



E Commands

This chapter describes the Cisco Nexus 1000V commands that begin with the letter E.

echo

To echo an argument back to the terminal screen, use the **echo** command.

echo [backslash-interpret] [*text*]

Syntax Description	-e (Optional) Interprets any character following a backslash character (\) as a formatting option. backslash-interpret (Optional) Interprets any character following a backslash character (\) as a formatting option. <i>text</i> (Optional) Text string to display. The text string is alphanumeric, case sensitive, can contain spaces, and has a maximum length of 200 characters. The text string can also contain references to CLI variables.
--------------------	---

Defaults	Displays a blank line.
----------	------------------------

Command Modes	Any
---------------	-----

SupportedUserRoles	network-admin
--------------------	---------------

Command History	Release	Modification
	4.0(4)SV1(1)	This command was introduced.

echo

Send document comments to nexus1k-docfeedback@cisco.com.

Usage Guidelines

You can use this command in a command script to display information while the script is running.

Table 1 lists the formatting keywords that you can insert in the text when you include the **-e** or **backslash-interpret** keyword.

Table 1 *Formatting Options for the echo Command*

Formatting Option	Description
\b	Back spaces.
\c	Removes the new line character at the end of the text string.
\f	Inserts a form feed character.
\n	Inserts a new line character.
\r	Returns to the beginning of the text line.
\t	Inserts a horizontal tab character.
\v	Inserts a vertical tab character.
\\\	Displays a backslash character.
\nnn	Displays the corresponding ASCII octal character.

Examples

This example shows how to display a blank line at the command prompt:

```
n1000v# echo
```

This example shows how to display a line of text at the command prompt:

```
n1000v# echo Script run at $(TIMESTAMP).
Script run at 2008-08-12-23.29.24.
```

This example shows how to use a formatting option in the text string:

```
n1000v# echo backslash-interpret This is line #1. \nThis is line #2.
This is line #1.
This is line #2.
```

Related Commands

Command	Description
run-script	Runs command scripts.

Send document comments to nexus1k-docfeedback@cisco.com.

end

To exit a configuration mode and return to Privileged EXEC mode, use the **end** command.

end

Syntax Description This command has no arguments or keywords.

Defaults None

Command Modes Any

SupportedUserRoles network-admin
network-operator

Command History	Release	Modification
	4.0(4)SV1(1)	This command was introduced.

Usage Guidelines This command differs from the **exit** command in that the exit command returns you to the configuration mode you were previously in. The **end** command always takes you completely out of configuration mode and places you in privileged EXEC mode.

Examples This example shows how to end the session in Global Configuration mode and return to privileged EXEC mode:

```
n1000v(config)# end
n1000v#
```

This example shows how to end the session in Interface Configuration mode and return to privileged EXEC mode:

```
n1000v(config-if)# end
n1000v#
```

Related Commands

Command	Description
exit	Exits the current command mode and returns you to the previous command mode.

 errdisable detect cause

Send document comments to nexus1k-docfeedback@cisco.com.

errdisable detect cause

To detect the reason an interface is error-disabled, use the **errdisable detect cause** command. To stop error detection, use the **no** form of this command. In the case of a policy installation failure, the no form of this command will not bring the port down.

errdisable detect cause {all | arp-inspection | dhcp-rate-limit | link-flap | loopback}

no errdisable detect cause {all | arp-inspection | dhcp-rate-limit | link-flap | loopback}

Syntax Description	all Enables error-disabled detection on all causes.
arp-inspection	Enables error-disabled detection on arp-inspection.
dhcp-rate-limit	Enables error-disabled detection on dhcp-rate-limit.
link-flap	Enables error-disabled disable detection on link-state flapping.
loopback	Enables error-disabled detection on a loopback.

Command Default	Disabled
-----------------	----------

Command Modes	Global configuration (config)
---------------	-------------------------------

SupportedUserRoles	network-admin
--------------------	---------------

Command History	Release	Modification
	4.0(4)SV1(2)	This command was introduced.

