
```

| Related Commands | Command | Description |
|------------------|------------------|-----------------------------------|
| | type http | Configures an HTTP SAA operation. |

insecure

To configure a line as insecure, use the **insecure** command in line configuration mode. To disable this function, use the **no** form of this command.

insecure

no insecure

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes Line configuration

| Command History | Release | Modification |
|-----------------|---------|------------------------------|
| | 10.0 | This command was introduced. |

Usage Guidelines Use this command to identify a modem line as insecure for DEC local area transport (LAT) classification.

Examples In the following example, line 10 is configured as an insecure dialup line:

```
Router(config)# line 10
Router(config-line)# insecure
```

international

If you are using Telnet to access a Cisco IOS platform and you want to display 8-bit and multibyte international characters (for example, Kanji) and print the Escape character as a single character instead of as the caret and bracket symbols (^[]), use the **international** command in line configuration mode. To display characters in 7-bit format, use the **no** form of this command.

international

no international

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes Line configuration

| Release | Modification |
|---------|------------------------------|
| 11.3 | This command was introduced. |

Usage Guidelines If you are configuring a Cisco IOS platform using the Cisco web browser user interface (UI), this function is enabled automatically when you enable the Cisco web browser UI using the **ip http server** global configuration command.

Examples The following example enables a Cisco IOS platform to display 8-bit and multibyte characters and print the Escape character as a single character instead of as the caret and bracket symbols (^[]) when you are using Telnet to access the platform:

```
line vty 4
  international
```

| Command | Description |
|-------------------------------|---|
| terminal international | Prints the Escape character as a single character instead of as the caret and bracket symbols (^[]) for a current Telnet session in instances when you are using Telnet to access a Cisco IOS platform and you want to display 8-bit and multibyte international characters (for example, Kanji). |

ip bootp server

To enable the Bootstrap Protocol (BOOTP) service on your routing device, use the **ip bootp server** command in global configuration mode. To disable BOOTP services, use the **no** form of the command.

ip bootp server

no ip bootp server

Syntax Description This command has no arguments or keywords.

Defaults Enabled

Command Modes Global configuration

Command History

| Release | Modification |
|---------|------------------------------|
| 11.2 | This command was introduced. |

Usage Guidelines

By default, the BOOTP service is enabled. When disabled, the **no ip bootp server** command will appear in the configuration file.

The integrated Dynamic Host Configuration Protocol (DHCP) server was introduced in Cisco IOS Release 12.0(1)T. Because DHCP is based on BOOTP, both of these services share the “well-known” UDP server port of 67 (per RFC 951, RFC 1534, and RFC 2131). If both the BOOTP server and DHCP server are disabled, ‘ICMP port unreachable’ messages will be sent in response to incoming requests on port 67, and the original incoming packet will be discarded.



Note

As with all minor services, the async line BOOTP service should be disabled on your system if you do not have a need for it in your network.

Any network device that has User Data Protocol (UDP), TCP, BOOTP, DHCP or Finger services should be protected by a firewall or have the services disabled to protect against Denial of Service attacks.

Examples

In the following example, BOOTP services are disabled on the router:

```
Router(config)# no ip bootp server
```

ip director cache refresh

To enable the DistributedDirector Cache Auto Refresh function, use the **ip director cache refresh** command in global configuration mode. To disable automatic background refresh, use the **no** form of this command.

ip director cache refresh

no ip director cache refresh

Syntax Description This command has no keywords or arguments.

Defaults Automatic background refresh is disabled.

Command Modes Global configuration

| Command History | Release | Modification |
|-----------------|----------|------------------------------|
| | 12.2(8)T | This command was introduced. |

Usage Guidelines The sorting cache on DistributedDirector must be enabled before you can use the **ip director cache refresh** command. To enable the sorting cache, use the **ip director cache** command.

Once automatic background refresh for the DistributedDirector cache is enabled, the cache will actively and continuously update every expired entry by processing a fake Domain Name System (DNS) request. The cache accumulates and updates answers to all past DNS queries received since cache auto refresh was initiated. Any repeat DNS request is always serviced directly from the cache.

Examples The following example enables automatic background refresh for the DistributedDirector cache:

```
Router(config)# ip director cache
Router(config)# ip director cache refresh

Router# show running-config

ip host myhost 172.2.2.10 172.2.2.20 172.2.2.30
.
.
.
ip director cache refresh
```

ip director cache size

To configure the variable size of the DistributedDirector cache, use the **ip director cache size** command in global configuration mode. To remove this command from the configuration file and restore the system to its default condition with respect to this command, use the **no** form of this command.

ip director cache size *entries*

no ip director cache size *entries*

| | | |
|---------------------------|----------------|---|
| Syntax Description | <i>entries</i> | Maximum number of cache entries. Range is from 1 to 4294967295. |
|---------------------------|----------------|---|

| | |
|-----------------|---------------------------------------|
| Defaults | Maximum number of cache entries: 2000 |
|-----------------|---------------------------------------|

| | |
|----------------------|----------------------|
| Command Modes | Global configuration |
|----------------------|----------------------|

| | | |
|------------------------|----------------|------------------------------|
| Command History | Release | Modification |
| | 12.2(8)T | This command was introduced. |

| | |
|-------------------------|--|
| Usage Guidelines | Use the ip director cache size command to configure the maximum number of cache entries that the DistributedDirector system will retain in its cache. This cache size is the maximum number of cache entries that are displayed when the user enters the show ip director cache command. |
|-------------------------|--|

| | |
|-----------------|---|
| Examples | The following example configures the maximum number of cache entries: |
|-----------------|---|

