Cisco VDS Service Broker Release 1.0.1 Software Commands

This chapter contains an alphabetical listing of all the commands in Cisco VDS Service Broker Release 1.0.1 software. The VDS-SB software CLI is organized into the following command modes:

- EXEC mode—For setting, viewing, and testing system operations. It is divided into two access levels, user and privileged. To use the privileged access level, enter the **enable** command at the user access level prompt and then enter the privileged EXEC password when you see the password prompt.
- Global configuration (config) mode—For setting, viewing, and testing the configuration of VDS-SB software features for the entire device. To use this mode, enter the **configure** command from privileged EXEC mode.
- Interface configuration (config-if) mode—For setting, viewing, and testing the configuration of a specific interface. To use this mode, enter the **interface** command from Global configuration mode.
- Other configuration modes—Several configuration modes are available from the Global configuration mode for managing specific features. The commands used to access these modes are marked with a footnote in Table 2-1.

See Chapter 1, "Using Command Modes," for a complete discussion of using CLI command modes.

Table 2-1 summarizes the VDS-SB commands and indicates the command mode for each command. The same command may have different effects when entered in a different command mode, and for this reason, they are listed and documented separately. In Table 2-1, when the first occurrence is entered in EXEC mode, the second occurrence is entered in Global configuration mode. When the first occurrence is entered in Global configuration mode, the second occurrence is entered in interface configuration mode.

The VDS-SB software device mode determines whether the VDS-SB device is functioning as a Service Broker (SB), or Videoscape Distribution Suite Manager (VDSM). The commands available from a specific CLI mode are determined by the VDS-SB device mode in effect. Table 2-1 also indicates the device mode for each command. *All* indicates that the command is available for every device mode.

Note When viewing this guide online, click the name of the command in the left column of the table to jump to the command page, which provides the command syntax, examples, and usage guidelines.

Note See Appendix A, "Acronyms" for an expansion of all acronyms used in this publication.

Table 2-1 CLI Commands

Command	Description	CLI Mode	Device Mode
access-lists	Configures the access control list entries.	Global configuration	SB
alarm	Configures alarms.	Global configuration	SB
asset	Configures the CISCO-ENTITY-ASSET-MIB.	Global configuration	All
banner	Configures the EXEC, login, and MOTD[1] banners.	Global configuration	All
cd	Changes the directory.	User-level EXEC and privileged-level EXEC	All
clear ip	Clears the IP configuration.	Privileged-level EXEC	All
clear logging	Clears the syslog messages saved in the disk file.	Privileged-level EXEC	All
clear statistics	Clears the statistics.	Privileged-level EXEC	All
clear transaction-log	Clears and archives the working transaction logs.	Privileged-level EXEC	SB
clear users	Clears the connections (login) of authenticated users.	Privileged-level EXEC	All
clock (EXEC Configuration)	Manages the system clock.	Privileged-level EXEC	All
clock (Global configuration)	Sets the summer daylight saving time of day and time zone.	Global configuration	All
cms (EXEC Configuration)	Configures the CMS[2]-embedded database parameters.	Privileged-level EXEC	All
cms (Global configuration)	Schedules the maintenance and enables the Centralized Management System on a given node.	Global configuration	All
configure	Enters configuration mode from privileged EXEC mode[3].	Privileged-level EXEC	All
copy	Copies the configuration or image files to and from the CD-ROM, flash memory, disk, or remote hosts.	Privileged-level EXEC	All
core-dump	Configures a coredump file.	Privileged-level EXEC	All
cpfile	Copies a file.	User-level EXEC and privileged-level EXEC	All
debug	Configures the debugging options.	Privileged-level EXEC	All

Table 2-1 CLI Commands (continued)

Command	Description	CLI Mode	Device Mode
delfile	Deletes a file.	User-level EXEC and privileged-level EXEC	All
deltree	Deletes a directory and its subdirectories.	User-level EXEC and privileged-level EXEC	All
device	Configures the mode of operation on a device.	Global configuration	All
dir	Displays the list of files in a directory.	User-level EXEC and privileged-level EXEC	All
disable	Turns off the privileged EXEC commands.	Privileged-level EXEC	All
disk (EXEC Configuration)	Allocates the disks among the CDNFS and sysfs file systems.	Privileged-level EXEC	All
disk (Global configuration)	Configures how the disk errors should be handled.	Global configuration	All
dnslookup	Resolves a host or domain name to an IP address.	User-level EXEC and privileged-level EXEC	All
enable (EXEC Configuration)	Accesses the privileged EXEC commands.	User-level EXEC and privileged-level EXEC	All
enable (Global Configuration)	Changes the enable password.	Global configuration	All
end	Exits configuration and privileged EXEC modes.	Global configuration	All
exec-timeout	Configures the length of time that an inactive Telnet or SSH session remains open.	Global configuration	All
exit	Exits from interface, Global configuration, or privileged EXEC modes.	All	All
expert-mode	Configures debugshell.	Global configuration	All
external-ip	Configures up to a maximum of eight external IP addresses.	Global configuration	All
find-pattern	Searches for a particular pattern in a file.	Privileged-level EXEC	All
ftp	Enables FTP[4] services.	Global configuration	All

Table 2-1 CLI Commands (continued)

Command	Description	CLI Mode	Device Mode
geo-location-server	Monitors primary and secondary servers.	User-level EXEC and privileged-level EXEC	All
gulp	Captures lossless gigabit packets and writes them to disk.	Privileged-level EXEC	All
help	Obtains online help for the command-line interface.	Global configuration and user-level EXEC	All
hostname	Configures the device network name.	Global configuration	All
http	Configures HTTP-related parameters	Privileged-level EXEC	SB
install	Installs a new version of the caching application.	Privileged-level EXEC	All
interface	Configures a Gigabit Ethernet or port channel interface. Provides access to interface configuration mode.	Global configuration	All
iostat	Shows CPU and I/O statistics for devices and partitions.	Global configuration	All
ip (Global configuration)	Configures the Internet Protocol.	Global configuration	All
ip (Interface configuration)	Configures the interface Internet Protocol.	Interface configuration	All
ip access-list	Creates and modifies the access lists for controlling access to interfaces or applications. Provides access to ACL configuration mode.	Global configuration	All
kernel	Configures the kernel.	Global configuration	All
line	Specifies the terminal line settings.	Global configuration	All
lls	Displays the files in a long-list format.	User-level EXEC and privileged-level EXEC	All
logging	Configures syslog[5].	Global configuration	All
ls	Lists the files and subdirectories in a directory.	User-level EXEC and privileged-level EXEC	All
mkdir	Makes a directory.	User-level EXEC and privileged-level EXEC	All

Table 2-1 CLI Commands (continued)

Command	Description	CLI Mode	Device Mode
mkfile	Makes a file (for testing).	User-level EXEC and privileged-level EXEC	All
model	Changes the CDE250 platform model number after a remanufacturing or rescue process.	User-level EXEC and privileged-level EXEC	All
mount-option	Configures the mount option profile for remote storage.	Global Configuration	SB
mpstat	Displays processor-related statistics.	Privileged-level EXEC	SB
netmon	Displays the transmit and receive activity on an interface.	Privileged-level EXEC	All
netstatr	Displays the rate of change of netstat statistics.	Privileged-level EXEC	All
no (Global configuration)	Negates a Global configuration command or sets its defaults.	Global configuration	All
no (Interface configuration)	Negates an interface command or sets its defaults.	Interface configuration	All
ntp	Configures the Network Time Protocol server.	Global configuration	All
ntpdate	Sets the NTP software clock.	Privileged-level EXEC	All
ping	Sends the echo packets.	User-level EXEC and privileged-level EXEC	All
port-channel	Configures the port channel load balancing options.	Global configuration	All
primary-interface	Configures a primary interface for the VDS-SB network to be a Gigabit Ethernet or port channel interface.	Global configuration	All
pwd	Displays the present working directory.	User-level EXEC and privileged-level EXEC	All
radius-server	Configures the RADIUS authentication.	Global configuration	All
reload	Halts a device and performs a cold restart.	Privileged-level EXEC	All
rename	Renames a file.	User-level EXEC and privileged-level EXEC	All
restore	Restores a device to its manufactured default status.	Privileged-level EXEC	All

Table 2-1 CLI Commands (continued)

Command	Description	CLI Mode	Device Mode
rmdir	Removes a directory.	User-level EXEC and privileged-level EXEC	All
script	Checks the errors in a script or executes a script.	Privileged-level EXEC	All
service	Specifies the type of service.	Privileged-level EXEC	All
setup	Configures service routing.	Global configuration	All
setup	Configures the basic configuration settings and a set of commonly used caching services.	Privileged-level EXEC	All
show aaa	Display the accounting, authentication, and authorization configuration	User-level EXEC and privileged-level EXEC	All
show access-lists	Displays the access control list configuration.	User-level EXEC and privileged-level EXEC	SB
show alarms	Displays information on various types of alarms, their status, and history.	User-level EXEC and privileged-level EXEC	All
show arp	Displays the Address Resolution Protocol entries.	User-level EXEC and privileged-level EXEC	All
show authentication	Displays the authentication configuration.	User-level EXEC and privileged-level EXEC	All
show banner	Displays information on various types of banners.	User-level EXEC and privileged-level EXEC	All
show bitrate	Displays the SB bit-rate configuration.	User-level EXEC and privileged-level EXEC	SB
show clock	Displays the system clock.	User-level EXEC and privileged-level EXEC	All
show cms	Displays the Centralized Management System protocol, embedded database content, maintenance status, and other information.	User-level EXEC and privileged-level EXEC	All
show debugging	Displays the state of each debugging option.	User-level EXEC and privileged-level EXEC	All

Table 2-1 CLI Commands (continued)

Command	Description	CLI Mode	Device Mode
show device-mode	Displays the configured or current mode of a VDSM, or SB	User-level EXEC and privileged-level EXEC	All
show disks	Displays the disk configurations.	User-level EXEC and privileged-level EXEC	All
show flash	Displays the flash memory information.	User-level EXEC and privileged-level EXEC	All
show ftp	Displays the caching configuration of the FTP.	User-level EXEC and privileged-level EXEC	All
show geo-location-server	Displays the Geo Location Server details.	User-level EXEC and privileged-level EXEC	All
show geo-location-service	Displays if location service is enabled or disabled.	User-level EXEC and privileged-level EXEC	All
show hardware	Displays the system hardware information.	User-level EXEC and privileged-level EXEC	All
show hosts	Displays the IP domain name, name servers, IP addresses, and host table.	User-level EXEC and privileged-level EXEC	All
show interface	Displays the hardware interface information.	User-level EXEC and privileged-level EXEC	All
show inventory	Displays the system inventory information.	User-level EXEC and privileged-level EXEC	All
show ip	Displays the contents of a particular host in the BGP routing table.	User-level EXEC and privileged-level EXEC	All
show lacp	Displays LACP information.	User-level EXEC and privileged-level EXEC	All
show logging	Displays the system logging configuration.	User-level EXEC and privileged-level EXEC	All
show mount-option	Displays mount options.	User-level EXEC and privileged-level EXEC	SB

Table 2-1 CLI Commands (continued)

Command	Description	CLI Mode	Device Mode
show ntp	Displays the Network Time Protocol configuration status.	User-level EXEC and privileged-level EXEC	All
show processes	Displays the process status.	User-level EXEC and privileged-level EXEC	All
show radius-server	Displays the RADIUS server information.	User-level EXEC and privileged-level EXEC	All
show running-config	Displays the current operating configuration.	User-level EXEC and privileged-level EXEC	All
show service-broker	Display the Service Broker configuration.	User-level EXEC and privileged-level EXEC	All
show services	Displays the services-related information.	User-level EXEC and privileged-level EXEC	All
show snmp	Displays the SNMP[6] parameters.	User-level EXEC and privileged-level EXEC	All
show ssh	Displays the Secure Shell status and configuration.	User-level EXEC and privileged-level EXEC	All
show standby	Displays the information related to the standby interface.	User-level EXEC and privileged-level EXEC	All
show startup-config	Displays the startup configuration.	User-level EXEC and privileged-level EXEC	All
show statistics	Display the Service Broker statistics.	User-level EXEC and privileged-level EXEC	All
show statistics access-lists	Displays the access control list statistics.	User-level EXEC and privileged-level EXEC	SB
show statistics admission	Displays admission control statistics.	User-level EXEC and privileged-level EXEC	SB
show statistics fd	Displays the file descriptors limits.	User-level EXEC and privileged-level EXEC	All

Table 2-1 CLI Commands (continued)

Command	Description	CLI Mode	Device Mode
show statistics icmp	Displays the ICMP[7] statistics.	User-level EXEC and privileged-level EXEC	All
show statistics ip	Displays the Internet Protocol statistics.	User-level EXEC and privileged-level EXEC	All
show statistics lsof	Displays the List of Open File descriptors.	User-level EXEC and privileged-level EXEC	All
show statistics netstat	Displays the Internet socket connection statistics.	User-level EXEC and privileged-level EXEC	All
show statistics radius	Displays the RADIUS authentication statistics.	User-level EXEC and privileged-level EXEC	All
show statistics services	Displays the services statistics.	User-level EXEC and privileged-level EXEC	All
show statistics snmp	Displays the SNMP statistics.	User-level EXEC and privileged-level EXEC	All
show statistics tacacs	Displays the Service Engine TACACS+ authentication and authorization statistics.	User-level EXEC and privileged-level EXEC	All
show statistics tcp	Displays the Transmission Control Protocol statistics.	User-level EXEC and privileged-level EXEC	All
show statistics transaction-logs	Displays the transaction log export statistics.	User-level EXEC and privileged-level EXEC	SB
show statistics udp	Displays the User Datagram Protocol statistics.	User-level EXEC and privileged-level EXEC	All
show tacacs	Displays TACACS+ authentication protocol configuration information.	User-level EXEC and privileged-level EXEC	All
show tech-support	Displays the system information for Cisco technical support.	User-level EXEC and privileged-level EXEC	All
show telnet	Displays the Telnet services configuration.	User-level EXEC and privileged-level EXEC	All

Table 2-1 CLI Commands (continued)

Command	Description	CLI Mode	Device Mode
show transaction-logging	Displays the transaction logging information.	User-level EXEC and privileged-level EXEC	SB
show url-signature	Displays the URL signature information.	User-level EXEC and privileged-level EXEC	SB
show user	Displays the user identification number and username information.	User-level EXEC and privileged-level EXEC	All
show users	Displays the specified users.	User-level EXEC and privileged-level EXEC	All
show version	Displays the software version.	User-level EXEC and privileged-level EXEC	All
shutdown (Interface configuration)	Shuts down the specified interface.	Interface configuration	All
shutdown (EXEC Configuration)	Shuts down the device (stops all applications and operating system).	Privileged-level EXEC	All
snmp-server community	Configures the community access string to permit access to the SNMP.	Global configuration	All
snmp-server contact	Specifies the text for the MIB object sysContact.	Global configuration	All
snmp-server enable traps	Enables the SNMP traps.	Global configuration	All
snmp-server group	Defines a user security model group.	Global configuration	All
snmp-server host	Specifies the hosts to receive SNMP traps.	Global configuration	All
snmp-server location	Specifies the path for the MIB object sysLocation.	Global configuration	All
snmp-server notify inform	Configures the SNMP inform request.	Global configuration	All
snmp-server user	Defines a user who can access the SNMP engine.	Global configuration	All
snmp-server view	Defines an SNMPv2[8] MIB view.	Global configuration	All
ss	Dumps socket statistics.	Privileged-level EXEC	All
ssh-key-generate	Generates the SSH host key.	Global configuration	All
sshd	Configures the SSH service parameters.	Global configuration	All

Table 2-1 CLI Commands (continued)

Command	Description	CLI Mode	Device Mode
sysreport	Saves the sysreport to a user-specified file.	Privileged-level EXEC	SB
tacacs	Configures TACACS+ server parameters.	Global configuration	All
tcpdump	Dumps the TCP traffic on the network.	Privileged-level EXEC	All
tcpdumpx	Dumps the network traffic with the tcpdump extension for a multi-interface capture.	Privileged-level EXEC	All
tcpmon	Searches all TCP connections.	Privileged-level EXEC	All
tcp	Configures TCP-related parameters.	Global configuration	All
telnet (EXEC Configuration)	Starts the Telnet client.	User-level EXEC and privileged-level EXEC	All
telnet (Global Configuration)	Enables Telnet service.	Global configuration	All
terminal	Sets the terminal output commands.	User-level EXEC and privileged-level EXEC	All
test-url	Tests the accessibility of a URL using FTP, HTTP, or HTTPS.	User-level EXEC and privileged-level EXEC	SB
top	Displays a dynamic real-time view of a running VDS-SB.	Privileged-level EXEC	All
traceroute	Traces the route to a remote host.	User-level EXEC and privileged-level EXEC	All
transaction-log force	Forces archiving of the working log file to make a transaction log file.	Privileged-level EXEC	SB
transaction-logs	Configures and enables the transaction logging parameters.	Global configuration	SB
type	Displays a file.	User-level EXEC and privileged-level EXEC	All
type-tail	Displays the last several lines of a file.	User-level EXEC and privileged-level EXEC	All
undebug	Disables debugging functions.	Privileged-level EXEC	All
url-signature	Configures the URL signature.	Global configuration	SB

Table 2-1 CLI Commands (continued)

Command	Description	CLI Mode	Device Mode
username	Establishes the username authentication.	Global configuration	All
vdsm	Configure the VDS-SB IP address to be used for the SBs , or configures the role and GUI parameters on a VDSM[9] device.	Global configuration	All
whoami	Displays the current user's name.	User-level EXEC and privileged-level EXEC	All
write	Writes or erases the startup configurations to NVRAM or to a terminal session, or writes the MIB persistence configuration to disk.	Privileged-level EXEC	All

1. MOTD = message-of-the-day
2. CMS = Centralized Management System
3. Commands used to access configuration modes.
4. FTP = File Transfer Protocol
5. syslog = system logging
6. SNMP = Simple Network Management Protocol
7. ICMP = Internet Control Message Protocol
8. SNMPv2 = Simple Network Management Protocol version 2
9. Virtual Service Broker Manager

access-lists

To configure access control list (ACL) entries, use the **access-lists** command in Global configuration mode. To remove access control list entries, use the **no** form of this command.

access-lists {**300** {**deny groupname** {**any** [**position** *number*] | *groupname* [**position** *number*]}} | {**permit groupname** {**any** [**position** *number*] | *groupname* [**position** *number*]}} | **enable**}

no access-lists {**300** {**deny groupname** {**any** [**position** *number*] | *groupname* [**position** *number*}} | {**permit groupname** {**any** [**position** *number*] | *groupname* [**position** *number*]}} | **enable**}

Syntax Description

300	Specifies the group name-based access control list (ACL).
deny	Specifies the rejection action.
groupname	Defines which groups are granted or denied access to content that is served by this SB.
any	Specifies any group name.
position	(Optional) Specifies the position of the ACL record within the access list.
number	(Optional) Position number within the ACL. The range is from 1 to 4294967294.
groupname	Name of the group that is permitted or denied from accessing the Internet using an SB.
permit	Specifies the permission action.
enable	Enables the ACL.

Defaults

None

Command Modes

Global configuration (config) mode.

Usage Guidelines

You can configure group authorization using an ACL only after a user has been authenticated against an LDAP HTTP-request Authentication Server. The use of this list configures group privileges when members of the group are accessing content provided by an SB. You can use the ACL to allow the users who belong to certain groups or to prevent them from viewing specific content. This authorization feature offers more granular access control by specifying that access is only allowed to specific groups.

Use the **access-lists enable** Global configuration command to enable the use of the ACL.

Use the **access-lists 300** command to permit or deny a group from accessing the Internet using an SB. For instance, use the **access-lists 300 deny groupname marketing** command to prevent any user from the marketing group from accessing content through an SB.

At least one login authentication method, such as local, TACACS+, or RADIUS, must be enabled.

Note We recommend that you configure the local login authentication method as the primary method.

The ACL contains the following feature enhancements and limitations:

- A user can belong to several groups.
- A user can belong to an unlimited number of groups within group name strings.
- A *group name strin*g is a case-sensitive string with mixed-case alphanumeric characters.
- Each unique group name string cannot exceed 128 characters.

Note If the unique group name string is longer than 128 characters, the group is ignored.

- Group names in a group name string are separated by a comma.
- Total string of individual group names cannot exceed 750 characters.

For Windows-based user groups, append the domain name in front of the group name in the form domain or group as follows:

For Windows NT-based user groups, use the domain NetBIOS name.

Wildcards

The **access-list** command does not use a netmask; it uses a wildcard bitmask. The source and destination IP and wildcard usage is as follows:

- **source_ip**—Number of the network or host from which the packet is being sent. There are three alternative ways to specify the source:
  - Use a 32-bit quantity in four-part dotted decimal format.
  - Use the **any** keyword => source and source-wildcard of 0.0.0.0 255.255.255.255.
  - Use the **host** keyword => specific source and source_wildcard equal 0.0.0.0.
- **source-wildcard**—Wildcard bits to be applied to source. Each wildcard bit set to 0 indicates the corresponding bit position in the source. Each wildcard bit set to 1 indicates that both a 0 bit and a 1 bit in the corresponding position of the IP address of the packet is considered a match to this access list entry.

