



R Commands

This chapter describes the Cisco NX-OS security commands that begin with R.

radius-server deadtime

To configure the dead-time interval for all RADIUS servers on a NX-OS 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	<i>minutes</i>	Number of minutes for the dead-time interval. The range is from 1 to 1440 minutes.
---------------------------	----------------	--

Defaults	0 minutes
-----------------	-----------

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

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

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

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

Send document comments to nexus7k-docfeedback@cisco.com

**Note**

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

The command does not require a license.

Examples

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

```
switch# config t
switch(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:

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

Related Commands

Command	Description
show radius-server	Displays RADIUS server information.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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

Sends the authentication request to the configured RADIUS server group

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(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.

This command does not require a license.

Examples

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

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

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

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

Related Commands

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

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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

<i>hostname</i>	RADIUS server Domain Name Server (DNS) name. The name is alphanumeric, case sensitive, and has a maximum of 256 characters.
<i>ipv4-address</i>	RADIUS server IPv4 address in the <i>A.B.C.D</i> format.
<i>ipv6-address</i>	RADIUS server IPv6 address in the <i>X:X:X:X</i> 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.
<i>shared-secret</i>	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 <i>port-number</i>	(Optional) Configures the RADIUS server port for accounting. The range is from 0 to 65535.
auth-port <i>port-number</i>	(Optional) Configures the RADIUS server port for authentication. The range is from 0 to 65535.
authentication	(Optional) Configures authentication.
retransmit <i>count</i>	(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 <i>time</i>	Specifies the time interval (in minutes) for monitoring the server. The range is from 1 to 1440 minutes.
password <i>password</i>	Specifies a user password in the test packets. The password is alphanumeric, case sensitive, and has a maximum of 32 characters.

Send document comments to nexus7k-docfeedback@cisco.com

username <i>name</i>	Specifies a username in the test packets. The is alphanumeric, not case sensitive, and has a maximum of 32 characters.
timeout <i>seconds</i>	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

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

SupportedUserRoles

network-admin
 vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

When the idle time interval is 0 minutes, periodic RADIUS server monitoring is not performed.
 This command does not require a license.

Examples

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

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

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands

Command	Description
show radius-server	Displays RADIUS server information.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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.
	<i>shared-secret</i>	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

Supported User Roles network-admin
vdc-admin

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

Usage Guidelines You must configure the RADIUS preshared key to authenticate the switch to 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 by using the **key** keyword in the **radius-server host** command.

This command does not require a license.

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

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

■ radius-server key

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands

Command	Description
show radius-server	Displays RADIUS server information.

Send document comments to nexus7k-docfeedback@cisco.com

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	<i>count</i>	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	
SupportedUserRoles	network-admin vdc-admin	
Command History	Release	Modification
	4.0(1)	This command was introduced.
Usage Guidelines	This command does not require a license.	
Examples	<p>This example shows how to configure the number of retransmissions to RADIUS servers:</p> <pre>switch# config t switch(config)# radius-server retransmit 3</pre> <p>This example shows how to revert to the default number of retransmissions to RADIUS servers:</p> <pre>switch# config t switch(config)# no radius-server retransmit 3</pre>	
Related Commands	Command	Description
	show radius-server	Displays RADIUS server information.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

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	<i>seconds</i>	Number of seconds between retransmissions to the RADIUS server. The range is from 1 to 60 seconds.
Defaults	1 second	
Command Modes	Global configuration	
Supported User Roles	network-admin vdc-admin	
Command History	Release	Modification
	4.0(1)	This command was introduced.
Usage Guidelines	This command does not require a license.	
Examples	<p>This example shows how to configure the timeout interval:</p> <pre>switch# config t switch(config)# radius-server timeout 30</pre> <p>This example shows how to revert to the default interval:</p> <pre>switch# config t switch(config)# no radius-server timeout 30</pre>	
Related Commands	Command	Description
	show radius-server	Displays RADIUS server information.

Send document comments to nexus7k-docfeedback@cisco.com

range

To specify a range of ports as a group member in an IP port object group, use the **range** command. To remove a port range group member from port object group, use the **no** form of this command.

[sequence-number] range starting-port-number ending-port-number

no { *sequence-number* | **range** *starting-port-number ending-port-number* }

Syntax Description

<i>sequence-number</i>	(Optional) Sequence number for this group member. Sequence numbers maintain the order of group members within an object group. Valid sequence numbers are from 1 to 4294967295. If you do not specify a sequence number, the device assigns a number that is 10 greater than the largest sequence number in the current object group.
<i>starting-port-number</i>	Lowest port number that this group member matches. Valid values are from 0 to 65535.
<i>ending-port-number</i>	Highest port number that this group member matches. Valid values are from 0 to 65535.

Defaults

None

Command Modes

IP port object group configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

IP port object groups are not directional. Whether a **range** command matches a source or destination port or whether it applies to inbound or outbound traffic depends upon how you use the object group in an ACL.

This command does not require a license.

Examples

This example shows how to configure an IP port object group named port-group-05 with a group member that matches traffic sent to or from port 137 through port 139:

```
switch# config t
switch(config)# object-group ip port port-group-05
switch(config-port-ogroup)# range 137 139
```

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands	Command	Description
	eq	Specifies an equal-to group member in an IP port object group.
	gt	Specifies a greater-than group member in an IP port object group.
	lt	Specifies a less-than group member in an IP port object group.
	neq	Specifies a not-equal-to group member in an IP port object group.
	object-group ip port	Configures an IP port object group.
	show object-group	Displays object groups.

Send document comments to nexus7k-docfeedback@cisco.com

remark

To enter a comment into an IPv4 or MAC access control list (ACL), use the **remark** command. To remove a **remark** command, use the **no** form of this command.

```
[sequence-number] remark remark
```

```
no {sequence-number | remark remark}
```

Syntax Description

<i>sequence-number</i>	(Optional) Sequence number of the remark command, which causes the device to insert the command in that numbered position in the access list. Sequence numbers maintain the order of rules within an ACL. A sequence number can be any integer between 1 and 4294967295. By default, the first rule in an ACL has a sequence number of 10. If you do not specify a sequence number, the device adds the rule to the end of the ACL and assigns to it a sequence number that is 10 greater than the sequence number of the preceding rule. Use the resequence command to reassign sequence numbers to remarks and rules.
<i>remark</i>	Text of the remark. This argument can be up to 100 alphanumeric, case-sensitive characters.

Defaults

No ACL contains a remark by default.

Command Modes

IP access-list configuration
MAC access-list configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

The *remark* argument can be up to 100 characters. If you enter more than 100 characters for the *remark* argument, the device accepts the first 100 characters and drops any additional characters.

Send document comments to nexus7k-docfeedback@cisco.com

Examples

This example shows how to create a remark in an IPv4 ACL and display the results:

```
switch# config t
switch(config)# ip access-list acl-ipv4-01
switch(config-acl)# 100 remark this ACL denies the marketing department access to the lab
switch(config-acl)# show access-list acl-ipv4-01
```

```
IP access list acl-ipv4-01
    100 remark this ACL denies the marketing department access to the lab
ciscobox(config-acl)#
```

Related Commands

Command	Description
ip access-list	Configures an IPv4 ACL.
mac access-list	Configures a MAC ACL.
show access-list	Displays all ACLs or one ACL.
statistics per-entry	Enables collection of statistics for each entry in an ACL.

Send document comments to nexus7k-docfeedback@cisco.com

replay-protection

To enable the data-path replay protection feature for Cisco TrustSec authentication on an interface, use the **replay-protection** command. To disable the data-path replay protection feature, use the **no** form of this command.

replay-protection

no replay-protection

Syntax Description This command has no arguments or keywords.

Defaults Enabled

Command Modes Cisco TrustSec 802.1X configuration

SupportedUserRoles network-admin
vdc-admin

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

Usage Guidelines To use this command, you must enable the Cisco TrustSec feature using the **feature cts** command. After using this command, you must enable and disable the interface using the **shutdown/no shutdown** command sequence for the configuration to take effect. This command requires the Advanced Services license.

Examples This example shows how to enable data-path protect for Cisco TrustSec authentication on an interface:

```
switch# config t
switch(config)# interface ethernet 2/3
switch(config-if)# cts dot1x
switch(config-if-cts-dot1x)# replay-protection
switch(config-if-cts-dot1x)# exit
switch(config-if)# shutdown
switch(config-if)# no shutdown
```

Send document comments to nexus7k-docfeedback@cisco.com

This example shows how to disable data-path protect for Cisco TrustSec authentication on an interface:

```
switch# config t
switch(config)# interface ethernet 2/3
switch(config-if)# cts dot1x
switch(config-if-cts-dot1x)# no replay-protection
switch(config-if-cts-dot1x)# exit
switch(config-if)# shutdown
switch(config-if)# no shutdown
```

Related Commands

Command	Description
cts dot1x	Enters Cisco TrustSec 802.1X configuration mode for an interface.
feature cts	Enables the Cisco TrustSec feature.
show cts interface	Displays the Cisco TrustSec configuration for interfaces.

Send document comments to nexus7k-docfeedback@cisco.com

resequence

To reassign sequence numbers to all rules in an access control list (ACL) or a time range, use the **resequence** command.

resequence *access-list-type* **access-list** *access-list-name* *starting-sequence-number* *increment*

resequence **time-range** *time-range-name* *starting-sequence-number* *increment*

Syntax Description		
<i>access-list-type</i>	Type of the ACL. Valid values for this argument are the following keywords:	<ul style="list-style-type: none"> • arp • ip • mac
access-list <i>access-list-name</i>	Specifies the name of the ACL, which can be up to 64 alphanumeric, case-sensitive characters.	
time-range <i>time-range-name</i>	Specifies the name of the time range, which can be up to 64 alphanumeric, case-sensitive characters.	
<i>starting-sequence-number</i>	Sequence number for the first rule in the ACL or time range.	
<i>increment</i>	Number that the device adds to each subsequent sequence number.	

Defaults None

Command Modes Global configuration

Supported User Roles network-admin
vdc-admin

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

Usage Guidelines The **resequence** command allows you to reassign sequence numbers to the rules of an ACL or time range. The new sequence number for the first rule is determined by the *starting-sequence-number* argument. Each additional rule receives a new sequence number determined by the *increment* argument. If the highest sequence number would exceed the maximum possible sequence number, then no sequencing occurs and the following message appears:

```
ERROR: Exceeded maximum sequence number.
```

The maximum sequence number is 4294967295.

This command does not require a license.

Send document comments to nexus7k-docfeedback@cisco.com

Examples

This example shows how to resequence an IPv4 ACL named ip-acl-01 with a starting sequence number of 100 and an increment of 10, using the **show ip access-lists** command to verify sequence numbering before and after the use of the **resequence** command:

```
switch# config t
switch(config)# show ip access-lists ip-acl-01

IP access list ip-acl-01
  7 permit tcp addrgroup lab-machines any
 10 permit udp addrgroup lab-machines any
 13 permit icmp addrgroup lab-machines any
 17 deny igmp any any
switch(config)# resequence ip access-list ip-acl-01 100 10
switch(config)# show ip access-lists ip-acl-01