```
Router(config)# ip director cache size 1500
Cache size shrunk to 1500
```

```
Router# show ip director cache
Director cache is on
Cache current size = 0 maximum size = 1500
Cache time for sort cache entries: 60 secs
Director sort cache hits = 0
```

| | | |
|-------------------------|-------------------------------|--|
| Related Commands | Command | Description |
| | ip director cache | Enables the sorting cache on DistributedDirector. |
| | ip director cache time | Configures how long the DistributedDirector system will retain per-client sorting information. |

ip director cache time

To configure how long the DistributedDirector system will retain per-client sorting information, use the **ip director cache time** command in global configuration mode. To remove this command from the configuration file and restore the system to its default condition with respect to this command, use the **no** form of this command.

ip director cache time *seconds*

no ip director cache time *seconds*

| | | |
|---------------------------|----------------|---|
| Syntax Description | <i>seconds</i> | Amount of time the per-client sorting information is retained, in number of seconds. Range is from 1 to 2147483. The default is 60 seconds. |
|---------------------------|----------------|---|

| | |
|-----------------|------------|
| Defaults | 60 seconds |
|-----------------|------------|

| | |
|----------------------|----------------------|
| Command Modes | Global configuration |
|----------------------|----------------------|

| | | |
|------------------------|----------------|------------------------------|
| Command History | Release | Modification |
| | 12.2(8)T | This command was introduced. |

| | |
|-------------------------|---|
| Usage Guidelines | Use the ip director cache time command to specify how long the DistributedDirector system will retain per-client sorting in its cache. This cache time is the maximum amount of cache time displayed when the user enters the show ip director cache command. |
|-------------------------|---|

| | |
|-----------------|--|
| Examples | The following example configures how long the DistributedDirector system will retain per-client sorting information: |
|-----------------|--|

```
Router(config)# ip director cache time 100
```

```
Router# show ip director cache
Director cache is on
Cache current size = 0 maximum size = 2000
Cache time for sort cache entries: 100 secs
Director sort cache hits = 0
```

| | | |
|-------------------------|-------------------------------|--|
| Related Commands | Command | Description |
| | ip director cache | Enables the sorting cache on DistributedDirector. |
| | ip director cache size | Configures the variable size of the DistributedDirector cache. |

ip director default priorities

To set a default priority for a specific metric on the DistributedDirector, use the **ip director default priorities** command in global configuration mode. To remove a default priority for a metric, use the **no** form of this command.

```
ip director default priorities [drp-int number] [drp-ext number] [drp-ser number]
[random number] [admin number] [drp-rtt number] [portion number] [availability number]
[route-map number] [boomerang number]
```

```
no ip director default priorities [drp-int number] [drp-ext number] [drp-ser number]
[random number] [admin number] [drp-rtt number] [portion number] [availability number]
[route-map number] [boomerang number]
```

Syntax Description

| | |
|---------------------|---|
| drp-int | (Optional) DRP internal metric. |
| <i>number</i> | Numeric value of a priority level for a given metric. Range is from 1 to 100. |
| drp-ext | (Optional) DRP external metric. |
| drp-ser | (Optional) DRP server metric. |
| random | (Optional) Random metric. |
| admin | (Optional) Administrative metric. |
| drp-rtt | (Optional) DRP round-trip time metric. |
| portion | (Optional) Portion metric. |
| availability | (Optional) Availability metric. |
| route-map | (Optional) Route-map metric. |
| boomerang | (Optional) Boomerang metric. |

Defaults

No default priorities are specified.

Command Modes

Global configuration

Command History

| Release | Modification |
|----------|---------------------------------|
| 12.2(4)T | This command was introduced. |
| 12.2(8)T | The boomerang metric was added. |

Usage Guidelines

Not all of the metrics need to be specified, but at least one must be specified. If the boomerang metric is specified for a given host name, then all metrics of lower priority (that is, having a higher priority number) than boomerang are always ignored.

The default priorities specified will take effect if no priorities are specified in the **ip director host priority** command or in the corresponding Domain Name System (DNS) text record for the host.

To set the default priority for several metrics, enter the metric keywords and values to be configured on the same line as the **ip director default priorities** command.

Examples

In the following example, the boomerang metric is selected as the default priority:

```
Router(config)# ip director default priorities boomerang 1

Router# show running-config

ip host boom1 172.2.2.10 172.2.2.20 172.2.2.30
ip director server 172.2.2.20 drp-association 172.4.4.2
ip director server 172.2.2.30 drp-association 172.4.4.3
ip director server 172.2.2.10 drp-association 172.4.4.1
ip director host boom1
no ip director cache
ip dns primary boom1 soa boom1 boom1@com
ip director host boom1 priority boomerang 1
no ip director drp synchronized
```

Related Commands

| Command | Description |
|--|--|
| ip director access-list | Defines an access list for DistributedDirector that specifies which subdomain names and host names should be sorted. |
| ip director cache | Enables the sorting cache on DistributedDirector. |
| ip director default priorities | Sets a default priority for a specific metric on DistributedDirector. |
| ip director default weights | Configures default weight metrics for DistributedDirector. |
| ip director host priority | Configures the order in which DistributedDirector considers metrics when picking a server. |
| ip director host weights | Sets host-specific weights for the metrics that DistributedDirector uses to determine the best server within a specific host name. |
| ip director server admin-pref | Configures a per-service administrative preference value. |
| ip director server portion | Sets the portion value for a specific server. |
| ip director server preference | Specifies DistributedDirector preference of one server over others or takes a server out of service. |
| show ip director default priority | Verifies the default configurations of DistributedDirector metrics. |
| show ip director default weights | Shows DistributedDirector default weights. |
| show ip director servers | Displays DistributedDirector server preference information. |

ip director default weights

To configure default weight metrics for DistributedDirector, use the **ip director default weights** command in global configuration mode. To set the defaults to zero, use the **no** form of this command.

