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

# Cisco Nexus 1000V Command Reference, Release 4.0(4)SV1(3)

April 19, 2012

**Americas Headquarters**
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-21798-01

*Cisco Nexus 1000V Command Reference, Release 4.0(4)SV1(3)*

# New or Changed Commands

This secion lists the new and changed information in this document by release, and where it is located. This section includes the following topics:

- "New and Changed Information in Release 4.0(4)SV1(3)"
- "New and Changed Information in Release 4.0(4)SV1(2)"

Table 2 lists and describes new and changed commands in Release 4.0(4)SV1(3).

***Table 1 New and Changed Information in Release 4.0(4)SV1(3)***

| New or Changed Command | Added | Changed | Removed | Feature | Configuration Document |
|---|---|---|---|---|---|
| **channel-group auto (port profile)** | | X | | Port Profile | *Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.0(4)SV1(3)* |
| **errdisable detect cause** | | X | | Dynamic ARP Inspection | *Cisco Nexus 1000V Security Configuration Guide, Release 4.0(4)SV1(3)* |
| **pinned-sgid** | | X | | Static Pinning | *Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.0(4)SV1(3)* |
| **show running-config port-profile** | | | X | Port Profile | Removed from:<br>*Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.0(4)SV1(3)* |
| **system mtu** | X | | | Port Profile | *Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.0(4)SV1(3)* |

Table 2 lists and describes new and changed commands in Release 4.0(4)SV1(2).

***Table 2 New and Changed Information in Release 4.0(4)SV1(2)***

| New or Changed Command | Added | Changed | Removed | Feature | Configuration Document |
|---|---|---|---|---|---|
| **capability iscsi-multipath** | X | | | iSCSI Multipath | *Cisco Nexus 1000V System Management Configuration Guide, Release 4.0(4)SV1(3)* |
| **capability l3control** | X | | | Layer 3 Control | *Cisco Nexus 1000V System Management Configuration Guide, Release 4.0(4)SV1(3)* |

*Table 2 New and Changed Information in Release 4.0(4)SV1(2)*

| New or Changed Command | Added | Changed | Removed | Feature | Configuration Document |
|---|---|---|---|---|---|
| **cd** | X | | | iSCSI Multipath | *Cisco Nexus 1000V System Management Configuration Guide, Release 4.0(4)SV1(3)* |
| **capability uplink** | | | X | Port Profile | Command removed from CLI<br>*Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.0(4)SV1(3)* |
| **channel-group auto (port profile)** | | X | | Port Profile | *Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.0(4)SV1(3)* |
| **clear ip arp inspection statistics vlan** | X | | | Dynamic ARP Inspection | *Cisco Nexus 1000V Security Configuration Guide, Release 4.0(4)SV1(3)* |
| **errdisable detect cause** | X | | | DHCP Snooping | *Cisco Nexus 1000V Security Configuration Guide, Release 4.0(4)SV1(3)* |
| **errdisable recovery cause** | X | | | Dynamic ARP Inspection | *Cisco Nexus 1000V Security Configuration Guide, Release 4.0(4)SV1(3)* |
| **errdisable recovery interval** | X | | | Dynamic ARP Inspection | *Cisco Nexus 1000V Security Configuration Guide, Release 4.0(4)SV1(3)* |
| **inherit port-profile** | X | | | Port Profile | *Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.0(4)SV1(3)* |
| **ip arp inspection limit** | X | | | Dynamic ARP Inspection | *Cisco Nexus 1000V Security Configuration Guide, Release 4.0(4)SV1(3)* |
| **ip arp inspection trust** | X | | | Dynamic ARP Inspection | *Cisco Nexus 1000V Security Configuration Guide, Release 4.0(4)SV1(3)* |
| **ip arp inspection validate** | X | | | Dynamic ARP Inspection | *Cisco Nexus 1000V Security Configuration Guide, Release 4.0(4)SV1(3)* |
| **ip arp inspection vlan** | X | | | Dynamic ARP Inspection | *Cisco Nexus 1000V Security Configuration Guide, Release 4.0(4)SV1(3)* |
| **ip dhcp snooping** | X | | | DHCP Snooping | *Cisco Nexus 1000V Security Configuration Guide, Release 4.0(4)SV1(3)* |
| **ip dhcp snooping limit rate** | X | | | DHCP Snooping | *Cisco Nexus 1000V Security Configuration Guide, Release 4.0(4)SV1(3)* |
| **ip dhcp snooping trust** | X | | | DHCP Snooping | *Cisco Nexus 1000V Security Configuration Guide, Release 4.0(4)SV1(3)* |
| **ip dhcp snooping vlan** | X | | | DHCP Snooping | *Cisco Nexus 1000V Security Configuration Guide, Release 4.0(4)SV1(3)* |
| **ip source binding** | X | | | IP Source Guard | *Cisco Nexus 1000V Security Configuration Guide, Release 4.0(4)SV1(3)* |
| **ip verify source dhcp-snooping-vlan** | X | | | DHCP Snooping | *Cisco Nexus 1000V Security Configuration Guide, Release 4.0(4)SV1(3)* |
| **password strength-check** | X | | | Security User Accounts | *Cisco Nexus 1000V Security Configuration Guide, Release 4.0(4)SV1(3)* |

*Table 2 New and Changed Information in Release 4.0(4)SV1(2)*

| New or Changed Command | Added | Changed | Removed | Feature | Configuration Document |
|---|---|---|---|---|---|
| **permit interface** | X | | | Security Access Lists | *Cisco Nexus 1000V Security Configuration Guide, Release 4.0(4)SV1(3)* |
| **pinned-sgid** | X | | | Static Pinning | *Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.0(4)SV1(3)* |
| **pinning id** | X | | | Static Pinning | *Cisco Nexus 1000V Interface Configuration Guide, Release 4.0(4)SV1(3)*<br>*Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.0(4)SV1(3)* |
| **port-security stop learning** | X | | | Port Seurity | *Cisco Nexus 1000V Security Configuration Guide, Release 4.0(4)SV1(3)* |
| **rule** | X | | | Security User Accounts | *Cisco Nexus 1000V Security Configuration Guide, Release 4.0(4)SV1(3)* |
| **server** | X | | | Security RADIUS | *Cisco Nexus 1000V Security Configuration Guide, Release 4.0(4)SV1(3)* |
| **service-port** | X | | | Virtual Service Domain | *Cisco Nexus 1000V System Management Configuration Guide, Release 4.0(4)SV1(3)* |
| **show access-list summary** | X | | | Security Access Lists | *Cisco Nexus 1000V Troubleshooting Guide, Release 4.0(4)SV1(3)* |
| **show banner motd** | X | | | System Management | *Cisco Nexus 1000V System Management Configuration Guide, Release 4.0(4)SV1(3)* |
| **show boot** | X | | | System Management | *Cisco Nexus 1000V Software Upgrade Guide, Release 4.0(4)SV1(3)* |
| **show class-map** | X | | | QoS | *Cisco Nexus 1000V Quality of Service Configuration Guide, Release 4.0(4)SV1(3)* |
| **show cli variables** | X | | | System Management | *Cisco Nexus 1000V Getting Started Guide, Release 4.0(4)SV1(3)* |
| **show cores** | X | | | System Management | *Cisco Nexus 1000V High Availability and Redundancy Configuration Guide, Release 4.0(4)SV1(3)* |
| **show file** | X | | | System Management | *Cisco Nexus 1000V System Management Configuration Guide, Release 4.0(4)SV1(3)* |
| **show flow exporter** | X | | | NetFlow | *Cisco Nexus 1000V System Management Configuration Guide, Release 4.0(4)SV1(3)* |
| **show flow interface** | X | | | NetFlow | *Cisco Nexus 1000V System Management Configuration Guide, Release 4.0(4)SV1(3)* |
| **show flow monitor** | X | | | NetFlow | *Cisco Nexus 1000V System Management Configuration Guide, Release 4.0(4)SV1(3)* |
| **show flow record** | X | | | NetFlow | *Cisco Nexus 1000V System Management Configuration Guide, Release 4.0(4)SV1(3)* |

*Table 2 New and Changed Information in Release 4.0(4)SV1(2)*

| New or Changed Command | Added | Changed | Removed | Feature | Configuration Document |
|---|---|---|---|---|---|
| **show interface brief** | X | | | Interface | *Cisco Nexus 1000V Getting Started Guide, Release 4.0(4)SV1(3)* |
| **show interface capabilities** | X | | | Interface | *Cisco Nexus 1000V Interface Configuration Guide, Release 4.0(4)SV1(3)* |
| **show interface ethernet** | | X | | Interface Rate Statistics | *Cisco Nexus 1000V Interface Configuration Guide, Release 4.0(4)SV1(3)* |
| **show interface status** | X | | | Interface | *Cisco Nexus 1000V Troubleshooting Guide, Release 4.0(4)SV1(3)* |
| **show interface vethernet** | | X | | Interface Rate Statistics | *Cisco Nexus 1000V Interface Configuration Guide, Release 4.0(4)SV1(3)* |
| **show interface virtual** | X | | | Interface | *Cisco Nexus 1000V Interface Configuration Guide, Release 4.0(4)SV1(3)* |
| **show interface virtual port-mapping** | X | | | Interface | *Cisco Nexus 1000V Interface Configuration Guide, Release 4.0(4)SV1(3)* |
| **show ip arp client** | X | | | Dynamic ARP Inspection | *Cisco Nexus 1000V Security Configuration Guide, Release 4.0(4)SV1(3)* |
| **show ip arp inspection vlan** | X | | | Dynamic ARP Inspection | *Cisco Nexus 1000V Security Configuration Guide, Release 4.0(4)SV1(3)* |
| **show ip arp statistics** | X | | | Dynamic ARP Inspection | *Cisco Nexus 1000V Security Configuration Guide, Release 4.0(4)SV1(3)* |
| **show ip access-list** | X | | | Security Access Lists | *Cisco Nexus 1000V Quality of Service Configuration Guide, Release 4.0(4)SV1(3)* |
| **show ip access-list summary** | X | | | Security Access Lists | *Cisco Nexus 1000V Quality of Service Configuration Guide, Release 4.0(4)SV1(3)* |
| **show ip arp inspection interface** | X | | | Dynamic ARP Inspection | *Cisco Nexus 1000V Security Configuration Guide, Release 4.0(4)SV1(3)* |
| **show ip arp inspection statistics** | X | | | Dynamic ARP Inspection | *Cisco Nexus 1000V Security Configuration Guide, Release 4.0(4)SV1(3)* |
| **show ip dhcp snooping** | X | | | DHCP Snooping | *Cisco Nexus 1000V Security Configuration Guide, Release 4.0(4)SV1(3)* |
| **show ip dhcp snooping binding** | X | | | DHCP Snooping | *Cisco Nexus 1000V Security Configuration Guide, Release 4.0(4)SV1(3)* |
| **show ip dhcp snooping statistics** | X | | | IGMP Snooping | *Cisco Nexus 1000V Troubleshooting Guide, Release 4.0(4)SV1(3)* |
| **show ip igmp snooping groups** | X | | | IGMP Snooping | *Cisco Nexus 1000V Troubleshooting Guide, Release 4.0(4)SV1(3)* |

