



## INDEX

---

### Numerics

#### 802.1X

- Cisco TrustSec and [9-12](#)
- configuration process [7-9](#)
- configuring [7-8 to 7-34](#)
- configuring AAA accounting methods [7-31](#)
- default settings [7-35](#)
- description [7-1 to 7-7](#)
- disabling authentication on the device [7-24](#)
- disabling on the device [7-25](#)
- displaying statistics [7-34](#)
- enabling MAC address authentication bypass [7-23](#)
- enabling multiply hosts on an interface [7-22](#)
- enabling RADIUS accounting [7-30](#)
- enabling single hosts on an interface [7-22](#)
- example configuration [7-35](#)
- guidelines [7-8](#)
- licensing requirements [7-7](#)
- limitations [7-8](#)
- MIBs [7-36](#)
- multiple host support [7-6](#)
- port security on same port [7-6](#)
- prerequisites [7-8](#)
- single host support [7-6](#)
- supported topologies [7-7](#)
- verifying configuration [7-34](#)
- virtualization support [7-7](#)

#### 802.1X authentication

- authorization states for ports [7-4](#)
- controlling on interfaces [7-12](#)
- disabling on the device [7-24](#)
- initiation [7-3](#)

#### 802.1X defaults

- resetting globally [7-26](#)
- resetting on interfaces [7-27](#)

#### 802.1X feature

- disabling on the device [7-25](#)
- enabling [7-10](#)

#### 802.1X reauthentication

- enabling global periodic [7-13](#)
- enabling periodic on interfaces [7-15](#)
- manual [7-16](#)
- setting retry counts on interfaces [7-32](#)

#### 802.1X retry counts

- setting globally [7-28](#)
- setting on interfaces [7-29](#)

#### 802.1X supplicants

- manually initializing [7-17](#)
- manual reauthentication [7-16](#)

#### 802.1X timers

- changes interface timers [7-19](#)
- changing global timers [7-18](#)

---

### A

#### AAA

- accounting [2-2](#)
- authentication [2-2](#)
- authorization [2-2](#)
- benefits [2-2](#)
- configuration process [2-8](#)
- configuring [2-7 to 2-18](#)
- configuring for Cisco TrustSec [9-14](#)
- default settings [2-19](#)
- description [2-1 to 2-6](#)

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

- enabling MSCHAP authentication [2-13](#)
- example configuration [2-19](#)
- guidelines [2-7](#)
- licensing requirements [2-7](#)
- limitations [2-7](#)
- MIBs [2-20](#)
- monitoring TACACS+ servers [4-3](#)
- prerequisites [2-7](#)
- standards [2-20](#)
- TACACS+ server groups [4-11](#)
- user login process [2-4](#)
- verifying configurations [2-19](#)
- virtualization support [2-6](#)
- AAA accounting
  - configuring default methods [2-15](#)
  - configuring methods for 802.1X [7-31](#)
- AAA accounting logs
  - clearing [2-18](#)
  - displaying [2-18](#)
- AAA login authentication
  - configuring console methods [2-8](#)
  - configuring default methods [2-10](#)
- AAA logins
  - enabling authentication failure messages [2-12](#)
- AAA protocols
  - RADIUS [2-2](#)
  - TACACS+ [2-2](#)
- AAA server groups
  - description [2-3](#)
- AAA servers
  - FreeRADIUS VSA format [3-4](#)
  - specifying SNMPv3 parameters [2-16, 2-18](#)
  - specifying user roles [2-18](#)
  - specifying user roles in VSAs [2-16](#)
- AAA services
  - configuration options [2-3](#)
  - remote [2-3](#)
  - security [2-2](#)
- access control lists
  - description [10-1 to 10-10](#)
  - order of application [10-3](#)
  - types of [10-2](#)
  - See also ARP ACLs
  - See also IP ACLs
  - See also MAC ACLs
  - See also policy-based ACLs
  - See also port ACLs
  - See also router ACLs
  - See also VLAN ACLs
- accounting
  - description [2-2](#)
  - VDC support [2-6](#)
- ARP ACLs
  - applying to VLANs [15-9](#)
  - changing [15-23](#)
  - creating [15-21](#)
  - description [15-21](#)
  - priority of ARP ACLs and DHCP snooping entries [15-4](#)
  - removing [15-24](#)
- ARP inspection
  - See dynamic ARP inspection
- authentication
  - 802.1X [7-3](#)
  - description [2-2](#)
  - local [2-2](#)
  - methods [2-4](#)
  - remote [2-2](#)
  - user logins [2-4](#)
- authentication, authorization, and accounting. See AAA
- authorization
  - description [2-2](#)
  - user logins [2-4](#)