```
ip director default weights {[drp-int number] [drp-ext number] [drp-ser number]
[drp-rtt number] [random number] [admin number] [portion number] [availability number]
[route-map number]}
```

```
no ip director default weights {[drp-int number] [drp-ext number] [drp-ser number]
[drp-rtt number] [random number] [admin number] [portion number] [availability number]
[route-map number]}
```

| Syntax Description | |
|------------------------------|---|
| drp-int <i>number</i> | <p>(Optional) Director Response Protocol (DRP) internal metric. The range is 1 to 100.</p> <p>This option sends a DRP request to all DRP server agents, asking them for the distance from themselves to the edge of their Border Gateway Protocol (BGP) autonomous system in the direction of the client originating the Domain Name System (DNS) query. This distance can be used along with the DRP external metric (drp-ext) to help determine the distance between the router and the client originating the DNS query.</p> <p>If the client and the DRP server agent are in the same autonomous system, this metric returns the Interior Gateway Protocol (IGP) cost metric between the client and the DRP server agent.</p> |
| drp-ext <i>number</i> | <p>(Optional) DRP external metric. The range is 1 to 100.</p> <p>This option sends a DRP request to all DRP server agents, asking them for the BGP distance between them and the client originating the DNS query. This distance represents the number of BGP hops between the autonomous system of the DRP server agent and the autonomous system of the client originating the DNS query. Because this is BGP information, the DRP server agents need to have access to full Internet BGP information in order for this metric to be useful.</p> |
| drp-ser <i>number</i> | <p>(Optional) DRP server metric. The range is 1 to 100.</p> <p>This option sends a DRP request to all DRP server agents, asking them for the IGP route metric between them and the distributed servers that they support. This distance can be used with the DRP internal metric (drp-int) to get a finer distance calculation between the distributed servers and the edge of the BGP autonomous system in the direction of the client originating the DistributedDirector query.</p> <p>If a true BGP border router is used as a DRP server agent, the DRP server metric will return the IGP route metric between the distributed server and the BGP border router (autonomous system edge). Because DRP server metrics should not change frequently, DistributedDirector issues DRP server queries (and caches the results) every 10 minutes.</p> |
| drp-rtt <i>number</i> | <p>(Optional) DRP round-trip time metric. The range is 1 to 100.</p> <p>This option sends a DRP request to all DRP server agents, asking them for the round-trip time between the DRP agent and the client originating the DNS query.</p> |

| | |
|----------------------------|---|
| random number | (Optional) Random metric. The range is 1 to 100. This option selects a random number for each distributed server and defines the “best” server as the one with the smallest random number assignment. Using this metric alone results in random redirection of clients to the distributed servers. Because this metric requires no routing table information, it does not trigger DRP requests to the DRP server agents. |
| admin number | (Optional) Administrative metric. The range is 1 to 100. This option specifies a simple preference of one server over another. If the administrative metric has been explicitly set to zero, the Director will not consider the server, so the server is taken out of service. |
| portion number | (Optional) Portion metric. The range is 1 to 100. This option assigns a load “portion” to each server such that servers with a higher portion value will receive a larger percentage of connections at any one time. |
| availability number | (Optional) Availability metric. The range is 1 to 65535. This option specifies the load information for the DistributedDirector. The default value is 65,535. |
| route-map number | (Optional) Route-map metric. The range is 1 to 100. This option specifies if a server should be offered to a client. |

Defaults

No default weights are specified.
The availability default value is 65535.

Command Modes

Global configuration

Command History

| Release | Modification |
|------------|---|
| 11.1(18)IA | This command was introduced. |
| 12.1(5)T | The availability and route-map metrics were added. |
| 12.2(4)T3 | The command name was changed slightly: default weights replaced default-weights . |

Usage Guidelines

Not all the metrics need to be configured; however, at least one metric must be configured when this command is used.

Default weights are used for all host names sorted by the DistributedDirector. To override default weights for a certain host, specify host-specific weights in the private DNS server configuration.

When the associated metric is referenced in the sorting decision, it will always be multiplied by the appropriate metric weight. In this way, you can specify that some metrics be weighted more than others. You may determine the weights that you want to use through experimentation. The weights given do not need to add up to 100.

The new availability metric allows the DistributedDirector to attempt to create a TCP connection to each distributed server on a configured port over a configurable time interval.

Examples

The following command configures default weights for the internal and external metrics:

```
Router(config)# ip director default weight drp-int 10 drp-ext 90
```

Related Commands

| Command | Description |
|--|--|
| debug ip director parse | Shows debugging information for DistributedDirector parsing of TXT information. |
| debug ip director sort | Shows debugging information for DistributedDirector IP address sorting. |
| ip director access-list | Defines an access list for the DistributedDirector that specifies which subdomain names and host names should be sorted. |
| ip director cache | Enables the sorting cache on the DistributedDirector. |
| ip director default priorities | Sets default priorities for a specific metric on the DistributedDirector. |
| ip director drp rttprobe | Sets the protocol used by DRP agents for RTT probing in DistributedDirector. |
| ip director host priority | Configures the order in which the DistributedDirector considers metrics when selecting a server. |
| ip director host weights | Sets host-specific weights for the metrics that the DistributedDirector uses to determine the best server within a specific host name. |
| ip director server admin-pref | Configures a per-service administrative preference value. |
| ip director server portion | Sets the portion value for a specific server. |
| ip director server preference | Specifies DistributedDirector preference of one server over others or takes a server out of service. |
| show ip director default priority | Verifies the default configurations of DistributedDirector metrics. |
| show ip director default weights | Shows the DistributedDirector default weights. |
| show ip director servers | Displays the DistributedDirector server preference information. |

ip director dfp security

To configure a security key for use when connecting to the Dynamic Feedback Protocol (DFP) client named, use the **ip director dfp security** command in global configuration mode. To turn off the security key, use the **no** form of this command.