  To specify the source wildcard, use a 32-bit quantity in four-part dotted decimal format. Place 1s in the bit positions you want to ignore.

Note Wildcard bits set to 1 need not be contiguous in the source wildcard. For example, a source wildcard of 0.255.0.64 would be valid.

Examples

The following example shows how to display the configuration of the ACL by using the **show access-lists 300** command:

```
ServiceBroker# show access-lists 300
Access Control List Configuration
  ---------------------------------
    Access Control List is enabled

    Groupname-based List (300)
    1. permit groupname techpubs
    2. permit groupname acme1
    3. permit groupname engineering
    4. permit groupname sales
    5. permit groupname marketing
    6. deny groupname any
```

The following example shows how to display statistical information for the ACL by using the **show statistics access-lists 300** command:

```
ServiceBroker# show statistics access-lists 300
    Access Control Lists Statistics
    ---------------------------------------
      Groupname and username-based List (300)
        Number of requests:         1
        Number of deny responses:   0
        Number of permit responses: 1
```

The following example shows how to reset the statistical information for the ACL by using the **clear statistics access-lists 300** command:

```
ServiceBroker# clear statistics access-lists 300
ServiceBroker(config)# access-lists 300 permit groupname acme1 position 2
```

Related Commands

Command	Description
show access-lists 300	Displays the ACL configuration.
show statistics access-list 300	Displays the ACL statistics.

alarm

To configure alarms, use the **alarm** command in Global configuration mode. To disable alarms, use the **no** form of this command.

alarm {**admin-shutdown-alarm enable** | **overload-detect** {**clear** *1-999* [**raise** *10-1000*] | **enable** | **raise** *10-1000* [**clear** *1-999*]}}

no alarm {**admin-shutdown-alarm enable** | **overload-detect** {**clear** *1-999* [**raise** *10-1000*] | **enable** | **raise** *10-1000* [**clear** *1-999*]}}

Syntax Description

admin-shutdown-alarm	Generates a linkdown alarm when an interface shuts down.
enable	Enables admin shutdown alarm overload detection.
overload-detect	Specifies alarm overload configuration.
clear	Specifies the threshold below which the alarm overload state on an SB is cleared and the Simple Network Management Protocol (SNMP) traps and alarm notifications to the Centralized Management System (CMS) resume. **Note** The **alarm overload-detect clear** command value must be less than the **alarm overload-detect raise** value.
1-999	Number of alarms per second that ends an alarm overload condition.
raise	(Optional) Specifies the threshold at which the CDE enters an alarm overload state and SNMP traps and alarm notifications to CMS are suspended.
10-1000	Number of alarms per second that triggers an alarm overload.
enable	Enables the detection of alarm overload situations.

Defaults

admin-shutdown-alarm: disabled

raise: 10 alarms per second

clear: 1 alarm per second

Command Modes

Global configuration (config) mode.

Usage Guidelines

The **alarm admin-shutdown-alarm** command must be enabled for an admin-shutdown alarm to take effect. If an admin-shutdown alarm occurs, disabling this option does not clear the outstanding alarm properly. There are two ways to avoid this situation:

- Clear the outstanding admin-shutdown alarm first before disabling this option.
- Disable this option and reboot, which clears this alarm.

When multiple applications running on an SB experience problems at the same time, numerous alarms are set off simultaneously, and an SBmay stop responding. Use the **alarm overload-detect** command to set an overload limit for the incoming alarms from the node Health Manager. If the number of alarms exceeds the maximum number of alarms allowed, an SB enters an alarm overload state until the number of alarms drops down to the number defined in the **clear**.

When an SB is in the alarm overload state, the following events occur:

- Alarm overload notification is sent to SNMP and the CMS. The **clear** and **raise** values are also communicated to SNMP and the CMS.
- SNMP traps and CMS notifications for subsequent alarm raise and clear operations are suspended.
- Alarm overload clear notification is sent.
- SB remains in the alarm overload state until the rate of incoming alarms decreases to the **clear** value.

Note In the alarm overload state, applications continue to raise alarms and the alarms are recorded within an SB. The **show alarms** and **show alarms history** command in EXEC configuration modes display all the alarms even in the alarm overload state.

Examples

The following example shows how to generate a linkdown alarm when an interface shuts down:

```
ServiceBroker(config)# alarm admin-shutdown-alarm enable
```

The following example shows how to enable the detection of alarm overload:

```
ServiceBroker(config)# alarm overload-detect enable
```

The following example shows how to set the threshold for triggering the alarm overload at 100 alarms per second:

```
ServiceBroker(config)# alarm overload-detect raise 100
```

The following example shows how to set the level for clearing the alarm overload at 10 alarms per second:

```
ServiceBroker(config)# alarm overload-detect clear 10
```

Related Commands

Command	Description
show alarms	Displays information on various types of alarms, their status, and history.
show alarm status	Displays the status of various alarms and alarm overload settings.

asset

To configure the CISCO-ENTITY-ASSET-MIB, use the **asset** command in Global configuration mode. To remove the asset tag name, use the **no** form of this command.

asset tag *name*

no asset tag *name*

Syntax Description

tag	Sets the asset tag.
name	Asset tag name string.

Defaults

None

Command Modes

Global configuration (config) mode.

Examples

The following example shows how to configure a tag name for the asset tag string:

```
ServiceBroker(config)# asset tag entitymib
```

banner

To configure the EXEC, login, and message-of-the-day (MOTD) banners, use the **banner** command in Global configuration mode. To disable the banner feature, use the **no** form of this command.

banner {**enable** | **exec** {**message** *line* | *message_text*} | **login** {**message** *line* | *message_text*} | **motd** {**message** *line* | *message_text*}}

no banner {**enable** | **exec** [**message**] | **login** [**message**] | **motd** [**message**]}

Syntax Description

enable	Enables banner support on the SB.
exec	Configures an EXEC banner.
message	Specifies a message to be displayed when an EXEC process is created.
line	EXEC message text on a single line. The SB translates the \n portion of the message to a new line when the EXEC banner is displayed to the user.
message_text	EXEC message text on one or more lines. Press the **Return** key or enter delimiting characters (\n) to specify an EXEC message to appear on a new line. Supports up to a maximum of 980 characters, including new line characters (\n). Enter a period (.) at the beginning of a new line to save the message and return to the prompt for the Global configuration mode. **Note** The EXEC banner content is obtained from the command- line input that the user enters after being prompted for the input.
login	Configures a login banner.
message	Specifies a message to be displayed before the username and password login prompts.
line	Login message text on a single line. The SB translates the \n portion of the message to a new line when the login banner is displayed to the user.
message_text	Login message text on one or more lines. Press the **Return** key or enter delimiting characters (\n) to specify a login message to appear on a new line. Supports up to a maximum of 980 characters, including new line characters (\n). Enter a period (.) at the beginning of a new line to save the message and return to the prompt for the Global configuration mode. **Note** The login banner content is obtained from the command-line input that the user enters after being prompted for the input.
motd	Configures an MOTD banner.
message	Specifies an MOTD message.
line	MOTD message text on a single line. The SB translates the \n portion of the message to a new line when the MOTD banner is displayed to the user.
message_text	MOTD message text on one or more lines. Press the **Return** key or enter delimiting characters (\n) to specify an MOTD message to appear on a new line. Supports up to a maximum of 980 characters, including new-line characters (\n). Enter a period (.) at the beginning of a new line to save the message and return to the prompt for the Global configuration mode. **Note** The MOTD banner content is obtained from the command line input that the user enters after being prompted for the input.

Defaults

Banner support is disabled by default.

Command Modes

Global configuration (config) mode.

Usage Guidelines

You can configure the following three types of banners in any VDS-SB software device mode:

- MOTD banner sets the message of the day. This message is the first message that is displayed when a login is attempted.
- Login banner is displayed after the MOTD banner but before the actual login prompt appears.
- EXEC banner is displayed after the EXEC CLI shell has started.

Note All these banners are effective on a console, Telnet, or a Secure Shell (SSH) Version 2 session.

After you configure the banners, enter the **banner enable** command to enable banner support on the SB. Enter the **show banner** command in EXEC configuration mode to display information about the configured banners.

Note When you run an SSH Version 1 client and log in to the SB, the MOTD and login banners are not displayed. You need to use SSH Version 2 to display the banners when you log in to the SB.

Examples

The following example shows how to enable banner support on the SB:

```
ServiceBroker(config)#  banner enable
```

The following example shows how to use the **banner motd message** command to configure the MOTD banner. In this example, the MOTD message consists of a single line of text.

```
ServiceBroker(config)#  banner motd message This is an VDS-SB 2.3 device
```

The following example shows how to use the **banner motd message** global command to configure a MOTD message that is longer than a single line. In this case, the SB translates the \n portion of the message to a new line when the MOTD message is displayed to the user.

```
ServiceBroker(config)#  banner motd message "This is the motd message.
\nThis is an VDS-SB 2.3 device\n"
```

The following example shows how to use the **banner login message** command to configure a MOTD message that is longer than a single line. In this case, SB A translates the \n portion of the message to a new line in the login message that is displayed to the user.

```
ServiceBroker(config)#  banner login message "This is login banner.
\nUse your password to login\n"
```

The following example shows how to use the **banner exec** command to configure an interactive banner. The **banner exec** command is similar to the **banner motd message** commands except that for the **banner exec** command, the banner content is obtained from the command-line input that the user enters after being prompted for the input.

```
ServiceBroker(config)# banner exec
Please type your MOTD messages below and end it with '.' at beginning of line:
(plain text only, no longer than 980 bytes including newline)
This is the EXEC banner.\nUse your VDS-SB username and password to log in to this SB.\n
.
Message has 99 characters.
ServiceBroker(config)#
```

Assume that the SB has been configured with the MOTD, login, and EXEC banners as shown in the previous examples. When a user uses an SSH session to log in to the SB, the user sees a login session that includes a MOTD banner and a login banner that asks the user to enter a login password as follows:

```
This is the motd banner.
This is an VDS-SB 2.3 device
This is login banner.
Use your password to login.

Cisco SB

admin@ce's password:
```

After the user enters a valid login password, the EXEC banner is displayed, and the user is asked to enter the VDS-SB username and password as follows:

```
Last login: Fri Oct  1 14:54:03 2004 from client
System Initialization Finished.
This is the EXEC banner.
Use your VDS-SB username and password to log in to this SB.
```

After the user enters a valid VDS-SB username and password, the SB CLI is displayed. The CLI prompt varies depending on the privilege level of the login account. In the following example, because the user entered a username and password that had administrative privileges (privilege level of 15), the EXEC configuration mode CLI prompt is displayed:

```
ServiceBroker#
```

Related Commands

Command	Description
show banner	Enables banner support on the SB.

cd

To change from one directory to another directory, use the **cd** command in EXEC configuration mode.

cd *directoryname*

Syntax Description

directoryname	Directory name.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Use this command to maneuver between directories and for file management. The directory name becomes the default prefix for all relative paths. Relative paths do not begin with a slash (/). Absolute paths begin with a slash (/).

Examples

The following example shows how to use a relative path:

```
ServiceBroker(config)# cd local1
```

The following example shows how to use an absolute path:

```
ServiceBroker(config)# cd /local1
```

Related Commands

Command	Description
deltree	Deletes a directory and its subdirectories.
dir	Displays the files in a long list format.
lls	Displays the files in a long list format.
ls	Lists the files and subdirectories in a directory.
mkdir	Makes a directory.
pwd	Displays the present working directory.

clear ip

To clear the IP configuration, use the **clear ip** command in EXEC configuration mode.

clear ip access-list counters [*standard_acl-num* | *extended_acl_num* | *acl-name*]

Syntax Description

access-list	Clears the IP access list statistical information.
counters	Clears the IP access list counters.
standard_acl_num	(Optional) Counters for the specified access list, identified using a numeric identifier. The range is from 1 to 99.
extended_acl_num	(Optional) Counters for the specified access list, identified using a numeric identifier. The range is from 100 to 199
acl-name	(Optional) Counters for the specified access list, identified using an alphanumeric identifier up to 30 characters, beginning with a letter.

Defaults

None

Command Modes

EXEC configuration mode.

Examples

The following example shows how to clear IP counters:

```
ServiceRouter# clear ip counters
ServiceRouter#
```

Related Commands

Command	Description
show ip bgp summary	Displays the status of all BGP connections.

clear logging

To clear the syslog messages saved in the disk file, use the **clear logging** command in EXEC configuration mode.

clear logging

Syntax Description

This command has no keywords or arguments.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

The **clear logging** command removes all current entries from the syslog.txt file, but does not make an archive of the file. It puts a "Syslog cleared" message in the syslog.txt file to indicate that the syslog has been cleared, as shown in the following example:

```
Feb 14 12:17:18 ServiceBroker# exec_clear_logging:Syslog cleared
```

Examples

The following example shows how to clear the syslogs:

```
ServiceRouter# clear logging
U11-CDE220-2#
```

clear statistics

Command	Description
ssh-key generate	Generates an ssh key.

To clear the statistics, use the **clear** s**tatistics** command in EXEC configuration mode.

On the SB:

clear statistics {**all** | **history** | **icmp** | **ip** | **radius** | **running** | **service-broker** | **snmp** | **tacacs** | **tcp** | **udp**}

On the VDSM:

clear statistics {**all** | **history** | **icmp** | **ip** | **radius** | **running** | **snmp** | **tacacs** | **tcp** | **udp**}

Syntax Description

all	Clears all statistics.
history	Clears the statistics history.
icmp	Clears the ICMP statistics.
ip	Clears the IP statistics.
radius	Clears the RADIUS statistics.
running	Clears the running statistics.
service-broker	Clears Service Broker statistics.
snmp	Clears the SNMP statistics.
tacacs	Clears the TACACS+ statistics.
tcp	Clears the TCP statistics.
udp	Clears the UDP statistics.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

The **clear statistics** command clears all statistical counters from the parameters given. Use this command to monitor fresh statistical data for some or all features without losing cached objects or configurations.

The **clear statistics all** commands clear only normal statistics.

Examples

The following example shows how to clear all statistics on the Service Broker:

```
ServiceRouter# clear statistics all
ServiceRouter#
```

Related Commands

Command	Description
show statistics	Displays statistics information.

clear transaction-log

To clear and archive the working transaction log files, use the **clear transaction-log** command in EXEC configuration mode.

clear transaction-log

Syntax Description

This command has no keywords or arguments.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

The **clear transaction-log** command causes the transaction log to be archived immediately to the SB hard disk. This command has the same effect as the **transaction-log force archive** command.

Examples

The following example shows that the **clear transaction-log** command forces the working transaction log file to be archived:

```
ServiceBroker# clear transaction-log
```

Related Commands

Command	Description
show statistics transaction-logs	Displays SB transaction log export statistics.
show transaction-logging	Displays transaction log information.
transaction-log force	Forces the archive or export of the transaction log.
transaction-logs	Configures and enables transaction logs.

clear users

To clear the connections (login) of authenticated users, use the **clear users** command in EXEC configuration mode.

clear users administrative

Syntax Description

administrative	Clears the connections of administrative users who have been authenticated through a remote login service.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

The **clear users administrative** command clears the connections for all administrative users who are authenticated through a remote login service, such as TACACS. This command does not affect an administrative user who is authenticated through the local database.

Examples

The following example shows how to clear the connections of the authenticated users:

```
ServiceRouter# clear users administrative
ServiceRouter#
```

Related Commands

Command	Description
show user	Displays the user identification number and username information for a particular user.
show users	Displays the specified users.
username	Establishes the username authentication.

clock (EXEC Configuration)

Command	Description
show statistics wmt	Displays the WMT statistics.
show wmt	Displays WMT bandwidth and proxy mode configuration.

To set or clear clock functions or update the calendar, use the **clock** command in EXEC configuration mode.

clock {**read-calendar** | **set** *time day month year* | **update-calendar**}

Syntax Description

read-calendar	Reads the calendar and updates the system clock.
set	Sets the time and date.
time	Current time in hh:mm:ss format (hh: 00 to 23; mm: 00 to 59; ss: 00 to 59).
day	Day of the month. The range is from 1 to 31.
month	Month of the year (January, February, March, April, May, June, July, August, September, October, November, December).
year	Year. The range is from 1993 to 2035.
update-calendar	Updates the calendar with the system clock.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

If you have an outside source on your network that provides time services (such as a Network Time Protocol [NTP] server), you do not have to set the system clock manually. Enter the local time when setting the clock. The SB calculates the Coordinated Universal Time (UTC) based on the time zone set by the **clock timezone** command.

Note We strongly recommend that you configure the SB for the NTP by using the **ntp** command. See the "ntp" section on page -128 for more details.

Note If you change the local time on the device, you must change the BIOS clock time as well; otherwise, the timestamps on the error logs are not synchronized. Changing the BIOS clock is required because the kernel does not handle time zones.

Two clocks exist in the system: the software clock and the hardware clock. The software uses the software clock. The hardware clock is used only at bootup to initialize the software clock. The calendar clock is the same as the hardware clock that runs continuously on the system, even if the system is powered off or rebooted. This clock is separate from the software clock settings that are erased when the system is powered cycled or rebooted.

The **set** keyword sets the software clock. If the system is synchronized by a valid outside timing mechanism, such as a NTP clock source, you do not have to set the system clock. Use this command if no other time sources are available. The time specified in this command is relative to the configured time zone.

To perform a one-time update of the hardware clock (calendar) from the software clock or to copy the software clock settings to the hardware clock (calendar), use the **clock update-calendar** command.

Examples

The following example shows how to set the software clock on the SB:

```
ServiceBroker# clock set 13:32:00 01 February 2000
```

Related Commands

Command	Description
clock timezone	Sets the clock timezone.
ntp	Configures the Network Time Protocol server.
show clock detail	Displays the UTC and local time.

clock (Global configuration)

To set the summer daylight saving time and time zone for display purposes, use the **clock** command in Global configuration mode. To disable this function, use the **no** form of this command.

clock {**summertime** *timezone* {**date** *startday startmonth startyear starthour endday endmonth endyear offset* | **recurring** {**1-4** *startweekday startmonth starthour endweekday endmonth endhour offset* | **first** *startweekday startmonth starthour endweekday endmonth endhour offset* | **last** *startweekday startmonth starthour endweekday endmonth endhour offset*}} | **timezone** {*timezone hoursoffset minutesoffset*}}

no clock {**summertime** *timezone* {**date** *startday startmonth startyear starthour endday endmonth endyear offset* | **recurring** {**1-4** *startweekday startmonth starthour endweekday endmonth endhour offset* | **first** *startweekday startmonth starthour endweekday endmonth endhour offset* | **last** *startweekday startmonth starthour endweekday endmonth endhour offset*}} | **timezone** {*timezone hoursoffset minutesoffset*}}

Syntax Description

summertime	Configures the summer or daylight saving time.
timezone	Name of the summer time zone.
date	Configures the absolute summer time.
startday	Date to start. The range is from 1 to 31.
startmonth	Month to start. The range is from January through December.
startyear	Year to start. The range is from 1993–2032.
starthour	Hour to start in (hh:mm) format. The range is from 0 to 23.
endday	Date to end. The range is from 1 to 31.
endmonth	Month to end. The range is from January through December.
endyear	Year to end. The range is from 1993–2032.
endhour	Hour to end in (hh:mm) format. The range is from 0 to 23.
offset	Minutes offset (see Table B-1) from Coordinated Universal Time (UTC) The range is from 0 to 59.
recurring	Configures the recurring summer time.
1-4	Configures the starting week number. The range is from 1 to 4.
first	Configures the summer time to recur beginning the first week of the month.
last	Configures the summer time to recur beginning the last week of the month.
startweekday	Day of the week to start. The range is from Monday to Friday.
startmonth	Month to start. The range is from January through December.
starthour	Hour to start in hh:mm format. The range is from 0 to 23.
endweekday	Weekday to end. The range is from Monday to Friday
endmonth	Month to end. The range is from January through December.
endhour	Hour to end in hour:minute (hh:mm) format. The range is from 0 to 23.
offset	Minutes offset (see Table B-1) from UTC. The range is from 0 to 59.
timezone	Configures the standard time zone.
timezone	Name of the time zone.

hoursoffset	Hours offset (see Table B-1) from UTC. The range is from –23 to +23.
minutesoffset	Minutes offset (see Table B-1) from UTC. The range is from 0 to 59.

Defaults

None

Command Modes

Global configuration (config) mode.

Usage Guidelines

To set and display the local and UTC current time of day without an NTP server, use the **clock timezone** command with the **clock set** command. The **clock timezone** parameter specifies the difference between UTC and local time, which is set with the **clock set** command in EXEC configuration mode. The UTC and local time are displayed with the **show clock detail** command in EXEC configuration mode.

Use the **clock** *timezone offset* command to specify a time zone, where *timezone* is the desired time zone entry from Table B-1 and *0 0* is the offset (ahead or behind) Coordinated Universal Time (UTC) in hours and minutes. UTC was formerly known as *Greenwich Mean Time* (GMT).

```
SB(config)# clock timezone timezone 0 0
```

Note The time zone entry is case sensitive and must be specified in the exact notation listed in the time zone table as shown in Appendix B, "Standard Time Zones." When you use a time zone entry from Table B-1, the system is automatically adjusted for daylight saving time.

Note If you change the local time on the device, you must change the BIOS clock time as well; otherwise, the timestamps on the error logs are not synchronized. Changing the BIOS clock is required because the kernel does not handle time zones.