---

## B

- BGP
  - using with Unicast RPF [19-2](#)

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

broadcast storms. See traffic storm control

## C

### Cisco

vendor ID [2-17, 3-3, 4-4](#)

### cisco-av-pair

specifying AAA user parameters [2-16, 2-18](#)

### Cisco TrustSec

architecture [9-1](#)

authentication [9-19](#)

authorization [9-9](#)

configuring [9-12 to 9-47](#)

data-path replay protection [9-21, 9-25](#)

default values [9-51](#)

description [9-1 to 9-11](#)

enabling [9-12](#)

enabling (example) [9-48](#)

environment data download [9-10](#)

example configurations [9-47 to 9-51](#)

guidelines [9-11](#)

IEEE 802.1AE support [9-3](#)

licensing [9-11](#)

limitations [9-11](#)

manual mode [9-27](#)

policy acquisition [9-9](#)

prerequisites [9-11](#)

RADIUS relay [9-10](#)

SAP operation modes [9-23](#)

SGACLs [9-6 to ??, 9-29 to 9-39](#)

SGTs [9-6 to ??, 9-32](#)

SXP [9-39 to 9-47](#)

verifying configuration [9-47](#)

virtualization support [9-11](#)

### Cisco TrustSec authentication

configuring [9-14, 9-19](#)

description [9-3 to 9-6](#)

### Cisco TrustSec authorization [9-9](#)

configuring [9-14](#)

Cisco TrustSec data-path replay protection

configuring [9-21, 9-25](#)

Cisco TrustSec device credentials

configuring [9-13](#)

description [9-6](#)

Cisco TrustSec device identities

configuring [9-13](#)

description [9-6](#)

Cisco TrustSec environment data

download [9-10](#)

Cisco TrustSec manual mode

configuring [9-27](#)

Cisco TrustSec nonseed devices

configuring [9-17](#)

description [9-17](#)

Cisco TrustSec seed devices

configuring [9-15](#)

description [9-10, 9-14](#)

example configuration [9-48](#)

Cisco TrustSec user credentials

description [9-6](#)

consoles

configuring AAA login authentication methods [2-8](#)

control plane class maps

configuring [20-9](#)

example configuration [20-19](#)

verifying configuration [20-19](#)

control plane policing. See CoPP

control plane policy maps

configuring [20-12](#)

example configuration [20-19](#)

verifying configuration [20-19](#)

control plane service policy

changing default policies [20-16](#)

configuring [20-15](#)

CoPP

clearing statistics [20-18](#)

configuring [20-9](#)

default policies [20-4](#)

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

- default settings [20-21](#)
  - description [20-1](#)
  - displaying configuration status information [20-17](#)
  - displaying statistics [20-17](#)
  - example configuration [20-19](#)
  - guidelines [20-8](#)
  - licensing [20-8](#)
  - limitations [20-8](#)
  - verifying configuration [20-19](#)
  - virtualization support [20-8](#)
  - CTS. See Cisco TrustSec
  - CTS authentication
    - rekeying an interface [9-26](#)
- 
- D**
- default setting
    - traffic storm control [18-6](#)
  - default settings
    - 802.1X [7-35](#)
    - AAA [2-19](#)
    - CoPP [20-21](#)
    - rate limits [21-7](#)
    - RBAC [6-15](#)
    - TACACS+ [4-22](#)
  - denial-of-service attacks
    - IP address spoofing, mitigating [19-3](#)
  - DHCP binding database
    - See DHCP snooping binding database
  - DHCP option 82
    - description [14-3](#)
  - DHCP snooping
    - binding database
      - See DHCP snooping binding database
    - description [14-1](#)
    - displaying DHCP bindings [14-17](#)
    - enabling feature [14-7](#)
    - enabling globally [14-8](#)
    - enabling on a VLAN [14-9](#)
    - interface trust state [14-13](#)
    - MAC address verification [14-10](#)
    - message exchange process [14-4](#)
    - minimum configuration [14-6](#)
    - option 82 [14-3](#)
    - overview [14-2](#)
    - relay agent [14-13](#)
  - DHCP snooping binding database
    - described [14-2](#)
    - entries [14-2](#)
  - documentation
    - additional publications [iii-xxv](#)
  - DoS attacks
    - Unicast RPF, deploying [19-4](#)
  - dynamic ARP inspection
    - additional validation [15-11](#)
    - applying ARP ACLs [15-9](#)
    - ARP cache poisoning [15-2](#)
    - ARP requests [15-2](#)
    - ARP spoofing attack [15-2](#)
    - configuring log buffer size [15-12](#)
    - configuring trust state [15-8](#)
    - description [15-1](#)
    - DHCP snooping binding database [15-3](#)
    - enabling on VLANs [15-7](#)
    - error-disabled recovery [15-10](#)
    - function of [15-3](#)
    - interface trust states [15-3](#)
    - logging of dropped packets [15-5](#)
    - man-in-the middle attack [15-2](#)
    - network security issues and interface trust states [15-3](#)
    - priority of ARP ACLs and DHCP snooping entries [15-4](#)
  - Dynamic Host Configuration Protocol snooping
    - See DHCP snooping
- 
- E**
- examples