Usage Guidelines	The error-disabled state is an operational state that is similar to the link-down state. You must enter the shutdown command and then the no shutdown command to recover an interface manually from the error-disabled state.
------------------	---

Examples	This example shows how to detect the cause of the error-disabled state for all applications:
	n1000v(config)# errdisable detect cause all n1000v(config)#

Related Commands	Command	Description
	shutdown	Brings the port down administratively.
	no shutdown	Brings the port up administratively.
	show interface status err-disabled	Displays the interfaces currently in the error-disabled state.

Send document comments to nexus1k-docfeedback@cisco.com.

errdisable recovery cause

To enable an application to automatically recover an interface from the error-disabled (errdisabled), use the **errdisable recovery cause** command. To return to the default setting, use the **no form** of this command.

```
errdisable recovery cause {all | arp-inspection | bpduguard | dhcp-rate-limit | link-flap |
    psecure-violation | security-violation | udld}
```

```
no errdisable recovery cause {all | arp-inspection | bpduguard | dhcp-rate-limit | link-flap |
    psecure-violation | security-violation | udld}
```

Syntax Description	
all	Enables automatic recovery from all causes for the error-disabled state.
arp-inspection	Enables automatic recovery from the ARP inspection error state.
bpduguard	Enables automatic recovery from BPDU Guard error-disabled state.
dhcp-rate-limit	Enables automatic recovery from the DHCP rate-limit error state.
link-flap	Enables automatic recovery from link-state flapping.
psecure-violation	Enables timer automatic recovery from the psecure violation disable state.
security-violation	Enables automatic recovery from the 802.1X violation disable state.
udld	Enables automatic recovery from the UDLD error-disabled state.

Command Default	Disabled				
Command Modes	Global configuration (config)				
SupportedUserRoles	network-admin				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>4.0(4)SV1(2)</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	4.0(4)SV1(2)	This command was introduced.
Release	Modification				
4.0(4)SV1(2)	This command was introduced.				

Usage Guidelines

Examples This example shows how to automatically recover from the error-disabled state for link flapping after you have enabled the recovery timer:

```
n1000v(config)# errdisable recovery cause link-flap
n1000v(config)#
```

■ **errdisable recovery cause**

Send document comments to nexus1k-docfeedback@cisco.com.

Related Commands	Command	Description
	errdisable recovery interval	Enables the recovery timer.
	show interface status err-disabled	Displays the interface error-disabled state.

Send document comments to nexus1k-docfeedback@cisco.com.

errdisable recovery interval

To enable the recovery timer, use the **errdisable recovery interval** command.

errdisable recovery interval *interval*

Syntax Description	<i>interval</i> Error detection for access-list installation failures. The range is from 30 to 65535.
---------------------------	---

Command Default	300 seconds
------------------------	-------------

Command Modes	Global configuration (config)
----------------------	-------------------------------

SupportedUserRoles	network-admin
---------------------------	---------------

Command History	Release	Modification
	4.0(4)SV1(2)	This command was introduced.

Usage Guidelines	Use the errdisable recovery interval command to configure the recovery timer.
-------------------------	--

Examples	This example shows how to configure the recovery timer:
	<pre>n1000v(config)# errdisable recovery interval 32 n1000v(config)#</pre>

Related Commands	Command	Description
	errdisable recovery	Enables the error-disabled recovery for an application.
	cause	
	show interface status	Displays the interface error-disabled state.
	err-disabled	

erspan-id

Send document comments to nexus1k-docfeedback@cisco.com.

erspan-id

To add an Encapsulated Remote Switch Port Analyzer (ERSPAN) ID to the session configuration and save it in the running configuration, use the **erspan-id** command.