The offset (ahead or behind) UTC in hours, as displayed in Table B-1, is in effect during winter time. During summer time or daylight saving time, the offset may be different from the values in the table and are calculated and displayed accordingly by the system clock.

Note An accurate clock and timezone setting is required for the correct operation of the HTTP proxy caches.

Examples

The following example shows how to specify the local time zone as Pacific Standard Time with an offset of 8 hours behind UTC:

```
ServiceBroker(config)# clock timezone PST -8
Custom Timezone: PST will be used.
```

The following example shows how to configure a standard time zone on the SB:

```
ServiceBroker(config)# clock timezone US/Pacific 0 0
Resetting offset from 0 hour(s) 0 minute(s) to -8 hour(s) 0 minute(s)
Standard Timezone: US/Pacific will be used.
ServiceBroker(config)#
```

The following example negates the time zone setting on the SB:

```
ServiceBroker(config)# no clock timezone
```

The following example shows how to configure daylight saving time:

```
ServiceBroker(config)# clock summertime PDT date 10 October 2001 23:59 29 April 2002 23:59
60
```

Related Commands

Command	Description
clock	To set the summer daylight saving time and time zone for display purposes.
show clock detail	Displays the UTC and local time.

cms (EXEC Configuration)

To configure the Centralized Management System (CMS) embedded database parameters, use the **cms** command in EXEC configuration mode.

cms {**config-sync** | **database** {**backup** | **create** | **delete** | **downgrade** [**script** *filename*] | **maintenance** {**full** | **regular**} | **restore** *filename* | **validate**} | **deregister** [**force**] | **recover** {**identity** *word*}}

Syntax Description

config-sync	Sets the node to synchronize configuration with the VDSM.
database	Creates, backs up, deletes, restores, or validates the CMS-embedded database management tables or files.
backup	Backs up the database management tables.
create	Creates the embedded database management tables.
delete	Deletes the embedded database files.
downgrade	Downgrades the CMS database.
script	(Optional) Downgrades the CMS database by applying a downgrade script.
filename	Downgraded script filename.
maintenance	Cleans and reindexes the embedded database tables.
full	Specifies a full maintenance routine for the embedded database tables.
regular	Specifies a regular maintenance routine for the embedded database tables.
restore	Restores the database management tables using the backup local filename.
filename	Database local backup filename.
validate	Validates the database files.
deregister	Removes the registration of the CMS proto device.
force	(Optional) Forces the removal of the node registration.
recover	Recovers the identity of an VDS-SB network device.
identity	Specifies the identity of the recovered device.
word	Identity of the recovered device.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

The VDS-SB network is a collection of SB and VDSM nodes. One primary VDSM retains the VDS-SB network settings and provides other VDS-SB network nodes with updates. Communication between nodes occurs over secure channels using the Secure Shell Layer (SSL) protocol, where each node on the VDS-SB network uses a Rivest, Shamir, Adelman (RSA) certificate-key pair to communicate with other nodes.

Use the **cms config-sync** command to enable registered SBs, and standby VDSM to contact the primary VDSM immediately for a getUpdate (get configuration poll) request before the default polling interval of 5 minutes. For example, when a node is registered with the primary VDSM and activated, it appears as Pending in the VDSM GUI until it sends a getUpdate request. The **cms config-sync** command causes the registered node to send a getUpdate request at once, and the status of the node changes as Online.

Use the **cms database create** command to initialize the CMS database. Before a node can join a VDS-SB network, it must first be registered and then activated. The **cms enable** command automatically registers the node in the database management tables and enables the CMS. The node sends its attribute information to the VDSM over the SSL protocol and then stores the new node information. The VDSM accepts these node registration requests without admission control and replies with registration confirmation and other pertinent security information required for getting updates. Activate the node using the VDSM GUI.

Once the node is activated, it automatically receives configuration updates and the necessary security RSA certificate-key pair from the VDSM. This security key allows the node to communicate with any other node in the VDS-SB network. The **cms deregister** command removes the node from the VDS-SB network by deleting registration information and database tables.

Note The **cms deregister** command cleans up the database automatically. You do not need to use the **cms database delete** command. If the deregistration fails, the best practice is to resolve any issues that caused the deregistration failure; for example, the Service Engine is the Content Acquirer of a delivery service and cannot be deleted or deactivated. Assign a different SB as the Content Acquirer in each delivery service where this SB is assigned as the Content Acquirer and try the **cms deregister** command again.

To back up the existing management database for the VDSM, use the **cms database backup** command. For database backups, specify the following items:

- Location, password, and user ID
- Dump format in PostgreSQL plain text syntax

The naming convention for backup files includes the time stamp.

When you use the **cms recover identity** *word* command when recovering lost registration information, or replacing a failed node with a new node that has the same registration information, specify the device recovery key that you configured in the Modifying Config Property, System.device.recovery.key window of the VDSM GUI.

Use the **lcm** command to configure local or central management (LCM) on an VDS-SB network device. The LCM feature allows settings configured using the device CLI or GUI to be stored as part of the VDS-SB network-wide configuration data (enable or disable).

When you enter the **cms lcm enable** command, the CMS process running on SBs, and the standby VDSM detects the configuration changes that you made on these devices using CLIs and sends the changes to the primary VDSM.

When you enter the **cms lcm disable** command, the CMS process running on SBs, and the standby VDSM does not send the CLI changes to the primary VDSM. Settings configured using the device CLIs are not sent to the primary VDSM.

If LCM is disabled, the settings configured through the VDSM GUI overwrite the settings configured from the SB; however, this rule applies only to those local device settings that have been overwritten by the VDSM when you have configured the local device settings. If you (as the local CLI user) change the local device settings after the particular configuration has been overwritten by the VDSM, the local device configuration is applicable until the VDSM requests a full-device statistics update from the SB

(clicking the **Force full database update** button from the Device Home window of the VDSM GUI triggers a full update). When the VDSM requests a full update from the device, the VDSM settings overwrite the local device settings.

The **cms deregister force** command should be used only as the last option, because the VDSM does not know about the device being removed. When executing the **cms deregister force** command, take note of any messages stating that the deregistration failed and make sure to resolve them before reregistering the device with the same VDSM or registering the device to another VDSM. The **cms deregister force** command forces the deregistration to continue.

Examples

The following example shows how to back up the database management tables:

```
VDSM# cms database backup
creating backup file with label `backup'
backup file local1/VDS-SB-db-9-22-2002-17-36.dump is ready. use `copy' commands to move
the backup file to a remote host.
```

The following example shows how to validate the database management tables:

```
VDSM# cms database validate
Management tables are valid
```

In the following example, the CMS deregistration process has problems deregistering the SB, but it proceeds to deregister it from the CMS database when the **force** option is used:

```
ServiceBroker# cms deregister force
Deregistration requires management service to be stopped.
You will have to manually start it. Stopping management service on this node...
This operation needs to restart http proxy and streaming proxies/servers (if running) for
memory reconfiguration. Proceed? [ no ] yes
management services stopped
Thu Jun 26 13:17:34 UTC 2003 [ I ] main: creating 24 messages
Thu Jun 26 13:17:34 UTC 2003 [ I ] main: creating 12 dispatchers
Thu Jun 26 13:17:34 UTC 2003 [ I ] main: sending eDeRegistration message to VDSM
10.107.192.168
...
ServiceBroker#
```

The following example shows the use of the **cms recover identity** command when the recovery request matches the SB record, and the VDSM updates the existing record and sends a registration response to the requesting SB:

```
ServiceBroker# cms recover identity default
Registering this node as Service Engine...
Sending identity recovery request with key default
Thu Jun 26 12:54:42 UTC 2003 [ I ] main: creating 24 messages
Thu Jun 26 12:54:42 UTC 2003 [ I ] main: creating 12 dispatchers
Thu Jun 26 12:54:42 UTC 2003 [ I ] main: Sending registration message to VDSM
10.107.192.168
Thu Jun 26 12:54:44 UTC 2003 [ W ] main: Unable to load device info file in TestServer
Thu Jun 26 12:54:44 UTC 2003 [ I ] main: Connecting storeSetup for SB.
Thu Jun 26 12:54:44 UTC 2003 [ I ] main: Instantiating AStore
'com.cisco.unicorn.schema.PSqlStore'...
Thu Jun 26 12:54:45 UTC 2003 [ I ] main: Successfully connected to database
Thu Jun 26 12:54:45 UTC 2003 [ I ] main: Registering object factories for persistent
store...
Thu Jun 26 12:54:51 UTC 2003 [ I ] main: Dropped Sequence IDSET.
Thu Jun 26 12:54:51 UTC 2003 [ I ] main: Successfully removed old management tables
Thu Jun 26 12:54:51 UTC 2003 [ I ] main: Registering object factories for persistent
store...
.
```

```
.
.
Thu Jun 26 12:54:54 UTC 2003 [ I ] main: Created Table FILE_VDSM.
Thu Jun 26 12:54:55 UTC 2003 [ I ] main: Created SYS_MESS_TIME_IDX index.
Thu Jun 26 12:54:55 UTC 2003 [ I ] main: Created SYS_MESS_NODE_IDX index.
Thu Jun 26 12:54:55 UTC 2003 [ I ] main: No Consistency check for store.
Thu Jun 26 12:54:55 UTC 2003 [ I ] main: Successfully created management tables
Thu Jun 26 12:54:55 UTC 2003 [ I ] main: Registering object factories for persistent
store...
Thu Jun 26 12:54:55 UTC 2003 [ I ] main: AStore Loading store data...
Thu Jun 26 12:54:56 UTC 2003 [ I ] main: ExtExpiresRecord Loaded 0 Expires records.
Thu Jun 26 12:54:56 UTC 2003 [ I ] main: Skipping Construction RdToClusterMappings on
non-VDSM node.
Thu Jun 26 12:54:56 UTC 2003 [ I ] main: AStore Done Loading. 327
Thu Jun 26 12:54:56 UTC 2003 [ I ] main: Created SYS_MESS_TIME_IDX index.
Thu Jun 26 12:54:56 UTC 2003 [ I ] main: Created SYS_MESS_NODE_IDX index.
Thu Jun 26 12:54:56 UTC 2003 [ I ] main: No Consistency check for store.
Thu Jun 26 12:54:56 UTC 2003 [ I ] main: Successfully initialized management tables
Node successfully registered with id 103
Registration complete.
ServiceBroker#
```

The following example shows the use of the **cms recover identity** command when the hostname of the SB does not match the hostname configured in the VDSM GUI:

```
ServiceBroker# cms recover identity default
Registering this node as Service Engine...
Sending identity recovery request with key default
Thu Jun 26 13:16:09 UTC 2003 [ I ] main: creating 24 messages
Thu Jun 26 13:16:09 UTC 2003 [ I ] main: creating 12 dispatchers
Thu Jun 26 13:16:09 UTC 2003 [ I ] main: Sending registration message to VDSM
10.107.192.168
There are no SB devices in CDN
register: Registration failed.
ServiceBroker#
```

Related Commands

Command	Description
cms enable	Enables the CMS.
show cms	Displays the CMS protocol, embedded database content, maintenance status, and other information.

cms (Global configuration)

To schedule maintenance and enable the Centralized Management System (CMS) on a given node, use the **cms** command in Global configuration mode. To negate these actions, use the **no** form of this command.

cms {**database maintenance** {**full** {**enable** | **schedule** *weekday* **at** *time*} | **regular** {**enable** | **schedule** *weekday* **at** *time*}} | **enable** | **rpc timeout** {**connection** *5-1800* | **incoming-wait** *10-600* | **transfer** *10-7200*}}

no cms {**database maintenance** {**full** {**enable** | **schedule** *weekday* **at** *time*} | **regular** {**enable** | **schedule** *weekday* **at** *time*}} | **enable** | **rpc timeout** {**connection** *5-1800* | **incoming-wait** *10-600* | **transfer** *10-7200*}}

Syntax Description

database maintenance	Configures the embedded database, clean, or reindex maintenance routine.
full	Configures the full maintenance routine and cleans the embedded database tables.
enable	Enables the full maintenance routine to be performed on the embedded database tables.
schedule	Sets the schedule for performing the maintenance routine.
weekday	Day of the week to start the maintenance routine. every-day—Every day Fri—every Friday Mon—every Monday Sat—every Saturday Sun—every Sunday Thu—every Thursday Tue—every Tuesday Wed—every Wednesday
at	Sets the maintenance schedule time of day to start the maintenance routine.
time	Time of day to start the maintenance routine. The range is from 0 to 23:0 to 59 in hh:mm format.
regular	Configures the regular maintenance routine and reindexes the embedded database tables.
enable	Enables the node CMS process.
rpc timeout	Configures the timeout values for remote procedure call connections.
connection	Specifies the maximum time to wait for when making a connection.
5-1800	Timeout period, in seconds. The default for the VDSM is 30; the default for the SB is 180.
incoming-wait	Specifies the maximum time to wait for a client response.
10-600	Timeout period, in seconds. The default is 30.
transfer	Specifies the maximum time to allow a connection to remain open.
10-7200	Timeout period, in seconds. The default is 300.

Defaults

database maintenance regular: enabled

database maintenance full: enabled

connection: 30 seconds for VDSM; 180 seconds for the SB

incoming wait: 30 seconds

transfer: 300 seconds

Command Modes

Global configuration (config) mode.

Usage Guidelines

Use the **cms database maintenance** command to schedule routine, full-maintenance cleaning (vacuuming) or a regular maintenance reindexing of the embedded database. The full maintenance routine runs only when the disk is more than 90 percent full and runs only once a week. Cleaning the tables returns reusable space to the database system.

The **cms enable** command automatically registers the node in the database management tables and enables the CMS process. The **no cms enable** command stops only the management services on the device and does not disable a primary sender. You can use the **cms deregister** command to remove a primary or backup sender SB from the VDS-SB network and to disable communication between two multicast senders.

Examples

The following example shows how to schedule a regular (reindexing) maintenance routine to start every Friday at 11:00 p.m.:

```
ServiceBroker(config)# cms database maintenance regular schedule Fri at 23:00
```

The following example shows how to enable the CMS process on an SB:

```
ServiceBroker(config)# cms enable
This operation needs to restart http proxy and streaming proxies/servers (if running) for
memory reconfiguration. Proceed? [ no ] yes
Registering this node as Service Engine...
Thu Jun 26 13:18:24 UTC 2003 [ I ] main: creating 24 messages
Thu Jun 26 13:18:25 UTC 2003 [ I ] main: creating 12 dispatchers
Thu Jun 26 13:18:25 UTC 2003 [ I ] main: Sending registration message to VDSM
10.107.192.168
Thu Jun 26 13:18:27 UTC 2003 [ I ] main: Connecting storeSetup for SB.
Thu Jun 26 13:18:27 UTC 2003 [ I ] main: Instantiating AStore
'com.cisco.unicorn.schema.PSqlStore'...
Thu Jun 26 13:18:28 UTC 2003 [ I ] main: Successfully connected to database
Thu Jun 26 13:18:28 UTC 2003 [ I ] main: Registering object factories for persistent
store...
Thu Jun 26 13:18:35 UTC 2003 [ I ] main: Dropped Sequence IDSET.
Thu Jun 26 13:18:35 UTC 2003 [ I ] main: Dropped Sequence GENSET.
Thu Jun 26 13:18:35 UTC 2003 [ I ] main: Dropped Table USER_TO_DOMAIN.
.
.
.
Thu Jun 26 13:18:39 UTC 2003 [ I ] main: Created Table FILE_VDSM.
Thu Jun 26 13:18:40 UTC 2003 [ I ] main: Created SYS_MESS_TIME_IDX index.
Thu Jun 26 13:18:40 UTC 2003 [ I ] main: Created SYS_MESS_NODE_IDX index.
Thu Jun 26 13:18:40 UTC 2003 [ I ] main: No Consistency check for store.
Thu Jun 26 13:18:40 UTC 2003 [ I ] main: Successfully created management tables
Thu Jun 26 13:18:40 UTC 2003 [ I ] main: Registering object factories for persistent
store...
```

```
Thu Jun 26 13:18:40 UTC 2003 [ I ] main: AStore Loading store data...
Thu Jun 26 13:18:41 UTC 2003 [ I ] main: ExtExpiresRecord Loaded 0 Expires records.
Thu Jun 26 13:18:41 UTC 2003 [ I ] main: Skipping Construction RdToClusterMappings on
non-VDSM node.
Thu Jun 26 13:18:41 UTC 2003 [ I ] main: AStore Done Loading. 336
Thu Jun 26 13:18:41 UTC 2003 [ I ] main: Created SYS_MESS_TIME_IDX index.
Thu Jun 26 13:18:41 UTC 2003 [ I ] main: Created SYS_MESS_NODE_IDX index.
Thu Jun 26 13:18:41 UTC 2003 [ I ] main: No Consistency check for store.
Thu Jun 26 13:18:41 UTC 2003 [ I ] main: Successfully initialized management tables
Node successfully registered with id 28940
Registration complete.
Warning: The device will now be managed by the VDSM. Any configuration changes
made via CLI on this device will be overwritten if they conflict with settings on the
VDSM.
Please preserve running configuration using 'copy running-config startup-config'.
Otherwise management service will not be started on reload and node will be shown
'offline' in VDSM UI.
management services enabled
ServiceBroker(config)#
```

Related Commands

Command	Description
cms database	Creates, backs up, deletes, restores, or validates the CMS-embedded database management tables or files.
show cms	Displays the CMS protocol, embedded database content, maintenance status, and other information.

configure

To enter Global configuration mode, use the **configure** command in EXEC configuration mode.

configure

To exit Global configuration mode, use the **end** or **exit** commands. In addition, you can press **Ctrl-Z** to exit from Global configuration mode.

Syntax Description

This command has no keywords or arguments.

Defaults

None

Command Modes

EXEC configuration mode.

Examples

The following example shows how to enable Global configuration mode:

```
ServiceBroker# configure
ServiceBrokerServiceBroker(config)#
```

Related Commands

Command	Description
end	Exits configuration and privileged EXEC configuration modes.
exit	Exits from interface, Global configuration, or privileged EXEC configuration modes.
show running-config	Displays the current operating configuration.
show startup-config	Displays the startup configuration.

copy

To copy the configuration or image data from a source to a destination, use the **copy** command in EXEC configuration mode.

copy cdnfs disk *url sysfs-filename*

copy disk {**ftp** {*hostname* | *ip-address*} *remotefiledir remotefilename localfilename* | **startup-config** *filename*}

copy ftp {**disk** {*hostname* | *ip-address*} *remotefiledir remotefilename localfilename* | **install** {*hostname* | *ip-address*} *remotefiledir remotefilename*}

copy http install {{*hostname* | *ip-address*} *remotefiledir remotefilename*} [**port** *port-num* [**proxy** {*hostname* | *ip-address*} | **username** *username password* [**proxy** {*hostname* | *ip-address*} *proxy_portnum*]] | **proxy** {*hostname* | *ip-address*} *proxy_portnum* | **username** *username password* [**proxy** {*hostname* | *ip-address*} *proxy_portnum*]]

copy running-config {**disk** *filename* | **startup-config**}

copy startup-config {**disk** *filename* | **running-config**}

copy system-status disk *filename*

copy tech-support {**disk** *filename* | *remotefilename*}

Syntax Description

cdnfs	Copies a file from the CDNFS to the sysfs.
disk	Copies a file to the disk.
url	URL of the CDNFS file to be copied to the sysfs.
sysfs-filename	Filename to be copied in the sysfs.
disk	Copies a local disk file.
ftp	Copies to a file on an FTP server.
hostname	Hostname of the FTP server.
ip-address	IP address of the FTP server.
remotefiledir	Directory on the FTP server to which the local file is copied.
remotefilename	Name of the local file after it has been copied to the FTP server.
localfilename	Name of the local file to be copied.
startup-config	Copies the configuration file from the disk to startup configuration (NVRAM).
filename	Name of the existing configuration file.
ftp	Copies a file from an FTP server.
disk	Copies a file to a local disk.
hostname	Hostname of the FTP server.
ip-address	IP address of the FTP server.
remotefiledir	Directory on the FTP server where the file to be copied is located.
remotefilename	Name of the file to be copied to the local disk.
localfilename	Name of the copied file as it appears on the local disk.

install	Copies the file from an FTP server and installs the software release file to the local device.
hostname	Name of the FTP server.
ip-address	IP address of the FTP server.
remotefiledir	Remote file directory.
remotefilename	Remote filename.
http install	Copies the file from an HTTP server and installs the software release file on a local device.
hostname	Name of the HTTP server.
ip-address	IP address of the HTTP server.
remotefiledir	Remote file directory.
remotefilename	Remote filename.
port	(Optional) Specifies the port to connect to the HTTP server. The default is 80.
port-num	HTTP server port number. The range is from 1 to 65535.
proxy	Allows the request to be redirected to an HTTP proxy server.
hostname	Name of the HTTP server.
ip-address	IP address of the HTTP server.
proxy_portnum	HTTP proxy server port number. The range is from 1 to 65535.
username	Specifies the username to access the HTTP proxy server.
username	User login name.
running-config	Copies the current system configuration.
disk	Copies the current system configuration to a disk file.
filename	Name of the file to be created on disk.
startup-config	Copies the running configuration to the startup configuration (NVRAM).
disk	Copies the startup configuration to a disk file.
filename	Name of the startup configuration file to be copied to the local disk.
running-config	Copies the startup configuration to a running configuration.
system-status disk	Copies the system status to a disk file.
filename	Name of the file to be created on the disk.
tech-support	Copies system information for technical support.
disk	Copies system information for technical support to a disk file.
filename	Name of the file to be created on disk.
remotefilename	Remote filename of the system information file to be created on the TFTP server. Use the complete pathname.