*Table 2 New and Changed Information in Release 4.0(4)SV1(2)*

| New or Changed Command | Added | Changed | Removed | Feature | Configuration Document |
|---|---|---|---|---|---|
| show ip verify source | X | | | IP Source Guard | *Cisco Nexus 1000V Interface Configuration Guide, Release 4.0(4)SV1(3)* |
| show license file | X | | | Licensing | *Cisco Nexus 1000V License Configuration Guide, Release 4.0(4)SV1(3)* |
| show license host-id | X | | | Licensing | *Cisco Nexus 1000V License Configuration Guide, Release 4.0(4)SV1(3)* |
| show mac access-lists | X | | | ACLs | *Cisco Nexus 1000V Security Configuration Guide, Release 4.0(4)SV1(3)* |
| show mac address-table | X | | | MAC Address Table | *Cisco Nexus 1000V Layer 2 Switching Configuration Guide, Release 4.0(4)SV1(3)* |
| show mac address-table aging-time | X | | | MAC Address Table | *Cisco Nexus 1000V Layer 2 Switching Configuration Guide, Release 4.0(4)SV1(3)* |
| show module | X | | | System Management | *Cisco Nexus 1000V Getting Started Guide, Release 4.0(4)SV1(3)* |
| show module vem mapping | X | | | VEM | *Cisco Nexus 1000V Getting Started Guide, Release 4.0(4)SV1(3)* |
| show monitor | X | | | System Management | *Cisco Nexus 1000V System Management Configuration Guide, Release 4.0(4)SV1(3)* |
| show monitor session | X | | | System Management | *Cisco Nexus 1000V System Management Configuration Guide, Release 4.0(4)SV1(3)* |
| show ntp peer-status | X | | | NTP | *Cisco Nexus 1000V System Management Configuration Guide, Release 4.0(4)SV1(3)* |
| show ntp peers | X | | | NTP | *Cisco Nexus 1000V System Management Configuration Guide, Release 4.0(4)SV1(3)* |
| show ntp statistics | X | | | NTP | *Cisco Nexus 1000V System Management Configuration Guide, Release 4.0(4)SV1(3)* |
| show password strength-check | X | | | Security | *Cisco Nexus 1000V Security Configuration Guide, Release 4.0(4)SV1(3)* |
| show policy-map | X | | | QoS | *Cisco Nexus 1000V Quality of Service Configuration Guide, Release 4.0(4)SV1(3)* |
| show policy-map interface | X | | | QoS | *Cisco Nexus 1000V Quality of Service Configuration Guide, Release 4.0(4)SV1(3)* |
| show port-profile | | X | | Port Profile | *Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.0(4)SV1(3)* |
| show port-profile expand-interface | X | | | Port Profile | *Cisco Nexus 1000V Troubleshooting Guide, Release 4.0(4)SV1(3)* |
| show port-security | X | | | Port Security | *Cisco Nexus 1000V Troubleshooting Guide, Release 4.0(4)SV1(3)* |
| show port-security address | X | | | High Availability | *Cisco Nexus 1000V High Availability and Redundancy Reference, Release 4.0* |

*Table 2 New and Changed Information in Release 4.0(4)SV1(2)*

| New or Changed Command | Added | Changed | Removed | Feature | Configuration Document |
|---|---|---|---|---|---|
| **show radius-server** | X | | | Security RADIUS | *Cisco Nexus 1000V Security Configuration Guide, Release 4.0(4)SV1(3)* |
| **show radius-server directed-request** | X | | | Security RADIUS | *Cisco Nexus 1000V Security Configuration Guide, Release 4.0(4)SV1(3)* |
| **show radius-server groups** | X | | | Security RADIUS | *Cisco Nexus 1000V Security Configuration Guide, Release 4.0(4)SV1(3)* |
| **show radius-server sorted** | X | | | Security RADIUS | *Cisco Nexus 1000V Security Configuration Guide, Release 4.0(4)SV1(3)* |
| **show radius-server statistics** | X | | | Security RADIUS | *Cisco Nexus 1000V Security Configuration Guide, Release 4.0(4)SV1(3)* |
| **show running-config diff** | X | | | System Management | *Cisco Nexus 1000V High Availability and Redundancy Reference, Release 4.0* |
| **show running-config interface ethernet** | X | | | Interface | *Cisco Nexus 1000V Interface Configuration Guide, Release 4.0(4)SV1(3)* |
| **show running-config interface vethernet** | X | | | Interface | *Cisco Nexus 1000V Interface Configuration Guide, Release 4.0(4)SV1(3)* |
| **show running-config port-profile** | | | X | Port Profile | Removed from:<br>*Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.0(4)SV1(3)* |
| **show ssh key** | X | | | Security SSH | *Cisco Nexus 1000V Security Configuration Guide, Release 4.0(4)SV1(3)* |
| **show ssh server** | X | | | Security SSH | *Cisco Nexus 1000V Security Configuration Guide, Release 4.0(4)SV1(3)* |
| **show snmp** | X | | | SNMP | *Cisco Nexus 1000V System Management Configuration Guide, Release 4.0(4)SV1(3)* |
| **show startup-config aaa** | X | | | Security AAA | *Cisco Nexus 1000V Security Configuration Guide, Release 4.0(4)SV1(3)* |
| **show startup-config radius** | X | | | Security RADIUS | *Cisco Nexus 1000V Security Configuration Guide, Release 4.0(4)SV1(3)* |
| **show startup-config security** | X | | | Security | *Cisco Nexus 1000V Security Configuration Guide, Release 4.0(4)SV1(3)* |
| **show svs connections** | X | | | Setup | *Cisco Nexus 1000V Getting Started Guide, Release 4.0(4)SV1(3)* |
| **show svs domain** | | X | | Layer 3 control | *Cisco Nexus 1000V System Management Configuration Guide, Release 4.0(4)SV1(3)* |
| **show svs neighbors** | X | | | VSM | *Cisco Nexus 1000V Troubleshooting Guide, Release 4.0(4)SV1(3)* |
| **show system error-id** | X | | | System Management | *Cisco Nexus 1000V Getting Started Guide, Release 4.0(4)SV1(3)* |

*Table 2 New and Changed Information in Release 4.0(4)SV1(2)*

| New or Changed Command | Added | Changed | Removed | Feature | Configuration Document |
|---|---|---|---|---|---|
| show system resources | X | | | System Management | *Cisco Nexus 1000V Troubleshooting Guide, Release 4.0(4)SV1(3)* |
| show tacacs-server | X | | | Security TACACS | *Cisco Nexus 1000V Security Configuration Guide, Release 4.0(4)SV1(3)* |
| show tcp client | X | | | Security | *Cisco Nexus 1000V Security Configuration Guide, Release 4.0(4)SV1(3)* |
| show tcp connection | X | | | Security | *Cisco Nexus 1000V Security Configuration Guide, Release 4.0(4)SV1(3)* |
| show tcp statistics | X | | | Security | *Cisco Nexus 1000V Security Configuration Guide, Release 4.0(4)SV1(3)* |
| show tech-support | X | | | System Management | *Cisco Nexus 1000V Troubleshooting Guide, Release 4.0(4)SV1(3)* |
| show telnet server | X | | | Security Telnet | *Cisco Nexus 1000V Security Configuration Guide, Release 4.0(4)SV1(3)* |
| show terminal | X | | | System Management | *Cisco Nexus 1000V Getting Started Guide, Release 4.0(4)SV1(3)* |
| show user-account | X | | | Security User Accounts | *Cisco Nexus 1000V Security Configuration Guide, Release 4.0(4)SV1(3)* |
| show users | X | | | Security User Accounts | *Cisco Nexus 1000V Security Configuration Guide, Release 4.0(4)SV1(3)* |
| show version | X | | | System Management | *Cisco Nexus 1000V System Management Configuration Guide, Release 4.0(4)SV1(3)* |
| show version image | X | | | System Management | *Cisco Nexus 1000V System Management Configuration Guide, Release 4.0(4)SV1(3)* |
| show virtual-service-domain brief | X | | | Virtual Service Domain | *Cisco Nexus 1000V System Management Configuration Guide, Release 4.0(4)SV1(3)* |
| show virtual-service-domain interface | X | | | Virtual Service Domain | *Cisco Nexus 1000V System Management Configuration Guide, Release 4.0(4)SV1(3)* |
| show virtual-service-domain name | X | | | Virtual Service Domain | *Cisco Nexus 1000V System Management Configuration Guide, Release 4.0(4)SV1(3)* |
| show vlan | X | | | Layer 2 Switching | *Cisco Nexus 1000V Interface Configuration Guide, Release 4.0(4)SV1(3)* |
| show vlan all-ports | X | | | Layer 2 Switching | *Cisco Nexus 1000V Troubleshooting Guide, Release 4.0(4)SV1(3)* |
| show vlan brief | X | | | Layer 2 Switching | *Cisco Nexus 1000V Layer 2 Switching Configuration Guide, Release 4.0(4)SV1(3)* |
| show vlan id | X | | | Layer 2 Switching | *Cisco Nexus 1000V Getting Started Guide, Release 4.0(4)SV1(3)* |
| show vlan private-vlan | X | | | Layer 2 Switching | *Cisco Nexus 1000V Layer 2 Switching Configuration Guide, Release 4.0(4)SV1(3)* |

*Table 2 New and Changed Information in Release 4.0(4)SV1(2)*

| New or Changed Command | Added | Changed | Removed | Feature | Configuration Document |
|---|---|---|---|---|---|
| **show vlan summary** | X | | | Layer 2 Switching | *Cisco Nexus 1000V Layer 2 Switching Configuration Guide, Release 4.0(4)SV1(3)* |
| **show vmware vc extension-key** | X | | | VEM | *Cisco Nexus 1000V Troubleshooting Guide, Release 4.0(4)SV1(3)* |
| **show vmware vem upgrade status** | X | | | VEM | *Cisco Nexus 1000V Software Upgrade Guide, Release 4.0(4)SV1(3)* |
| **show xml server status** | X | | | XML API | *Cisco Nexus 1000V XML API User Guide, Release 4.0(4)SV1(3)* |
| **snmp-server aaa-user cache-timeout** | X | | | SNMP | *Cisco Nexus 1000V System Management Configuration Guide, Release 4.0(4)SV1(3)* |
| **snmp-server community** | X | | | SNMP | *Cisco Nexus 1000V System Management Configuration Guide, Release 4.0(4)SV1(3)* |
| **snmp-server contact** | X | | | SNMP | *Cisco Nexus 1000V System Management Configuration Guide, Release 4.0(4)SV1(3)* |
| **snmp-server globalEnforcePriv** | X | | | SNMP | *Cisco Nexus 1000V System Management Configuration Guide, Release 4.0(4)SV1(3)* |
| **snmp-server host** | X | | | SNMP | *Cisco Nexus 1000V System Management Configuration Guide, Release 4.0(4)SV1(3)* |
| **snmp-server location** | X | | | SNMP | *Cisco Nexus 1000V System Management Configuration Guide, Release 4.0(4)SV1(3)* |
| **snmp-server protocol enable** | X | | | SNMP | *Cisco Nexus 1000V System Management Configuration Guide, Release 4.0(4)SV1(3)* |
| **snmp-server tcp-session** | X | | | SNMP | *Cisco Nexus 1000V System Management Configuration Guide, Release 4.0(4)SV1(3)* |
| **snmp-server user** | X | | | SNMP | *Cisco Nexus 1000V System Management Configuration Guide, Release 4.0(4)SV1(3)* |
| **snmp trap link-status** | X | | | SNMP | *Cisco Nexus 1000V System Management Configuration Guide, Release 4.0(4)SV1(3)* |
| **speed** | X | | | Interface | *Cisco Nexus 1000V Interface Configuration Guide, Release 4.0(4)SV1(3)* |
| **sub-group** | | X | | virtual Port Channel Host Mode (vPC-HM) | *Cisco Nexus 1000V Interface Configuration Guide, Release 4.0(4)SV1(3)* |
| **sub-group-id** | | X | | vPC-HM | *Cisco Nexus 1000V Interface Configuration Guide, Release 4.0(4)SV1(3)* |
| **svs mode** | X | | | Layer 3 control | *Cisco Nexus 1000V System Management Configuration Guide, Release 4.0(4)SV1(3)* |

