CHAPTER 15

R Commands

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

radius-server deadtime

To configure the dead-time interval for all RADIUS servers used by a device, use the **radius-server deadtime** command. To revert to the default, use the **no** form of this command.

radius-server deadtime *minutes*

no radius-server deadtime *minutes*

Syntax Description

minutes	Number of minutes for the dead-time interval. The range is from 1 to 1440 minutes.

Defaults

0 minutes

Command Modes

Global configuration (config)

SupportedUserRoles

network-admin

Command History

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

Usage Guidelines

The dead-time interval is the number of minutes before the device checks a RADIUS server that was previously unresponsive.

Note The default idle timer value is 0 minutes. When the idle time interval is 0 minutes, periodic RADIUS server monitoring is not performed.

Examples

This example shows how to configure the global dead-time interval for all RADIUS servers to perform periodic monitoring:

```
n1000v# config t
n1000v(config)# radius-server deadtime 5
```

This example shows how to revert to the default for the global dead-time interval for all RADIUS servers and disable periodic server monitoring:

```
n1000v# config t
n1000v(config)# no radius-server deadtime 5
```

Related Commands

Command	Description
show radius-server	Displays RADIUS server information.

radius-server directed-request

To allow users to send authentication requests to a specific RADIUS server when logging in, use the **radius-server directed request** command. To revert to the default, use the **no** form of this command.

radius-server directed-request

no radius-server directed-request

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration (config)

SupportedUserRoles

network-admin

Command History

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

Usage Guidelines

You can specify the *username@vrfname*:*hostname* during login, where *vrfname* is the virtual routing and forwarding (VRF) instance to use and *hostname* is the name of a configured RADIUS server. The username is sent to the RADIUS server for authentication.

Examples

This example shows how to allow users to send authentication requests to a specific RADIUS serve when logging in:

```
n1000v# config t
n1000v(config)# radius-server directed-request
```

This example shows how to disallow users to send authentication requests to a specific RADIUS server when logging in:

```
n1000v# config t
n1000v(config)# no radius-server directed-request
```

Related Commands

Command	Description
show radius-server directed-request	Displays the directed request RADIUS server configuration.

radius-server host

To configure RADIUS server parameters, use the **radius-server host** command. To revert to the default, use the **no** form of this command.

radius-server host {*hostname* | *ipv4-address* | *ipv6-address*}
[**key** [**0** | **7**] *shared-secret* [**pac**]] [**accounting**]
[**acct-port** *port-number*] [**auth-port** *port-number*] [**authentication**] [**retransmit** *count*]
[**test** {**idle-time** *time* | **password** *password* | **username** *name*}]
[**timeout** *seconds* [**retransmit** *count*]]

no radius-server host {*hostname* | *ipv4-address* | *ipv6-address*}
[**key** [**0** | **7**] *shared-secret* [**pac**]] [**accounting**]
[**acct-port** *port-number*] [**auth-port** *port-number*] [**authentication**] [**retransmit** *count*]
[**test** {**idle-time** *time* | **password** *password* | **username** *name*}]
[**timeout** *seconds* [**retransmit** *count*]]

Syntax Description

hostname	RADIUS server Domain Name Server (DNS) name. The name is alphanumeric, case sensitive, and has a maximum of 256 characters.
ipv4-address	RADIUS server IPv4 address in the *A.B.C.D* format.
ipv6-address	RADIUS server IPv6 address in the *X:X:X::X* format.
key	(Optional) Configures the RADIUS server preshared secret key.
0	(Optional) Configures a preshared key specified in clear text to authenticate communication between the RADIUS client and server. This is the default.
7	(Optional) Configures a preshared key specified in encrypted text (indicated by 7) to authenticate communication between the RADIUS client and server.
shared-secret	Preshared key to authenticate communication between the RADIUS client and server. The preshared key can include any printable ASCII characters (white spaces are not allowed), is case sensitive, and has a maximum of 63 characters.
pac	(Optional) Enables the generation of Protected Access Credentials (PAC) on the RADIUS Cisco Access Control Server (ACS) for use with Cisco TrustSec.
accounting	(Optional) Configures accounting.
acct-port *port-number*	(Optional) Configures the RADIUS server port for accounting. The range is from 0 to 65535.
auth-port *port-number*	(Optional) Configures the RADIUS server port for authentication. The range is from 0 to 65535.
authentication	(Optional) Configures authentication.
retransmit *count*	(Optional) Configures the number of times that the device tries to connect to a RADIUS server(s) before reverting to local authentication. The range is from 1 to 5 times and the default is 1 time.
test	(Optional) Configures parameters to send test packets to the RADIUS server.
idle-time *time*	Specifies the time interval (in minutes) for monitoring the server. The range is from 1 to 1440 minutes.
password *password*	Specifies a user password in the test packets. The password is alphanumeric, case sensitive, and has a maximum of 32 characters.