erspan-id *flow_id*

Syntax Description	<i>flow_id</i> Flow ID to be assigned to the ERSPAN session. The range is 1–1023.												
Defaults	None												
Command Modes	CLI ERSPAN source configuration (config-erspan-src)												
SupportedUserRoles	network-admin												
Command History	<table border="1"> <thead> <tr> <th>Release</th><th>Modification</th></tr> </thead> <tbody> <tr> <td>4.0(4)SV1(1)</td><td>This command was introduced.</td></tr> </tbody> </table>	Release	Modification	4.0(4)SV1(1)	This command was introduced.								
Release	Modification												
4.0(4)SV1(1)	This command was introduced.												
Usage Guidelines	The session ERSPAN ID is added to the ERSPAN header of the encapsulated frame and can be used at the termination box to differentiate between various ERSPAN streams of traffic.												
Examples	<p>This example shows how to add ERSPAN ID 51 to the session configuration and save it in the running configuration:</p> <pre>n1000v# config t n1000v(config)# monitor session type erspan-source n1000v(config-erspan-src)# erspan_id 51 n1000v(config-erspan-src) #</pre>												
Related Commands	<table border="1"> <thead> <tr> <th>Command</th><th>Description</th></tr> </thead> <tbody> <tr> <td>monitor session type erspan-source</td><td>Creates a session with the given session number and puts you in the CLI ERSPAN source configuration mode.</td></tr> <tr> <td>source</td><td>For the specified session, configures the source and the direction of traffic to monitor, and saves this information in the running configuration.</td></tr> <tr> <td>filter vlan</td><td>For the specified ERSPAN session, configures the VLANs, VLAN lists, or VLAN ranges to be monitored.</td></tr> <tr> <td>ip ttl</td><td>Specifies the IP time-to-live value for the packets in the ERSPAN traffic.</td></tr> <tr> <td>ip prec</td><td>Specifies the IP precedence value for the packets in the ERSPAN traffic.</td></tr> </tbody> </table>	Command	Description	monitor session type erspan-source	Creates a session with the given session number and puts you in the CLI ERSPAN source configuration mode.	source	For the specified session, configures the source and the direction of traffic to monitor, and saves this information in the running configuration.	filter vlan	For the specified ERSPAN session, configures the VLANs, VLAN lists, or VLAN ranges to be monitored.	ip ttl	Specifies the IP time-to-live value for the packets in the ERSPAN traffic.	ip prec	Specifies the IP precedence value for the packets in the ERSPAN traffic.
Command	Description												
monitor session type erspan-source	Creates a session with the given session number and puts you in the CLI ERSPAN source configuration mode.												
source	For the specified session, configures the source and the direction of traffic to monitor, and saves this information in the running configuration.												
filter vlan	For the specified ERSPAN session, configures the VLANs, VLAN lists, or VLAN ranges to be monitored.												
ip ttl	Specifies the IP time-to-live value for the packets in the ERSPAN traffic.												
ip prec	Specifies the IP precedence value for the packets in the ERSPAN traffic.												

Send document comments to nexus1k-docfeedback@cisco.com.

Command	Description
mtu	Specifies a maximum transmission unit (MTU) size for the ERSPAN traffic.
show monitor session	Displays the ERSPAN session configuration as it exists in the running configuration.

exec-timeout

Send document comments to nexus1k-docfeedback@cisco.com.

exec-timeout

To configure the length of time, in minutes, that an inactive Telnet or SSH session remains open before it is automatically shut down, use the **exec-timeout** command. To remove an exec timeout setting, use the **no** form of this command.

exec-timeout *time*

no exec-timeout [*time*]

Syntax Description	time	Timeout time, in minutes. The range of valid values is 0 to 525600. If a session remains inactive longer than this specified time period, then it is automatically closed.
---------------------------	-------------	---

Defaults	No timeout is configured.
-----------------	---------------------------

Command Modes	Console configuration (config-console)
----------------------	--

SupportedUserRoles	network-admin
---------------------------	---------------

Command History	Release	Modification
	4.0(4)SV1(1)	This command was introduced.

Usage Guidelines	When you set <i>time</i> to 0, exec timeout is disabled.
-------------------------	--

Examples	This example shows how to configure an inactive session timeout for the console port:
-----------------	---

```
n1000v# configure terminal
n1000v(config)# line console
n1000v(config-com1)# exec-timeout 20
```

This example shows how to configure an inactive session timeout for the virtual terminal:

```
n1000v# configure terminal
n1000v(config)# line vty
n1000v(config-line)# exec-timeout 20
```

This example shows how to remove an exec timeout on the console port:

```
n1000v(config)# configure terminal
DocTeamVSM(config)# line console
n1000v(config-console)# no exec-timeout
n1000v(config-console)#
```

Send document comments to nexus1k-docfeedback@cisco.com.