*Table 2 New and Changed Information in Release 4.0(4)SV1(2)*

| New or Changed Command | Added | Changed | Removed | Feature | Configuration Document |
|---|---|---|---|---|---|
| system vlan | X | | | Port Profile | *Cisco Nexus 1000V Getting Started Guide, Release 4.0(4)SV1(3)*<br>*Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.0(4)SV1(3)*<br>*Cisco Nexus 1000V System Management Configuration Guide, Release 4.0(4)SV1(3)* |
| tacacs+ enable | X | | | Security TACACS | *Cisco Nexus 1000V Security Configuration Guide, Release 4.0(4)SV1(3)* |
| terminal monitor | X | | | | *Cisco Nexus 1000V Troubleshooting Guide, Release 4.0(4)SV1(3)* |
| username admin password | X | | | Security User Accounts | *Cisco Nexus 1000V Password Recovery Guide* |
| virtual-service-domain | X | | | Virtual Service Domain | *Cisco Nexus 1000V System Management Configuration Guide, Release 4.0(4)SV1(3)* |
| vlan policy deny | X | | | Access Lists | *Cisco Nexus 1000V Security Configuration Guide, Release 4.0(4)SV1(3)* |
| vmware vem upgrade complete | X | | | VEM Upgrade | *Cisco Nexus 1000V Software Upgrade Guide, Release 4.0(4)SV1(3)* |
| vmware vem upgrade notify | X | | | VEM Upgrade | *Cisco Nexus 1000V Software Upgrade Guide, Release 4.0(4)SV1(3)* |
| vmware vem upgrade proceed | X | | | VEM Upgrade | *Cisco Nexus 1000V Software Upgrade Guide, Release 4.0(4)SV1(3)* |
| xml server max-session sessions | X | | | XML API | *Cisco Nexus 1000V XML API User Guide, Release 4.0(4)SV1(3)* |
| xml server terminate session session-number | X | | | XML API | *Cisco Nexus 1000V XML API User Guide, Release 4.0(4)SV1(3)* |
| xml server timeout seconds | X | | | XML API | *Cisco Nexus 1000V XML API User Guide, Release 4.0(4)SV1(3)* |

# Preface

The purpose of this document is to provide a reference for the commands availabe in the Cisco Nexus 1000V CLI including complete command syntax, command modes, command history, defaults, usage guidelines, and examples.

This preface describes the audience, organization, and conventions of the *Cisco Nexus 1000V Command Reference, Release 4.0(4)SV1(3)*, and how to obtain related documentation.

This chapter includes the following topics:



## Audience

This publication is for experienced users who configure and maintain the Cisco Nexus 1000V.

## Organization

This reference is organized as follows:

| Chapter | Description |
|---|---|
| A Commands | Describes the commands that begin with the letter A. |
| B Commands | Describes the commands that begin with the letter B. |
| C Commands | Describes the commands that begin with the letter C. |
| D Commands | Describes the commands that begin with the letter D. |
| E Commands | Describes the commands that begin with the letter E. |
| F Commands | Describes the commands that begin with the letter F. |
| G Commands | Describes the commands that begin with the letter G. |
| I Commands | Describes the commands that begin with the letter I. |

| Chapter | Description |
|---|---|
| L Commands | Describes the commands that begin with the letter L. |
| M Commands | Describes the commands that begin with the letter M. |
| N Commands | Describes the commands that begin with the letter N. |
| O Commands | Describes the commands that begin with the letter O. |
| P Commands | Describes the commands that begin with the letter P. |
| Q Commands | Describes the commands that begin with the letter Q. |
| R Commands | Describes the commands that begin with the letter R. |
| S Commands | Describes the commands that begin with the letter S. |
| Show Commands | Describes the **show** commands. |
| T Commands | Describes the commands that begin with the letter T. |
| U Commands | Describes the commands that begin with the letter U. |
| V Commands | Describes the commands that begin with the letter V. |
| W Commands | Describes the commands that begin with the letter W. |
| X Commands | Describes the commands that begin with the letter X. |

# Document Conventions

Command descriptions use these conventions:

| Convention | Description |
|---|---|
| **boldface font** | Commands and keywords are in boldface. |
| *italic font* | Arguments for which you supply values are in italics. |
| [ ] | Elements in square brackets are optional. |
| [ x \| y \| z ] | Optional alternative keywords are grouped in brackets and separated by vertical bars. |
| string | A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks. |

Screen examples use these conventions:

| | |
|---|---|
| `screen font` | Terminal sessions and information that the switch displays are in screen font. |
| **`boldface screen font`** | Information you must enter is in boldface screen font. |
| *`italic screen font`* | Arguments for which you supply values are in italic screen font. |
| < > | Nonprinting characters, such as passwords, are in angle brackets. |
| [ ] | Default responses to system prompts are in square brackets. |
| !, # | An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line. |

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

This document uses the following conventions:

**Note** Means reader *take note*. Notes contain helpful suggestions or references to material not covered in the manual.

**Caution** Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

**Tip** Means *the following information will help you solve a problem.*

# Available Documents

This section lists the documents used with the Cisco Nexus 1000 and available on Cisco.com at the following url:

http://www.cisco.com/en/US/products/ps9902/tsd_products_support_series_home.html

## General Information

*Cisco Nexus 1000V Documentation Roadmap, Release 4.0(4) SV1(3)*

*Cisco Nexus 1000V Release Notes, Release 4.0(4)SV1(3)*

*Cisco Nexus 1000V Compatibility Information, Release 4.0(4)SV1(3)*

*Cisco Nexus 1010 Management Software Release Notes, Release 4.0(4)SP1(1)*

## Install and Upgrade

*Cisco Nexus 1000V Software Installation Guide, Release 4.0(4)SV1(3)*

*Cisco Nexus 1000V Software Upgrade Guide, Release 4.0(4)SV1(3)*

*Cisco Nexus 1000V VEM Software Installation and Upgrade Guide, Release 4.0(4)SV1(3)*

*Cisco Nexus 1010 Virtual Services Appliance Hardware Installation Guide*

## Configuration Guides

*Cisco Nexus 1000V License Configuration Guide, Release 4.0(4)SV1(3)*

*Cisco Nexus 1000V Getting Started Guide, Release 4.0(4)SV1(3)*

*Cisco Nexus 1000V High Availability and Redundancy Configuration Guide, Release 4.0(4)SV1(3)*

*Cisco Nexus 1000V Interface Configuration Guide, Release 4.0(4)SV1(3)*

*Cisco Nexus 1000V Layer 2 Switching Configuration Guide, Release 4.0(4)SV1(3)*

*Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.0(4)SV1(3)*

*Cisco Nexus 1000V Quality of Service Configuration Guide, Release 4.0(4)SV1(3)*

*Cisco Nexus 1000V Security Configuration Guide, Release 4.0(4)SV1(3)*

*Cisco Nexus 1000V System Management Configuration Guide, Release 4.0(4)SV1(3)*

*Cisco Nexus 1010 Software Configuration Guide, Release 4.0(4)SP1(1)*

### Programming Guide

*Cisco Nexus 1000V XML API User Guide, Release 4.0(4)SV1(3)*

### Reference Guides

*Cisco Nexus 1000V Command Reference, Release 4.0(4)SV1(3)*

*Cisco Nexus 1000V MIB Quick Reference*

*Cisco Nexus 1010 Command Reference, Release 4.0(4)SP1(1)*

### Troubleshooting and Alerts

*Cisco Nexus 1000V Troubleshooting Guide, Release 4.0(4)SV1(3)*

*Cisco Nexus 1000V Password Recovery Guide*

*Cisco NX-OS System Messages Reference*

### Network Analysis Module Documentation

*Cisco Network Analysis Module Software Documentation Guide, 4.2*

*Cisco Nexus 1000V NAM Virtual Service Blade Installation and Configuration Guide*

*Network Analysis Module Command Reference Guide, 4.2*

*User Guide for the Cisco Network Analysis Module Virtual Service Blades, 4.2*

*Cisco Network Analysis Module Software Release Notes, 4.2*

# Obtaining Documentation and Submitting a Service Request

For information about obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

# A Commands

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

## aaa authentication login console

To configure AAA authentication methods for console logins, use the **aaa authentication login console** command. To revert to the default, use the **no** form of this command.

**aaa authentication login console** {**group** *group-list*} [**none**] | **local** | **none**}

**no aaa authentication login console** {**group** *group-list* [**none**] | **local** | **none**}

**Syntax Description**

| | |
|---|---|
| **group** | Specifies to use a server group for authentication. |
| *group-list* | Specifies a space-separated list of server groups. The list can include the following:<br>• **radius** for all configured RADIUS servers.<br>• **tacacs+** for all configured TACACS+ servers.<br>• Any configured RADIUS or TACACS+ server group name. |
| **none** | Specifies to use the username for authentication. |
| **local** | Specifies to use the local database for authentication. |

**Defaults**

**local**

**Command Modes**

Global configuration (config)

**SupportedUserRoles**

network-admin

## Command History

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

## Usage Guidelines

The **group radius, group tacacs+**, and **group** *group-list* methods refer to a set of previously defined RADIUS or TACACS+ servers. Use the **radius-server host** or **tacacs-server host** command to configure the host servers. Use the **aaa group server** command to create a named group of servers.

Use the **show aaa group** command to display the RADIUS server groups on the device.

If you specify more that one server group, the software checks each group in the order that you specify in the list.

If you specify the **group** method or **local** method and they fail, then the authentication can fail. If you specify the **none** method alone or after the **group** method, then the authentication always succeeds.

## Examples

This example shows how to configure the AAA authentication console login methods:

```
n1000v# config t
n1000v(config)# aaa authentication login console group radius
```

This example shows how to revert to the default AAA authentication console login method:

```
n1000v# config t
n1000v(config)# no aaa authentication login console group radius
```

## Related Commands

| Command | Description |
|---|---|
| **aaa group server** | Configures AAA server groups. |
| **radius-server host** | Configures RADIUS servers. |
| **show aaa authentication** | Displays AAA authentication information. |
| **show aaa group** | Displays the AAA server groups. |
| **tacacs-server host** | Configures TACACS+ servers. |

# aaa authentication login default

To configure the default AAA authentication methods, use the **aaa authentication login default** command. To revert to the default, use the **no** form of this command.

**aaa authentication login default** {**group** *group-list*} [**none**] | **local** | **none**}

**no aaa authentication login default** {**group** *group-list* [**none**] | **local** | **none**}

## Syntax Description

| | |
|---|---|
| **group** | Specifies a server group list to be used for authentication. |
| *group-list* | Space-separated list of server groups that can include the following:<br>• **radius** for all configured RADIUS servers.<br>• **tacacs+** for all configured TACACS+ servers.<br>• Any configured RADIUS or TACACS+ server group name. |
| **none** | (Optional) Specifies to use the username for authentication. |
| **local** | Specifies to use the local database for authentication. |

## Defaults

**local**

## Command Modes

Global configuration (config)

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

The **group radius, group tacacs+**, and **group** *group-list* methods refer to a set of previously defined RADIUS or TACACS+ servers. Use the **radius-server host** or **tacacs-server host** command to configure the host servers. Use the **aaa group server** command to create a named group of servers.

Use the **show aaa group** command to display the RADIUS server groups on the device.

If you specify more that one server group, the software checks each group in the order that you specify in the list.

If you specify the **group** method or **local** method and they fail, then the authentication fails. If you specify the **none** method alone or after the **group** method, then the authentication always succeeds.