username *name*	Specifies a username in the test packets. The is alphanumeric, not case sensitive, and has a maximum of 32 characters.
timeout *seconds*	Specifies the timeout (in seconds) between retransmissions to the RADIUS server. The default is 5 seconds and the range is from 1 to 60 seconds.

Defaults

Parameter	Default
Accounting port	1813
Authentication port	1812
Accounting	enabled
Authentication	enabled
Retransmission count	1
Idle-time	none
Server monitoring	disabled
Timeout	5 seconds
Test username	test
Test password	test

Command Modes

Global configuration (config)

SupportedUserRoles

network-admin

Command History

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

Usage Guidelines

When the idle time interval is 0 minutes, periodic RADIUS server monitoring is not performed.

Examples

This example shows how to configure RADIUS server authentication and accounting parameters:

```
n1000v# config terminal
n1000v(config)# radius-server host 10.10.2.3 key HostKey
n1000v(config)# radius-server host 10.10.2.3 auth-port 2003
n1000v(config)# radius-server host 10.10.2.3 acct-port 2004
n1000v(config)# radius-server host 10.10.2.3 accounting
n1000v(config)# radius-server host radius2 key 0 abcd
n1000v(config)# radius-server host radius3 key 7 1234
n1000v(config)# radius-server host 10.10.2.3 test idle-time 10
n1000v(config)# radius-server host 10.10.2.3 test username tester
n1000v(config)# radius-server host 10.10.2.3 test password 2B9ka5
```

Related Commands

Command	Description
show radius-server	Displays RADIUS server information.

radius-server key

To configure a RADIUS shared secret key, use the **radius-server key** command. To remove a configured shared secret, use the **no** form of this command.

radius-server key [**0** | **7**] *shared-secret*

no radius-server key [**0** | **7**] *shared-secret*

Syntax Description

0	(Optional) Configures a preshared key specified in clear text to authenticate communication between the RADIUS client and server.
7	(Optional) Configures a preshared key specified in encrypted text to authenticate communication between the RADIUS client and server.
shared-secret	Preshared key used to authenticate communication between the RADIUS client and server. The preshared key can include any printable ASCII characters (white spaces are not allowed), is case sensitive, and has a maximum of 63 characters.

Defaults

Clear text

Command Modes

Global configuration (config)

SupportedUserRoles

network-admin

Command History

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

Usage Guidelines

You must configure the RADIUS preshared key to authenticate the switch on the RADIUS server. The length of the key is restricted to 63 characters and can include any printable ASCII characters (white spaces are not allowed). You can configure a global key to be used for all RADIUS server configurations on the switch. You can override this global key assignment for an individual host by using the **key** keyword in the **radius-server host** command.

Examples

This example shows how to provide various scenarios to configure RADIUS authentication:

```
n1000v# config terminal
n1000v(config)# radius-server key AnyWord
n1000v(config)# radius-server key 0 AnyWord
n1000v(config)# radius-server key 7 public pac
```

Related Commands

Command	Description
show radius-server	Displays RADIUS server information.

radius-server retransmit

To specify the number of times that the device should try a request with a RADIUS server, use the **radius-server retransmit** command. To revert to the default, use the **no** form of this command.

radius-server retransmit *count*

no radius-server retransmit *count*

Syntax Description

count	Number of times that the device tries to connect to a RADIUS server(s) before reverting to local authentication. The range is from 1 to 5 times.