IP access list ip-acl-01
 100 permit tcp addrgroup lab-machines any
 110 permit udp addrgroup lab-machines any
 120 permit icmp addrgroup lab-machines any
 130 deny igmp any any
```

Related Commands

Command	Description
arp access-list	Configures an ARP ACL.
ip access-list	Configures an IPv4 ACL.
mac access-list	Configures a MAC ACL.
show access-lists	Displays all ACLs or a specific ACL.

Send document comments to nexus7k-docfeedback@cisco.com

role feature-group name

To create or specify a user role feature group and enter user role feature group configuration mode, use the **role feature-group name** command. To delete a user role feature group, use the **no** form of this command.

role feature-group name *group-name*

no role feature-group name *group-name*

Syntax Description	<i>group-name</i>	User role feature group name. The <i>group-name</i> has a maximum length of 32 characters and is a case-sensitive, alphanumeric character string.
---------------------------	-------------------	---

Defaults	None
-----------------	------

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

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

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

Usage Guidelines The NX-OS software provides the default user role feature group L3 for Layer 3 features. You cannot modify or delete the L3 user role feature group.

This command does not require a license.

Examples This example shows how to create a user role feature group and enter user role feature group configuration mode:

```
switch# config t
switch(config)# role feature-group name MyGroup
switch(config-role-featuregrp)#
```

This example shows how to remove a user role feature group:

```
switch# config t
switch(config)# no role feature-group name MyGroup
```

■ role feature-group name

Send document comments to nexus7k-docfeedback@cisco.com

Related Commands	Command	Description
	feature-group name	Specifies or creates a user role feature group and enters user role feature group configuration mode.
	show role feature-group	Displays the user role feature groups.

Send document comments to nexus7k-docfeedback@cisco.com

role name

To create or specify a user role and enter user role configuration mode, use the **role name** command. To delete a user role, use the **no** form of this command.

role name *role-name*

no role name *role-name*

Syntax Description	<i>role-name</i>	User role name. The <i>role-name</i> has a maximum length of 16 characters and is a case-sensitive, alphanumeric character string.
---------------------------	------------------	--

Defaults	None
-----------------	------

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

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

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

Usage Guidelines	<p>The NX-OS software provides four default user roles:</p> <ul style="list-style-type: none"> • network-admin—Complete read-and-write access to the entire NX-OS device (only available in the default VDC) • network-operator—Complete read access to the entire NX-OS device (only available in the default VDC) • vdc-admin—Read-and-write access limited to a VDC • vdc-operator—Read access limited to a VDC
-------------------------	--

You cannot change or remove the default user roles.

This command does not require a license.

Examples	This example shows how to create a user role and enter user role configuration mode:
-----------------	--

```
switch# config t
switch(config)# role MyRole
switch(config-role)#
```

■ role name

Send document comments to nexus7k-docfeedback@cisco.com

This example shows how to remove a user role:

```
switch# config t  
switch(config)# no role name MyRole
```

Related Commands

Command	Description
show role	Displays the user roles.

Send document comments to nexus7k-docfeedback@cisco.com

rule

To configure rules for a user role, use the **rule** command. To delete a rule, use the **no** form of this command.

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

```
no rule number
```

Syntax Description

<i>number</i>	Sequence number for the rule. The NX-OS software applies the rule with the highest value first and then the rest in descending order. The range is 1 to 256.
deny	Denies access to commands or features.
permit	Permits access to commands or features.
command <i>command-string</i>	Specifies a command string.
read	Specifies read access.
read-write	Specifies read and write access.
feature <i>feature-name</i>	(Optional) Specifies a feature name. Use the show role feature command to list the NX-OS feature names.
feature-group <i>group-name</i>	(Optional) Specifies a feature group.

Defaults

None

Command Modes

User role configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You can configure up to 256 rules for each role.

The rule number that you specify determines the order in which the rules are applied. Rules are applied in descending order. For example, if a role has three rules, rule 3 is applied before rule 2, which is applied before rule 1.

This command does not require a license.

Send document comments to nexus7k-docfeedback@cisco.com

Examples

This example shows how to add rules to a user role:

```
switch# config t
switch(config)# role MyRole
switch(config-role)# rule 1 deny command clear users
switch(config-role)# rule 1 permit read-write feature-group L3
```

This example shows how to remove rule from a user role:

```
switch# config t
switch(config)# role MyRole
switch(config-role)# no rule 10
```

Related Commands

Command	Description
role name	Creates or specifies a user role name and enters user role configuration mode.
show role	Displays the user roles.