Defaults

HTTP server port: 80

Default working directory for sysfs files: /local1

Command Modes

EXEC configuration mode.

Usage Guidelines

The **copy cdnfs** command in EXEC configuration mode copies data files from of the CDNFS to the sysfs for further processing. For example, you can use the **install** *imagefilename* command in EXEC configuration mode to provide the copied files to the command.

The **copy disk ftp** command copies files from a sysfs partition to an FTP server. The **copy disk startup-config** command copies a startup configuration file to NVRAM.

The **copy ftp disk** command copies a file from an FTP server to a sysfs partition.

Use the **copy ftp install** command to install an image file from an FTP server. Part of the image goes to the disk and part goes to the flash memory.

Use the **copy http install** command to install an image file from an HTTP server and install it on a local device. It transfers the image from an HTTP server to the SB using HTTP as the transport protocol and installs the software on the device. Part of the image goes to the disk and part goes to the flash memory. You can also use this command to redirect your transfer to a different location or HTTP proxy server, by specifying the **proxy** *hostname* | *ip-address* option. A username and a password have to be authenticated with the remote HTTP server if the server is password protected and requires authentication before the transfer of the software release file to the SB is allowed.

Use the **copy running-config** command to copy the running system configuration to a sysfs partition or flash memory. The **copy running-config startup-config** command is equivalent to the **write memory** command.

The **copy startup-config** command copies the startup configuration file to a sysfs partition.

The **copy system-status** command creates a file on a sysfs partition containing hardware and software status information.

The **copy tech-support tftp** command copies technical support information to a a sysfs partition.

Related Commands

Command	Description
install	Installs a new version of the caching application.
reload	Halts a device and performs a cold restart.
show running-config	Displays the current operating configuration.
show startup-config	Displays the startup configuration.
write	Writes or erases the startup configurations to NVRAM or to a terminal session, or writes the MIB persistence configuration to disk.

core-dump

To configure a coredump file, use the **core-dump** command in EXEC configuration mode.

core-dump {backtrace {all| *word*} | **service** { **cms force | dns force | service-broker force | wmt pid**}}

Syntax Description

backtrace	Displays the backtrace of a coredump file.
all	Displays the backtraces of all core files.
word	Specifies the name of the core file.
service	Creates a core dump of a specific service.
force	Forces a core dump of the service.
cms	Specifies cms services.
dns	Specifies dns services.
service-broker	Specifies service-broker services.
wmt	Specifies wmt services.
pid	Specifies the PID of the process.

Defaults

None

Command Modes

EXEC configuration mode.

Examples

The following example shows how to display the backtrace of all coredump files:

```
ServiceBroker# core backtrace al
```

cpfile

To make a copy of a file, use the **cpfile** command in EXEC configuration mode.

cpfile *oldfilename newfilename*

Syntax Description

oldfilename	Name of the file to be copied.
newfilename	Name of the copy to be created.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Use this command to create a copy of a file. Only sysfs files can be copied.

Examples

The following example shows how to create a copy of a file:

```
ServiceBroker# cpfile syslog.txt syslog.txt.save
```

Related Commands

Command	Description
copy	Copies the configuration or image files to and from the CD-ROM, flash memory, disk, or remote hosts.
dir	Displays the files in a long-list format.
lls	Displays the files in a long-list format.
ls	Lists the files and subdirectories in a directory.
mkfile	Makes a file (for testing).
rename	Renames a file.
rmdir	Removes a directory.

debug

To monitor and record caching application functions, use the **debug** command in EXEC configuration mode. To disable these functions, use the **no** form of this command.

debug *option*

no debug *option*

Syntax Description

option	Specifies the debugger type; see the Usage Guidelines section for valid values.

Defaults

debug all: default logging level is ERROR.

Command Modes

EXEC configuration mode.

Usage Guidelines

We recommend that you use the **debug** command only at the direction of Cisco TAC because the SB performance is affected when you enter the **debug** command.

You can use the **logging disk priority debug** command with the **debug** command. This configuration causes the debugging messages to be logged in the syslog file, which is available in the /local1 directory by default. You can then download the messages from the SB, copy them to a local disk file (for example, using the **copy disk ftp** command), and forward the logs to Cisco TAC for further investigation.

By default, system log messages are logged to the console and you need to copy and paste the output to a file. However, this method of obtaining logs is more prone to errors than capturing all messages in the syslog.txt file. When you use system logging to a disk file instead of system logging to a console, there is no immediate feedback that debug logging is occurring, except that the syslog.txt file gets larger (you can track the lines added to the syslog.txt file by entering the **type-tail syslog.txt follow** command). When you have completed downloading the system logs to a local disk, disable the debugging functions by using the **undebug** command (see the "undebug" section on page -347 section for more details), and reset the level of logging disk priority to any other setting that you want (for example, **notice** priority).

Table 2-2 shows valid values for the **debug** command options.

Table 2-2 debug Command Options

access-lists 300	Debugs the ACL.
dump	Dumps the ACL contents.
query	Queries the ACL configuration.
username *username*	Queries the ACL username.
groupname *groupnames*	Queries the ACL group name or names of groups of which the user is a member. Each group name must be separated by a comma.
all	Enables all debugging.

Table 2-2 debug Command Options

authentication	Debugs authentication.
user	Debugs the user login against the system authentication.
cli	Debugs the CLI command.
all	Debugs all CLI commands.
bin	Debugs the CLI command binary program.
pam	Debugs the CLI command pam.
parser	Debugs the CLI command parser.
cms	Debugs the CMS.
dataserver	Debugs the data server.
all	Debuts all data server functions.
clientlib	Debugs the data server client library module.
server	Debugs the data server module.
dhcp	Debugs the DHCP.
emdb	Embedded database debug commands.
logging	Debugs logging.
all	Debugs all logging functions.
malloc	Debug commands for memory allocation.
cache-app	Debugging commands for cache application memory allocation.
all	Sets the debug level to all.
caller-accounting	Collects statistics for every distinct allocation call-stack.
catch-double-free	Alerts if application attempts to release the same memory twice.
check-boundaries	Checks boundary over and under run scribble.
check-free-chunks	Checks if free chunks are over-written after release.
clear-on-alloc	Ensures all allocations are zero-cleared.
statistics	Allocator use statistical summary.
dns-server	DNS Caching Service memory allocation debugging.
all	Sets the debug level to all.
caller-accounting	Collects statistics for every distinct allocation call-stack.
catch-double-free	Alerts if application attempts to release the same memory twice.
check-boundaries	Checks boundary over and under run scribble.
log-directory	Memory allocation debugging log directory.
word	Directory path name.
ntp	Debugs NTP.
rpc	Displays the remote procedure call (RPC) logs.
detail	Displays the RPC logs of priority *detail* level or higher.
trace	Displays the RPC logs of priority *trace* level or higher.

Table 2-2 debug Command Options

service-broker	Debug commands for the Service Broker.
service-monitor	Debug commands for the Service Monitor.
snmp	Debugs SNMP.
agent	SNMP agent debug.
all	Debugs all SNMP functions.
cli	Debugs the SNMP CLI.
main	Debugs the SNMP main.
mib	Debugs the SNMP MIB.
traps	Debugs the SNMP traps.
standby	Debugs standby functions.
all	(Optional) Debugs all standby functions.
stats	Debugs the statistics.
all	Debugs all statistics functions.
collection	Debugs the statistics collection.
computation	Debugs the statistics computation.
history	Debugs the statistics history.
translog	Debugs the transaction logging.
all	Debugs all transaction logging.
archive	Debugs the transaction log archive.
export	Debugs the transaction log FTP export.

Debugging Keywords

All modules have **debug error** as the default level if they support the **error** keyword; however, when you execute the **show debug** command, the error does not display.

Some modules have two debugging keywords (**error** and **trace**), but you cannot enable both at the same time. See the table above to identify commands with only the **error** and **trace** keywords.

Some modules have the **all** keyword through which you can enable both the **error** and **trace** keywords at the same time. This results in *debug set to everything*. See Table 2-2 to identify commands with the **all** keyword.

Note When debugging is set to trace level, it uses a lot of the CPU on the SB to handle error log writing. When writing the trace-level error logs reaches 100 percent of the CPU usage, 504 timeout error messages start to occur. Therefore, trace-level error logging should not be enabled in production systems.

Related Commands

Command	Description
show debugging	Displays the state of each debugging option.
undebug	Disables the debugging functions (see also **debug**).

delfile

To delete a file, use the **delfile** command in EXEC configuration mode.

delfile *filename*

Syntax Description

filename	Name of the file to delete.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Use this command to remove a file from a sysfs partition.

Examples

The following example shows how to delete a file:

```
ServiceBroker# delfile /local1/tempfile
```

Related Commands

Command	Description
cpfile	Copies a file.
deltree	Deletes a directory and its subdirectories.
mkdir	Creates a directory.
mkfile	Creates a file (for testing).
rmdir	Removes a directory.

deltree

To remove a directory with its subdirectories and files, use the **deltree** command in EXEC configuration mode.

deltree *directory*

Syntax Description

directory	Name of the directory tree to delete.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Use this command to remove a directory and all files within the directory from the SB sysfs file system. Do not remove files or directories required for proper SB functioning.

Examples

The following example shows how to delete a directory from the /local1 directory:

```
ServiceBroker# deltree /local1/testdir
```

Related Commands

Command	Description
delfile	Deletes a file.
mkdir	Creates a directory.
mkfile	Creates a file (for testing).
rmdir	Removes a directory.

device

To configure the mode of operation on a device as a VDSM or SB, use the **device** command in Global configuration mode. To reset the mode of operation on a device, use the **no** form of this command.

device mode {**service-broker** | **videoscape-distribution-suite-manager**}

no device mode {**service-broker** | **videoscape-distribution-suite-manager**}

Syntax Description

mode	Sets the mode of operation of a device to VDSM, SB.
service-broker	Configures the device operation mode as an SB.
videoscape-distribution-suite-manager	Configures the device to function as a VDSM

Defaults

The default device operation mode is SB.

Command Modes

Global configuration (config) mode.

Usage Guidelines

A VDSM is the content management and device management station of an VDS-SB network that allows you to specify what content is to be distributed, and where the content should be distributed. If an SB is deployed in the VDS-SB network, the SB redirects the client based on redirecting policy. An SB is the device that serves content to the clients. There are typically many SBs deployed in an VDS-SB network, each serving a local set of clients. IP/TV brings movie-quality video over enterprise networks to the desktop of the VDS-SB network user.

Because different device modes require disk space to be used in different ways, disk space must also be configured when the device mode changes from being an SB to VDSM (or the other way around). You must reboot the device before the configuration changes to the device mode take effect.

Disks must be configured before device configuration is changed. Use the **disk configure** command to configure the disk before reconfiguring the device to the SB mode. Disk configuration changes using the **disk configure** command takes effect after the next device reboot.

To enable VDS-SB network-related applications and services, use the **cms enable** command. Use the **no** form of this command to disable the VDS-SB network.

All VDS-SB devices ship from the factory as SBs. Before configuring network settings for VDSMs and SBs using the CLI, change the device from an SB to the proper device mode.

Configuring the device mode is not a supported option on all hardware models. However, you can configure some hardware models to operate as any one of the four content networking device types. Devices that can be reconfigured using the **device mode** command are shipped from the factory by default as SBs.

To change the device mode of your SB, you must also configure the disk space allocations, as required by the different device modes, and reboot the device for the new configuration to take effect.

When you change the device mode to an SB or VDSM, you may need to reconfigure the system file system (sysfs). However, SBs and VDSMs do not require any disk space other than sysfs. When you change the device mode to an SB or a VDSM, disk configuration changes are not required because the device already has some space allotted for sysfs. sysfs disk space is always preconfigured on a factory-fresh VDS-SB network device.

If you are changing the device mode of an SB or a VDSM back to an SB, configure disk space allocations for the caching, pre-positioning (CDNFS) and system use (sysfs) file systems that are used on the SB. You can configure disk space allocations either before or after you change the device mode to an SB.

Examples

The following examples show the configuration from the default mode, SB to the VDSM, modes:

```
ServiceBroker(config)# device mode virtual-origin-system-manager

VDSM(config)# device mode service-broker

ServiceRouter(config)# device mode service-broker
```

Related Commands

Command	Description
show device-mode	Displays the configured or current mode of a VDSM, or SB device.

dir

To view a long list of files in a directory, use the **dir** command in EXEC configuration mode.

dir [*directory*]

Syntax Description

directory	(Optional) Name of the directory to list.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Use this command to view a detailed list of files contained within the working directory, including names, sizes, and time created. The equivalent command is **lls**.

Examples

The following example shows how to view a list of files in a directory:

```
ServiceBroker# dir
size            time of last change                name
--------------  -------------------------          -----------
       3931934  Tue Sep 19 10:41:32 2000           errlog-cache-20000918-164015
           431  Mon Sep 18 16:57:40 2000           ii.cfg
           431  Mon Sep 18 17:27:46 2000           ii4.cfg
           431  Mon Sep 18 16:54:50 2000           iii.cfg
          1453  Tue Sep 19 10:34:03 2000           syslog.txt
          1024  Tue Sep 19 10:41:31 2000  <DIR>    testdir
```

Related Commands

Command	Description
lls	Displays the files in a long list format.
ls	Lists the files and subdirectories in a directory.

disable

To turn off privileged command in EXEC configuration mode, use the **disable** command in EXEC configuration mode.

disable

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

The **disable** command places you in the user-level EXEC shell. To turn privileged EXEC configuration mode back on, use the **enable** command.

Examples

The following example shows how to enter the user-level EXEC configuration mode:

```
ServiceBroker# disable
ServiceBroker>
```

Related Commands

Command	Description
enable	Accesses the privileged EXEC commands.

disk (EXEC Configuration)

To configure disks and allocate disk space for devices that are using the CDS software, use the **disk** command in EXEC configuration mode.

disk {**erase** *diskname* | **mark** *diskname* {**bad** | **good**} | **policy apply** | **recover-cdnfs-volumes** | **recover-system-volumes** | **repair** *diskname* **sector** *sector_address_in_decimal* | **unuse** *diskname*}

Syntax Description

erase	Erases drive (DANGEROUS).
diskname	Name of the disk to be erased (disk00, disk01, and so on).
mark	Marks a disk drive as good or bad.
diskname	Name of the disk to be marked (disk01, disk02, and so on).
bad	Marks the disk drive as bad.
good	Marks the disk drive as good.
policy	Applies disk policy management.
apply	Invokes the disk policy manager for a disk.
recover-cdnfs-volumes	Erases all CDNFS volumes and reboots.
recover-system-volumes	Erases all SYSTEM and SYSFS volumes.
repair	Repairs the drive.
diskname	Name of the disk to be repaired (disk00, disk01, and so on).
sector	Repairs an uncorrectable sector.
sector_address_in_decimal	Name of the sector address in decimal.
unuse	Stops applications from using a disk drive.
diskname	Name of the disk to be stopped for application use (disk01, disk02, and so on).

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

The disk space in the CDS software is allocated on a per-file system basis, rather than on a per-disk basis.

The CDNFS amounts are reported by the actual usable amounts of storage for applications. Because of the internal file system overhead of approximately 3 percent, the reported amounts may be smaller than what you configured.

To view disk details, use the **show disk details** command.

Note The **show disk details** command shows the amount of disk space that is allocated to system use. This detail is not shown by using the **show disk current** command.

To show the space allocation in each individual file system type, use the **show statistics cdnfs** command.

After upgrading, the disk space allocation remains the same as previously configured.

Remapping of Bad Sectors on Disk Drives

The **disk erase** command in EXEC configuration mode performs a low-level format of the SCSI or SATA disks. This command erases all the content on the disk.

If a disk drive continues to report a failure after you have used the **disk erase** command, you must replace the disk drive.

Caution Be careful when using the **disk erase** command because this command causes all content on the specified disk to be deleted.

Note SCSI and SATA drives can be reformatted.

Erasing Disk Drives

The **disk erase** command replaced the **disk reformat** command. This command erases all the content on the disk. The sequence to erase a disk with the **disk erase** and then use the **disk policy apply** commands. If a disk drive continues to report a failure after you have used the **disk erase** command, you must replace the disk drive.

Caution Be careful when using the **disk erase** command because this command causes all content on the specified disk to be deleted.

Disk Hot Swapping

A new disk is recognized and the RAID is rebuilt when the device is rebooted. After inserting the new disk, enter the **disk policy apply** command to force the VDS-SB software to detect the new disk and rebuild the RAID.

Note RAID is not supported for generic hardware (UCS servers). These systems have a single un-RAIDed system disk. Any disk replacement requires that the system first be taken off-line.

The disk policy's design, when adding new disks, is to always favor safety. If when a new disk is added, the disk manager detects “degraded” or “bad” system volumes, the new disk is used to repair the system volumes. Thus, the disk manager always strives to have two disks allocated to the system volumes. If when a new disk is added, the system volumes are “normal” or “syncing,” the new disk is added to the cdnfs volume.

Note For the CDE220-2S3i,and the CDE220-2S3, because the system disks are internal drives, if the system disk is “bad,” the CDE should be replaced.

Repairing a Disk

The **disk repair** command re pairs the bad sector, including the proximal sectors. All data on the drive is lost, but the sectors are repaired and available for data storage again. This command provides equivalent functionality as the repair-disk utility. The disk repair command takes approximately three hours to complete per disk; after the repair disk command completes, reboot the SB to ensure all VDS-SB software services are functioning correctly.

Caution The device should be off-line before running the **disk repair** command. Because this command involves complex steps, we recommend you contact Cisco Technical Support before running this command.

The **disk repair** command not only repairs the bad sectors, but reformats the entire drive, so all data on the drive is lost. The difference between the **disk repair** command and the **disk erase** command is that the **disk erase** command only re-initializes the file system and does not repair bad sectors.

A minor alarm is set when an LSE is detected. After the sector is repaired with the disk repair command, the alarm is turned off.

```
Minor Alarms:
-------------
     Alarm ID             Module/Submodule     Instance
     -------------------- -------------------- ------------------------
   1 badsector            sysmon               disk11
     May 19 20:40:38.213 UTC, Equipment Alarm, #000003, 1000:445011
     "Device: /dev/sdl, 1 Currently unreadable (pending) sectors"
```

Stopping Applications from Using a Disk Drive

The **disk unuse** command in EXEC configuration mode allows you to stop applications from using a specific disk drive (for example, disk01) without having to reboot the device.

Note When executing the **disk unuse** command, any applications using the disk will be terminated. Off-line the device before executing this command.

The **disk unuse** command has the following behavior:

- Cannot be used with system disk if the state of RAID-1 is not “Normal”.
- Cannot be used with the CDNFS disk, which contains the “/uns-symlink-tree” directory.
- Can be used with any disk except as in scenario 1 and 2 above.

Examples

The following example shows how to repair the sector 4660 on disk 02:

```
ServiceBroker# disk repair disk02 sector 4660
```

Note A system disk cannot be unused in a non-RAID system (generic/ucs).