Defaults

1 retransmission

Command Modes

Global configuration (config)

SupportedUserRoles

network-admin

Command History

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

Examples

This example shows how to configure the number of retransmissions to RADIUS servers:

```
n1000v# config t
n1000v(config)# radius-server retransmit 3
```

This example shows how to revert to the default number of retransmissions to RADIUS servers:

```
n1000v# config t
n1000v(config)# no radius-server retransmit 3
```

Related Commands

Command	Description
show radius-server	Displays RADIUS server information.

radius-server timeout

To specify the time between retransmissions to the RADIUS servers, use the **radius-server timeout** command. To revert to the default, use the **no** form of this command.

radius-server timeout *seconds*

no radius-server timeout *seconds*

Syntax Description

seconds	Number of seconds between retransmissions to the RADIUS server. The range is from 1 to 60 seconds.

Defaults

5 seconds

Command Modes

Global configuration (config)

SupportedUserRoles

network-admin

Command History

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

Examples

This example shows how to configure the timeout interval:

```
n1000v# config t
n1000v(config)# radius-server timeout 30
```

This example shows how to revert to the default interval:

```
n1000v# config t
n1000v(config)# no radius-server timeout 30
```

Related Commands

Command	Description
show radius-server	Displays RADIUS server information.

rate-mode dedicated

To set the dedicated rate mode for the specified ports, use the **rate-mode dedicated** command.

rate-mode dedicated

no rate-mode

Syntax Description

This command has no arguments or keywords.

Command Default

Shared rate mode is the default.

Command Modes

Interface configuration (config-if)

SupportedUserRoles

network-admin

Command History

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

Usage Guidelines

Use the **rate-mode dedicated** command to set the dedicated rate mode for the specified ports.

On a 32-port 10-Gigabit Ethernet module, each set of four ports can handle 10 gigabits per second (Gb/s) of bandwidth. You can use the rate-mode parameter to dedicate that bandwidth to the first port in the set of four ports or share the bandwidth across all four ports.

Note When you dedicate the bandwidth to one port, you must first administratively shut down the ports in the group, change the rate mode to dedicated, and then bring the dedicated port administratively up.

Table 15-1 identifies the ports that are grouped together to share each 10 Gb/s of bandwidth and which port in the group can be dedicated to utilize the entire bandwidth.

Table 15-1 Dedicated and Shared Ports

Ports Groups that Can Share Bandwidth	Ports that Can be Dedicated to Each 10-Gigabit Ethernet of Bandwidth
1, 3, 5, 7	1
2, 4, 6, 8	2
9, 11, 13, 15	9
10, 12, 14, 16	10

Table 15-1 Dedicated and Shared Ports

Ports Groups that Can Share Bandwidth	Ports that Can be Dedicated to Each 10-Gigabit Ethernet of Bandwidth
17, 19, 21, 23	17
18, 20, 22, 24	18
25, 27, 29, 31	25
26, 28, 30, 32	26

When you enter the **rate-mode dedicated** command, the full bandwidth of 10 Gb is dedicated to one port. When you dedicate the bandwidth, all subsequent commands for the port are for dedicated mode.

Examples

This example shows how to configure the dedicated rate mode for Ethernet ports 4/17, 4/19, 4/21, and 4/23:

```
n1000v# config t
n1000v(config)# interface ethernet 4/17, ethernet 4/19, ethernet 4/21, ethernet 4/23
n1000v(config-if)# shutdown
n1000v(config-if)# interface ethernet 4/17
n1000v(config-if)# rate-mode dedicated
n1000v(config-if)# no shutdown
n1000v(config-if)#
```

Related Commands

Command	Description
show interface	Displays interface information, which includes the current rate mode dedicated.

record

To configure a NetFlow flow record, use the **record** command. To remove the flow record configuration, use the **no** form of the command.

record {*name* | **netflow ipv4** {**original-input** | **original-output** | **netflow protocol-port**} | **netflow-original**}

no record {*name* | **netflow ipv4** {**original-input** | **original-output** | **netflow protocol-port**} | **netflow-original**}