```
ip director dfp security ip-address md5 string [timeout]
```

```
no ip director dfp security ip-address md5 string [timeout]
```

Syntax Description

| | |
|-------------------|--|
| <i>ip-address</i> | IP address for the service. |
| md5 | Security data authentication. Message Digest 5. |
| <i>string</i> | Security key. |
| <i>timeout</i> | (Optional) Amount of time, in seconds, during which DistributedDirector will continue to accept a previously defined security key. The default value is 0 seconds. |

Defaults

The timeout default value is 0 seconds.

Command Modes

Global configuration

Command History

| Release | Modification |
|----------|------------------------------|
| 12.1(5)T | This command was introduced. |

Usage Guidelines

The **ip director dfp security** command should be entered before configuring the **ip director dfp** command, resulting in a connection being made, but it can be entered independently of making a connection.

DFP allows servers to take themselves Out-of-Service and place themselves back In-Service. This function could result in a security risk because a network that is hacked could be shut down even though all the servers are still performing. An optional security vector is included in DFP to allow each message to be verified. The security vector is used to describe the security algorithm being used and to provide the data for that algorithm. The security vector itself is also extensible in that it specifies which security algorithm is being used. This specification allows different levels of security from MD5 to Data Encryption Standard (DES) to be used without overhauling the protocol and disrupting any installed base of equipment. If a receiving unit is configured for the specified security type, all DFP packets must contain that security vector or they are ignored. If a receiving unit is not configured for any security type, the security vector does not have to be present, and if it is present, it is ignored while the rest of the message is processed normally.

Examples

The following example configures the security key hello:

```
ip director dfp security 10.0.0.1 md5 hello 60
```

| Related Commands | Command | Purpose |
|------------------|------------------------|---|
| | ip director dfp | Configures the DistributedDirector DFP agent with which the DistributedDirector should communicate. |

ip director dfp

To configure the DistributedDirector Dynamic Feedback Protocol (DFP) agent with which the DistributedDirector should communicate, use the **ip director dfp** command in global configuration mode. To turn off the DFP agent, use the **no** form of this command.

```
ip director dfp ip-address [port] [retry number] [attempts seconds] [timeout seconds]
```

```
no ip director dfp ip-address [port] [retry number] [attempts seconds] [timeout seconds]
```

| Syntax Description | | |
|-------------------------|--|---|
| <i>ip-address</i> | | IP address. |
| <i>port</i> | | (Optional) Port number to which the distributed servers are configured. The default value is 8080. |
| retry number | | (Optional) Number of times a connection will be attempted. The default value is 5 attempts. |
| attempts seconds | | (Optional) Delay, in seconds, between each attempt. The default value is 10,000 seconds. |
| timeout seconds | | (Optional) Maximum amount of time, in seconds, for which DFP information is assumed valid. The default value is 10,000 seconds. |

Defaults

The port default value is 8080.

The retry default value is 5 attempts.

The attempts default value is 10000 seconds.

The timeout default value is 10000 seconds.

Command Modes

Global configuration

Command History

| Release | Modification |
|----------|------------------------------|
| 12.1(5)T | This command was introduced. |

Usage Guidelines

A connection is attempted a specified number of times with a delay of a specified number of seconds between each attempt. Once a connection is established, the DFP protocol will run. If a time interval update has not occurred for this DFP session, the connection breaks and is reestablished as described above.

Examples

The following example configures the DistributedDirector to communicate with a specified DFP agent:

```
ip director dfp 10.0.0.1 retry 3 attempts 60 timeout 6000
```

ip director drp rttprobe

To set the protocol used by Director Response Protocol (DRP) agents for round-trip time (RTT) probing in DistributedDirector, use the **ip director drp rttprobe** command in global configuration mode. To disable the use of a protocol, use the **no** form of the command.

ip director drp rttprobe [tcp | icmp]

no ip director drp rttprobe [tcp | icmp]

| Syntax Description | tcp | (Optional) Transmission Control Protocol. This is the default. |
|--------------------|------|--|
| | icmp | (Optional) Internet Control Message Protocol. |

Defaults TCP

Command Modes Global configuration

| Command History | Release | Modification |
|-----------------|----------|------------------------------|
| | 12.2(4)T | This command was introduced. |

Usage Guidelines Both protocols can be activated, in which case DistributedDirector will instruct DRP agents to return the RTT collected from either the TCP or Internet Control Message Protocol (ICMP) protocol, whichever becomes available first. At any time, at least one of the protocols must be active.

To use only one protocol, enable the protocol you want to use, and then disable the protocol that was already configured.

```
Router(config)# ip director drp rttprobe icmp
Router(config)# no ip director drp rttprobe tcp
```

Examples The following example shows that ICMP is configured for use by DRP agents for RTT probing:

```
Router(config)# ip director drp rttprobe icmp
```

| Related Commands | Command | Description |
|------------------|---------------------------------------|--|
| | ip director access-list | Defines an access list for the DistributedDirector that specifies which subdomain names and host names should be sorted. |
| | ip director cache | Enables the sorting cache on the DistributedDirector. |
| | ip director default priorities | Sets default priorities for a specific metric on the DistributedDirector. |
| | ip director default weights | Configures default weight metrics for the DistributedDirector. |

| Command | Description |
|--|--|
| ip director host priority | Configures the order in which the DistributedDirector considers metrics when selecting a server. |
| ip director host weights | Sets host-specific weights for the metrics that the DistributedDirector uses to determine the best server within a specific host name. |
| ip director server admin-pref | Configures a per-service administrative preference value. |
| ip director server portion | Sets the portion value for a specific server. |
| ip director server preference | Specifies DistributedDirector preference of one server over others or takes a server out of service. |
| show ip director default priority | Verifies the default configurations of DistributedDirector metrics. |
| show ip director default weights | Shows the DistributedDirector default weights. |
| show ip director servers | Displays the DistributedDirector server preference information. |

ip director drp synchronized

To activate clock synchronization between DistributedDirector and Director Response Protocol (DRP), use the **ip director drp synchronized** command in global configuration mode. To deactivate synchronization between the clocks in DistributedDirector and the DRPs, use the **no** form of this command.

ip director drp synchronized

no ip director drp synchronized

Syntax Description This command has no arguments or keywords.

Defaults Clock synchronization is deactivated.

Command Modes Global configuration

| Command History | Release | Modification |
|-----------------|----------|------------------------------|
| | 12.2(8)T | This command was introduced. |

Usage Guidelines This command is used in conjunction with boomerang racing.

When the **ip dir drp synchronized** command is configured, DistributedDirector specifies an absolute time at which the DRP agent should respond to the DNS client.

When **no ip director drp synchronized** is configured (which is the default), DistributedDirector specifies a relative time (based on the delay measured between DistributedDirector and the DRP agent) at which the DRP agent should respond to the Domain Name Service (DNS) client.

Examples In the following example, DistributedDirector and DRP clock synchronization are activated:

```
Router(config)# ip director drp synchronized

Router(config)# show running-config

ip host boom1 172.2.2.10 172.2.2.20 172.2.2.30
ip director server 172.2.2.20 drp-association 172.4.4.2
ip director server 172.2.2.30 drp-association 172.4.4.3
ip director server 172.2.2.10 drp-association 172.4.4.1
ip director host boom1
.
.
.
ip director drp synchronized
```

ip director host priority

To configure the order in which the DistributedDirector considers metrics when picking a server, use the **ip director host priority** command in global configuration mode. To turn off metric priorities, use the **no** form of this command.

```
ip director host host-name priority {[drp-int number] [drp-ext number] [drp-ser number]
[drp-rtt number] [random number] [admin number] [portion number] [availability number]
[route-map number]}
```

```
no ip director host host-name priority {[drp-int number] [drp-ext number] [drp-ser number]
[drp-rtt number] [random number] [admin number] [portion number] [availability number]
[route-map number]}
```

| Syntax Description | |
|------------------------------|--|
| <i>host-name</i> | Name of the host that maps to one or more IP addresses. Use the <i>host-name</i> argument to name the host that maps to one or more IP addresses. Do not use an IP address. |
| drp-int <i>number</i> | (Optional) Director Response Protocol (DRP) internal metric. The range is 1 to 100. This option sends a DRP request to all DRP server agents, asking them for the distance from themselves to the edge of their Border Gateway Protocol (BGP) autonomous system in the direction of the client originating the Domain Name System (DNS) query. This distance can be used along with the DRP external metric (drp-ext) to help determine the distance between the router and the client originating the DNS query. If the client and the DRP server agent are in the same autonomous system, this metric returns the Interior Gateway Protocol (IGP) cost metric between the client and the DRP server agent. |
| drp-ext <i>number</i> | (Optional) DRP external metric. The range is 1 to 100. This option sends a DRP request to all DRP server agents, asking them for the BGP distance between them and the client originating the DNS query. This distance represents the number of BGP hops between the autonomous system of the DRP server agent and the autonomous system of the client originating the DNS query. Because this is BGP information, the DRP server agents need to have access to full Internet BGP information in order for this metric to be useful. |
| drp-ser <i>number</i> | (Optional) DRP server metric. The range is 1 to 100. This option sends a DRP request to all DRP server agents, asking them for the IGP route metric between them and the distributed servers that they support. This distance can be used with the DRP internal metric (drp-int) to get a finer distance calculation between the distributed servers and the edge of the BGP autonomous system in the direction of the client originating the DistributedDirector query. If a true BGP border router is used as a DRP server agent, the DRP server metric will return the IGP route metric between the distributed server and the BGP border router (autonomous system edge). Because DRP server metrics should not change frequently, DistributedDirector issues DRP server queries (and caches the results) every 10 minutes. |

| | |
|-----------------------------------|---|
| drp-rtt <i>number</i> | (Optional) DRP round-trip time metric. The range is 1 to 100. This option sends a DRP request to all DRP server agents, asking them for the round-trip time between the DRP agent and the client originating the DNS query. |
| random <i>number</i> | (Optional) Random metric. The range is 1 to 100. This option selects a random number for each distributed server and defines the “best” server as the one with the smallest random number assignment. Using this metric alone results in random redirection of clients to the distributed servers. Because this metric requires no routing table information, it does not trigger DRP requests to the DRP server agents. |
| admin <i>number</i> | (Optional) Administrative metric. The range is 1 to 100. This option specifies a simple preference of one server over another. If the administrative metric has been explicitly set to zero, the Director will not consider the server, so the server is taken out of service. |
| portion <i>number</i> | (Optional) Portion metric. The range is 1 to 100. This option assigns a load “portion” to each server such that servers with a higher portion value will receive a larger percentage of connections at any one time. |
| availability <i>number</i> | (Optional) Availability metric. The range is 1 to 65,535. This option specifies the load information for the DistributedDirector. The default value is 65,535. |
| route-map <i>number</i> | (Optional) Route-map metric. The range is 1 to 100. This option specifies if a server should be offered to a client. |

Defaults

The availability default value is 65,535.

Command Modes

Global configuration

Command History

| Release | Modification |
|------------|--|
| 11.1(18)IA | This command was introduced. |
| 12.1(5)T | This command was integrated into 12.1 T. The availability and route-map metrics were added. |
| 12.2(8)T | The boomerang metric was added. |

Usage Guidelines

Not all of the metrics need to be specified, but at least one must be specified. If the boomerang metric is specified at a given priority level, then all other metrics of lower priority (that is, having a higher priority number) for that host name are ignored. If the boomerang metric is being considered, then it is the final step in determining the best server.

The **availability** keyword allows the DistributedDirector to attempt to create a TCP connection to each distributed server on a configured port over a configurable time interval.

If multiple servers end up with the same metric value, the next metric is considered to determine the “best” server. If multiple metrics have the same priority value, the metrics are added to obtain a *composite metric*. For example, if two metrics have the same priority value, they are first multiplied by their weight values (if specified) and then added together to form the composite metric.

If you do not specify weights for a group of distributed servers, there are no default weights for the Director, and if you have specified priority values, the weight values are set to 1.

Any metrics that have a nonzero weight and that are assigned no priority value are set to a priority value of 101. They are considered after all other metrics that have priority values. As a result, if no priority values are specified for any metric, metrics are treated additively to form one composite metric.

If you do not use priority and multiple servers have the same metric value, the server whose last IP address was looked at will be returned as the “best” server. If you want to return a random IP address in the case of a tie, use metric priority with the **random** metric as the last criterion.

To turn off all priorities on all metrics associated with the defined host name, use the **no ip director host priority** command. You can turn off the priority for a specific metric or metrics using the **no ip director host host-name priority [drp-int number] [drp-ext number] [drp-ser number] [drp-rtt number] [random number] [admin number] [portion number] [availability number] [route-map number]** command.

Examples

The following example sets the external metric as the first priority and the administrative metric as the second priority:

```
Router(config)# ip director host www.xyz.com priority drp-ext 1 admin 2
```

The following example specifies the per-host priority of the metric, with a host named boom1, where the DRP internal metric is specified with a priority number of 1 and boomerang is specified with a priority number of 2:

```
Router(config)# ip director host BOOM1 priority drp-int 1 boomerang 2
```

```
Router(config)# do show running-config
```

```
ip host BOOM1 172.2.2.10 172.2.2.20 172.2.2.30
.
.
.
ip director host BOOM1
no ip director cache
ip dns primary boom1 soa boom1 boom1@com
ip director host boom1 priority drp-int 1 boomerang 2
```

Related Commands

| Command | Description |
|--|--|
| ip director default priorities | Sets a default priority for a specific metric on DistributedDirector. |
| ip director default weights | Configures default weight metrics for DistributedDirector. |
| ip director host connect | Enables the DistributedDirector to verify that a server is available. |
| ip director host weights | Sets host-specific weights for the metrics that DistributedDirector uses to determine the best server within a specific host name. |
| show ip director default priority | Verifies the default configurations of DistributedDirector metrics. |

| Command | Description |
|---|--|
| show ip director default weights | Shows DistributedDirector default weights. |
| show ip director hosts | Displays DistributedDirector host information. |

ip director host weights

To set host-specific weights for the metrics that the DistributedDirector uses to determine the best server within a specific host name, use the **ip director host weights** command in global configuration mode. To turn off weights for a host, use the **no** form of this command.

```
ip director host host-name weights {[drp-int number] [drp-ext number] [drp-ser number]
[drp-rtt number] [random number] [admin number] [portion number] [availability number]
[route-map number]}
```

```
no ip director host host-name weights {[drp-int number] [drp-ext number] [drp-ser number]
[drp-rtt number] [random number] [admin number] [portion number] [availability number]
[route-map number]}
```

| Syntax Description | |
|------------------------------|---|
| <i>host-name</i> | Name of the host that maps to one or more IP addresses. Do not use an IP address. |
| drp-int <i>number</i> | <p>(Optional) Director Response Protocol (DRP) internal metric. The range is 1 to 100.</p> <p>This option sends a DRP request to all DRP server agents, asking them for the distance from themselves to the edge of their Border Gateway Protocol (BGP) autonomous system in the direction of the client originating the Domain Name System (DNS) query. This distance can be used along with the DRP external metric (drp-ext) to help determine the distance between the router and the client originating the DNS query.</p> <p>If the client and the DRP server agent are in the same autonomous system, this metric returns the Interior Gateway Protocol (IGP) cost metric between the client and the DRP server agent.</p> |
| drp-ext <i>number</i> | <p>(Optional) DRP external metric. The range is 1 to 100.</p> <p>This option sends a DRP request to all DRP server agents, asking them for the BGP distance between them and the client originating the DNS query. This distance represents the number of BGP hops between the autonomous system of the DRP server agent and the autonomous system of the client originating the DNS query. Because this is BGP information, the DRP server agents need to have access to full Internet BGP information in order for this metric to be useful.</p> |
| drp-ser <i>number</i> | <p>(Optional) DRP server metric. The range is 1 to 100.</p> <p>This option sends a DRP request to all DRP server agents, asking them for the IGP route metric between them and the distributed servers that they support. This distance can be used with the DRP internal metric (drp-int) to get a finer distance calculation between the distributed servers and the edge of the BGP autonomous system in the direction of the client originating the DistributedDirector query.</p> <p>If a true BGP border router is used as a DRP server agent, the DRP server metric will return the IGP route metric between the distributed server and the BGP border router (autonomous system edge). Because DRP server metrics should not change frequently, DistributedDirector issues DRP server queries (and caches the results) every 10 minutes.</p> |

| | |
|-----------------------------------|---|
| drp-rtt <i>number</i> | (Optional) DRP round-trip time metric. The range is 1 to 100. This option sends a DRP request to all DRP server agents, asking them for the round-trip time between the DRP agent and the client originating the DNS query. |
| random <i>number</i> | (Optional) Random metric. The range is 1 to 100. This option selects a random number for each distributed server and defines the “best” server as the one with the smallest random number assignment. Using this metric alone results in random redirection of clients to the distributed servers. Because this metric requires no routing table information, it does not trigger DRP requests to the DRP server agents. |
| admin <i>number</i> | (Optional) Administrative metric. The range is 1 to 100. This option specifies a simple preference of one server over another. If the administrative metric has been explicitly set to zero, the Director will not consider the server, so the server is taken out of service. |
| portion <i>number</i> | (Optional) Portion metric. The range is 1 to 100. This option assigns a load “portion” to each server such that servers with a higher portion value will receive a larger percentage of connections at any one time. |
| availability <i>number</i> | (Optional) Availability metric. The range is 1 to 65,535. This option specifies the load information for the DistributedDirector. The default value is 65,535. |
| route-map <i>number</i> | (Optional) Route-map metric. The range is 1 to 100. This option specifies if a server should be offered to a client. |

**Note**

No host weights are set. If the **ip director default-weights** command is configured, the configured weights are the default.

Defaults

The availability default value is 65,535.

Command Modes

Global configuration

Command History

| Release | Modification |
|------------|--|
| 11.1(25)IA | This command was introduced. |
| 12.0(3)T | This command was integrated into Cisco IOS Release 12.0(3)T. |
| 12.1(5)T | The availability and route-map metrics were added. |

Usage Guidelines

Use host-specific weights when you want to use different metric weights for different virtual host names (for example, www.xyz.com and ftp.xyz.com).

The new availability metric allows the DistributedDirector to attempt to create a TCP connection to each distributed server on a configured port over a configurable time interval.

If desired, host-specific weights can instead be configured on the DistributedDirector default DNS server.

For example, you could configure host-specific weights with the following DNS TXT record:

```
hostname in txt "ciscoDD: weights { [drp-int number] [drp-ext number] [drp-ser number]
[random number] [admin number] }"
```

To use the default weights for all metrics associated with this host name, use the **no ip director host weights** command. To use the default weights for a specific metric or metrics, use the **no ip director host host-name weights [drp-int number] [drp-ext number] [drp-ser number] [drp-rtt number] [random number] [admin number] [portion number] [availability number] [route-map number]** command.

Examples

The following example sets the DRP internal metric to 4:

```
Router(config)# ip director host www.xyz.com weights drp-int 4
```

Related Commands

| Command | Description |
|------------------------------------|---|
| ip director default-weights | Configures default weight metrics for the DistributedDirector. |
| show ip director dfp | Displays information about the current status of the DistributedDirector connections with a particular DFP agent. |

ip director server availability

To configure a default availability value for all ports on a server, use the **ip director server availability** command in global configuration mode. To restore the default, use the **no** form of this command.

ip director server *ip-address* **availability** { *availability-value* | **dfp** [*availability-value*] }

no ip director server *ip-address* **availability** { *availability-value* | **dfp** [*availability-value*] }

| Syntax Description | | |
|---|--|--|
| <i>ip-address</i> | | IP address. |
| <i>availability-value</i> | | Availability value as it would be represented on the DistributedDirector system. The range is 0 to 65,535. |
| dfp [<i>availability-value</i>] | | Availability value as it would be represented on the LocalDirector system. The range for value is 0 to 65,535. |

Defaults The availability default value is 65,535.

Command Modes Global configuration

| Command History | Release | Modification |
|-----------------|----------|------------------------------|
| | 12.1(5)T | This command was introduced. |

Usage Guidelines There are two methods for specifying a default availability value. These two methods exist because the LocalDirector and the DistributedDirector deal with values in two different ways. All metrics for the DistributedDirector are arranged such that lower is better; however the LocalDirector load information is calculated such that higher is better. Thus, the DistributedDirector translates the metric value upon receipt from the LocalDirector by subtracting the availability from the maximum possible value of 65,535.

Examples To configure a default availability to be used if there is no other valid availability information, the following configuration would suffice. The following example shows how to specify the LocalDirector load and DistributedDirector availability, respectively:

```
ip director server 10.0.0.1 availability dfp 1
ip director server 10.0.0.1 availability 65534
```

To make the availability clear and to allow for specifying numbers in both schemes easily, there are two methods of specifying availability information. If the servers are running multiple serves, it may be necessary to configure the default availability value on a per-port basis by using the **ip director server port availability** command.

```
ip director server 10.0.0.1 port availability dfp 65535
ip director server 10.0.0.20 port availability dfp 65535
```

Related Commands

| Command | Description |
|---|--|
| ip director server port availability | Configures a default availability value for a specific port on a server. |

ip director server port availability

To configure a default availability value for a specific port on a server, use the **ip director server port availability** command in global configuration mode. To restore the default, use the **no** form of this command.

```
ip director server ip-address port availability {availability-value | dfp [availability-value]}
```

```
no ip director server ip-address port availability {availability-value | dfp [availability-value]}
```

| Syntax Description | | |
|--------------------|---|--|
| | <i>ip-address</i> | IP address. |
| | <i>availability-value</i> | Availability value as it would be represented on the DistributedDirector system. The range is 0 to 65,535. |
| | dfp [<i>availability-value</i>] | Availability value as it would be represented on the LocalDirector system. The range for value is 0 to 65,535. |

Defaults The availability default value is 65,535.

Command Modes Global configuration

| Command History | Release | Modification |
|-----------------|----------|------------------------------|
| | 12.1(5)T | This command was introduced. |

Usage Guidelines There are two methods for specifying a default availability value. These two methods exist because the LocalDirector and the DistributedDirector deal with values in two different ways. All metrics for the DistributedDirector are arranged such that lower is better; however the LocalDirector load information is calculated such that higher is better. Thus, the DistributedDirector translates the metric value upon receipt from the LocalDirector by subtracting the availability from the maximum possible value of 65,535.

Examples To make the availability clear and to allow for specifying numbers in both schemes easily, there are two methods of specifying availability information. If the servers are running multiple serves, it may be necessary to configure the default availability value on a per-port basis by using the **ip director server port availability** command.