The following examples show usage of the **disk unuse** command and the resultant actions:

```
ServiceBroker# disk unuse disk00
disk00 has key CDNFS data and can not be unused!

ServiceBroker# disk unuse disk01
This will restart applications currently using disk01
and unmount all partitions on disk01.
```

```
Do you want to continue? (Yes/No): yes
[WARNING] CDNFS and RAID SYSTEM partitions detected on disk01
To safely remove a RAID SYSTEM disk, the entire drive must be erased. This
operation has little effect on the RAID-ed SYSTEM volumes, as their data can
be resynced. However, because the drive also contains non-RAID CDNFS
data, it will result in loss of all CDNFS data for this drive!
Unuse disk01, erasing all CDNFS data? (Yes/No): yes
disk01 is now unused.
All partitions on disk01 have been erased.

ServiceBroker# disk unuse disk02
This will restart applications currently using disk02
and unmount all partitions on disk02.
Do you want to continue? (Yes/No): yes
disk02 is now unused
```

The following example shows how to view disk details:

```
ServiceBroker# show disk details
disk00: Normal (h02 c00 i00 l00 - mptsas) 476940MB(465.8GB)
disk00/01: SYSTEM 5120MB(5.0GB) mounted internally
disk00/02: SYSTEM 2560MB(2.5GB) mounted internally
disk00/04: SYSTEM 1536MB(1.5GB) mounted internally
disk00/05: SYSFS 32767MB(32.0GB) mounted at /local1
disk00/06: CDNFS 434948MB(424.8GB) mounted internally
disk01: Normal (h02 c00 i01 l00 - mptsas) 476940MB(465.8GB)
Unallocated: 476940MB(465.8GB)
disk02: Normal (h02 c00 i02 l00 - mptsas) 476940MB(465.8GB)
disk02/01: CDNFS 476932MB(465.8GB) mounted internally
```

The following example shows how to display the current disk space configuration:

```
ServiceBroker# show disk current
Local disks:
    SYSFS 32.0GB 0.7%
    CDNFS 4616.0GB 99.3%
```

The following examples show how to view space allocation in each file system type:

```
ServiceBroker# show statistics cdnfs

CDNFS Statistics:
------------------
Volume on :
  size of physical filesystem:             444740904 KB
  space assigned for CDNFS purposes:       444740904 KB
  number of CDNFS entries:                        40 entries
  space reserved for CDNFS entries:        436011947 KB
  available space for new entries:           8728957 KB
  physical filesystem space in use:        435593864 KB
  physical filesystem space free:            9147040 KB
  physical filesystem percentage in use:          98 %

Volume on :
  size of physical filesystem:             444740904 KB
  space assigned for CDNFS purposes:       444740904 KB
  number of CDNFS entries:                        43 entries
  space reserved for CDNFS entries:        436011384 KB
  available space for new entries:           8729520 KB
  physical filesystem space in use:        435593720 KB
  physical filesystem space free:            9147184 KB
  physical filesystem percentage in use:          98 %

Volume on :
  size of physical filesystem:             488244924 KB
```

```
  space assigned for CDNFS purposes:       488244924 KB
  number of CDNFS entries:                        48 entries
  space reserved for CDNFS entries:        479612533 KB
  available space for new entries:           8632391 KB
  physical filesystem space in use:        479152708 KB
  physical filesystem space free:            9092216 KB
  physical filesystem percentage in use:          99 %
```

The following example shows how to erase all CDNFS volumes and reboot the SB:

```
ServiceBroker# disk recover-cdnfs-volumes
This will erase all CDNFS volumes.
Any applications using CDNFS, including streaming applications, will be killed and the
system will be rebooted.
Please make sure you have offloaded the SB on the VDSM GUI so the SB is no longer sending
traffic to this SB.
Are you sure you want to proceed? [no] yes Are you really sure you want to proceed to
recover and reload? [yes/no] yes

Stopping all services (this may take several minutes) ...
diskman will now recover CDNFS volumes...
CDNFS recovery complete, rebooting now...
```

Related Commands

Command	Description
disk (Global configuration mode)	Configures how the disk errors should be handled.
show cdnfs	Displays the CDS network file system information.
show disk	Displays the disk configurations.
show disk details	Displays more detailed SMART disk monitoring information.
show statistics	Displays statistics by module.

disk (Global configuration)

To configure how disk errors should be handled and to define a disk device error-handling threshold, use the **disk** command in Global configuration mode. To remove the device error-handling options, use the **no** form of this command.

disk error-handling {**bad-sectors-mon-period** *minutes* | **reload** | **threshold** {**alarm-bad-sectors** *bad-sectors* | **alarm-remapped-sectors** *remapped-sectors* | **bad-sectors** bad-sectors | **errors** errors}}

no disk error-handling {bad-sectors-mon-period minutes | reload | threshold {alarm-bad-sectors bad-sectors | alarm-remapped-sectors remapped-sectors | bad-sectors bad-sectors | errors errors}}

Syntax Description

error-handling	Configures disk error handling.
bad-sectors-mon-period	Active bad sectors monitoring period (minutes).
minutes	Default value is 1440 minutes (24 hours); 0 disables sector monitoring. The range is from 0 to 525600.
reload	Whether to reload system if SYSFS disk(s) have problems.
threshold	Configure disk error handling thresholds.
alarm-bad-sectors	Configures the bad sector alarm threshold.
bad-sectors	Number of bad sectors allowed before the disk is marked as bad. The range is from 0 to 100. The default value is 15. The value 0 means that the disk should never be marked as bad.
alarm-remapped-sectors	Configure SMARTinfo remapped sectors alarm threshold (hard drives only).
remapped-sectors	Number of remapped sectors before alarm is triggered. Default value is 128 (hard drives only). The range is from 0 to 8192.
bad-sectors	Configure number of allowed (Active) bad sectors before disk is marked bad. **Note** Only applies to bad sectors detected since system boot.
bad-sectors	Number of bad sectors allowed before disk is marked bad. Default value is 30; 0 means the disk is never mark bad. The range is from 0 to 100.
errors	Configure number of allowed disk errors before marking disk bad. **Note** Only applies to disk or sector errors detected since system boot.
errors	The number of disk errors allowed before the disk is marked bad. Default value is 500; 0 means never mark disk bad. The range is from 0-100000.

Defaults

Bad sector minutes: 1440

Bad sectors alarm: 15

Remapped sectors: 128

Disk bad sectors: 30

Errors: 500

Command Modes

Global configuration (config) mode.

Usage Guidelines

To operate properly, the SB must have critical disk drives. A critical disk drive is the first disk drive that also contains the first sysfs (system file system) partition. It is referred to as disk00. Disk00 is not guaranteed to be the system drive or the 'key' CDNFS drive. For example, the system drives on a 2S6 are internal (disk24 and disk25), and the 'key' CDNSF disk is typically disk00, although it can move to other disks as a result of a missing or bad disk00.

The sysfs partition is used to store log files, including transaction logs, system logs (syslogs), and internal debugging logs. It can also be used to store image files and configuration files on an SB.

Note A critical drive is a disk drive that is either disk00 or a disk drive that contains the first sysfs partition. Smaller single disk drive SBs have only one critical disk drive. Higher-end SBs that have more than one disk drive may have more than one critical disk drive.

When an SB is booted and a critical disk drive is not detected at system startup time, the VDS-SB system on the SB runs at a degraded state. On a generic UCS system the boot partition resides on the system disk (single disk, no RAID). In the event that this disk dies, the system is unbootable. If one of the critical disk drives goes bad at run time, the VDS-SB system applications can malfunction, hang, or crash, or the VDS-SB system can hang or crash. Monitor the critical disk drives on an SB and report any disk drive errors to Cisco TAC.

In a RAIDed system, if a single system disk fails, the system handles the failure seamlessly (apart from any would be CDNFS partitions). If the 'key' CDNFS disk, typically the lowest numbered disk containing CDNFS, fails the system enters an bad state and must be rebooted. In a non-RAID system, if the system disk fails, the system is no longer boots.

With an VDS-SB system, a disk device error is defined as any of the following events:

- Small Computer Systems Interface (SCSI) or Integrated Drive Electronics (IDE) device error is printed by a Linux kernel.
- Disk device access by an application (for example, an open(2), read(2), or write(2) system call) fails with an EIO error code.
- Disk device that existed at startup time is not accessible at run time.

The disk status is recorded in flash (nonvolatile storage). When an error on an SB disk device occurs, a message is written to the system log (syslog) if the sysfs partition is still intact, and an SNMP trap is generated if SNMP is configured on the SB.

In addition to tracking the state of critical disk drives, you can define a disk device error-handling threshold on the SB. If the number of disk device errors reaches the specified threshold, the corresponding disk device is automatically marked as bad.

If the specified threshold is exceeded, the SB either records this event or reboots. If the automatic reload feature is enabled and this threshold is exceeded, then the VDS-SB system automatically reboots the SB. For more information about specifying this threshold, see the "Specifying the Disk Error-Handling Threshold" section on page 2-63.

You can remap bad (but unused) sectors on a SCSI drive and SATA drives using the **disk repair** command.

Disk Latent Sector Error Handling

Latent Sector Errors (LSE) are when a particular disk sector cannot be read from or written to, or when there is an uncorrectable ECC error. Any data previously stored in the sector is lost. There is also a high probability that sectors in close proximity to the known bad sector have as yet undetected errors, and therefore are included in the repair process.

The syslog file shows the following disk I/O error message and smartd error message when there are disk sector errors:

Apr 28 21:00:26 U11-CDE220-2 kernel: %SE-SYS-4-900000: end_request: I/O error, dev sdd, sector 4660

Apr 28 21:00:26 U11-CDE220-2 kernel: %SE-SYS-3-900000: Buffer I/O error on device sdd, logical block 582

Apr 28 21:04:54 U11-CDE220-2 smartd[7396]: %SE-UNKNOWN-6-899999: Device: /dev/sdd, SMART Prefailure Attribute: 1 Raw_Read_Error_Rate changed from 75 to 73

Apr 28 21:04:54 U11-CDE220-2 smartd[7396]: %SE-UNKNOWN-6-899999: Device: /dev/sdd, SMART Usage Attribute: 187 Reported_Uncorrect changed from 99 to 97

Apr 28 21:04:54 U11-CDE220-2 smartd[7396]: %SE-UNKNOWN-2-899999: Device: /dev/sdd, ATA error count increased from 1 to 3

Specifying the Disk Error-Handling Threshold

You can configure a disk error-handling threshold to determine how many disk errors or bad sectors can be detected before the disk drive is automatically marked as bad.

The **disk error-handling threshold bad-sectors** command determines how many bad sectors can be detected before the disk drive is automatically marked as bad. By default, this threshold is set to 15. To change the default threshold, use the **disk error-handling threshold bad-sectors** command. Specify 0 if you never want the disk drive to be marked as bad.

If the bad disk drive is a critical disk drive, and the automatic reload feature (**disk error-handling reload** command) is enabled, then the VDS-SB software marks the disk drive as bad and the SB is automatically reloaded. After the SB is reloaded, a syslog message and an SNMP trap are generated.

The **disk error-handling threshold errors** command determines how many disk errors can be detected before the disk drive is automatically marked as bad. By default, this threshold is set to 500. To change the default threshold, use the **disk error-handling threshold errors** command. Specify 0 if you never want the disk drive to be marked as bad.

By default, the automatic reload feature is disabled on an SB. To enable the automatic reload feature, use the **disk error-handling reload** command. After enabling the automatic reload feature, use the **no disk error-handling reload** command to disable it.

Examples

The following example shows that five disk drive errors for a particular disk drive (for example, disk00) are allowed before the disk drive is automatically marked as bad:

```
ServiceBroker(config)# disk error-handling threshold errors 5
```

Related Commands

Command	Description
disk (EXEC mode)	Allocates the disks among the CDNFS and sysfs file systems.
show disk	Displays the disk configurations.
show disk details	Displays currently effective configurations with more details.

dnslookup

To resolve a host or domain name to an IP address, use the **dnslookup** command in EXEC configuration mode.

dnslookup *line*

Syntax Description

line	Domain name of host on the network.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

The **dnslookup** command accepts IP address. If an IP address is specified in the dnslookup command, the server replies to a query including the IP address and the IP address displays in the output of the and **tcpdump** and **netstat** commands and all logs.

Examples

The following examples show that the **dnslookup** command is used to resolve the hostname *myhost* to IP address 172.31.69.11, *cisco.com* to IP address 192.168.219.25, and an IP address used as a hostname to 10.0.11.0:

```
ServiceBroker# dnslookup myhost
official hostname: myhost.cisco.com
          address: 172.31.69.11

ServiceBroker# dnslookup cisco.com
official hostname: cisco.com
         address: 192.168.219.25

ServiceBroker# dnslookup 10.0.11.0
official hostname: 10.0.11.0
          address: 10.0.11.0
```

enable (EXEC Configuration)

To access privileged commands in EXEC configuration modes, use the **enable** command in EXEC configuration mode.

enable

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

To access privileged EXEC configuration mode from EXEC configuration mode, use the **enable** command. The **disable** command takes you from privileged EXEC configuration mode to user EXEC configuration mode.

Examples

The following example shows how to access privileged EXEC configuration mode:

```
ServiceBroker> enable
ServiceBroker#
```

Related Commands

Command	Description
disable	Turns off the privileged EXEC commands.
exit	Exits from interface, Global configuration, or privileged EXEC configuration modes.

enable (Global Configuration)

To modify enable password parameters, use the **enable password** command in Global configuration mode.

enable password {0 | 1 | *word*}

Syntax Description

password	Assigns a privileged-level password.
0	Specifies an unencrypted password will follow.
1	Specifies a hidden password will follow.
word	The unencrypted (cleartext) user password.

Defaults

None

Command Modes

Global configuration mode.

Examples

The following example shows how to assign a privileged-level unencrypted password:

```
ServiceBroker> enable password 0 xxxx
ServiceBroker#
```

end

To exit Global configuration mode, use the **end** command in Global configuration mode.

end

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Global configuration (config) mode.

Usage Guidelines

Use the **end** command to exit Global configuration mode after completing any changes to the running configuration. To save new configurations to NVRAM, use the **write** command.

In addition, you can press **Ctrl-Z** to exit Global configuration mode.

Examples

The following example shows how to exit Global configuration mode:

```
ServiceBroker(config)# end
ServiceBroker#
```

Related Commands

Command	Description
exit	Exits from interface, Global configuration, or privileged EXEC configuration modes.

exec-timeout

To configure the length of time that an inactive Telnet or Secure Shell (SSH) session remains open, use the **exec-timeout** command in Global configuration mode. To revert to the default value, use the **no** form of this command.

exec-timeout *timeout*

no exec-timeout

Syntax Description

timeout	Timeout in minutes. The range is from 0–44640. The default is 15.

Defaults

The default is 15 minutes.

Command Modes

Global configuration (config) mode.

Usage Guidelines

A Telnet or SSH session with the SB can remain open and inactive for the interval of time specified by the **exec-timeout** command. When the exec-timeout interval elapses, the SB automatically closes the Telnet or SSH session.

Configuring a timeout interval of 0 minutes by entering the **exec-timeout 0** command is equivalent to disabling the session-timeout feature.

Examples

The following example shows how to configure a timeout of 100 minutes:

```
ServiceBroker(config)# exec-timeout 100
```

The following example negates the configured timeout of 100 minutes and reverts to the default value of 15 minutes:

```
ServiceBroker(config)# no exec-timeout
```

Related Commands

Command	Description
sshd	Configures the SSH service parameters.
telnet enable	Enables the Telnet services.

exit

To access commands in EXEC configuration mode shell from the global, interface, and debug configuration command shells, use the **exit** command.

exit

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

EXEC, Global configuration (config), and interface configuration (config-if) modes.

Usage Guidelines

Use the **exit** command in any configuration mode to return to EXEC configuration mode. Using this command is equivalent to pressing the **Ctrl-Z** key or entering the **end** command.

The **exit** command issued in the user-level EXEC shell terminates the console or Telnet session. You can also use the **exit** command to exit other configuration modes that are available from the Global configuration mode for managing specific features (see the commands marked with a footnote in Table 2-1).

Examples

The following example shows how to exit the Global configuration mode and return to the privileged-level EXEC configuration mode:

```
ServiceBroker(config)# exit
ServiceBroker#
```

The following example shows how to exit the privileged-level EXEC configuration mode and return to the user-level EXEC configuration mode:

```
ServiceBroker# exit
ServiceBroker>
```

Related Commands

Command	Description
end	Exits configuration and privileged EXEC configuration modes.

expert-mode

To configure debugshell, use the **expert-mode** command in Global configuration mode.

expert-mode password [**encrypted**] *password*

Syntax Description

password	Sets the expert mode password.
encrypted	(Optional) Encrypts the password.
password	The encrypted password.

Defaults

None

Command Modes

Global configuration (config) mode.

Usage Guidelines

This is a customer configurable password for allowing to enter engineering mode for troubleshooting purposes. The function prompts the user for the current admin password to verify that the user attempting to set the expert-mode password is authorized to do so. If the user is authenticated, the user is prompted twice to enter the new expert-mode password. The new expert-mode password is encrypted prior to being persisted.

Examples

The following example shows how to configure debugshell:

```
ServiceBroker(config)# expert-mode password encrypted xxxx
New Expert Mode Password: xxxx
Confirm New Expert Mode Password: xxxx
Password successfully changed
```

external-ip

To configure up to eight external Network Address Translation (NAT) IP addresses, use the **external-ip** command in Global configuration mode. To remove the NAT IP addresses, use the **no** form of this command.

external-ip *ip_addresses*

no external-ip *ip_addresses*

Syntax Description

ip_addresses	A maximum of eight external or NAT IP addresses can be configured.

Defaults

None

Command Modes

Global configuration (config) mode.

Usage Guidelines

Use this command to configure up to eight Network Address Translation IP addresses to allow the router to translate up to eight internal addresses to registered unique addresses and translate external registered addresses to addresses that are unique to the private network. If the IP address of the RTSP gateway has not been configured on the SB, then the external IP address is configured as the IP address of the RTSP gateway.

In an VDS-SB network, there are two methods for a device registered with the VDSM (SBs, or the standby VDSM) to obtain configuration information from the primary VDSM. The primary method is for the device to periodically poll the primary VDSM on port 443 to request a configuration update. You cannot configure this port number. The backup method is when the VDSM pushes configuration updates to a registered device as soon as possible by issuing a notification to the registered device on port 443. This method allows changes to take effect in a timelier manner. You cannot configure this port number even when the backup method is being used. VDS-SB networks do not work reliably if devices registered with the VDSM are unable to poll the VDSM for configuration updates. When a receiver SB requests the content and content metadata from a forwarder SB, it contacts the forwarder SB on port 443.

When a device (SBs at the edge of the network, SBs, and primary or standby VDSMs) is inside a NAT firewall, those devices that are inside the same NAT use one IP address (the inside local IP address) to access the device and those devices that are outside the NAT use a different IP address (the NAT IP address or inside global IP address) to access the device. A centrally managed device advertises only its inside local IP address to the VDSM. All other devices inside the NAT use the inside local IP address to contact the centrally managed device that resides inside the NAT. A device that is not inside the same NAT as the centrally managed device cannot contact it without a special configuration.

If the primary VDSM is inside a NAT, you can allow a device outside the NAT to poll it for getUpdate requests by configuring a static translation (NAT IP address or inside global IP address) for the VDSM's inside local IP address on its NAT, and using this address, rather than the VDSM's inside local IP address in the **VDSM ip** *ip_address* command when you register the device to the VDSM. If an SB is inside a NAT and the VDSM is outside the NAT, you can allow the SB to poll for getUpdate requests by configuring a static translation (NAT IP address or inside global IP address) for the SB's inside local address on its NAT.

Note Static translation establishes a one-to-one mapping between your inside local address and an inside global address. Static translation is useful when a host on the inside must be accessible by a fixed address from the outside.

Examples

The following example shows how to configure four external NAT IP addresses:

```
ServiceBroker(config)# external-ip 192.168.43.1 192.168.43.2 192.168.43.3 192.168.43.4
```

find-pattern

To search for a particular pattern in a file, use the **find-pattern** command in EXEC configuration mode.

find-pattern {**binary** *filename* | **case** {**binary** *filename* | **count** *filename* | **lineno** *filename* | **match** *filename* | **nomatch** *filename* | **recursive** *filename*} | **count** *filename* | **lineno** *filename* | **match** *filename* | **nomatch** *filename* | **recursive** *filename*}

Syntax Description

binary	Does not suppress the binary output.
filename	Filename.
case	Matches the case-sensitive pattern.
count	Prints the number of matching lines.
lineno	Prints the line number with output.
match	Prints the matching lines.
nomatch	Prints the nonmatching lines.
recursive	Searches a directory recursively.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

Use this command to search for a particular regular expression pattern in a file.

Examples

The following example shows how to search a file recursively for a case-sensitive pattern:

```
ServiceBroker# find-pattern case recursive admin removed_core
-rw-------    1 admin    root     95600640 Oct 12 10:27 /local/local1/core_dir/c
ore.2.2.1.b5.eh.2796
-rw-------    1 admin    root     97054720 Jan 11 11:31 /local/local1/core_dir/c
ore.cache.5.3.0.b131.cnbuild.14086
-rw-------    1 admin    root     96845824 Jan 11 11:32 /local/local1/core_dir/c
ore.cache.5.3.0.b131.cnbuild.14823
-rw-------    1 admin    root     101580800 Jan 11 12:01 /local/local1/core_dir/
core.cache.5.3.0.b131.cnbuild.15134
-rw-------    1 admin    root     96759808 Jan 11 12:59 /local/local1/core_dir/c
ore.cache.5.3.0.b131.cnbuild.20016
-rw-------    1 admin    root     97124352 Jan 11 13:26 /local/local1/core_dir/c
ore.cache.5.3.0.b131.cnbuild.30249
-rw-------    1 admin    root     98328576 Jan 11 11:27 /local/local1/core_dir/c
ore.cache.5.3.0.b131.cnbuild.8095
```

The following example searches a file for a pattern and prints the matching lines:

```
ServiceBroker# find-pattern match 10 removed_core
Tue Oct 12 10:30:03 UTC 2004
-rw-------    1 admin    root     95600640 Oct 12 10:27 /local/local1/core_dir/c
ore.5.2.1.b5.eh.2796
-rw-------    1 admin    root     101580800 Jan 11 12:01 /local/local1/core_dir/
core.cache.5.3.0.b131.cnbuild.15134
```

The following example searches a file for a pattern and prints the number of matching lines:

```
ServiceBroker# find-pattern count 10 removed_core
3
```

Related Commands

Command	Description
cd	Changes the directory.
dir	Displays the list of files in a directory.
lls	Displays the files in a long list format.
ls	Lists the files and subdirectories in a directory.

ftp

To enable File Transfer Protocol (FTP) services, use the **ftp** command in Global configuration mode. To cancel the request, use the **no** form of this command.

ftp enable

no ftp enable

Syntax Description

enable	Enables FTP services.

Defaults

None

Command Modes

Global configuration (config) mode.