## Examples

This example shows how to configure the AAA authentication console login method:

```
n1000v# config t
n1000v(config)# aaa authentication login default group radius
```

This example shows how to revert to the default AAA authentication console login method:

```
n1000v# config t
n1000v(config)# no aaa authentication login default group radius
```

## Related Commands

| Command | Description |
|---|---|
| **aaa group server** | Configures AAA server groups. |
| **radius-server host** | Configures RADIUS servers. |
| **show aaa authentication** | Displays AAA authentication information. |
| **show aaa group** | Displays the AAA server groups. |
| **tacacs-server host** | Configures TACACS+ servers. |

# aaa authentication login error-enable

To configure an AAA authentication failure message to display on the console, use the **aaa authentication login error-enable** command. To remove the error message, use the **no** form of this command.

**aaa authentication login error-enable**

**no aaa authentication login error-enable**

## 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

If none of the remote AAA servers respond when a user logs in, the authentication is processed by the local user database. If you have enabled the display, one of the following message is generated for the user:

```
Remote AAA servers unreachable; local authentication done.
Remote AAA servers unreachable; local authentication failed.
```

## Examples

This example shows how to enable the display of AAA authentication failure messages to the console:

```
n1000v# config t
n1000v(config)# aaa authentication login error-enable
```

This example shows how to disable the display of AAA authentication failure messages to the console:

```
n1000v# config t
n1000v(config)# no aaa authentication login error-enable
```

**Related Commands**

| Command | Description |
|---|---|
| **show aaa authentication login error-enable** | Displays the status of the AAA authentication failure message display. |

# aaa authentication login mschap

To enable Microsoft Challenge Handshake Authentication Protocol (MSCHAP) authentication at login, use the **aaa authentication login mschap** command. To disable MSCHAP, use the **no** form of this command.

**aaa authentication login mschap**

**no aaa authentication login mschap**

## 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. |

## Examples

This example shows how to enable MSCHAP authentication:

```
n1000v# config t
n1000v(config)# aaa authentication login mschap
```

This example shows how to disable MSCHAP authentication:

```
n1000v# config t
n1000v(config)# no aaa authentication login mschap
```

## Related Commands

| Command | Description |
|---|---|
| **show aaa authentication login mschap** | Displays the status of MSCHAP authentication. |

# aaa group server radius

To create a RADIUS server group, use the **aaa group server radius** command. To delete a RADIUS server group, use the **no** form of this command.

**aaa group server radius** *group-name*

**no aaa group server radius** *group-name*

## Syntax Description

| | |
|---|---|
| *group-name* | RADIUS server group name.The name is alphanumeric and case-sensitive. The maximum length is 64 characters. |

## 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 RADIUS server group and enter RADIUS Server Configuration mode for configuring the specified server group:

```
n1000v# config t
n1000v(config)# aaa group server radius RadServer
n1000v(config-radius)#
```

This example shows how to delete a RADIUS server group:

```
n1000v# config t
n1000v(config)# no aaa group server radius RadServer
```

## Related Commands

| Command | Description |
|---|---|
| **show aaa groups** | Displays server group information. |
| **radius-server host** | Defines the IP address or hostname for a RADIUS server. |

# aaa group server tacacs+

To create a TACACS+ server group, use the **aaa group server tacacs+** command. To delete a TACACS+ server group, use the **no** form of this command.

**aaa group server tacacs+** *group-name*

**no aaa group server tacacs+** *group-name*

## Syntax Description

| | |
|---|---|
| *group-name* | TACACS+ server group name. The name is alphanumeric and case-sensitive. The maximum length is 64 characters. |

## Defaults

None

## 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 enable TACACS+ using the **tacacs+ enable** command before you can configure TACACS+.

## Examples

This example shows how to create a TACACS+ server group:

```
n1000v# config t
n1000v(config)# aaa group server tacacs+ TacServer
n1000v(config-radius)#
```

This example shows how to delete a TACACS+ server group:

```
n1000v# config t
n1000v(config)# no aaa group server tacacs+ TacServer
```

## Related Commands

| Command | Description |
|---|---|
| **tacacs+ enable** | Enables TACACS+. |
| **show aaa groups** | Displays server group information. |

# attach module

To access the standby Virtual Supervisor Module (VSM) console from the active VSM, use the **attach module** command.

**attach module** *module-number*

## Syntax Description

| | |
|---|---|
| *module-number* | Number that identifies an existing module. The range is 1–66.<br>**Note** Only one value, 2, is operational. |

## 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 attach to the console of the secondary VSM:

```
n1000v# config t
n1000v(config)# attach module 2
n1000v#
```

## Usage Guidelines

Although the allowable range of module numbers is from 1–66, only one value, 2, is operational.

## Related Commands

| Command | Description |
|---|---|
| **show cores** | Displays a list of cores. |
| **show processes log** | Displays a list of process logs. |
| **show system redundancy status** | Checks redundancy status. |
| **show system internal sysmgr state** | Checks the system internal sysmgr state. |
| **reload module** | Reloads a module. |

# B Commands

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

## bandwidth (interface)

To set the inherited and received bandwidth for an interface, use the **bandwidth** command. To restore the default value, use the **no** form of this command.

**bandwidth** {*kbps*}

**no bandwidth** {*kbps*}

**Syntax Description**

| | |
|---|---|
| *kbps* | Intended bandwidth, in kilobits per second. Valid values are 1 to 10000000. |

**Defaults**

1000000 kbps

**Command Modes**

Interface configuration (config-if)

**SupportedUserRoles**

network-admin

**Command History**

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

**Usage Guidelines**

The **bandwidth** command sets an informational parameter to communicate only the current bandwidth to the higher-level protocols; you cannot adjust the actual bandwidth of an interface using this command.

**Note** This is a routing parameter only. It does not affect the physical interface.

## Examples

This example shows how to configure the bandwidth 30000 kbps:

```
n1000v(config-if)# bandwidth 30000
```

## Related Commands

| Command | Description |
|---|---|
| **show interface** | Displays the interface configuration information. |

# banner motd

To configure a message of the day (MOTD) banner, use the **banner motd** command.

**banner motd** [*delimiting-character message delimiting-character*]

**no banner motd** [*delimiting-character message delimiting-character*]

## Syntax Description

| | |
|---|---|
| *delimiting-character* | The character used to signal the beginning and end of the message text, for example, in the following message, the delimiting character is #.<br>#Testing the MOTD# |
| *message* | Specifies the banner message, restricted to 40 lines with a maximum of 80 characters in each line. |

## Defaults

"User Access Verification" is the default message of the day.

## Command Modes

Configuration (config)

## Command History

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

## Usage Guidelines

The MOTD banner is displayed on the terminal before the login prompt whenever you log in.

The message is restricted to 40 lines and 80 characters per line.

To create a multiple-line MOTD banner, press Enter before typing the delimiting character to start a new line. You can enter up to 40 lines of text.

Follow these guidelines when choosing your delimiting character:

- Do not use the *delimiting-character* in the *message* string.
- Do not use **"** and **%** as delimiters.

## Examples

This example shows how to configure and then display a banner message with the text, "Testing the MOTD."

```
n1000v# config terminal
n1000v(config)# banner motd #Testing the MOTD#
n1000v(config)# show banner motd
Testing the MOTD
```

This example shows how to configure and then display a multiple-line MOTD banner:

```
n1000v(config)# banner motd #Welcome to authorized users.
> Unauthorized access prohibited.#
n1000v(config)# show banner motd
Welcome to authorized users.
Unauthorized access prohibited.
```

This example shows how to revert to the default MOTD banner:

```
n1000v# config terminal
n1000v(config)# no banner motd
n1000v(config)# show banner motd
User Access Verification
```

## Related Commands

| Command | Description |
|---|---|
| **show banner motd** | Displays the MOTD banner. |

# boot auto-copy

To enable automatic copying of boot image files to the standby supervisor module, use the **boot auto-copy** command. To disable automatic copying, use the **no** form of this command.

**boot auto-copy**

**no boot auto-copy**

## Syntax Description

This command has no arguments or keywords.

## Defaults

Enabled

## Command Modes

Global configuration (config)

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

When automatic copying of image files is enabled, the Cisco NX-OS software copies the image files referred to by the boot variable to the standby supervisor module. These image files must be present in local memory on the active supervisor module. For kickstart and system boot variables, only those image files that are configured for the standby supervisor module are copied.

## Examples

This example shows how to enable automatic copying of boot image files to the standby supervisor module:

```
n1000v# configure terminal
n1000v(config)# boot auto-copy
Auto-copy administratively enabled
```

## Related Commands

| Command | Description |
|---|---|
| **boot kickstart** | Configures the kickstart boot variable. |
| **boot system** | Configures the system boot variable. |
| **copy** | Copies files. |
| **show boot** | Displays boot variable configuration information. |

# boot kickstart

To configure the boot variable for the kickstart image, use the **boot kickstart** command. To clear the kickstart image boot variable, use the **no** form of this command.

**boot kickstart** [*filesystem*:[*//directory*] | *directory*]*filename* [**sup-1**] [**sup-2**]

**no boot kickstart**

## Syntax Description

| | |
|---|---|
| *filesystem*: | (Optional) Name of a file system. Valid values are **bootflash** or **slot0**. |
| *//directory* | (Optional) Name of a directory. The directory name is case sensitive. |
| *filename* | Name of the kickstart image file. The filename is case sensitive. |
| **sup-1** | (Optional) Configures the kickstart boot for the active supervisor module only. |
| **sup-2** | (Optional) Configures the kickstart boot for the standby supervisor module only. |

## Defaults

Configures the kickstart boot variable for both supervisor modules.

## Command Modes

Global configuration (config)

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

The kickstart boot variable is used for loading software images when booting up. You must copy the kickstart image to the device before you reload.

## Examples

This example shows how to configure the kickstart boot variable for both supervisor modules:

```
n1000v# configure terminal
n1000v(config)# boot kickstart bootflash:kickstart-image
```

This example shows how to configure the kickstart boot variable for the active supervisor module:

```
n1000v# configure terminal
n1000v(config)# boot kickstart bootflash:kickstart-image sup-1
```

This example shows how to clear the kickstart boot variable:

```
n1000v# configure terminal
n1000v(config)# no boot kickstart
```

## Related Commands

| Command | Description |
|---|---|
| **boot system** | Configures the boot variable for the system software image. |
| **copy** | Copies files. |
| **show boot** | Displays boot variable configuration information. |

# boot system

To configure the boot variable for the system image, use the **boot system** command. To clear the system image boot variable, use the **no** form of this command.

**boot system** [*filesystem*:[*//directory*] | *directory*]*filename* [**sup-1**] [**sup-2**]

**no boot system**

## Syntax Description

| | |
|---|---|
| *filesystem*: | (Optional) Name of a file system. Valid values are **bootflash** or **slot0**. |
| *//directory* | (Optional) Name of a directory. The directory name is case sensitive. |
| *filename* | Name of the system image file. The filename is case sensitive. |
| **sup-1** | (Optional) Configures the system boot for the sup-1 supervisor module only. |
| **sup-2** | (Optional) Configures the system boot for the sup-2 supervisor module only. |

## Defaults

Configures the system boot variable for both supervisor modules.

## Command Modes

Global configuration (config)

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

The system boot variable is used for loading images when booting up. You must copy the system image to the device before you reload.

## Examples

This example shows how to configure the system boot variable for both supervisor modules:

```
n1000v# configure terminal
n1000v(config)# boot system bootflash:system-image
```

This example shows how to configure the system boot variable for the sup-1 supervisor module:

```
n1000v# configure terminal
n1000v(config)# boot system bootflash:system-image sup-1
```

This example shows how to clear the system boot variable:

```
n1000v# configure terminal
n1000v(config)# no boot system
```

**Related Commands**

| Command | Description |
|---|---|
| **boot kickstart** | Configures the boot variable for the kickstart software image. |
| **show boot** | Displays boot variable configuration information. |

# C Commands

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

## cache size

To specify a cache size for a Netflow flow monitor, use the **cache size** command. To remove the cache size for a flow monitor, use the **no** form of this command.