Syntax Description

name	Specifies the name of a new NetFlow flow record.
netflow ipv4	Specifies a predefined NetFlow flow record that uses traditional IPv4 NetFlow collection schemes.
original-input	Specifies a predefined NetFlow flow record that uses traditional IPv4 input.
original-output	Specifies a predefined NetFlow flow record that uses traditional IPv4 output.
netflow protocol-port	Specifies the NetFlow flow record that uses the protocol and ports aggregation scheme.
netflow-original	Specifies a NetFlow flow record that uses traditional IPv4 input with origin ASs.

Defaults

None

Command Modes

Flow monitor configuration (config-flow-monitor)

SupportedUserRoles

network-admin

Command History

Release	Modification
4.2(1)SV1(4)	This command was modified to change the **protocol-port** attribute to **netflow protocol-port**.
4.0(4)SV1(1)	This command was introduced.

Usage Guidelines

A flow record defines the information that NetFlow gathers, such as packets in the flow and the types of counters gathered per flow. You can define new flow records or use the pre-defined flow record.

Examples

This example shows how to configure a flow record to use a the predefined traditional IPv4 input NetFlow record:

```
n1000v# config t
n1000v(config)# flow monitor testmon
```

```
n1000v(config-flow-monitor)# record netflow ipv4 original-input
n1000v(config-flow-monitor)#
```

This example shows how to remove the predefined traditional IPv4 input NetFlow flow record configuration:

```
n1000v# config t
n1000v(config)# flow monitor testmon
n1000v(config-flow-monitor)# no record netflow ipv4 original-input
n1000v(config-flow-monitor)#
```

Related Commands

Command	Description
show flow monitor	Displays NetFlow monitor configuration information.
show flow record	Displays NetFlow record configuration information.

reload

To reboot both the primary and secondary VSM in a redundant pair, use the **reload** command.

reload

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Any

SupportedUserRoles

network-admin

Command History

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

Usage Guidelines

To reboot only one of the VSMs in a redundant pair, use the **reload module** command instead.

Before reloading, use the **copy running-configuration to startup-configuration** command to preserve any configuration changes made since the previous reboot or restart.

Examples

This example shows how to reload both the primary and secondary VSM:

```
n1000v(config)# reload
!!!WARNING! there is unsaved configuration!!!
This command will reboot the system. (y/n)?  [n] y
2010 Sep  3 11:33:35 bl-n1000v %PLATFORM-2-PFM_SYSTEM_RESET: Manual system restart from
Command Line Interface
```

Related Commands

Command	Description
reload module	Reloads the specified VSM (1 or 2) in a redundant pair.

reload module

To reload one of the VSMs in a redundant pair, use the **reload module** command.

reload module *module* [**force-dnld**]

Syntax Description

module	The module number: • 1 (primary VSM) • 2 (secondary VSM)
force-dnld	(Optional) Reboots the specified module to force NetBoot and image download.

Defaults

None

Command Modes

Any

SupportedUserRoles

network-admin

Command History

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

Usage Guidelines

To reboot both the VSMs in a redundant pair, use the **reload** command instead.

Before reloading, use the **copy running-configuration to startup-configuration** command to preserve any configuration changes made since the previous reboot or restart.

Examples

This example shows how to reload VSM 2, the secondary VSM in a redundant pair:

```
n1000v# reload module 2
!!!WARNING! there is unsaved configuration!!!
This command will reboot the system. (y/n)?  [n] y
2010 Sep  3 11:33:35 bl-n1000v %PLATFORM-2-PFM_SYSTEM_RESET: Manual system restart from
Command Line Interface
```

Related Commands

Command	Description
show version	Displays information about the software version.
reload	Reboots both the primary and secondary VSM.

remote

To connect to remote machines, use the **remote** command. To disconnect, use the **no** form of this command.

remote {**ip address** *address* | **hostname** *name*}

no remote {**ip address** *address* | **hostname** *name*}

Syntax Description

ipaddress	Specifies an IP address.
address	IPv4 address. The format is A.B.C.D.
hostname	Specifies the remote host name.
name	Host name. The range of valid values is 1 to 128.