Examples

The following example shows how to enable FTP services:

```
ServiceRouter# ftp enable
```

Related Commands

Command	Description
show ftp	Displays the caching configuration of the FTP.

geo-location-server

To monitor primary and secondary servers, use the **geo-location-server** command in EXEC configuration mode. To disable monitoring, restore default values for timeoutand poll-rate, use the no form of this command.

geo-location-server { geo-pre-cache-file | monitor | poll-rate | timeout | primary | secondary | pre-cache }

no geo-location-server { geo-pre-cache-file | monitor | poll-rate | timeout | primary | secondary | pre-cache }

Syntax Description

geo-pre-cache-file	Configures Geo Pre-Cache config file.
monitor	Enables or Disables Geolocation Server monitoring.
poll-rate	Configures Geolocation Server polling interval.
timeout	Configures Geolocation Server timeout.
primary	Configures Primary Geolocation server ip address and port.
secondary	Configures Secondary Geolocation server ip address and port.
pre-cache	Configures Geo Pre-Cache settings.

Defaults

Monitor: enabled

Poll-rate: 60 seconds

Timeout: 1 second

Command Modes

EXEC configuration mode.

Examples

The following example shows how to enable geo-location-server monitor for the SB:

```
ServiceBroker# geo-location-server monitor
ServiceBroker# show geo-location-server
Geo Location server monitoring is enabled
Geo Location server poll rate 60 seconds
Geo Location server timeout 1 seconds
Geo pre-cache size is 500
```

The following example shows how to disable geo-location-server monitor for the SB:

```
ServiceBroker# no geo-location-server monitor
ServiceBroker# show geo-location-server
Geo Location server monitoring is disabled
Geo Location server poll rate 60 seconds
Geo Location server timeout 1 seconds
Geo pre-cache size is 500
```

gulp

To capture lossless gigabit packets and write them to disk, use the **gulp** command in EXEC configuration mode.

gulp *line*

Syntax Description		
	line	(Optional) Specifies gulp options, enter **-h** to get help.

Task ID

None

Command Modes

EXEC configuration mode.

Usage Guidelines

The **gulp** utility captures lossless gigabit packets and writes them to disk, as well as captures packets remotely. The **gulp** utility has the ability to read directly from the network.

To view the list of options, enter **gulp --h**.

```
ServiceBroker# gulp --help

Usage: /ruby/bin/gulp [--help | options]
    --help      prints this usage summary
    supported options include:
      -d        decapsulate Cisco ERSPAN GRE packets (sets -f value)
      -f "..."  specify a pcap filter - see manpage and -d
      -i eth#|- specify ethernet capture interface or '-' for stdin
      -s #      specify packet capture "snapshot" length limit
      -r #      specify ring buffer size in megabytes (1-1024)
      -c        just buffer stdin to stdout (works with arbitrary data)
      -x        request exclusive lock (to be the only instance running)
      -X        run even when locking would forbid it
      -v        print program version and exit
      -Vx...x   display packet loss and buffer use - see manpage
      -p #      specify full/empty polling interval in microseconds
      -q        suppress buffer full warnings
      -z #      specify write blocksize (power of 2, default 65536) for long-term capture
      -o dir    redirect pcap output to a collection of files in dir
      -C #      limit each pcap file in -o dir to # times the (-r #) size
      -W #      overwrite pcap files in -o dir rather than start #+1
      -B        check if select(2) would ever have blocked on write
      -Y        avoid writes which would block
```

Table 2-3 lists the gulp options and provides a description of each.

Table 2-3 gulp Options

Option	Description
-d	Decapsulates packets from a Cisco Encapsulated Remote SPAN Port (ERSPAN). Sets the pcap filter expression to "proto gre" and strips off Cisco GRE headers (50 bytes) from the packets captured. (If used with -f option note that arguments are processed left to right).
-f	Specify a pcap filter expression. This may be useful to select one from many GRE streams if using -d, or if not using -d, because filtering out packets in the kernel is more efficient than passing them first through the **gulp** utility and then filtering them out.
-i *eth#*	Specify the network interface to read from. The default is eth1 or the value of the environment variable $CAP_IFACE, if present. Specifying a hyphen (-) as the interface reads a pcap file from the standard input instead. (If you forget the -d option during a live capture, you can decapsulate offline this way.)
-r #	Specify a ring buffer size (in megabytes). Values from 1–1024 are permitted. The default is 100. If possible, the ring buffer is locked into RAM.
-c	Copy and buffer bytes from stdin to stdout—do not read packets from the network and do not assume anything about the format of the data. This may be useful to improve the real-time performance of another application.
-s #	Specify packet capture snapshot length. By default, complete packets are captured. For efficiency, captured packets can be truncated to a given length during the capture process, which reduces capture overhead and pcap file sizes. (If used with the -d option, it specifies the length after decapsulation.)
-x	Use file locking to request (by way of exclusive lock) that this is the only instance of the **gulp** utility running. If other instances are already running, they must be stopped before the **gulp** utility can start with this option.
-X	Override an exclusive lock (-x option) and run anyway. An instance of **gulp** started this way holds a shared lock if no exclusive locks were broken; otherwise, it holds no locks at all (causing a subsequent attempt to get an exclusive lock to succeed).
-v	Print program version and exit.
-V xxxxxxxx	If the string of Xs is wide enough (10 or more), it is overwritten twice per second with a brief capture status update consisting of one digit followed by two percentages. The digit is the number of decimal digits in the actual count of lost packets (0 indicates no drops). The two percentages are the current and maximum ring buffer utilization. The updated argument string can be seen with the ps -x option (or equivalent). If the string of Xs is too short to hold the information above, a more verbose status line is written, twice per second, to standard error instead. The first method is probably more useful to occasionally check on long captures and the second is more convenient while experimenting and setting up a capture.
-p #	Specify the thread polling interval (in microseconds). The reader and writer threads poll at this interval when the ring buffer is full or empty. Polling (even frequently) on modern hardware consumes immeasurably few resources. The default interval is 1000.
-q	Suppress warnings about the ring buffer being full. If input is not from a live capture, no data is lost when the ring buffer fills so the warning can be safely suppressed. If stdin is actually a file, warning suppression happens automatically.
-z #	Specify output write block size. Any power of two between 4096 and 65536. The default is 65536.

Table 2-3 gulp Options (continued)

Option	Description
-o *dir*	Redirects pcap output into a collection of files in the specified directory. Pcap files are named pcap###, where ### starts at 000 and increments. The directory must exist and be writable by the user running the **gulp** utility.
-C #	When using the -o option, start a new pcap file when the old one reaches about # times the size of the ring buffer. The default value is 10 and the default ring buffer size is 100MB; so by default, pcap files grow to about 1000 MB before a new one is started. Since some programs read an entire pcap file into memory when using it, splitting the output into chunks can be helpful.
-W #	Specifies a maximum number of pcap files to create before overwriting them. The default is to never overwrite them. This option allows capturing to occur indefinitely with finite disk space.
-B	This option enables the code to check before each write whether the write would block. When the **gulp** utility exits, it announces whether any writes would have been blocked.
-Y	This option writes which ones would be blocked, but are deferred until they are not blocked.

Examples

The following example shows how to get a basic capture on eth1 with a pcap filter:

```
ServiceBroker# gulp -i eth1 -f "..." > pcapfile
```

The ellipsis (...) refers to the Berkeley Packet Filter (pcap) expressions, such as “host foo.”

The following example shows how to get a capture of the 10 most recent files of a 200 MB ring buffer to 1000 MB files:

```
ServiceBroker# gulp -i eth1 -r 200 -C 10 -W 10 -o pcapdir
```

Related Commands

Command	Description
netmon	Displays the transmit and receive activity on an interface.
netstatr	Displays the rate of change of netstat statistics.
ss	Dumps socket statistics.
tcpmon	Searches all TCP connections.

help

To obtain online help for the command-line interface, use the **help** command in EXEC and Global configuration modes.

help

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

EXEC configuration and Global configuration (config) modes.

Usage Guidelines

You can get help at any point in a command by entering a question mark (**?**). If nothing matches, the help list is empty, and you must back up until entering a **?** shows the available options.

Two styles of help are provided:

- Full help is available when you are ready to enter a command argument (for example, **show ?**). In addition, full help describes each possible argument.
- Partial help is provided when you enter an abbreviated command and you want to know what arguments match the input (for example, **show stat?**).

Examples

The following example shows the output of the **help** command in EXEC configuration mode:

```
ServiceBroker# 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 stat?'.)
```

hostname

To configure the device's network hostname, use the **hostname** command in Global configuration mode. To reset the hostname to the default setting, use the **no** form of this command.

hostname *name*

no hostname

Syntax Description

name	New hostname for the device; the name is case sensitive. The name may be from 1 to 30 alphanumeric characters.

Defaults

The default hostname is the SB model number.

Command Modes

Global configuration (config) mode.

Usage Guidelines

Use this command to configure the hostname for the SB. The hostname is used for the command prompts and default configuration filenames. This name is also used by content routing and conforms to the following rules:

- It can use only alphanumeric characters and hyphens (-).
- Maximum length is 30 characters.
- Following characters are considered invalid and cannot be used when naming a device: @, # , $,%, ^, &, *, (), | , \””/, <>.

Examples

The following example changes the hostname to Sandbox:

```
ServiceBroker(config)# hostname Sandbox
Sandbox(config)#
```

The following example removes the hostname:

```
ServiceBroker(config)# no hostname
NO-HOSTNAME(config)#
```

Related Commands

Command	Description
dnslookup	Resolves a host or domain name to an IP address.
ip	Configures the IP.
show hosts	Displays the IP domain name, name servers, IP addresses, and host table.

http

To configure HTTP-related parameters, use the **http** command in EXEC configuration mode.

http asx-302-redirect enable

Syntax Description

asx-302-redirect	Configures 302 response for asx requests.
enable	Enables 302 redirection for asx requests.

Defaults

None

Command Modes

EXEC configuration mode.

Examples

The following example shows how to install a .bin file on the SB:

```
ServiceBroker# install VDS-SB-2.2.1.7-K9.bin
```

install

To install the VDS-SB software image, use the **install** command in EXEC configuration mode.

install *imagefile_name*

Syntax Description

imagefile_name	Name of the .bin file that you want to install.

Defaults

None

Command Modes

EXEC configuration mode.

Usage Guidelines

The **install** command loads the system image into flash memory and the disk.

To install a system image, copy the image file to the sysfs directory local1 or local2. Before entering the **install** command, change the present working directory to the directory where the system image resides. When the **install** command is executed, the image file is expanded. The expanded files overwrite the existing files in the SB. The newly installed version takes effect after the system image is reloaded.

Note The **install** command does not accept .pax files. Files should be of the .bin type (for example, VDS-SB-2.2.1.7-K9.bin). Also, if the release being installed does not require a new system image, then it may not be necessary to write to flash memory. If the newer version has changes that require a new system image to be installed, then the **install** command may result in a write to flash memory.

Examples

The following example shows how to install a .bin file on the SB:

```
ServiceBroker# install VDS-SB-2.2.1.7-K9.bin
```

Related Commands

Command	Description
copy ftp install	Installs an image file from an FTP server onto a local device.
copy http install	Installs an image file from an HTTP server onto a local device.
reload	Halts a device and performs a cold restart.

interface

To configure a Gigabit Ethernet or port channel interface, use the **interface** command in Global configuration mode. To disable selected options, restore default values, or enable a shutdown interface, use the **no** form of this command.

interface {**GigabitEthernet** *slot/port_num* [**autosense** | **bandwidth** {**10** | **100** | **1000**} | **channel-group** *group_interface* | **description** *line* | **full-duplex** | **half-duplex** | **ip** {**access-group** {*access_list_num* {**in** | **out**} | *name*} | **address** {*ip_address_netmask* | **range** *low_num high_num netmask*} | **ipv6** {**access-group** {*access_list_num* {**in** | **out**} | *access_list_name* {**in** | **out**}} | **address** {*range low_num high_num netmask* {*prefix* | *subnet_mask*} | *ip_addr/mask*} | **mtu** *mtu_size* | **shutdown** | **standby** *num* [**priority** *num*] | **tx-queue-limit** *queue_length*] | **PortChannel** *num* [**autosense** | **bandwidth** {**10** | **100** | **1000**} | **description** line | **full-duplex** | **half-duplex** | **ip** *line* | **ipv6** *line* | **lacp** | **shutdown** | **standby** *num* [**priority** num] | **Standby** *group_number* [**description** *line* | **errors** *error_num* | **ip address** {*ip_address_netmask* | **range** *low_num high_num netmask*}| **ipv6 address** {**range** *low_num high_num netmask* {*prefix* | *subnet_mask*} | *ip_addr/mask*} | **shutdown**] | **TenGigabitEthernet** *slot/port_num* [**autosense** | **bandwidth** {**10** | **100** | **1000**} **channel-group** *group_interface* | **description** *line* | **full-duplex** | **half-duplex** | **ip** {**access-group** {*access_list_num* {**in** | **out**} | *name*} | **address** {*ip_address_netmask* | **range** *low_num high_num netmask*} | **ipv6** {*acccess-group* {*access_list_num* {**in** | **out**}| *access_list_name* {**in** | **out**}} | **address** {**range** *low_num high_num netmask* {*prefix* | *subnet_mask*} | *ip_addr/mask*} | **mtu** *mtu_size* | **shutdown** | **standby** *num* [**priority** *num*] | **tx-queue-limit** *queue_length*]

no interface {**GigabitEthernet** *slot/port_num* [**autosense** | **bandwidth** {**10** | **100** | **1000**} | **channel-group** *group_interface* | **description** *line* | **full-duplex** | **half-duplex** | **ip** {**access-group** {*access_list_num* {**in** | **out**} | *name*} | **address** {*ip_address_netmask* | **range** *low_num high_num netmask*} | **ipv6** {**access-group** {*access_list_num* {**in** | **out**}| *access_list_name* {**in** | **out**}} | **address** {*range low_num high_num netmask* {*prefix* | *subnet_mask*} | *ip_addr/mask*} | **mtu** *mtu_size* | **shutdown** | **standby** *num* [**priority** *num*] | **tx-queue-limit** *queue_length*] | **PortChannel** *num* [**autosense** | **bandwidth** {**10** | **100** | **1000**} | **description** line | **full-duplex** | **half-duplex** | **ip** *line* | **ipv6** *line* | **lacp** | **shutdown** | **standby** *num* [**priority** num] | **Standby** *group_number* [**description** *line* | **errors** *error_num* | **ip address** {*ip_address_netmask* | **range** *low_num high_num netmask*}| **ipv6 address** {**range** *low_num high_num netmask* {*prefix* | *subnet_mask*} | *ip_addr/mask*} | **shutdown**] | **TenGigabitEthernet** *slot/port_num* [**autosense** | **bandwidth** {**10** | **100** | **1000**} **channel-group** *group_interface* | **description** *line* | **full-duplex** | **half-duplex** | **ip** {**access-group** {*access_list_num* {**in** | **out**} | *name*} | **address** {*ip_address_netmask* | **range** *low_num high_num netmask*} | **ipv6** {*acccess-group* {*access_list_num* {**in** | **out**}| *access_list_name* {**in** | **out**}} | **address** {**range** *low_num high_num netmask* {*prefix* | *subnet_mask*} | *ip_addr/mask*} | **mtu** *mtu_size* | **shutdown** | **standby** *num* [**priority** *num*] | **tx-queue-limit** *queue_length*]

Syntax Description

GigabitEthernet	Selects a Gigabit Ethernet interface to configure.
slot/port_num	Slot and port number for the selected interface. The slot range is from 1 to 14; the port range is from 0 to 0. The slot number and port number are separated with a forward slash character (/).
autosense	(Optional) Specifies interface autosense.
bandwidth	(Optional) Configures the interface bandwidth.
10	Specifies the interface bandwidth as 10 Mbits per second.
100	Specifies the interface bandwidth as 100 Mbits per second.

1000	Specifies the interface bandwidth as 1000 Mbits per second.
channel-group	(Optional) Configures the EtherChannel group.
group_interface	EtherChannel group to which the interface belongs. The range is 1 to 4.
description	(Optional) Specifies interface specific description.
line	Text describing this interface
full-duplex	(Optional) Specifies full-duplex.
half-duplex	(Optional) Specifies half-duplex.
ip	(Optional) Interface Internet Protocol configuration commands.
access-group	Specifies access control for packets.
acccess_list_num	IP access list (standard or extended).
in	Specifies inbound packets.
out	Specifies outbound packets.
name	Specifies the access-list name.
address	Sets the IP address of the interface.
ip_address	IP address of the interface
netmask	Netmask of the interface.
range	IP address range.
low_num	IP address low range of the interface.
high_num	IP address low range of the interface.
netmask	Netmask of the interface.
access-group	Specifies access control for packets.
ip_access_list	IP access list (standard or extended).
in	Inbound packets.
out	Outbound packets.
access-list-name	Specifies an access list name.
prefix	Interface prefix. The range is from 1 to 128.
mtu	Sets the interface Maximum Transmission Unit (MTU).
mtu_size	MTU size in bytes. The range is 576 to 9216.
shutdown	(Optional) Shuts down the specific portchannel interface.
standby	(Optional) Standby interface configuration commands.
interface_group_num	Group number for the selected interface. The range is from 1 to 4.
priority	Sets the priority of the interface. Default value is 100.
standby_group_priority	Set the priority of the interface for the standby group. The range is from 0 to 4294967295.
tx-queue-limit	Sets the interface maximum Transmission Queue Length.
queue_length	Sets the limit on the transmission queue length. The range is from 1000 to 80000.
PortChannel	Selects the Ethernet Channel of interfaces to be configured.
num	Sets the Ethernet Channel interface number. The range is from 1 to 4.
lacp	Specifies Link Aggregation Control Protocol.
Standby	Specifies a standby group number.
standby_group_num	Standby group number. The range is from 1 to 4.

description	(Optional) Standby interface description.
line	Text describing this interface.
errors	Sets the maximum number of errors allowed on this interface.
error_num	Maximum number of errors allowed on this interface for the standby group. The range is from 1 to 2147483647.
ip	Sets the IP address of the standby group.
address	Sets the IP address of the interface.
standby_group_ip_addr	IP address of the standby group.
standby_group_ netmask	Netmask of the standby group.
range	Sets the IP address range of the standby group.
low_range	IP address low range of an interface.
high_range	IP address high range of an interface.
interface_netmask	Netmask of the interface.
TenGigabitEthernet	Selects a ten Gigabit Ethernet interface to configure.

Defaults

Standby priority: 100.

Command Modes

Global configuration (config) mode.

Usage Guidelines

Note The Gigabit Ethernet interfaces are shared between CIMC and UCS for UCS devices (specifically UCS220). The default values for duplex, speed, auto negotiation and advertising *cannot* be changed.

String to Be Set as Cookie Port Channel (EtherChannel) Interface

EtherChannel for Cisco VDS Service Broker supports the grouping of up to four same- network interfaces into one virtual interface. This grouping allows the setting or removing of a virtual interface that consists of two Gigabit Ethernet interfaces. EtherChannel also provides interoperability with Cisco routers, switches, and other networking devices or hosts supporting EtherChannel, load balancing, and automatic failure detection and recovery based on current link status of each interface.

You can use the Gigabit Ethernet ports to form an EtherChannel. A physical interface can be added to an EtherChannel subject to the device configuration.

Configuring Multiple IP Addresses

The Multiple Logical IP Addresses feature supports up to 24 unique IP addresses within the same subnet for the same interface.

When you configure multiple IP addresses on an SB using either the range option or using individual commands, the **show running-config** output displays all the IP addresses individually. The netmask value is unique for each interface, so under a single interface you cannot have multiple IP addresses with different netmask values.

Examples

The following example shows how to create an EtherChannel. The port channel is port channel 2 and is assigned an IP address of 10.10.10.10 and a netmask of 255.0.0.0:

```
ServiceBroker# configure
ServiceBroker(config)# interface PortChannel 2
ServiceBroker(config-if)# exit
```

The following example how to remove an EtherChannel:

```
ServiceBroker(config)# interface PortChannel 2
ServiceBroker(config-if)# exit
ServiceBroker(config)# no interface PortChannel 2
```

The following example shows a sample output of the **show running-config** command in EXEC configuration mode:

```
ServiceBroker# show running-config
.
.
.
interface GigabitEthernet 0/0
description This is an interface to the WAN
ip address 192.168.1.200 255.255.255.0
bandwidth 100
exit
.
.
```

The following example shows the sample output of the **show interface** command:

```
ServiceBroker# show interface GigabitEthernet 1/0
Description: This is the interface to the lab
type: Ethernet
```

The following example shows how to create standby groups on SBs:

```
ServiceBroker(config)# interface GigabitEthernet 1/0 standby 2 priority 300
ServiceBroker(config)# interface GigabitEthernet 2/0 standby 2 priority 200
ServiceBroker(config)# interface GigabitEthernet 3/0 standby 2 priority 100
ServiceBroker(config)# interface standby 2 errors 10000
```

The following example shows how to configure multiple IP addresses using a range command:

```
ServiceBroker(config)# interface PortChannel 2
ServiceBroker(config-if)# ip address range 2.2.2.3 2.2.2.6 255.255.255.0
```

The following example shows a sample output of the **show running-config** command in EXEC configuration mode after configuring multiple IP addresses:

```
ServiceBroker# show running-config
.
interface PortChannel 4
 ip address 2.2.2.3 255.255.255.0
 ip address 2.2.2.4 255.255.255.0
 ip address 2.2.2.5 255.255.255.0
 ip address 2.2.2.6 255.255.255.0
 exit
```

Related Commands

Command	Description
show interface	Displays the hardware interface information.
show running-config	Displays the current operating configuration.
show startup-config	Displays the startup configuration.

iostat

To Show CPU and I/O statistics for devices and partitions, use the **iostat** command in EXEC configuration mode.

iostat [*line*]

Syntax Description

line	Specifies iostat options.