**cache size** *value*

**no cache size** *value*

**Syntax Description**

| | |
|---|---|
| *value* | Size in number of entries. The range is 256 to 16384 entries. |

**Defaults**

4096 entries

**Command Modes**

Netflow monitor configuration (**config-flow-monitor**)

**SupportedUserRoles**

network-admin

**Command History**

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

**Usage Guidelines**

Use the **cache-size** command to limit the impact of the Netflow flow monitor cache on memory and performance.

**Examples**

This example shows how to configure the cache size for a Netflow flow monitor named MonitorTest, and then display the configuration:

```
n1000v# config t
n1000v(config)# flow monitor MonitorTest
n1000v(config-flow-monitor)# cache size 15000
n1000v(config-flow-monitor)# show flow monitor MonitorTestFlow
Monitor monitortest:
     Use count: 0
     Inactive timeout: 600
     Active timeout: 1800
     Cache Size: 15000
n1000v(config-flow-monitor)#
```

This example shows how to remove a cache size from a flow monitor:

```
n1000v# config t
n1000v(config)# flow monitor MonitorTest
n1000v(config-flow-monitor)# no cache size
n1000v(config-flow-monitor)#show flow monitor MonitorTestFlow
n1000v(config-flow-monitor)#
Monitor monitortest:
     Use count: 0
     Inactive timeout: 600
     Active timeout: 1800
     Cache Size: 4096
n1000v(config-flow-monitor)#
```

## Related Commands

| Command | Description |
|---|---|
| **show flow monitor** | Displays information about the flow monitor cache module. |
| **flow monitor** | Creates a flow monitor. |
| **timeout** | Specifies an aging timer and its value for aging entries from the cache. |
| **record** | Adds a flow record to the flow monitor. |
| **exporter** | Adds a flow exporter to the flow monitor. |

# capability l3control

To configure the Layer 3 capability for a port profile, use the **capability** command. To remove a capability from a port profile, use the **no** form of this command.

**capability l3control**

**no capability l3control**

## Syntax Description

| | |
|---|---|
| **l3control** | Configures a port profile to be used for one of the following Layer 3 communication purposes:<br>• The management interface used for Layer 3 communication between the VSM and VEMs.<br>• To carry NetFlow ERSPAN traffic. |

## Defaults

None

## Command Modes

Port profile configuration (config-port-prof)

## SupportedUserRoles

network-admin

## Command History

| Release | Modification |
|---|---|
| 4.0(4)SV1(1) | Introduced the **capability uplink** command to designate a port profile as an uplink. |
| 4.0(4)SV1(2) | Removed the **capability uplink** command. A port profile used as an uplink is now designated as type Ethernet instead.<br>Added the **capability l3control** command. |

## Usage Guidelines

If you are configuring a port profile for Layer 3 control, then you must first configure the transport mode as Layer 3 using the **svs mode** command for the VSM domain.

## Examples

This example shows how to configure a port profile to be used for Layer 3 communication purposes:

```
n1000v# config t
n1000v(config)# port-profile testprofile
n1000v(config-port-prof)# capability l3control
n1000v(config-port-prof)#
```

This example shows how to remove the Layer 3 configuration from the port profile:

```
n1000v# config t
```

```
n1000v(config)# port-profile testprofile
n1000v(config-port-prof)# no capability l3control
n1000v(config-port-prof)#
```

## Related Commands

| Command | Description |
|---|---|
| **show port-profile name** [*name*] | Displays the port profile configuration. |
| **port-profile** *name* | Places you into port profile configuration mode for creating and configuring a port profile. |

# capability iscsi-multipath

To configure a port profile to be used with the ISCSI Multipath protocol, use the **capability iscsi-multipath** command. To remove the capability from a port profile, use the **no** form of this command.

**capability iscsi-multipath**

**no capability iscsi-multipath**

## Syntax Description

This command has no arguments or keywords.

## Defaults

None

## Command Modes

Port profile configuration (config-port-prof)

## SupportedUserRoles

network-admin

## Command History

| Release | Modification |
|---|---|
| 4.0(4)SV1(2) | Added the **capability iscsi multipath** command. |

## Usage Guidelines

If you are configuring a port profile for ISCSI Multipath, then you must first configure the port profile in switchport mode.

## Examples

This example shows how to configure a port profile to be used with ISCSI Multipath protocol:

```
n1000v# config t
n1000v(config)# port-profile testprofile
n1000v(config-port-prof)# switchport mode access
n1000v(config-port-prof)# capability iscsi-multipath
n1000v(config-port-prof)#
```

This example shows how to remove the ISCSI multipath configuration from the port profile:

```
n1000v# config t
n1000v(config)# port-profile testprofile
n1000v(config-port-prof)# no capability iscsi-multipath
n1000v(config-port-prof)#
```

## Related Commands

| Command | Description |
|---|---|
| **show port-profile name** [*name*] | Displays the port profile configuration. |
| **port-profile** *name* | Places you into port profile configuration mode for creating and configuring a port profile. |

# cd

To change to a different directory from the one you are currently working in, use the **cd** command.

**cd** [*filesystem*:[*//directory*] | *directory*]

## Syntax Description

| | |
|---|---|
| *filesystem*: | (Optional) Name of the file system. Valid file systems are **bootflash** and **volatile**. |
| *//directory* | (Optional) Name of the directory. The directory name is case sensitive. |

## Defaults

**bootflash**

## Command Modes

Any

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

You can only change to the directories that are on the active supervisor module.

Use the present working directory (**pwd)** command to verify the name of the directory you are currently working in.

## Examples

This example shows how to change to a different directory on the current file system:

```
n1000v# cd my-scripts
```

This example shows how to change from the file system you are currently working in to a different file system:

```
n1000v# cd volatile:
```

This example shows how to revert back to the default directory, bootflash:

```
n1000v# cd
```

## Related Commands

| Command | Description |
|---|---|
| **pwd** | Displays the name of the directory you are currently working in. |

# cdp advertise

To specify the CDP version to advertise, use the **cdp advertise** command. To remove the cdp advertise configuration, use the **no** form of this command.

**cdp advertise** {**v1** | **v2**}

**no cdp advertise** [**v1** | **v2**]

## Syntax Description

| | |
|---|---|
| **v1** | CDP Version 1. |
| **v2** | CDP Version 2. |

## Defaults

CDP Version 2

## 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 set CDP Version 1 as the version to advertise:

```
n1000v(config)# cdp advertise v1
```

This example shows how to remove CDP Version 1 as the configuration to advertise:

```
n1000v(config)# no cdp advertise v1
```

## Related Commands

| Command | Description |
|---|---|
| **show cdp global** | Displays the CDP configuration. |

# cdp enable (global)

To enable Cisco Discovery Protocol (CDP) globally on all interfaces and port channels, use the **cdp enable** command. To disable CDP globally, use the **no** form of this command.

**cdp enable**

**no cdp enable**

## Syntax Description

This command has no arguments or keywords.

## Defaults

Enabled on all interfaces and port channels

## Command Modes

Global configuration (config)

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

CDP can only be configured on physical interfaces and port channels.

## Examples

This example shows how to enable CDP globally and then show the CDP configuration:

```
n1000v# config t
n1000v(config)# cdp enable
n1000v(config)# show cdp global
Global CDP information:
    CDP enabled globally
    Refresh time is 60 seconds
    Hold time is 180 seconds
    CDPv2 advertisements is enabled
    DeviceID TLV in System-Name(Default) Format
```

This example shows how to disable CDP globally and then show the CDP configuration:

```
n1000v(config)# no cdp enable
n1000v# show cdp global
Global CDP information:
    CDP disabled globally
    Refresh time is 60 seconds
    Hold time is 180 seconds
    CDPv2 advertisements is enabled
    DeviceID TLV in System-Name(Default) Format
n1000v(config)#
```

## Related Commands

| Command | Description |
|---|---|
| **show cdp global** | Displays the CDP configuration. |
| **cdp enable** (interface or port channel) | Enables CDP on an interface or port channel. |

# cdp enable (interface or port channel)

To enable Cisco Discovery Protocol (CDP) on an interface or port channel, use the **cdp enable** command. To disable it, use the **no** form of this command.

**cdp enable**

**no cdp enable**

## Syntax Description

This command has no arguments or keywords.

## Defaults

None

## Command Modes

Interface configuration (config-if)

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

CDP can only be configured on physical interfaces and port channels.

## Examples

This example shows how to enable CDP on port channel 2:

```
n1000v# config t
n1000v(config)# interface port-channel2
n1000v(config-if)# cdp enable
n1000v(config-if)#
```

This example shows how to disable CDP on mgmt0:

```
n1000v# config t
n1000v(config)# interface mgmt0
n1000v(config-if)# no cdp enable
n1000v(config-if)# show cdp interface mgmt0
        mgmt0 is up
        CDP disabled on interface
        Sending CDP packets every 60 seconds
        Holdtime is 180 seconds
n1000v(config-if)#
```

## Related Commands

| Command | Description |
|---|---|
| **show cdp interface** | Displays the CDP configuration for an interface. |
| **show cdp neighbors** | Displays your device from the upstream device. |
| **cdp advertise** | Assigns the CPD version the interface will advertise—CDP Version 1 or CDP Version 2. |
| **cdp format device ID** | Assigns the CDP device ID |
| **cdp holdtime** | Sets the maximum amount of time that CDP holds onto neighbor information before discarding it. |

# cdp format device-id

To specify the device ID format for CDP, use the **cdp format device-id** command. To remove it, use the **no** form of this command.

**cdp format device-id** {**mac-address** | **serial-number** | **system-name**}

**no cdp format device-id** {**mac-address** | **serial-number** | **system-name**}

## Syntax Description

| | |
|---|---|
| **mac-address** | MAC address of the Chassis. |
| **serial-number** | Chassis serial number. |
| **system-name** | System name/Fully Qualified Domain Name (Default). |

## Defaults

System name/Fully Qualified Domain Name

## Command Modes

Global configuration (config)

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

CDP must be enabled globally before you configure the device ID format.

You can configure CDP on physical interfaces and port channels only.

## Examples

This example shows how to configure the CDP device ID with the MAC address format and then display the configuration:

```
n1000v(config)# cdp format device-id mac-address
n1000v(config)# show cdp global
Global CDP information:
CDP enabled globally
     Sending CDP packets every 5 seconds
     Sending a holdtime value of 10 seconds
     Sending CDPv2 advertisements is disabled
     Sending DeviceID TLV in Mac Address Format
```

This example shows how to remove the CDP device ID MAC address format from the configuration:

```
n1000v(config)# no cdp format device-id mac-address
```

## Related Commands

| Command | Description |
|---|---|
| **show cdp global** | Displays CDP global configuration parameters. |
| **show cdp interface** | Displays the CDP configuration for an interface. |
| **show cdp neighbors** | Displays your device from the upstream device. |
| **cdp advertise** | Assigns the CPD version the interface will advertise—CDP Version 1 or CDP Version 2. |
| **cdp enable interface** | Enables CDP on an interface or port channel. |
| **cdp holdtime** | Sets the maximum amount of time that CDP holds onto neighbor information before discarding it. |

# cdp holdtime

To do set the maximum amount of time that CDP holds onto neighbor information before discarding it, use the **cdp holdtime** command. To remove the CDP holdtime configuration, use the **no** form of this command.