Defaults

None

Command Modes

SVS connection configuration (config-svs-conn)

SupportedUserRoles

network-admin

Command History

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

Examples

This example shows how to connect to a remote machine:

```
n1000v# configure terminal
n1000v(config)# svs connection svsconn1
n1000v(config-svs-conn)# remote hostname server1
n1000v(config-svs-conn)#
```

Related Commands

Command	Description
show svs	Displays SVS information.

remote-as <AS>

To specify Autonomous System Number of the neighbor, use the **remote-as <AS>** command.

remote-as <AS>

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Any.

SupportedUserRoles

network-admin

network-operator

Command History

Release	Modification
5.2(1)SV3(1.1)	This command was introduced.

Examples

This example shows how to configure Autonomous System Number of the neighbor:

```
n1000v(config-router-neighbor)# remote-as 1
```

Related Commands

Command	Description
remote	Connects to remote machines.

resequence

To resequence a list with sequence numbers, use the **resequence** command.

resequence {{{**ip** | **mac**} **access-list**} | **time-range**} *name number increment*

Syntax Description

ip	Indicates resequencing of an IP access-list.
mac	Indicates resequencing of a MAC access-list.
access-list	Indicates resequencing of an access list.
time-range	Indicates resequencing of a time-range.
name	(Optional) List name.
number	(Optional) Starting sequence number.
increment	(Optional) Step to increment the sequence number.

Defaults

None

Command Modes

Global configuration (config)

SupportedUserRoles

network-admin

Command History

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

Examples

This example shows how to resequence the first entry in the MAC ACL named aclOne:

```
n1000v# configure terminal
n1000v(config)# resequence mac access-list aclOne 1 2
n1000v(config)#
```

Related Commands

Command	Description
show access-list	Displays ACLs.

retain route-target all

To retain all the routes regardless of Target-VPN community, use the **retain route-target all** command.

retain route-target all

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Command Modes

Any.

SupportedUserRoles

network-admin

network-operator

Command History

Release	Modification
5.2(1)SV3(1.1)	This command was introduced.

Examples

This example shows how to retain all the routes regardless of Target-VPN community:

```
n1000v(config-router-af)# retain route-target all
```

Related Commands

Command	Description
show access-list	Displays ACLs.

rmdir

To remove a directory, use the **rmdir** command.

rmdir [*filesystem***:**[*//module/*]]*directory*

Syntax Description

*filesystem***:**	(Optional) Name of a file system. The name is case sensitive.
//module/	(Optional) Identifier for a supervisor module. Valid values are **sup-active**, **sup-local**, **sup-remote**, or **sup-standby**. The identifiers are case sensitive.
directory	Name of a directory. The name is case sensitive.

Defaults

Removes the directory from the current working directory.

Command Modes

Any

SupportedUserRoles

network-admin

Command History

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

Examples

This example shows how to remove the my_files directory:

```
n1000v# rmdir my_files
```

Related Commands

Command	Description
cd	Changes the current working directory.
dir	Displays the directory contents.
pwd	Displays the name of the current working directory.

role name

To create a user role, use the **role name** command. To remove the role, use the **no** form of this command.

role name *role-name*

no role name *role-name*

Syntax Description

role-name	Creates a user role of this name.

Defaults

None

Command Modes

Global configuration (config)

SupportedUserRoles

network-admin

Command History

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

Examples

This example shows how to create a role named UserA:

```
n1000v # config t
n1000v(config)# role name UserA
```

This example shows how to remove the UserA role:

```
n1000v(config)# no role UserA
```

Related Commands

Command	Description
show role	Displays the available user roles and their rules.
interface policy	Denies users assigned to this role access to all interfaces unless specifically permitted.
permit interface	Specifies the interface(s) that users assigned to this role can access.
vlan policy	Denies users assigned to this role access to all VLANs unless specifically permitted.
permit vlan	Specifies the VLAN(s) that users assigned to this role can access.

route-reflector-client

To configure a neighbor as Route reflector client, use the **route-reflector-client** command.

route-reflector-client

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Command Modes

Any.