Defaults

None

Command Modes

EXEC configuration mode.

Examples

The following example shows how to display CPU statistics:

```
ServiceBroker# iostat
Linux 2.6.32.52-cds-64 (W14-UCS220-2)   10/16/12        _x86_64_        (32 CPU)

avg-cpu:  %user   %nice %system %iowait  %steal   %idle
           0.00    0.03    0.03    0.00    0.00   99.93

Device:            tps    kB_read/s    kB_wrtn/s    kB_read    kB_wrtn
sdc               1.79         7.24        30.89     580715    2478770
sdd               0.00         0.05         0.03       4143       2057

ServiceBroker#
```

ip (Global configuration)

To change initial network device configuration settings, use the **ip** command in Global configuration mode. To delete or disable these settings, use the **no** form of this command.

ip {**access-list** (see "ip access-list" section on page 99) | **default-gateway** *ip_address* [*gateway_ip_addr*] | **domain-name** *name1 name2 name3* | **name-server** *ip_addresses* | **path-mtu-discovery enable** | **route** *dest_IP_addr dest_netmask default_gateway* [**interface** *source_IP_addr*]}

no ip {**access-list** | **default-gateway** *ip_address* [*gateway_ip_addr*] | **domain-name** *name1 name2 name3* | **name-server** *ip_addresses* | **path-mtu-discovery enable** | **route** *dest_IP_addr dest_netmask default_gateway* [**interface** *source_IP_addr*]}

Syntax Description

access-list	Specifies the access list.
default-gateway	Specifies the default gateway (if not routing IP).
ip_address	IP address of the default gateway.
gateway_ip_addr	(Optional) Gateway IP address (maximum of 14).
domain-name	Specifies domain names.
name1 through *name3*	Domain name (up to three can be specified).
name-server	Specifies the address of the name server.
ip_addresses	IP addresses of the domain server (up to a maximum of eight).
path-mtu-discovery	Configures RFC 1191 Path Maximum Transmission Unit (MTU) discovery.
enable	Enables Path MTU discovery.
route	Specifies the net route.
dest_IP_addr	Destination route address.
dest_netmask	Netmask address.
default_gateway	Gateway address.
interface	Configures source policy routing to route outgoing traffic using the same interface where the request was received.
source_IP_addr	IP address of the interface configured for source policy routing.

Defaults

None

Command Modes

Global configuration (config) mode.

Usage Guidelines

To define a default gateway, use the **ip default-gateway** command. Only one default gateway can be configured. To remove the IP default gateway, use the **no** form of this command. The SB uses the default gateway to route IP packets when there is no specific route found to the destination.

To define a default domain name, use the **ip domain-name** command. To remove the IP default domain name, use the **no** form of this command. Up to three domain names can be entered. If a request arrives without a domain name appended in its hostname, the proxy tries to resolve the hostname by appending *name1*, *name2*, and *name3* in that order until one of these names succeeds.

The SB appends the configured domain name to any IP hostname that does not contain a domain name. The appended name is resolved by the DNS server and then added to the host table. The SB must have at least one domain name server specified for hostname resolution to work correctly.

To specify the address of one or more name servers to use for name and address resolution, use the **ip name-server** *ip_addresses* command. To disable IP name servers, use the **no** form of this command. For proper resolution of the hostname to the IP address or the IP address to the hostname, the SB uses DNS servers. Use the **ip name-server** command to point the SB to a specific DNS server. You can configure up to eight servers.

Path MTU autodiscovery discovers the MTU and automatically sets the correct value. Use the **ip path-mtu-discovery enable** command to start this autodiscovery utility. By default, this feature is enabled. When this feature is disabled, the sending device uses a packet size that is smaller than 576 bytes and the next hop MTU. Existing connections are not affected when this feature is turned on or off.

The Cisco VDS Service Broker software supports IP Path MTU Discovery, as defined in RFC 1191. When enabled, Path MTU Discovery discovers the largest IP packet size allowable between the various links along the forwarding path and automatically sets the correct value for the packet size. By using the largest MTU that the links bear, the sending device can minimize the number of packets that it must send.

Note IP Path MTU Discovery is useful when a link in a network goes down, forcing the use of another, different MTU-sized link. IP Path MTU Discovery is also useful when a connection is first being established and the sender has no information at all about the intervening links.

IP Path MTU Discovery is started by the sending device. If a server does not support IP Path MTU Discovery, the receiving device has no mechanism available to avoid fragmenting datagrams generated by the server.

Use the **ip route** command to add a specific static route for a network or host. Any IP packet designated for the specified destination uses the configured route.

To configure static IP routing, use the **ip route** command. To remove the route, use the **no** form of this command. Do not use the **ip route 0.0.0.0 0.0.0.0** command to configure the default gateway; use the **ip default-gateway** command instead.

Source Policy Routes

To configure source policy routing, use the **ip route** command with the interface option. By using source policy routing, the reply packet to a client leaves the SB on the same interface where the request came in. Source policy routing tables are automatically instantiated based on the interface subnets defined on the system. The policy routes are added automatically to the policy routing tables based on the nexthop gateway of the routes in the main routing table.

When configuring multiple IP address you must configure a default gateway in the same subnet. You can configure multiple gateways (up to 14).

The CDE220-2S3i supports multiple IP addresses, which includes specifying the default gateway and IP routes. The IP routes, source policy routes, were added to ensure incoming traffic would go out the same interface it came in on. An IP route was added using the **interface** keyword and has the following syntax:

ip route <*dest_IP_addr*> <*dest_netmask*> <*default_gateway*> *interface* <*source_IP_addr*>

In the following example, all destination traffic (IP address of 0.0.0.0 and netmask of 0.0.0.0) sent from the source interface, 8.1.0.2, uses the default gateway, 8.1.0.1. This is a default policy route.

ip route 0.0.0.0 0.0.0.0 8.1.0.1 interface 8.1.0.2

A non-default policy route defines a specific destination (IP address and netmask). The following **ip route** command is an example of a non-default policy route:

ip route 10.1.1.0 255.255.255.0 <*gateway*> interface <*source_IP_addr*>

Because you had to define the default gateway for all the interfaces as part of the multi-port support feature, the equivalent source policy route is automatically generated in the routing table. The following example shows the output for the **show ip route** command after upgrading the software with the default source policy routes highlighted in bold and the non-default policy routes highlighted in italics:

```
ServiceBroker# show ip route

Destination      Gateway          Netmask
---------------- ---------------- ----------------
172.22.28.0      8.1.0.1          255.255.255.128
6.21.1.0         0.0.0.0          255.255.255.0
8.2.1.0          0.0.0.0          255.255.255.0
8.2.2.0          0.0.0.0          255.255.255.0
171.70.77.0      8.1.0.1          255.255.255.0
8.1.0.0          0.0.0.0          255.255.0.0
0.0.0.0          8.1.0.1          0.0.0.0
0.0.0.0          8.2.1.1          0.0.0.0
0.0.0.0          8.2.2.1          0.0.0.0

Source policy routing table for interface 8.1.0.0/16
172.22.28.0      8.1.0.1          255.255.255.128
171.70.77.0      8.1.0.1          255.255.255.0
8.1.0.0          0.0.0.0          255.255.0.0
0.0.0.0          8.1.0.1          0.0.0.0

Source policy routing table for interface 8.2.1.0/24
8.2.1.0          0.0.0.0          255.255.255.0
0.0.0.0          8.2.1.1          0.0.0.0

Source policy routing table for interface 8.2.2.0/24
8.2.2.0          0.0.0.0          255.255.255.0
0.0.0.0          8.2.2.1          0.0.0.0
```

If you have a default source policy route where the gateway is not defined as a default gateway, then you must add it after upgrading the software. For example, if you had a source policy route with a gateway of 6.23.1.1 for a source interface of 6.23.1.12, and you did not specify the gateway as one of the default gateways, you would need to add it.

If you have a non-default source policy route, then you must add it as a regular static route (without the obsoleted interface keyword) after upgrading the software. This route is then added to the main routing table as well as the policy routing table.

Differentiated Services

The differentiated services (DiffServ) architecture is based on a simple model where traffic entering a network is classified and possibly conditioned at the boundaries of the network. The class of traffic is then identified with a differentiated services (DS) code point or bit marking in the IP header. Within the core of the network, packets are forwarded according to the per-hop behavior associated with the DS code point.

DiffServ describes a set of end-to-end QoS (Quality of Service) capabilities. End-to-end QoS is the ability of the network to deliver service required by specific network traffic from one end of the network to another. QoS in the VDS-SB software supports differentiated services.

With differentiated services, the network tries to deliver a particular kind of service based on the QoS specified by each packet. The network uses the QoS specification to classify, mark, shape, and police traffic, and to perform intelligent queueing.

Differentiated services is used for several mission-critical applications and for providing end-to-end QoS. Typically, differentiated services is appropriate for aggregate flows because it performs a relatively coarse level of traffic classification.

DS Field Definition

A replacement header field, called the *DS field*, is defined by differentiated services. The DS field supersedes the existing definitions of the IPv4 ToS octet (RFC 791) and the IPv6 traffic class octet.

A currently unused (CU) 2-bit field is reserved for explicit congestion notification (ECN). The value of the CU bits is ignored by DS-compliant interfaces when determining the PHB to apply to a received packet.

Per-Hop Behaviors

RFC 2475 defines PHB as the externally observable forwarding behavior applied at a DiffServ-compliant node to a DiffServ Behavior Aggregate (BA).

A PHB refers to the packet scheduling, queueing, policing, or shaping behavior of a node on any given packet belonging to a BA, as configured by a service level agreement (SLA) or a policy map.

There are four available standard PHBs:

- Default PHB (as defined in RFC 2474)
- Class-Selector PHB (as defined in RFC 2474)
- Assured Forwarding (AFny) PHB (as defined in RFC 2597)
- Expedited Forwarding (EF) PHB (as defined in RFC 2598)

The following sections describe the PHBs.

Assured Forwarding PHB

Assured Forwarding PHB is nearly equivalent to Controlled Load Service, which is available in the integrated services model. AFny PHB defines a method by which BAs can be given different forwarding assurances.

For example, network traffic can be divided into the following classes:

- Gold—Traffic in this category is allocated 50 percent of the available bandwidth.
- Silver—Traffic in this category is allocated 30 percent of the available bandwidth.
- Bronze—Traffic in this category is allocated 20 percent of the available bandwidth.

The AFny PHB defines four AF classes: AF1, AF2, AF3, and AF4. Each class is assigned a specific amount of buffer space and interface bandwidth according to the SLA with the service provider or policy map.

Within each AF class, you can specify three drop precedence (dP) values: 1, 2, and 3. Assured Forwarding PHB can be expressed as shown in the following example: AFny. In this example, n represents the AF class number (1, 2, or 3) and y represents the dP value (1, 2, or 3) within the AFn class.

In instances of network traffic congestion, if packets in a particular AF class (for example, AF1) need to be dropped, packets in the AF1 class are dropped according to the following guideline:

dP(AFny) >= dP(AFnz) >= dP(AFnx)

where dP (AFny) is the probability that packets of the AFny class are dropped and y denotes the dP within an AFn class.

In the following example, packets in the AF13 class are dropped before packets in the AF12 class, which in turn are dropped before packets in the AF11 class:

dP(AF13) >= dP (AF12) >= dP(AF11)

The dP method penalizes traffic flows within a particular BA that exceed the assigned bandwidth. Packets on these offending flows could be re-marked by a policer to a higher drop precedence.

Expedited Forwarding PHB

Resource Reservation Protocol (RSVP), a component of the integrated services model, provides a guaranteed bandwidth service. Applications, such as Voice over IP (VoIP), video, and online trading programs, require this type of service. The EF PHB, a key ingredient of DiffServ, supplies this kind of service by providing low loss, low latency, low jitter, and assured bandwidth service.

You can implement EF by using priority queueing (PQ) and rate limiting on the class (or BA). When implemented in a DiffServ network, EF PHB provides a virtual leased line or premium service. For optimal efficiency, however, you should reserve EF PHB for only the most critical applications because, in instances of traffic congestion, it is not feasible to treat all or most traffic as high priority.

EF PHB is suited for applications such as VoIP that require low bandwidth, guaranteed bandwidth, low delay, and low jitter.

IP Precedence for ToS

IP precedence allows you to specify the class of service (CoS) for a packet. You use the three precedence bits in the IPv4 header's type of service (ToS) field for this purpose.

Using the ToS bits, you can define up to six classes of service. Other features configured throughout the network can then use these bits to determine how to treat the packet. These other QoS features can assign appropriate traffic-handling policies including congestion management strategy and bandwidth allocation. For example, although IP precedence is not a queueing method, queueing methods such as weighted fair queueing (WFQ) and Weighted Random Early Detection (WRED) can use the IP precedence setting of the packet to prioritize traffic.

By setting precedence levels on incoming traffic and using them with the VDS-SB software QoS queueing features, you can create differentiated service. You can use features, such as policy-based routing (PBR) and Committed Access Rate (CAR), to set the precedence based on an extended access list classification. For example, you can assign the precedence based on the application or user or by destination and source subnetwork.

So that each subsequent network element can provide service based on the determined policy, IP precedence is usually deployed as close to the edge of the network or the administrative domain as possible. IP precedence is an edge function that allows core or backbone QoS features, such as WRED, to forward traffic based on CoS. You can also set IP precedence in the host or network client, but this setting can be overridden by the service provisioning policy of the domain within the network.

The following QoS features can use the IP precedence field to determine how traffic is treated:

- Distributed-WRED
- WFQ
- CAR

How the IP Precedence Bits Are Used to Classify Packets

You use the three IP precedence bits in the ToS field of the IP header to specify a CoS assignment for each packet. You can partition traffic into up to six classes—the remaining two classes are reserved for internal network use—and then use policy maps and extended ACLs to define network policies in terms of congestion handling and bandwidth allocation for each class.

Each precedence corresponds to a name. These names, which continue to evolve, are defined in RFC 791. The numbers and their corresponding names, are listed from least to most important.

IP precedence allows you to define your own classification mechanism. For example, you might want to assign the precedence based on an application or an access router. IP precedence bit settings 96 and 112 are reserved for network control information, such as routing updates.

The IP precedence field occupies the three most significant bits of the ToS byte. Only the three IP precedence bits reflect the priority or importance of the packet, not the full value of the ToS byte.

Examples

The following example shows how to configure a default gateway for the SB:

```
ServiceBroker(config)# ip default-gateway 192.168.7.18
```

The following example disables the default gateway:

```
ServiceBroker(config)# no ip default-gateway
```

The following example shows how to configure a static IP route for the SB:

```
ServiceBroker(config)# ip route 172.16.227.128 255.255.255.0 172.16.227.250
```

The following example negates the static IP route:

```
ServiceBroker(config)# no ip route 172.16.227.128 255.255.255.0 172.16.227.250
```

The following example shows how to configure a default domain name for the SB:

```
ServiceBroker(config)# ip domain-name cisco.com
```

The following example negates the default domain name:

```
ServiceBroker(config)# no ip domain-name
```

The following example shows how to configure a name server for the SB:

```
ServiceBroker(config)# ip name-server 10.11.12.13
```

The following example disables the name server:

```
ServiceBroker(config)# no ip name-server 10.11.12.13
```

The following example shows how to configure source policy routing for the SB interface assigned with the IP address 192.168.1.5:

```
ServiceBroker(config)# ip route 0.0.0.0 0.0.0.0 192.168.1.1 interface 192.168.1.5
```

Related Commands

Command	Description
ip (Interface configuration)	Configures the interface Internet Protocol.
show ip routes	Displays the IP routing table.

ip (Interface configuration)

To configure the interface Internet Protocol, use the **interface** command in interface configuration mode. To delete or disable these settings, use the **no** form of this command.

ip {**access-group** {*num* {**in** | **out**} {*name* {**in** | **out**} | **address** {*ip_addr netmask* | **range** {*ip_addr_low ip_addr_high netmask*}}

no ip {**access-group** {*num* {**in** | **out**} {*name* {**in** | **out**} | **address** {*ip_addr netmask* | **range** {*ip_addr_low ip_addr_high netmask*}}

Syntax Description

access-group	Specifies access control for incoming or outgoing packets.
num	Specifies an IP access list by number, in standard or extended form. The range is from 1-199.
in	Configures the IP access list that apply to inbound packets.
out	Configures the IP access list that apply to outbound packets.
name	Name of the access list.
in	Configures the access list name inbound packets.
out	Configures the access list name outbound packets.
address	Set the IP address of an interface.
ip-addr	IP address of the interface.
netmask	Netmask of the interface.
range	Specifies the IP address range.
ip_addr_low	IP address low range of an interface.
ip_addr_high	IP address high range of an interface.
netmask	Netmask of the interface.

Defaults

None

Command Modes

Interface configuration (config-if) mode.

Usage Guidelines

You can configure multiple IP addresses for Gigabit Ethernet, port channel and Standby interfaces in the SBs. With multiple IP support, the SBs can stream the content under a specific IP while having another stream with different source IP address under the same interface.

The **ip** command configures up to 24 unique IP addresses within the same subnet for the same Gigabit Ethernet, port channel and Standby interface. You can add and delete IP addresses for each interface without affecting other configured IP addresses.

Note All IP addresses configured in the same interface must be in the same subnet.

The **ip range** command adds and deletes an IP address range per interface without affecting other configured IP addresses, and it notifies the SB and VDSM on the added and deleted IP address. The IP address can only be deleted when it is already disassociated from the delivery service. If the delivery service's IP address has been updated, for example from 10.1.1.1 to 10.1.1.5, the service is not interrupted. The new stream uses the new IP address.

Examples

Configuring an IP Address Range

The following example shows how to configure an IP address in a range:

```
ServiceBroker(config)# interface PortChannel 1
ServiceBroker(config-if)# ip address 2.2.2.2 255.255.255.0
ServiceBroker(config-if)# ip address range 2.2.2.3 2.2.2.10 255.255.255.0
ServiceBroker(config-if)# ip address range 2.2.2.12 2.2.2.20 255.255.255.0
```

If the user configures an IP address range but one or more of the IP addresses in the range matched with an already configured IP address, the configuration is still accepted. For example, if interface PortChannel 1 has the following configuration:

```
interface PortChannel 1
ip address 2.2.2.2 255.255.255.0
ip address 2.2.2.3 255.255.255.0
ip address 2.2.2.5 255.255.255.0
ip address 2.2.2.12 255.255.255.0
```

The following configuration is accepted and the IP address in the range (not the same subnet) is rejected:

```
ServiceBroker# configure terminal
ServiceBroker(config)# interface PortChannel 1
ServiceBroker(config-if)# ip address range 2.2.2.3 2.2.2.4 255.255.255.0
ServiceBroker(config-if)# end
```

If the interface PortChannel 1 has the following configuration:

```
interface PortChannel 1
ip address 2.2.2.2 255.255.255.0
ip address 2.2.2.5 255.255.255.0
ip address 2.2.2.12 255.255.255.0
```

And you enter the following commands:

```
ServiceBroker# configure terminal
ServiceBroker(config)# interface PortChannel 1
ServiceBroker(config-if)# ip address range 2.2.3.9 2.2.3.15 255.255.255.0
ServiceBroker(config-if)# end
```

It is an invalid IP address range and an incompatible netmask.