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

AAA configurations [2-19](#)

---

## F

feature groups

creating [6-10](#)

Fibre Channel interfaces

default settings [5-15, 8-44](#)

FreeRADIUS

VSA format for role attributes [2-17, 3-4](#)

---

## G

Galois/Counter Mode. See GCM

GCM

Cisco TrustSec SAP encryption [9-3](#)

GCM authentication. See GMAC

GMAC

Cisco TrustSec SAP authentication [9-3](#)

---

## I

IDs

Cisco vendor ID [2-17, 3-3, 4-4](#)

interfaces

controlling 802.1X authentication [7-12](#)

default settings [5-15, 8-44](#)

enabling periodic 802.1X reauthentication [7-15](#)

setting 802.1X reauthentication retry counts [7-32](#)

setting 802.1X retransmission retry counts [7-29](#)

IP ACLs

changing an IP ACL [10-13](#)

configuring [10-11 to 10-19](#)

creating an IP ACL [10-12](#)

default settings [10-31](#)

guidelines [10-11](#)

licensing [10-10](#)

limitations [10-11](#)

prerequisites [10-11](#)

removing an IP ACL [10-14](#)

verifying configuration [10-20](#)

virtualization support [10-10](#)

IP Source Guard

description [16-1](#)

enabling [16-3](#)

static IP source entries [16-4](#)

---

## K

key chain

end-time [17-2](#)

lifetime [17-2](#)

start-time [17-2](#)

keychain management

configuring a key [17-5](#)

configuring lifetimes [17-7](#)

configuring text for a key [17-6](#)

creating a keychain [17-3](#)

description [17-1](#)

---

## L

licensing

802.1X [7-7](#)

AAA [2-7](#)

Cisco TrustSec [9-11](#)

CoPP [20-8](#)

IP ACLs [10-10](#)

RADIUS [3-4](#)

rate limits [21-2](#)

TACACS+ [4-6](#)

traffic storm control [18-3](#)

Unicast RPF [19-3](#)

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

---

## M

### MAC ACLs

- changing a MAC ACL [11-3](#)
- creating a MAC ACL [11-2](#)
- removing a MAC ACL [11-5](#)
- virtualization support [10-10](#)

### MAC addresses

- enabling authentication bypass for 802.1X [7-23](#)

### management interfaces

- default settings [5-15, 8-44](#)

### mgmt0 interfaces

- default settings [5-15, 8-44](#)

### MIBs

- 802.1X [7-36](#)
- AAA [2-20](#)

### Microsoft Challenge Handshake Authentication Protocol. See MSCHAP

### MSCHAP

- enabling authentication [2-13](#)

### multicast storms. See traffic storm control

### multiple hosts

- enabling for 802.1X [7-22](#)

---

## N

### network-admin user role

- description [6-3](#)

### Network Admission Control

- See NAC

### network-operator user role

- description [6-3](#)

---

## O

### object groups

- configuring [10-21](#)
- description [10-9](#)
- verifying [10-24](#)

---

## P

### passwords

- strong characteristics [6-2](#)

### policing policies

- default classes [20-5](#)
- description [20-4](#)
- lenient default policy [20-7](#)
- moderate default policy [20-6](#)
- strict default policy [20-6](#)

### policy-based ACLs

- creating object groups [10-21](#)
- description [10-9](#)
- verifying object groups [10-24](#)

### port ACLs

- applying [10-18](#)
- definition [10-2](#)

### port-based authentication

- configuring
  - manual reauthentication of a client [7-16](#)
- encapsulation [7-2](#)

### ports

- authorization states for 802.1X [7-4](#)