Related Commands	Command	Description
	show terminal	Displays the terminal configuration, including the timeout value.
	show users	Displays the currently active user sessions.

exit

Send document comments to nexus1k-docfeedback@cisco.com.

exit

To exit a configuration mode or exit the CLI, use the **exit** command.

exit

Syntax Description This command has no arguments or keywords.

Defaults None

Command Modes Any

SupportedUserRoles network-admin
network-operator

Command History	Release	Modification
	4.0(4)SV1(1)	This command was introduced.

Examples This example shows how to exit global configuration mode. The CLI returns you to the EXEC mode.

```
n1000v(config)# exit
n1000v#
```

This example shows how to exit interface configuration mode. The CLI returns you to the global configuration mode.

```
n1000v(config-if)# exit
n1000v(config)#
```

This example shows how to exit the CLI.

```
n1000v# exit
```

Related Commands

Command	Description
end	Returns to the EXEC command mode.

Send document comments to nexus1k-docfeedback@cisco.com.

exporter

To add an existing flow exporter to a specific flow monitor and save it in the running configuration, use the **exporter** command. To remove the flow exporter for a specific flow monitor, use the **no** form of this command.

exporter *name*

no exporter *name*

Syntax Description	<i>name</i>	Name of the flow exporter to be added for the flow monitor.						
Defaults	None							
Command Modes	CLI flow monitor configuration (config-flow-monitor)							
SupportedUserRoles	network-admin							
Command History	<table border="1"> <thead> <tr> <th>Release</th><th>Modification</th></tr> </thead> <tbody> <tr> <td>4.0(4)SV1(1)</td><td>This command was introduced.</td></tr> </tbody> </table>		Release	Modification	4.0(4)SV1(1)	This command was introduced.		
Release	Modification							
4.0(4)SV1(1)	This command was introduced.							
Examples	<p>This example shows how to add the flow exporter called Exportv9 and save it in the running configuration:</p> <pre>n1000v# config t n1000v(config)# flow monitor MonitorTest n1000v(config-flow-monitor)# exporter Exportv9 n1000v(config-flow-monitor)#</pre> <p>This example shows how to remove the flow exporter called Exportv9:</p> <pre>n1000v# config t n1000v(config)# flow monitor MonitorTest n1000v(config-flow-monitor)# no exporter Exportv9 n1000v(config-flow-monitor)#</pre>							
Related Commands	<table border="1"> <thead> <tr> <th>Command</th><th>Description</th></tr> </thead> <tbody> <tr> <td>flow monitor</td><td>Creates a flow monitor, by name, saves it in the running configuration, and then puts you in the CLI flow monitor configuration mode.</td></tr> <tr> <td>description</td><td>Adds a descriptive string for the specified flow monitor and saves it in the running configuration.</td></tr> </tbody> </table>		Command	Description	flow monitor	Creates a flow monitor, by name, saves it in the running configuration, and then puts you in the CLI flow monitor configuration mode.	description	Adds a descriptive string for the specified flow monitor and saves it in the running configuration.
Command	Description							
flow monitor	Creates a flow monitor, by name, saves it in the running configuration, and then puts you in the CLI flow monitor configuration mode.							
description	Adds a descriptive string for the specified flow monitor and saves it in the running configuration.							

Send document comments to nexus1k-docfeedback@cisco.com.

Command	Description
exporter	Adds an existing flow exporter for the specified monitor and saves it in the running configuration.
record	Adds an existing flow record for the specified monitor and saves it in the running configuration.
timeout	Specifies, for the specified monitor, an aging timer and its value for aging entries from the cache, and saves them in the running configuration.
cache	Specifies the cache size for the specified monitor and saves it in the running configuration.