SupportedUserRoles

network-admin

network-operator

Command History

Release	Modification
5.2(1)SV3(1.1)	This command was introduced.

Examples

This example shows how to configure a neighbor as Route reflector client:

```
n1000v(config-router-neighbor-af)# route-reflector-client
```

Related Commands

Command	Description
show role	Displays the available user roles and their rules.
permit vlan	Specifies the VLAN(s) that users assigned to this role can access.

router bgp <AS>

To configure Border Gateway Protocol (BGP) with Autonomous system number, use the **router bgp <AS>** command.

router bgp <AS>

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Any.

SupportedUserRoles

network-admin

network-operator

Command History

Release	Modification
5.2(1)SV3(1.1)	This command was introduced.

Examples

This example shows how to configure Border Gateway Protocol (BGP) with Autonomous system number:

```
n1000v(config)# router bgp <AS>
```

Related Commands

Command	Description
show role	Displays the available user roles and their rules.

router-id A.B.C.D

To manually specify the IP address to use as router-id, use the **router-id A.B.C.D** command.

router-id A.B.C.D

Syntax Description

This command has no arguments or keywords.

Defaults

None

Command Modes

Any.

SupportedUserRoles

network-admin

network-operator

Command History

Release	Modification
5.2(1)SV3(1.1)	This command was introduced.

Examples

This example shows how to manually specify the IP address to use as router-id:

```
n1000v(config-router)# router-id 17.17.17.31
```

Related Commands

Command	Description
router bgp <AS>	Configures Border Gateway Protocol (BGP) with Autonomous system number.

rule

To create a rule defining criteria for a user role, use the **rule** command. To remove a rule, use the **no** form of this command.

rule *number* {**deny** | **permit**} {**read** | **read-write** [**feature** *feature-name* | **feature-group** *group-name*] | **command** *command-name*}

no rule *number*

Syntax Description

number	Number that identifies this rule.
deny	Indicates that the user is denied the ability to perform a function.
permit	Indicates that the user is permitted to perform a function.
read	Specifies whether the assigned user has read access.
read-write	Specifies whether the assigned user has read-write access.
feature	(Optional) Specifies a feature for the rule.
feature-name	Name of an individual feature, such as syslog or TACACS+, whose access can be defined in this rule.
feature-group	(Optional) Specifies a feature type.
group-name	Grouping of features whose access can be defined in a rule.
command	Specifies a command for this rule.
command-name	Single command, or group of commands collected in a regular expression, whose access can be defined in a rule.

Defaults

None

Command Modes

Role configuration (config-role)

SupportedUserRoles

network-admin

Command History

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

Usage Guidelines

The *rule number* specifies the order in which the rule is applied, in descending order. For example, if a role has three rules, rule 3 is applied first, rule 2 is applied next, and rule 1 is applied last. You can configure up to 256 rules for each role.

Examples

This example shows how to create a rule that denies access to the **clear users** command:

```
n1000v# config t
n1000v(config)# role name UserA
n1000v(config-role)# rule 1 deny command clear users
n1000v(config-role)#
```

This example shows how to remove the rule 1 configuration:

```
n1000v# config t
n1000v(config)# role name UserA
n1000v(config-role)# no rule 1
```

Related Commands

Command	Description
username	Configures information about the user.
show role	Displays the user role configuration.

run-script

To run a command script that is saved in a file, use the **run-script** command.

run-script {**bootflash:** | **volatile:**} *filename*

Syntax Description

bootflash:	Indicates that the file containing the command script is located in the Bootflash file system.
volatile:	Indicates that the file containing the command script is located in the Volatile file system.
filename	The name of the file containing the command script. The name is case sensitive.

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 run a command script that is saved in the Sample file on the Volatile file system.

```
n1000v(config)# run-script volatile:Sample
n1000v(config)#
```

Related Commands

Command	Description
cd	Changes the current working directory.
copy	Copies files.
dir	Displays the contents of the working directory.
pwd	Displays the name of the present working directory (pwd).