**cdp holdtime** *seconds*

**no cdp holdtime** *seconds*

## Syntax Description

| | |
|---|---|
| *seconds* | The range is from 10 to 255 seconds. |

## Defaults

180 seconds

## Command Modes

Global configuration (config)

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

CDP must be enabled globally before you configure the device ID format.

You can configure CDP on physical interfaces and port channels only.

## Examples

This example shows how to set the CDP holdtime to 10 second:

```
n1000v(config)# cdp holdtime 10
```

This example shows how to remove the CDP holdtime configuration:

```
n1000v(config)# no cdp holdtime 10
```

## Related Commands

| Command | Description |
|---|---|
| **show cdp global** | Displays CDP global configuration parameters. |
| **show cdp neighbors** | Displays the upstream device from your device. |

# cdp timer

To set the refresh time for CDP to send advertisements to neighbors, use the **cdp timer** command. To remove the CDP timer configuration, use the **no** form of this command.

**cdp timer** *seconds*

**no cdp timer** *seconds*

## Syntax Description

| | |
|---|---|
| *seconds* | The range is from 5 to 254 seconds. |

## Defaults

60 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 CDP timer to 10 seconds:

```
n1000v(config)# cdp timer 10
```

This example shows how to remove the CDP timer configuration:

```
n1000v(config)# no cdp timer 10
```

## Related Commands

| Command | Description |
|---|---|
| **show cdp global** | Displays CDP global configuration parameters. |
| **show cdp neighbors** | Displays the upstream device from your device. |

# channel-group auto (port profile)

To create and define a channel group for all interfaces that belong to a port profile, use the **channel-group auto** command. To remove the channel group, use the **no** form of this command.

**channel-group auto** [**mode** *channel_mode*] [**sub-group** *sg-type*{**cdp** | **manual**}] [**mac-pinning**]

**no channel-group**

## Syntax Description

| | |
|---|---|
| **mode** *channel_mode* | (Optional) Specifies a channeling mode:<br>• **on**<br>• **active** (uses LACP)<br>• **passive** (uses LACP) |
| **sub-group** *sg-type* | (Optional) Specifies to create subgroups for managing the traffic flow when the port profile connects to multiple upstream switches. The feature is also called virtual port channel host mode (vPC-HM). |
| **cdp** | Specifies to create subgroups using Cisco Discovery Protocol (CDP). |
| **manual** | Specifies to create subgroups manually. |
| **mac-pinning** | (Optional) Specifies to attach VEMs to an upstream switch that does not support port-channels. There are a maximum of 32 subgroups per port channel, so a maximum of 32 Ethernet port members can be assigned. |

## Defaults

None

## Command Modes

Port profile configuration (config-port-prof)

## SupportedUserRoles

network-admin

## Command History

| Release | Modification |
|---|---|
| 4.0(4)SV1(1) | This command was introduced. |
| 4.0(4)SV1(2) | Support for manual creation of subgroups and **mac-pinning**. |

## Usage Guidelines

The **channel-group auto** command creates a unique port channel for all interfaces that belong to the same module. The channel group is automatically assigned when the port profile is assigned to the first interface. Each additional interface that belongs to the same module is added to the same port channel. In VMware environments, a different port channel is created for each module.

- The channel group mode must be set to **on** when configuring vPC-HM.
- When configuring a port channel for a port profile that connects to two or more upstream switches, note the following:

- You need to know whether CDP is configured in the upstream switches.

  If configured, CDP creates a subgroup for each upstream switch to manage its traffic separately.

  If not configured, then you must manually configure subgroups to manage the traffic flow on the separate switches.
- When configuring a port channel for vPC-HM and the upstream switches do not support port channels, you can use MAC pinning, which will automatically assign each Ethernet member port to a unique sub-group.
- If vPC-HM is not configured when port channels connect to two different upstream switches, the VMs behind the Cisco Nexus 1000V receive duplicate packets from the network for broadcasts and multicasts.
- You can also configure vPC-HM on the interface. For more information, see the *Cisco Nexus 1000V Interface Configuration Guide, Release 4.0(4)SV1(3)*.

## Examples

This example shows how to configure a port profile for a port channel that connects to a single upstream switch and then display the configuration:

```
n1000v# config t
n1000v(config)# port-profile AccessProf
n1000v(config-port-prof)# channel-group auto mode on
n1000v(config-port-prof)# show port-profile name AccessProf
port-profile AccessProf
  description: allaccess4
  status: disabled
  capability uplink: yes
  port-group: AccessProf
  config attributes:
    switchport mode access
    channel-group auto mode on
  evaluated config attributes:
    switchport mode access
    channel-group auto mode on
  assigned interfaces:
n1000v(config-port-prof)#
```

This example shows how to remove the channel group configuration from the port profile and then display the configuration:

```
n1000v# config t
n1000v(config)# port-profile AccessProf
n1000v(config-port-prof)# no channel-group
n1000v(config-port-prof)# show port-profile name AccessProf
port-profile AccessProf
  description: allaccess4
  status: disabled
  capability uplink: yes
  port-group: AccessProf
  config attributes:
    switchport mode access
evaluated config attributes:
    switchport mode access
assigned interfaces:
n1000v(config-port-prof)#
```

This example shows how to configure a port profile for a port channel that connects to multiple upstream switches that have CDP enabled and then display the configuration:

```
n1000v# config t
n1000v(config)# port-profile uplinkProf
n1000v(config-port-prof)# channel-group auto mode on sub-group cdp
n1000v(config-port-prof)# show port-profile name uplinkProf
port-profile uplinkProf
  description:
  type: vethernet
  status: disabled
  capability l3control: no
  pinning control-vlan: -
  pinning packet-vlan: -
  system vlans: none
  port-group:
  max ports: 32
  inherit:
  config attributes:
    channel-group auto mode on sub-group cdp
  evaluated config attributes:
    channel-group auto mode on sub-group cdp
  assigned interfaces:
```

## Related Commands

| Command | Description |
|---|---|
| **show port-profile name** *profile-name* | Displays the port profile configuration. |
| **port-profile** *profile-name* | Creates a port profile and places you into global configuration mode for the named port profile. |

# channel-group (interface)

To create a port channel group or to move an interface from one port channel group to another, use the **channel-group** command. To remove the channel group configuration from an interface, use the **no** form of this command.

**channel-group** *number* [**force**] [**mode** {**active** | **on** | **passive**}]

**no channel-group** [*number*]

## Syntax Description

| | |
|---|---|
| *number* | Number of the channel group. The maximum number of port channels that can be configured is 256. The allowable range of channel group numbers that can be assigned is from 1 to 4096. |
| **force** | Forces the interface to join the channel group, although some parameters are not compatible. See Usage Guidelines below for information about the compatibility parameters and which ones can be forced. |
| **mode** | Specifies the port channel mode of the interface. |
| **on** | This is the default channel mode.<br>All port channels that are not running LACP remain in this mode. If you attempt to change the channel mode to active or passive before enabling LACP, the device returns an error message.<br>After you enable LACP globally, you enable LACP on each channel by configuring the channel mode as either active or passive. An interface in this mode does not initiate or respond to LACP packets. When an LACP attempts to negotiate with an interface in the on state, it does not receive any LACP packets and becomes an individual link with that interface; it does not join the channel group. |
| **active** | Specifies that when you enable the Link Aggregation Control Protocol (LACP), this command enables LACP on the specified interface. Interface is in active negotiating state, in which the port initiates negotiations with other ports by sending LACP packets. |
| **passive** | Specifies that when you enable LACP, this command enables LACP only if an LACP device is detected.The interface is in a passive negotiation state, in which the port responds to LACP packets that it receives but does not initiate LACP negotiation. |

## Defaults

The default mode is **on**.

## Command Modes

Interface configuration (config-if)

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

A port channel in the **on** channel mode is a pure port channel and can aggregate a maximum of eight ports. It does not run LACP.

If an existing port channel is not running LACP you cannot change the mode for it or any of its interfaces. If you try to do so, the channel mode remains **on** and an error message is generated.

When you delete the last physical interface from a port channel, the port channel remains. To delete the port channel completely, use the **no** form of the **port-channel** command.

When an interface joins a port channel, the following attributes are removed and replaced with the those of the port channel:

- Bandwidth
- Delay
- Extended Authentication Protocol over UDP
- VRF
- IP address
- MAC address
- Spanning Tree Protocol
- NAC
- Service policy
- Quality of Service (QoS)
- ACLs

The following attributes remain unaffected when an interface joins or leaves a port channel:

- Beacon
- Description
- CDP
- LACP port priority
- Debounce
- UDLD
- MDIX
- Rate mode
- Shutdown
- SNMP trap

You do not have to create a port channel interface before you assign a physical interface to a channel group. A port channel interface is created automatically when the channel group gets its first physical interface, if it is not already created.

## Examples

This example shows how to add an interface to LACP channel group 5 in active mode:

```
n1000v(config-if)# channel-group 5 mode active
n1000v(config-if)#
```

## Related Commands

| Command | Description |
|---|---|
| **show interface port-channel** | Displays information about the traffic on the specified port channel interface. |
| **show port-channel summary** | Displays information on the port channels. |
| **feature lacp** | Enables the LACP feature globally |
| **show lacp port-channel** | Displays LACP information. |
| **show port-channel compatibility-parameters** | Displays the list of compatibility checks that the Cisco Nexus 1000V uses. |

# check logflash

To check the compactFlash, use the **check logflash** command.

**check logflash** [**bad-blocks**]

## Syntax Description

| | |
|---|---|
| **bad-blocks** | (Optional) Finds bad blocks in compactFlash. |

## Defaults

None

## 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 check compactFlash:

```
n1000v# check logflash
```

# class (policy map type qos)

To add an existing Quality of Service (QoS) class to a policy map, use the **class** command. To remove a QoS class from a policy map, use the **no** form of this command.

**class** [**type qos**] {*class-map-name* | **class-default**} [**insert-before** [**type qos**] *before-class-map-name*]

**no class** {*class-map-name* | **class-default**}

## Syntax Description

| | |
|---|---|
| **type qos** | (Optional) Specifies the class type to be QoS. QoS is the default class type. |
| *class-map-name* | Adds the specified name of an existing class to the policy map. |
| **class-default** | Adds the class-default to a policy map. The class-default matches all traffic not classified in other classes. |
| **insert-before** *before-class-map-name* | (Optional) Specifies the sequence of this class in the policy by identifying the class map it should precede. If not specified, the class is placed at the end of the list of classes in the policy. Policy actions in the first class that matches the traffic type are performed. |

## Defaults

type QoS

The default is to reference a new class map at the end of the policy map.

The class named class-default matches all traffic not classified in other classes.

## Command Modes

Policy map configuration (config-pmap)

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

Policy actions in the first class that matches the traffic type are performed.

The class named class-default matches all traffic not classified in other classes.

## Examples

This example shows how to add a class map in sequence to the end of a policy map:

```
n1000v(config)# policy-map my_policy1
n1000v(config-pmap)# class traffic_class2
n1000v(config-pmap-c-qos)#
```

This example shows how to insert a class map in sequence before an existing class map in a policy map:

```
n1000v(config)# policy-map my_policy1
n1000v(config-pmap-qos)# class insert-before traffic_class2 traffic_class1
n1000v(config-pmap-c-qos)#
```

This example shows how to add the class-default class map to a policy map:

```
n1000v(config)# policy-map my_policy1
n1000v(config-pmap-qos)# class class-default
n1000v(config-pmap-c-qos)#
```

This example shows how to remove a class map reference from a policy map:

```
n1000v(config)# policy-map my_policy1
n1000v(config-pmap)# no class traffic_class1
n1000v(config-pmap)#
```

## Related Commands

| Command | Description |
|---|---|
| **policy-map** | Creates or modifies a policy map. |
| **set cos** | Assigns a CoS to a QoS policy map. |
| **set dscp** | Assigns a DSCP value for a traffic class in a QoS policy map. |
| **set precedence** | Assigns a precedence value for the IP headers in a specific traffic class in a QoS policy map. |
| **set discard-class** | Assigns a discard-class value for a class of traffic in a QoS policy map. |
| **show class-map qos** | Displays class maps. |
| **show policy-map** | Displays policy maps and statistics. |

# class-map

To create or modify a QoS class map that defines a class of traffic, use the **class-map** command. To remove a class map, use the **no** form of this command.