### port security

- 802.1X on same port [7-6](#)
- description [13-1](#)
- enabling globally [13-7](#)
- enabling on an interface [13-8](#)
- MAC move [13-4](#)
- static MAC address [13-10](#)
- violations [13-4](#)

### preshared keys

- TACACS+ [4-3](#)

---

## R

### RADIUS

- configuring global preshared keys [3-7](#)
- configuring servers [3-5 to 3-17](#)

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

- configuring timeout intervals [3-12](#)
  - configuring transmission retry counts [3-12](#)
  - default settings [3-20](#)
  - description [3-1 to 3-5](#)
  - example configurations [3-20](#)
  - licensing [3-4](#)
  - network environments [3-2](#)
  - operation [3-2](#)
  - prerequisites [3-5](#)
  - specifying server at login [3-11](#)
  - verifying configuration [3-19](#)
  - virtualization support [3-4](#)
  - VSAs [3-3](#)
  - RADIUS accounting
    - enabling for 802.1X [7-30](#)
  - RADIUS server groups
    - configuring [3-9](#)
  - RADIUS servers
    - configuration process [3-6](#)
    - configuring accounting attributes [3-14](#)
    - configuring authentication attributes [3-14](#)
    - configuring dead-time intervals [3-17](#)
    - configuring hosts [3-6](#)
    - configuring periodic monitoring [3-16](#)
    - configuring preshared keys [3-8](#)
    - configuring timeout interval [3-13](#)
    - configuring transmission retry count [3-13](#)
    - displaying statistics [3-19](#)
    - example configurations [3-20](#)
    - manually monitoring [3-18](#)
    - monitoring [3-3](#)
    - verifying configuration [3-19](#)
  - rate limits
    - clearing statistics [21-6](#)
    - configuring [21-3](#)
    - default settings [21-7](#)
    - description [21-1](#)
    - displaying statistics [21-5](#)
    - example configuration [21-7](#)
    - guidelines [21-2](#)
    - licensing [21-2](#)
    - limitations [21-2](#)
    - verifying configuration [21-6](#)
    - virtualization support [21-2](#)
  - RBAC
    - configuring [6-8 to 6-14](#)
    - default settings [6-15](#)
    - description [6-3](#)
    - example configuration [6-15](#)
    - verifying configuration [6-15](#)
    - See also user roles
  - related documents [iii-xxv](#)
  - Reverse Path Forwarding. See Unicast RPF
  - router ACLs
    - applying [10-16](#)
    - definition [10-2](#)
  - RPF. See Unicast RPF
  - rules. See user role rules
- 
- S**
- SAP
    - configuring operation modes [9-23](#)
  - Security Association Protocol. See SAP
  - security group access lists. See SGACLs
  - security group tag. See SGT
  - server groups. See AAA server groups
  - SGACL policies
    - configuration process [9-30](#)
    - displaying downloads [9-38](#)
    - enabling enforcement for VLANs [9-30](#)
    - enabling enforcement for VRFs [9-31](#)
    - manually configuring [9-35 to 9-37](#)
  - SGACLs
    - configuring [9-29 to 9-39](#)
    - description [9-6 to ??](#)
    - manually mapping for SGTs [9-33](#)
  - SGACLs policies