Configuring an IP Address

The following example shows how to configure an individual IP address:

```
ServiceBroker(config)# interface PortChannel 1
ServiceBroker(config-if)# ip address 2.2.2.2 255.255.255.0
ServiceBroker(config-if)# ip address 2.2.2.3 255.255.255.0
ServiceBroker(config-if)# ip address 2.2.2.10 255.255.255.0
```

Removing an IP Address

The following example shows how to remove an IP address range configuration:

```
ServiceBroker(config)# interface PortChannel 1
```

```
ServiceBroker(config-if)# no ip address range 2.2.2.3 2.2.2.10 255.255.255.0
```

The following example shows how to remove an IP address configuration:

```
ServiceBroker(config)# interface PortChannel 1
ServiceBroker(config-if)# no ip address 2.2.2.3 255.255.255.
```

Related Commands

Command	Description
interface (Global configuration)	Configures a Gigabit Ethernet or port channel interface.
show interface	Displays the hardware interface information.
show running-config	Displays the current operating configuration.

ip access-list

To create and modify access lists for controlling access to interfaces or applications, use the **ip access-list standard** or **ip access-list extended** command in Global configuration modes. To remove access control lists, use the **no** form of this command.

ip access-list {**extended** {*acl_num* [**delete** *num* | **deny** {*num* {*ip address* | *any* | *host*} | **gre** {*ip address* | *any* | *host*} | **icmp** {*ip address* | *any* | *host*} | **ip** {*ip address* | *any* | *host*} | **tcp** {*ip address* | *any* | *host*} | **udp** {*ip address* | *any* | *host*}} | **insert** {*num* {**deny** | **permit**} | **list** {*start_line_num* | *end_line_num*} | **move** {*old_line_num* | *new_line_num*} | **permit** {*num* {*ip address* | *any* | *host*} | **gre** {*ip address* | *any* | *host*} | **icmp** {*ip address* | *any* | *host*} | **ip** {*ip address* | *any* | *host*} | **tcp** {*ip address* | *any* | *host*} | **udp** {*ip address* | *any* | *host*}}] | *acl_name* [**delete** *num* | **deny**{*num* {*ip address* | *any* | *host*} | **gre** {*ip address* | *any* | *host*} | **icmp** {*ip address* | *any* | *host*} | **ip** {*ip address* | *any* | *host*} | **tcp** {*ip address* | *any* | *host*} | **udp** {*ip address* | *any* | *host*}} | **insert** {*num* {**deny** | **permit**} | **list** {*start_line_num* | *end_line_num*} | **move** {*old_line_num* | *new_line_num*} | **permit** {*num* {*ip address* | *any* | *host*} | **gre** {*ip address* | *any* | *host*} | **icmp** {*ip address* | *any* | *host*} | **ip** {*ip address* | *any* | *host*} | **tcp** {*ip address* | *any* | *host*} | **udp** {*ip address* | *any* | *host*}}] | {**standard** {*acl_num* | *acl_name* {**delete** *num* | **deny** {*num* {*ip address* | *any* | *host*} | **gre** {*ip address* | *any* | *host*} | **icmp** {*ip address* | *any* | *host*} | **ip** {*ip address* | *any* | *host*} | **tcp** {*ip address* | *any* | *host*} | **udp** {*ip address* | *any* | *host*}} | **insert** {*num* {**deny** | **permit**} | **list** {*start_line_num* | *end_line_num*} | **move** {*old_line_num* | *new_line_num*} | **permit** {*ip address* | *any* | *host*}}}}

no ip access-list {**extended** {*acl_num* [**delete** *num* | **deny** {*num* {*ip address* | *any* | *host*} | **gre** {*ip address* | *any* | *host*} | **icmp** {*ip address* | *any* | *host*} | **ip** {*ip address* | *any* | *host*} | **tcp** {*ip address* | *any* | *host*} | **udp** {*ip address* | *any* | *host*}} | **insert** {*num* {**deny** | **permit**} | **list** {*start_line_num* | *end_line_num*} | **move** {*old_line_num* | *new_line_num*} | **permit** {*num* {*ip address* | *any* | *host*} | **gre** {*ip address* | *any* | *host*} | **icmp** {*ip address* | *any* | *host*} | **ip** {*ip address* | *any* | *host*} | **tcp** {*ip address* | *any* | *host*} | **udp** {*ip address* | *any* | *host*}}] | *acl_name* [**delete** *num* | **deny**{*num* {*ip address* | *any* | *host*} | **gre** {*ip address* | *any* | *host*} | **icmp** {*ip address* | *any* | *host*} | **ip** {*ip address* | *any* | *host*} | **tcp** {*ip address* | *any* | *host*} | **udp** {*ip address* | *any* | *host*}} | **insert** {*num* {**deny** | **permit**} | **list** {*start_line_num* | *end_line_num*} | **move** {*old_line_num* | *new_line_num*} | **permit** {*num* {*ip address* | *any* | *host*} | **gre** {*ip address* | *any* | *host*} | **icmp** {*ip address* | *any* | *host*} | **ip** {*ip address* | *any* | *host*} | **tcp** {*ip address* | *any* | *host*} | **udp** {*ip address* | *any* | *host*}}] | {**standard** {*acl_num* | *acl_name* {**delete** *num* | **deny** {*num* {*ip address* | *any* | *host*} | **gre** {*ip address* | *any* | *host*} | **icmp** {*ip address* | *any* | *host*} | **ip** {*ip address* | *any* | *host*} | **tcp** {*ip address* | *any* | *host*} | **udp** {*ip address* | *any* | *host*}} | **insert** {*num* {**deny** | **permit**} | **list** {*start_line_num* | *end_line_num*} | **move** {*old_line_num* | *new_line_num*} | **permit** {*ip address* | *any* | *host*}}}}

Syntax Description

standard	Enables the standard ACL configuration mode.
acl_num	Access list to which all commands entered from access list configuration mode apply, using a numeric identifier. For standard access lists, the valid range is 1 to 99; for extended access lists, the valid range is 100 to 199.
acl_name	Access list to which all commands entered from ACL configuration mode apply, using an alphanumeric string of up to 30 characters, beginning with a letter.
delete	(Optional) Deletes the specified entry.
num	(Optional) Position of condition to delete. The range is from 1 to 500.
deny	(Optional) Causes packets that match the specified conditions to be dropped.

num	IP Protocol Number.
ip address	Source IP address.
any	Any source host.
host	A single host address.
gre	Specifies GRE Tunneling by Cisco.
icmp	Specifies Internet Control Message Protocol.
ip	Specifies Any IP Protocol.
tcp	Specifies Transport Control Protocol.
udp	Specifies User Datagram Protocol.
insert	(Optional) Inserts the conditions following the specified line number into the access list.
num	Identifies the position at which to insert a new condition.
deny	Specifies packets to deny.
permit	Specifies packets to permit.
list	(Optional) Lists the specified entries (or all entries when none are specified).
start_line_num	(Optional) Line number from which the list begins.
end_line_num	(Optional) Last line number in the list.
move	(Optional) Moves the specified entry in the access list to a new position in the list.
old_line_num	Line number of the entry to move.
new_line_num	New position of the entry. The existing entry is moved to the following position in the access list.
permit	(Optional) Causes packets that match the specified conditions to be accepted for further processing.
extended	Enables the extended ACL configuration mode.

Defaults

An access list drops all packets unless you configure at least one **permit** entry.

Command Modes

Global configuration (config) mode.

Usage Guidelines

Standard ACL Configuration Mode Commands

To work with a standard access list, enter the **ip access-list standard** command from the Global configuration mode prompt. The CLI enters a configuration mode in which all subsequent commands apply to the current access list.

To add a line to the standard IP ACL, enter the following command. For example, choose a purpose (permit or deny) that specifies whether a packet is to be passed or dropped, enter the source IP address, and enter the source IP wildcard address as follows:

[**insert** *line_num*] {**deny** | **permit**} {*source_ip* [*wildcard*] | **host** *source_ip* | **any**}

To delete a line from the standard IP ACL, enter the following command:

delete *line_num*

To display a list of specified entries within the standard IP ACL, enter the following command:

list [*start_line_num* [*end_line_num*]]

To move a line to a new position within the standard IP ACL, enter the following command:

move *old_line_num new_line_num*

To return to the CLI Global configuration mode prompt, enter the following command:

exit

To negate a standard IP ACL, enter the following command:

no {**deny** | **permit**} {*source_ip* [*wildcard*] | **host** *source_ip* | **any**}

Extended ACL Configuration Mode Commands

To work with an extended access list, enter the **ip access-list extended** command from the Global configuration mode prompt. The CLI enters a configuration mode in which all subsequent commands apply to the current access list.

To delete a line from the extended IP ACL, enter the following command:

delete *line_num*

To move a line to a new position within the extended IP ACL, enter the following command:

move *old_line_num new_line_num*

To display a list of specified entries within the standard IP ACL, enter the following command:

list [*start_line_num* [*end_line_num*]]

To return to the CLI Global configuration mode prompt, enter the following command:

exit

To add a condition to the extended IP ACL, note that the options depend on the chosen protocol.

For IP, enter the following command to add a condition:

[**insert** *line_num*] {**deny** | **permit**} {**gre** | **ip** | *proto_num*} {*source_ip* [*wildcard*] | **host** *source_ip* | **any**} {*dest_ip* [*wildcard*] | **host** *dest_ip* | **any**}

no {**deny** | **permit**} {**gre** | **ip** | *proto_num*} {*source_ip* [*wildcard*] | **host** *source_ip* | **any**} {*dest_ip* [*wildcard*] | **host** *dest_ip* | **any**}

where if you enter *proto_num* is 47 or 0, they represent the equivalent value for GRE or IP.

For TCP, enter the following command to add a condition:

[**insert** *line_num*] {**deny** | **permit**} {**tcp** | *proto_num*} {*source_ip* [*wildcard*] | **host** *source_ip* | **any**} [*operator port* [*port*]] {*dest_ip* [*wildcard*] | **host** *dest_ip* | **any**} [*operator port* [*port*]] [**established**]

no {**deny** | **permit**} {**tcp** | *proto_num*} {*source_ip* [*wildcard*] | **host** *source_ip* | **any**} [*operator port* [*port*]] {*dest_ip* [*wildcard*] | **host** *dest_ip* | **any**} [*operator port* [*port*]] [**established**]

where *proto_num* can be 6, which is the equivalent value for TCP.

For UDP, enter the following command to add a condition:

[**insert** *line_num*] {**deny** | **permit**} {**udp** | *proto_num*} {*source_ip* [*wildcard*] | **host** *source_ip* | **any**} [*operator port* [*port*]] {*dest_ip* [*wildcard*] | **host** *dest_ip* | **any**} [*operator port* [*port*]]

no {**deny** | **permit**} {**udp** | *proto_num*} {*source_ip* [*wildcard*] | **host** *source_ip* | **any**} [*operator port* [*port*]] {*dest_ip* [*wildcard*] | **host** *dest_ip* | **any**} [*operator port* [*port*]]

where *proto_num* can be 17, which is the equivalent value for UDP.

For ICMP, enter the following command to add a condition:

[**insert** *line_num*] {**deny** | **permit**} {**icmp** | *proto_num*} {*source_ip* [*wildcard*] | **host** *source_ip* | **any**} {*dest_ip* [*wildcard*] | **host** *dest_ip* | **any**} [*icmp_type* [*code*] | *icmp_msg*]

no {**deny** | **permit**} {**icmp** | *proto_num*} {*source_ip* [*wildcard*] | **host** *source_ip* | **any**} {*dest_ip* [*wildcard*] | **host** *dest_ip* | **any**} [*icmp_type* [*code*] | *icmp_msg*]

where *proto_num* can be 2, which is the equivalent value for ICMP.

For extended IP ACLs, the **wildcard** keyword is required if the **host** keyword is not specified. For a list of the keywords that you can use to match specific ICMP message types and codes, see Table 2-6. For a list of supported UDP and TCP keywords, see Table 2-4 and Table 2-5.

Use access lists to control access to specific applications or interfaces on an SB. An ACL consists of one or more condition entries that specify the kind of packets that the SB drops or accepts for further processing. The SB applies each entry in the order in which it occurs in the access list, which by default, is the order in which you configured the entry.

The following are some examples of how IP ACLs can be used in environments that have SBs:

- SB resides on the customer premises and is managed by a service provider, and the service provider wants to secure the device for its management only.
- SB is deployed anywhere within the enterprise. As with routers and switches, the administrator wants to limit Telnet and SSH access to the IT source subnets.
- Application layer proxy firewall with a hardened outside interface has no ports exposed. (*Hardened* means that the interface carefully restricts which ports are available for access, primarily for security reasons. With an outside interface, many types of security attacks are possible.) The SB's outside address is Internet global, and its inside address is private. The inside interface has an IP ACL to limit Telnet and SSH access to the SB.
- SB is deployed as a reverse proxy in an untrusted environment. The SB administrator wants to allow only port 80 inbound traffic on the outside interface and outbound connections on the back-end interface.

Within ACL configuration mode, you can use the editing commands (**list**, **delete**, and **move**) to display the current condition entries, to delete a specific entry, or to change the order in which the entries are evaluated. To return to Global configuration mode, enter **exit** at the ACL configuration mode prompt.

To create an entry, use a **deny** or **permit** keyword and specify the type of packets that you want the SB to drop or to accept for further processing. By default, an access list denies everything because the list is terminated by an implicit **deny any** entry. You must include at least one **permit** entry to create a valid access list.

After creating an access list, you can include the access list in an access group using the **access-group** command, which determines how the access list is applied. You can also apply the access list to a specific application using the appropriate command. A reference to an access list that does not exist is the equivalent of a **permit any** condition statement.

To work with access lists, enter either the **ip access-list standard** or **ip access-list extended** Global configuration command. Identify the new or existing access list with a name up to 30 characters long beginning with a letter or with a number. If you use a number to identify a standard access list, it must be between 1 and 99; for an extended access list, use a number from 100 to 199. Use a standard access list for providing access to the SNMP server or to the TFTP gateway or server.

After you identify the access list, the CLI enters the appropriate configuration mode and all subsequent commands apply to the specified access list.

ip access-list standard Command

You typically use a standard access list to allow connections from a host with a specific IP address or from hosts on a specific network. To allow connections from a specific host, use the **permit host** *source_ip* option and replace *source_ip* with the IP address of the specific host.

To allow connections from a specific network, use the **permit** *source_ip wildcard* option. Replace *source_ip* with a network ID or the IP address of any host on the network that you want to specify. Replace *wildcard* with the dotted decimal notation for a mask that is the reverse of a subnet mask, where a 0 indicates a position that must be matched and a 1 indicates a position that does not matter. For instance, the wildcard 0.0.0.255 causes the last eight bits in the source IP address to be ignored. Therefore, the **permit 192.168.1.0 0.0.0.255** entry allows access from any host on the 192.168.1.0 network.

ip access-list extended Command

Use an extended access list to control connections based on the destination IP address or based on the protocol type. You can combine these conditions with information about the source IP address to create more restrictive conditions. Table 2-4 lists the UDP keywords that you can use with extended access lists.

Table 2-4 UDP Keywords and Port Numbers

CLI Keyword	Description	UDP Port Number
bootpc	BOOTP[1] client service	68
bootps	BOOTP server service	67
domain	DNS[2] service	53
netbios-dgm	NetBIOS datagram service	138
netbios-ns	NetBIOS name resolution service	137
netbios-ss	NetBIOS session service	139
nfs	Network File System service	2049
ntp	Network Time Protocol settings	123
snmp	Simple Network Management Protocol service	161
snmptrap	SNMP traps	162
tftp	Trivial File Transfer Protocol service	69

1. BOOTP = bootstrap protocol
2. DNS = Domain Name System

Table 2-5 lists the TCP keywords that you can use with extended access lists.

Table 2-5 TCP Keywords and Port Numbers

CLI Keyword	Description	TCP Port Number
domain	Domain Name System	53
exec	Remote process execution	512
ftp	File Transfer Protocol service	21
ftp-data	FTP data connections (used infrequently)	20
nfs	Network File System service applications	2049
rtsp	Real-Time Streaming Protocol applications	554
ssh	Secure Shell login	22
telnet	Remote login using telnet	23
www	World Wide Web (HTTP) service	80

Table 2-6 lists the keywords that you can use to match specific ICMP message types and codes.

Table 2-6 Keywords for ICMP Message Type and Code

Field	Description
administratively-prohibited	Messages that are administratively prohibited from being allowed access.
alternate-address	Messages that specify alternate IP addresses.
conversion-error	Messages that denote a datagram conversion error.
dod-host-prohibited	Messages that signify a DoD[1] protocol Internet host denial.
dod-net-prohibited	Messages that specify a DoD protocol network denial.
echo	Messages that are used to send echo packets to test basic network connectivity.
echo-reply	Messages that are used to send echo reply packets.
general-parameter-problem	Messages that report general parameter problems.
host-isolated	Messages that indicate that the host is isolated.
host-precedence-unreachable	Messages that have been received with the protocol field of the IP header set to one (ICMP) and the type field in the ICMP header set to three (Host Unreachable). This is the most common response. Large numbers of this datagram type on the network are indicative of network difficulties or hostile actions.
host-redirect	Messages that specify redirection to a host.
host-tos-redirect	Messages that specify redirection to a host for type of service-based (ToS) routing.
host-tos-unreachable	Messages that denote that the host is unreachable for ToS-based routing.
host-unknown	Messages that specify that the host or source is unknown.
host-unreachable	Messages that specify that the host is unreachable.

Table 2-6 Keywords for ICMP Message Type and Code (continued)

Field	Description
information-reply	Messages that contain domain name replies.
information-request	Messages that contain domain name requests.
mask-reply	Messages that contain subnet mask replies.
mask-request	Messages that contain subnet mask requests.
mobile-redirect	Messages that specify redirection to a mobile host.
net-redirect	Messages that are used for redirection to a different network.
net-tos-redirect	Messages that are used for redirection to a different network for ToS-based routing.
net-tos-unreachable	Messages that specify that the network is unreachable for the ToS-based routing.
net-unreachable	Messages that specify that the network is unreachable.
network-unknown	Messages that denote that the network is unknown.
no-room-for-option	Messages that specify the requirement of a parameter, but that no room is unavailable for it.
option-missing	Messages that specify the requirement of a parameter, but that parameter is not available.
packet-too-big	Messages that specify that the ICMP packet requires fragmentation but the DF[2] bit is set.
parameter-problem	Messages that signify parameter-related problems.
port-unreachable	Messages that specify that the port is unreachable.
precedence-unreachable	Messages that specify that host precedence is not available.
protocol-unreachable	Messages that specify that the protocol is unreachable.
reassembly-timeout	Messages that specify a timeout during reassembling of packets.
redirect	Messages that have been received with the protocol field of the IP header set to one (ICMP) and the type field in the ICMP header set to five (Redirect). ICMP redirect messages are used by routers to notify the hosts on the data link that a better route is available for a particular destination.
router-advertisement	Messages that contain ICMP router discovery messages called *router advertisements*.
router-solicitation	Messages that are multicast to ask for immediate updates on neighboring router interface states.
source-quench	Messages that have been received with the protocol field of the IP header set to one (ICMP) and the type field in the ICMP header set to four (Source Quench). This datagram may be used in network management to provide congestion control. A source quench packet is issued when a router is beginning to lose packets because of the transmission rate of a source. The source quench is a request to the source to reduce the rate of a datagram transmission.
source-route-failed	Messages that specify the failure of a source route.

Table 2-6 Keywords for ICMP Message Type and Code (continued)

Field	Description
time-exceeded	Messages that specify information about all instances when specified times were exceeded.
timestamp-reply	Messages that contain time stamp replies.
timestamp-request	Messages that contain time stamp requests.
traceroute	Messages that specify the entire route to a network host from the source.
ttl-exceeded	Messages that specify that ICMP packets have exceeded the Time-To-Live configuration.
unreachable	Messages that are sent when packets are denied by an access list; these packets are not dropped in the hardware but generate the ICMP-unreachable message.

1. DoD = department of defense
2. DF = do not fragment

Examples

The following example shows how to create an access list to allow all web traffic and to allow only a specific host administrative access using Secure Shell (SSH):

```
ServiceBroker(config)# ip access-list extended example
ServiceBroker(config-ext-nacl)# permit tcp any any eq www
ServiceBroker(config-ext-nacl)# permit tcp host 10.1.1.5 any eq ssh
ServiceBroker(config-ext-nacl)# exit
```

The following example shows how to activate the access list for an interface:

```
ServiceBroker(config)# interface gigabitethernet 1/0
ServiceBroker(config-if)# exit
```

The following example shows how this configuration appears when you enter the **show running-configuration** command:

```
...
!
ip access-list extended example
 permit tcp any any eq www
 permit tcp host 10.1.1.5 any eq ssh
 exit
. . .
```

Related Commands

Command	Description
clear ip access-list counters	Clears the IP access list statistical information.
show ip access-list	Displays the access lists that are defined and applied to specific interfaces or applications.

kernel

To configure the kernel, use the **kernel** command in Global configuration mode. To disable the kernel configuration, use the **no** form of this command.

kernel {kdb | optimization network}

no kernel {kdb | optimization network}

Syntax Description

kdb	Specifies the kernel debugger (kdb).
optimization	Enables kernel performance optimization.
network	Optimizes network performance.

Defaults

Kdb is disabled by default.

Command Modes

Global configuration (config) mode.

Usage Guidelines

Once enabled, KDB is automatically activated when kernel problems occur. Once activated, all normal functioning of the VDS-SB device is suspended until KDB is manually deactivated. The KDB prompt looks like this prompt:

```
[ 0 ] kdb>
```

To deactivate KDB, enter **go** at the KDB prompt. If KDB was automatically activated because of kernel problems, you must reboot to recover from the issue. If you activated KDB manually for diagnostic purposes, the system resumes normal functioning in whatever state it was when you activated KDB. In either case, if you enter **reboot**, the system restarts and normal operation resumes.

Examples

The following example shows how to enable KDB:

```
ServiceBroker(config)# kernel kdb
```

The following example shows how to disable KDB:

```
ServiceBroker(config)# no kernel kdb
```

line

To specify terminal line settings, use the **line** command in Global configuration mode. To disable terminal line settings, use the **no** form of this command.

line console carrier-detect

no line console carrier-detect

Syntax Description

console	Configures the console terminal line settings.
carrier-detect	Sets the device to check the carrier detect signal before writing to the console.

Defaults

This feature is disabled by default.

Command Modes

Global configuration (config) mode.

Usage Guidelines

You should enable carrier detection if you connect the SB, or VDSM to a modem for receiving calls. If you are using a null modem cable with no carrier detect pin, the device might appear unresponsive on the console until the carrier detect signal is asserted. To recover from a misconfiguration, you should reboot the device and set the 0x2000 bootflag to ignore the carrier detect setting.

Examples

The following example shows how to specify terminal line settings:

```
ServiceBroker(config)# line console carrier-detect
```