**class-map** [**type qos**] [**match-any** | **match-all**] *class-map-name*

**no class-map** [**type qos**] [**match-any** | **match-all**] *class-map-name*

## Syntax Description

| | |
|---|---|
| **type qos** | (Optional) Specifies the component type QoS for the class map. By default, the class map type is QoS. |
| **match-any** | (Optional) Specifies that if the packet matches any of the matching criteria configured for this class map, then this class map is applied to the packet. |
| **match-all** | (Optional) Specifies that if the packet matches all the matching criteria configured for this class map, then this class map is applied to the packet. This is the default action if **match-any** is not specified. |
| *class-map-name* | Name assigned to the class map. The name class-default is reserved. |

## Defaults

type QoS
match-all

## Command Modes

Global configuration (config)

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

Hyphen, underscore, and alphabetic characters are allowed in the class map name.

Forty characters are the maximum allowed in the class map name.

Characters in the class map name are case sensitive.

## Examples

This example shows how to create a class map and enter the QoS class map configuration mode to configure the specified map:

```
n1000v# configure terminal
n1000v(config)# class-map my_class1
n1000v(config-cmap-qos)#
```

This example shows how to remove the QoS class map named *my_class1*:

```
n1000v(config)# no class-map my_class1
n1000v(config)#
```

## Related Commands

| Command | Description |
|---|---|
| **show class-map qos** | Displays class maps. |
| **match class-map** | Configures the traffic class by matching packets based on match criteria in another class map. |
| **match packet length** | Configures the traffic class by matching packets based on packet lengths. |

# clear access-list counters

To clear the counters for IP and MAC access control list(s) (ACLs), use the **clear access-list counters** command.

**clear access-list counters** [*access-list-name*]

## Syntax Description

| | |
|---|---|
| *access-list-name* | (Optional) Name of the ACL whose counters the device clears. The name can be up to 64 alphanumeric, case-sensitive characters. |

## Defaults

None

## Command Modes

Any

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

If you specify an ACL, the name can be up to 64 alphanumeric, case-sensitive characters.

## Examples

This example shows how to clear counters for all IP and MAC ACLs:

```
n1000v# clear access-list counters
n1000v#
```

This example shows how to clear counters for an IP ACL named acl-ip-01:

```
n1000v# clear access-list counters acl-ip-01
n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **clear ip access-list counters** | Clears counters for IP ACLs. |
| **clear mac access-list counters** | Clears counters for MAC ACLs. |
| **show access-lists** | Displays information about one or all IP and MAC ACLs. |

# clear cdp

To clear Cisco Discovery Protocol(CDP) information on an interface, use the **clear cdp** command.

**clear cdp** {**counters** [**interface** *slot/port*] | **table** [**interface** *slot/port*]}

## Syntax Description

| | |
|---|---|
| **counters** | Clear CDP counters on all interfaces. |
| **interface** *slot/port* | (Optional) Clear CDP counters on a specified interface . |
| **table** | Clear CDP cache on all interfaces. |

## 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 clear CDP counters on all interfaces:

```
n1000V# clear cdp counters
```

This example shows how to clear CDP cache on all interfaces:

```
n1000V# clear cdp table
```

## Related Commands

| Command | Description |
|---|---|
| **show cdp all** | Displays all interfaces that have CDP enabled. |
| **show cdp entry** | Displays the CDP database entries |
| **show cdp global** | Displays the CDP global parameters. |
| **show cdp interface** *intrface-type slot-port* | Displays the CDP interface status |

# clear cli history

To clear the history of commands you have entered into the CLI, use the **clear cli history** command.

**clear cli history**

## 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

Use the **show cli history** command to display the history of the commands that you entered at the command-line interface (CLI).

## Examples

This example shows how to clear the command history:

```
n1000v# clear cli history
```

## Related Commands

| Command | Description |
|---|---|
| **show cli history** | Displays the command history. |

# clear cores

To clear the core files, use the **clear cores** command.

**clear cores** [**archive**]

| Syntax Description | | |
|---|---|---|
| | **archive** | (Optional) Clears the core file on the logflash filesystem. |

**Defaults** None

**Command Modes** Any

**SupportedUserRoles** network-admin

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

**Usage Guidelines** Use the **show system cores** command to display information about the core files.

**Examples** This example shows how to clear the core file:

```
n1000v# clear cores
```

This example shows how to clear the core on the logflash filesystem:

```
n1000v# clear cores archive
```

| Related Commands | Command | Description |
|---|---|---|
| | **show system cores** | Displays the core filename. |
| | **system cores** | Configures the core filename. |

# clear counters

To clear interface counters, use the **clear counters** command.

**clear counters [ interface {all | ethernet** *slot/port* **| loopback** *virtual-interface-number* **| mgmt | port-channel** *port-channel-number* **| vethernet** *interface-number*} **]**

## Syntax Description

| | |
|---|---|
| **interface** | Clears interface counters. |
| **all** | Clears all interface counters. |
| **ethernet** *slot/port* | Clears Ethernet interface counters. The range is 1 to 66. |
| **loopback** *virtual-interface-number* | Clears loopback interface counters. The range is 0 to 1023. |
| **mgmt** | Clears the mangement interface (mgmt0). |
| **port-channel** *port-channel-number* | Clears port-channel interfaces. The range is 1 to 4096. |
| **vethernet** *interface-number* | Clears virtual Ethernel interfaces. The range is 1 to 1048575. |

## 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 clear the Ethernet interface counters:

```
n1000v(config)# clear counters ethernet 2/1
```

## Related Commands

| Command | Description |
|---|---|
| **show interface counters** | Displays the interface status, which includes the counters. |

# clear debug-logfile

To clear the contents of the debug logfile, use the **clear debug-logfile** command.

**clear debug-logfile** *filename*

## Syntax Description

| | |
|---|---|
| *filename* | Name of the debug logfile to clear. |

## Defaults

None

## 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 clear the debug logfile:

```
n1000v# clear debug-logfile syslogd_debugs
```

## Related Commands

| Command | Description |
|---|---|
| **debug logfile** | Configures a debug logging file. |
| **debug logging** | Enable debug logging. |
| **show debug logfile** | Displays the contents of the debug logfile. |

# clear flow exporter

To clear the statistics for a Flexible NetFlow flow exporter, use the **clear flow exporter** command in Any.

**clear flow exporter** {**name** *exporter-name* | *exporter-name*}

## Syntax Description

| | |
|---|---|
| **name** | Indicates that a flow exporter will be specified by name. |
| *exporter-name* | Name of an existing flow exporter. |

## Command Default

None

## Command Modes

Any

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

You must have already enabled traffic monitoring with Flexible NetFlow using an exporter before you can use the **clear flow exporter** command.

## Examples

The following example clears the statistics for the flow exporter named NFC-DC-PHOENIX:

```
n1000v# clear flow exporter name NFC-DC-PHOENIX
n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **clear flow exporter** | Clears the statistics for exporters. |
| **flow exporter** | Creates a flow exporter. |
| **show flow exporter** | Displays flow exporter status and statistics. |

# clear ip access-list counters

To clear the counters for IP access control lists (ACLs), use the **clear ip access-list counters** command.

**clear ip access-list counters** [*access-list-name*]

## Syntax Description

| | |
|---|---|
| *access-list-name* | (Optional) Name of the IP ACL whose counters you want cleared. The name can be up to 64 alphanumeric, case-sensitive characters. |

## Defaults

None

## Command Modes

Any

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

If specifying an ACL by name, it can be up to 64 alphanumeric, case-sensitive characters.

## Examples

This example shows how to clear counters for all IP ACLs:

```
n1000v# clear ip access-list counters
n1000v#
```

This example shows how to clear counters for an IP ACL named acl-ip-101:

```
n1000v# clear ip access-list counters acl-ip-101
n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **clear access-list counters** | Clears counters for IP and MAC ACLs. |
| **clear mac access-list counters** | Clears counters for MAC ACLs. |
| **show access-lists** | Displays information about one or all IP and MAC ACLs. |
| **show ip access-lists** | Displays information about one or all IP ACLs. |

# clear ip arp inspection statistics vlan

To clear the Dynamic ARP Inspection (DAI) statistics for a specified VLAN, use the **clear ip arp inspection statistics vlan** command.

**clear ip arp inspection statistics vlan** *vlan-list*

## Syntax Description

| | |
|---|---|
| *vlan-list* | Range of VLAN IDs from 1 to 4094 that you can clear DAI statistics from. |

## Defaults

None

## Command Modes

Any

## SupportedUserRoles

network-admin

## Command History

| Release | Modification |
|---|---|
| 4.0(4)SV1(2) | This command was introduced. |

## Examples

This example shows how to clear the DAI statistics for VLAN 2:

```
n1000v# clear ip arp inspection statistics vlan 2
n1000v#
```

This example shows how to clear the DAI statistics for VLANs 5 through 12:

```
n1000v# clear ip arp inspection statistics vlan 5-12
n1000v#
```

This example shows how to clear the DAI statistics for VLAN 2 and VLANs 5 through 12:

```
n1000v# clear ip arp inspection statistics vlan 2,5-12
n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **ip arp inspection vlan** | Enables or disables DAI for a list of VLANs. |
| **show ip arp inspection statistics** | Displays the DAI statistics. |

# clear ip dhcp snooping binding

To clear dynamically added entries from the DHCP snooping binding database, use the **clear ip dhcp snooping binding** command.

**clear ip dhcp snooping binding** [**vlan** *vlan-id* **mac** *mac-addr* **ip** *ip-addr* **interface** *interface-id*]

## Syntax Description

| | |
|---|---|
| **vlan** | (Optional) Specifies the VLAN to clear. |
| *vlan-id* | ID of the specified VLAN. |
| **mac** | (Optional) Specifies the MAC address associated with this VLAN. |
| *mac-addr* | MAC address associated with this VLAN. |
| **ip** | (Optional) Specifies the IP address associated with this VLAN. |
| *ip-addr* | IP address associated with this VLAN. |
| **interface** | (Optional) Specifies the interface associated with this VLAN. |
| *interface-id* | ID of the interface. |

## 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 clear dynamically added entries from the DHCP snooping binding database:

```
n1000v# clear ip dhcp snooping binding
n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **show ip dhcp snooping binding** | Displays the DHCP snooping binding database. |
| **ip dhcp snooping** | Enables DHCP snooping globally. |
| **ip dhcp snooping vlan** | Enables DHCP snooping on the VLANs specified by *vlan-list*. |
| **ip dhcp snooping verify mac-address** | Enables DHCP snooping MAC address verification. |

# clear ip igmp interface statistics

To clear the IGMP statistics for an interface, use the **clear ip igmp interface statistics** command.

**clear ip igmp interface statistics** [*if-type if-number*]

## Syntax Description

| | |
|---|---|
| *if-type* | (Optional) Interface type. For more information, use the question mark (?) online help function. |
| *if-number* | (Optional) Interface number. |

## 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 clear IGMP statistics for an interface:

```
n1000v# clear ip igmp interface statistics ethernet 2/1
n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **show ip igmp interface** | Displays information about IGMP interfaces. |

# clear ip igmp snooping statistics vlan

To clear the IGMP snooping statistics for VLANs, use the **clear ip igmp snooping statistics vlan** command.