```
ip director server 10.0.0.1 port availability dfp 65535
ip director server 10.0.0.20 port availability dfp 65535
```

To configure a default availability to be used if there is no other valid availability information, the following configuration would suffice. The following example shows how to specify the LocalDirector load and DistributedDirector availability, respectively:

```
ip director server 10.0.0.1 availability dfp 1
ip director server 10.0.0.1 availability 65534
```

Related Commands

| Command | Description |
|--|--|
| ip director server availability | Configures a default availability value for all ports on a server. |

ip dns server

To enable the Domain Name System (DNS) server on a router, use the **ip dns server** command in global configuration mode. To disable the DNS server, use the **no** form of the command.

ip dns server

no ip dns server

Syntax Description This command has no arguments or keywords.

Defaults The DNS server is disabled.

Command Modes Global configuration

| Command History | Release | Modification |
|-----------------|----------|------------------------------|
| | 12.2(4)T | This command was introduced. |

Usage Guidelines Use the command to enable the DNS server as needed.

Examples In the following example, the DNS server is enabled:

```
Router(config)# ip dns server
```

ip drp domain

To add a new domain to the DistributedDirector client or to configure an existing domain, use the **ip drp domain** command in global configuration mode. To remove this command from the configuration file and restore the system to its default condition with respect to this command, use the **no** form of this command.

ip drp domain *domain-name*

no ip drp domain *domain-name*

| Syntax Description | <i>domain-name</i> | Specified domain name. |
|--------------------|--------------------|------------------------|
|--------------------|--------------------|------------------------|

| Defaults | No default domain is configured. |
|----------|----------------------------------|
|----------|----------------------------------|

| Command Modes | Global configuration |
|---------------|----------------------|
|---------------|----------------------|

| Command History | Release | Modification |
|-----------------|----------|------------------------------|
| | 12.2(8)T | This command was introduced. |

| Usage Guidelines | <p>The ip drp domain command can be used only on a Director Response Protocol (DRP) agent. The boomerang client is the DRP agent.</p> <p>Enabling this command puts the client in boomerang configuration mode.</p> <p>Use the ip drp domain command to enter a new or existing domain name. Entering a new domain name creates a new domain, and entering an existing domain name allows the user to configure the specified domain. When a domain name is configured on the boomerang client, the user can configure specific parameters, such as server address, aliases, and time to live (TTL) values, for that domain.</p> <p>When a Director Response Protocol (DRP) agent receives a Domain Name System (DNS) racing message from boomerang servers such as DistributedDirector, the DRP agent extracts the specified domain name (for example, www.cisco.com) in the DNS message.</p> |
|------------------|--|
|------------------|--|

| Examples | In the following example, a domain named “www.boom1.com” is added on the boomerang client: |
|----------|--|
|----------|--|

```
Router(config)# ip drp domain www.boom1.com
```

```
Router# show running-config
```

```
.
```

```
.
```

```
ip drp domain www.boom1.com
```

Related Commands

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

ip finger

To configure a system to accept Finger protocol requests (defined in RFC 742), use the **ip finger** command in global configuration mode. To disable this service, use the **no** form of this command.

ip finger [rfc-compliant]

no ip finger

| | | |
|---------------------------|----------------------|---|
| Syntax Description | rfc-compliant | (Optional) Configures the system to wait for “Return” or “/W” input when processing Finger requests. This keyword should not be used for those systems. |
|---------------------------|----------------------|---|

| | |
|-----------------|----------|
| Defaults | Disabled |
|-----------------|----------|

| | |
|----------------------|----------------------|
| Command Modes | Global configuration |
|----------------------|----------------------|

| | | |
|------------------------|-------------------|--|
| Command History | Release | Modification |
| | 11.3 | This command was introduced. |
| | 12.1(5), 12.1(5)T | This command was changed from being enabled by default to being disabled by default. |

| | |
|-------------------------|--|
| Usage Guidelines | <p>The Finger service allows remote users to view the output equivalent to the show users [wide] command.</p> <p>When ip finger is configured, the router will respond to a telnet a.b.c.d finger command from a remote host by immediately displaying the output of the show users command and then closing the connection.</p> <p>When the ip finger rfc-compliant command is configured, the router will wait for input before displaying anything (as required by RFC 1288). The remote user can then enter the Return key to display the output of the show users EXEC command, or enter /W to display the output of the show users wide EXEC command. After this information is displayed, the connection is closed.</p> |
|-------------------------|--|



Note As with all minor services, the Finger service should be disabled on your system if you do not have a need for it in your network.

Any network device that has UDP, TCP, BOOTP, or Finger services should be protected by a firewall or have the services disabled to protect against Denial of Service attacks.

Because of the potential for hung lines, the **rfc-compliant** form of this command should not be configured for devices with more than 20 simultaneous users.

Examples

The following example disables the Finger protocol:

```
Router(config)# no ip finger
```

ip ftp passive

To configure the router to use only passive FTP connections, use the **ip ftp passive** command in global configuration mode. To allow all types of FTP connections, use the **no** form of this command.

ip ftp passive

no ip ftp passive

Syntax Description This command has no arguments or keywords.

Defaults All types of FTP connections are allowed.

Command Modes Global configuration

| Command History | Release | Modification |
|-----------------|---------|------------------------------|
| | 10.3 | This command was introduced. |

Examples In the following example, the router is configured to use only passive FTP connections:

```
Router(config)# ip ftp passive
```

| Related Commands | Command | Description |
|------------------|--------------------------------|--|
| | ip ftp password | Specifies the password to be used for FTP connections. |
| | ip ftp source-interface | Specifies the source IP address for FTP connections. |
| | ip ftp username | Configures the username for FTP connections. |