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

- acquisition [9-9](#)
  - SGT Exchange Protocol. See SXP
  - SGTs
    - description [9-6 to ??](#)
    - manually configuring [9-32](#)
    - manually mapping [9-33](#)
  - single hosts
    - enabling for 802.1X [7-22](#)
  - SNMPv3
    - specifying AAA parameters [2-16](#)
    - specifying parameters for AAA servers [2-18](#)
  - SSH
    - generating server key-pairs [1-3, 5-1](#)
  - statistics
    - 802.1X [7-34](#)
    - RADIUS servers [3-19](#)
    - TACACS+ [4-21](#)
    - traffic storm control [18-5](#)
  - superuser role. See network-admin user role
  - SXP
    - configuration process [9-39](#)
    - configuring [9-39 to 9-47](#)
    - configuring peer connections [9-40](#)
    - default passwords [9-43](#)
    - enabling [9-40](#)
    - reconcile period [9-45](#)
    - retry period [9-46](#)
    - source IP address [9-44](#)
  - displaying statistics [4-21](#)
  - enabling [4-7](#)
  - example configurations [4-22](#)
  - global preshared keys [4-3](#)
  - guidelines [4-6](#)
  - licensing requirements [4-6](#)
  - limitations [4-6](#)
  - prerequisites [4-6](#)
  - preshared key [4-3](#)
  - specifying TACACS+ servers at login [4-13](#)
  - user login operation [4-2](#)
  - verifying configuration [4-22](#)
  - virtualization [4-5](#)
  - VSAAs [4-4](#)
- TACACS+ servers
- configuration process [4-7](#)
  - configuring dead-time interval [4-18](#)
  - configuring hosts [4-8](#)
  - configuring periodic monitoring [4-17](#)
  - configuring preshared keys [4-10](#)
  - configuring server groups [4-11](#)
  - configuring TCP ports [4-16](#)
  - configuring timeout interval [4-15](#)
  - displaying statistics [4-21](#)
  - manually monitoring [4-19](#)
  - monitoring [4-3](#)
  - privilege levels [4-5](#)
  - verifying configuration [4-22](#)
- TCP ports
- TACACS+ servers [4-16](#)
- time ranges
- absolute [10-8](#)
  - changing a time range [10-27](#)
  - configuring [10-25 to 10-30](#)
  - creating a time range [10-25](#)
  - description [10-8](#)
  - periodic [10-9](#)
  - removing a time range [10-29](#)
  - verifying configuration [10-30](#)
- 
- T**
- TACACS+
- advantages over RADIUS [4-2](#)
  - configuring [4-6 to 4-21](#)
  - configuring global preshared keys [4-9](#)
  - configuring global timeout interval [4-14](#)
  - default settings [4-22](#)
  - description [4-1 to 4-5](#)
  - disabling [4-20](#)

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

## traffic storm control

- configuring [18-3](#)
- default settings [18-6](#)
- description [18-1](#)
- displaying statistics [18-5](#)
- example configuration [18-5](#)
- guidelines [18-3](#)
- licensing [18-3](#)
- limitations [18-3](#)
- verifying configuration [18-5](#)
- virtualization support [18-3](#)

## U

Unicast Reverse Path Forwarding. See Unicast RPF

## Unicast RPF

- BGP attributes [19-2](#)
- BOOTP and [19-4](#)
- configuring [19-4](#)
- default settings [19-6](#)
- deploying [19-4](#)
- description [19-1](#)
- DHCP and [19-4](#)
- example configurations [19-6](#)
- FIB [19-1](#)
- guidelines [19-3](#)
- implementation [19-2](#)
- licensing [19-3](#)
- limitations [19-3](#)
- loose mode [19-4](#)
- statistics [19-3](#)
- strict mode [19-4](#)
- tunneling and [19-4](#)
- verifying configuration [19-6](#)
- virtualization support [19-3](#)

unicast storms. See traffic storm control

## user accounts

- configuring [6-5, 6-6](#)
- description [6-2](#)

example configuration [6-15](#)

guidelines [6-4](#)

password characteristics [6-2](#)

verifying configuration [6-15](#)

virtualization support [6-4](#)

user accounts limitations [6-4](#)

## user logins

authentication process [2-4](#)

authorization process [2-4](#)

configuring AAA login authentication methods [2-10](#)

## user role rules

description [6-3](#)

## user roles

change VLAN policies [6-12](#)

changing interface policies [6-11](#)

changing VRF policies [6-13](#)

creating [6-8](#)

creating feature groups [6-10](#)

defaults [6-3](#)

description [6-3](#)

example configuration [6-15](#)

guidelines [6-4](#)

limitations [6-4](#)

specifying on AAA servers [2-16, 2-18](#)

verifying configuration [6-15](#)

virtualization support [6-4](#)

## V

### vdc-admin user role

description [6-3](#)

### vdc-operator user role

description [6-3](#)

vendor-specific attributes. See VSAs

## virtualization

802.1X [7-7](#)

AAA [2-6](#)

Cisco TrustSec [9-11](#)

CoPP [20-8](#)

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

RADIUS [3-4](#)

rate limits [21-2](#)

TACACS+ [4-5](#)

traffic storm control [18-3](#)

user accounts [6-4](#)

user roles [6-4](#)

#### VLAN ACLs

applying a VACL [12-6](#)

creating and changing VACLs [12-3](#)

definition [10-2](#)

description [12-1](#)

removing a VACL [12-5](#)

#### VLANs

enabling SGACL policy enforcement [9-30](#)

#### VRFs

enabling SGACL policy enforcement [9-31](#)

#### VSAs

format [2-17](#)

protocol options [2-17, 3-4, 4-5](#)

support description [2-17](#)