**clear ip igmp snooping statistics vlan** {*vlan-id* | **all**}

## Syntax Description

| | |
|---|---|
| *vlan-id* | VLAN number. The range is from 1 to 3967 and 4048 to 4093. |
| **all** | Applies to all VLANs. |

## 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 clear IGMP snooping statistics for VLAN 1:

```
n1000v# clear ip igmp snooping statistics vlan 1
n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **show ip igmp snooping statistics vlan** | Displays IGMP snooping statistics by VLAN. |

# clear lacp counters

To clear the statistics for all interfaces for Link Aggregation Control Protocol (LACP) groups, use the **clear lacp counters** command.

**clear lacp counters** [**interface port-channel** *channel-number*]

## Syntax Description

| | |
|---|---|
| *channel-number* | (Optional) LACP port-channel number. The range of values is from 1 to 4096. |

## Defaults

None

## Command Modes

Any

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

If you clear counters for a specific port channel, the allowable port channel numbers are from 1 to 4096.

If you do not specify a channel number, the LACP counters for all LACP port groups are cleared.

If you clear counters for a static port-channel group, without the aggregation protocol enabled, the device ignores the command.

## Examples

This example shows how to clear all the LACP counters:

```
n1000v(config)# clear lacp counters
n1000v(config) #
```

This example shows how to clear all LACP counters for the LACP port-channel group 20:

```
n1000v(config)# clear lacp counters interface port-channel 20
n1000v(config)#
```

## Related Commands

| Command | Description |
|---|---|
| **show lacp counters** | Displays information about LACP statistics. |

# clear license

To uninstall a license file from a VSM, or to uninstall an evaluation license before installing a permanent license, use the **clear license** command.

**clear license** *filename*

## Syntax Description

| | |
|---|---|
| *filename* | Name of the license file to be uninstalled. |

## Defaults

None

## Command Modes

Any

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

If a license is in use, you cannot uninstall it. Before uninstalling the license file, all licenses must first be transferred from the VEMs to the VSM license pool.

**Caution** **Service Disruption**
When you uninstall a license file from a VSM, the vEthernet interfaces on the VEMs are removed from service and the traffic flowing to them from virtual machines is dropped. This traffic flow is not resumed until you add a new license file with licenses for the VEMs. We recommend notifying the server administrator that you are uninstalling a license and that this will cause the vEthernet interfaces to shut down.

## Examples

This example shows how to remove the Enterprise.lic license file from a VSM:

```
n1000v# clear license Enterprise.lic
Clearing license Enterprise.lic:
SERVER this_host ANY
VENDOR cisco

Do you want to continue? (y/n) y
Clearing license ..done
n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **show license** | Displays license information. |
| **install license** | Installs a license file(s) on a VSM |
| **svs license transfer src-vem** | Transfers licenses from a source VEM to another VEM, or to the VSM pool of available licenses. |

# clear line

To end a session on a specified vty, use the **clear line** command.

**clear line** *word*

## Syntax Description

| | |
|---|---|
| *word* | Specifies the vty name. |

## 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 end a session on a specified vty:

```
n1000v(config)# clear line
```

## Related Commands

| Command | Description |
|---|---|
| **show users** | Displays active user sessions. |

# clear logging logfile

Use the **clear logging logfile** command to clear messages from the logging file.

**clear logging logfile**

## Syntax Description

This command has no arguments or keywords.

## Defaults

None

## Command Modes

Any

## SupportedUserRoles

Super user

## Command History

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

## Examples

This example shows how to clear messages from the logging file:

```
n1000v# clear logging logfile
n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **show logging logfile** | Displays the logs in the local log file. |

# clear logging session

Use the **clear logging session** command to clear the current logging session.

**clear logging session**

## Syntax Description

This command has no arguments or keywords.

## Defaults

None

## Command Modes

Any

## SupportedUserRoles

Super user

## Command History

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

## Examples

This example shows how to clear the current logging session:

```
n1000v# clear logging session
n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **show logging session** | Displays logging session status |

# clear mac access-list counters

To clear the counters for MAC access control lists (ACLs), use the **clear mac access-list counters** command.

**clear mac access-list counters** [*access-list-name*]

## Syntax Description

| | |
|---|---|
| *access-list-name* | (Optional) Name of the MAC ACL whose counters you want to clear. The name can be up to 64 alphanumeric, case-sensitive characters. |

## Defaults

None

## Command Modes

Any

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

If you want counters cleared for a specific MAC ACL, the name can be up to 64 alphanumeric, case-sensitive characters.

## Examples

This example shows how to clear counters for all MAC ACLs:

```
n1000v# clear mac access-list counters
n1000v#
```

This example shows how to clear counters for a MAC ACL named acl-mac-0060:

```
n1000v# clear mac access-list counters acl-mac-0060
n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **clear access-list counters** | Clears counters for IP and MAC ACLs. |
| **clear ip access-list counters** | Clears counters for IP ACLs. |
| **show access-lists** | Displays information about one or all IP and MAC ACLs. |
| **show mac access-lists** | Displays information about one or all MAC ACLs. |

# clear mac address-table dynamic

To clear the dynamic address entries from the MAC address table in Layer 2, use the **clear mac address-table dynamic** command.

**clear mac address-table dynamic** [[**address** *mac_addr*] [**vlan** *vlan-id*] [**interface** {*type slot/port* | **port-channel** *number*}]

## Syntax Description

| | |
|---|---|
| **address** *mac_addr* | (Optional) Specifies the MAC address to remove from the table. Use the format XXXX.XXXX.XXXX. |
| **vlan** *vlan-id* | (Optional) Specifies the VLAN from which the MAC address should be removed from the table. The range of valid values is from 1 to 4094. |
| **interface** {*type slot/port* \| **port-channel** *number*}] | (Optional) Specifies the interface. Use either the type of interface, the slot number, and the port number, or the port-channel number. |

## Defaults

None

## Command Modes

Any

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

Use the **clear mac address-table dynamic** command with no arguments to remove all dynamic entries from the table.

To clear static MAC addresses from the table, use the **no mac address-table static** command.

If the **clear mac address-table dynamic** command is entered with no options, all dynamic addresses are removed. If you specify an address but do not specify an interface, the address is deleted from all interfaces. If you specify an interface but do not specify an address, the device removes all addresses on the specified interfaces.

## Examples

This example shows how to clear all the dynamic Layer 2 entries from the MAC address table:

```
n1000v(config)# clear mac address-table dynamic
n1000v(config) #
```

This example shows how to clear all the dynamic Layer 2 entries from the MAC address table for VLAN 20 on port 2/20:

```
n1000v(config)# clear mac address-table dynamic vlan 20 interface ethernet 2/20
n1000v(config)#
```

## Related Commands

| Command | Description |
|---|---|
| **show mac address-table** | Displays the information about the MAC address table. |

# clear ntp statistics

To clear the Network Time Protocol statistics, use the **clear ntp statistics** command.

**clear ntp statistics** {**all-peers** | **io** | **local** | **memory**}

## Syntax Description

| | |
|---|---|
| **all-peers** | Clear statistics for all NTP peers. |
| **io** | Clear IO statistics. |
| **local** | Clear local statistics. |
| **memory** | Clear memory statistics. |

## 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 clear statistics for all NTP peers:

```
n1000v(config)# clear ntp statistics all-peers
```

## Related Commands

| Command | Description |
|---|---|
| **show ntp peers** | Displays information about NTP peers. |

# clear port-security

To clear dynamically-learned, secure MAC address(es), use the **clear port-security** command.

**clear port-security** {**dynamic**} {**interface vethernet** *veth-number* | **address** *address*} [**vlan** *vlan-id*]

## Syntax Description

| | |
|---|---|
| **dynamic** | Specifies that you want to clear dynamically-learned, secure MAC addresses. |
| **interface vethernet** *veth-number* | Specifies the interface of the dynamically learned, secure MAC addresses that you want to clear. |
| **address** *address* | Specifies a single MAC address to be cleared, where *address* is the MAC address. |
| **vlan** *vlan-id* | Specifies the VLAN of the secure MAC addresses to be cleared. Valid VLAN IDs are from 1 to 4096. |

## Defaults

**dynamic**

## 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 dynamically learned, secure MAC addresses from the veth1 interface:

```
n1000v# config t
n1000v(config)# clear port-security dynamic interface veth 1
```

This example shows how to remove the dynamically learned, secure MAC address 0019.D2D0.00AE:

```
n1000v# config t
n1000v(config)# clear port-security dynamic address 0019.D2D0.00AE
```

## Related Commands

| Command | Description |
|---|---|
| **debug port-security** | Provides debugging information for port security. |
| **show port-security** | Shows information about port security. |
| **switchport port-security** | Enables port security on a Layer 2 interface. |

# clear qos statistics

To clear the counters for QoS statistics, use the **clear qos statistics** command.

**clear qos statistics** {**interface** [**ethernet** *type/slot* | **vethernet** *number* | **port-channel** *number*] } [**input type qos** | **output type qos**]}

## Syntax Description

| | |
|---|---|
| **interface** | (Optional) Identifies a specific interface for which to clear statistics. |
| **input type qos** | (Optional) Clears only input QoS statistics. |
| **output type qos** | (Optional) Clears only output QoS statistics. |

## 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

If you do not specify an interface, the counters are cleared for all interfaces.

## Examples

This example shows how to clear QoS statistics for all interfaces:

```
n1000v# clear qos statistics
n1000v#
```

This example shows how to clear all input QoS statistics for veth2:

```
n1000v# clear qos statistics veth2 input type qos
n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **qos statistics** | Enables or disables QoS statistics. |
| **show policy-map** | Displays the policy map configuration for all policy maps or for a specified policy map. |

# clear ssh hosts

To clear the Secure Shell (SSH) host sessions, use the **clear ssh hosts** command.

**clear ssh hosts**

## 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. |

## Examples

This example shows how to clear all SSH host sessions:

```
n1000v# clear ssh hosts
```

## Related Commands

| Command | Description |
|---|---|
| **ssh server enable** | Enables the SSH server. |

# clear system reset-reason

To clear the device reset-reason history, use the **clear system reset-reason** command.

**clear system reset-reason**

## 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. |

## Examples

This example shows how to clear reset-reason history:

```
n1000v# clear system reset-reason
```

## Related Commands

| Command | Description |
|---|---|
| **show system reset-reason** | Displays the device reset-reason history. |

# clear user

To clear a user session, use the **clear user** command.

**clear user** *user-id*

| Syntax Description | | |
|---|---|---|
| | *user-id* | User identifier. |

**Defaults** None

**Command Modes** Any

**SupportedUserRoles** network-admin

**Command History**

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

**Usage Guidelines** Use the **show users** command to display the current user sessions on the device.

**Examples** This example shows how to clear all SSH host sessions:

```
n1000v# clear user user1
```

**Related Commands**

| Command | Description |
|---|---|
| **show users** | Displays the user session information. |

# cli var name

To define a command line interface (CLI) variable for a terminal session, use the **cli var name** command. To remove the CLI variable, use the **no** form of this command.

**cli var name** *variable-name variable-text*

**cli no var name** *variable-name*

## Syntax Description

| | |
|---|---|
| *variable-name* | Name of the variable. The name is alphanumeric, case sensitive, and has a maximum of 31 characters. |
| *variable-text* | Variable text. The text is alphanumeric, can contain spaces, and has a maximum of 200 characters. |

## Defaults

None

## Command Modes

Any

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

You can reference a CLI variable using the following syntax:

**$**(variable-name)

Instances where you can use variables in include the following:

- Command scripts
- Filenames

You cannot reference a variable in the definition of another variable.

You can use the predefined variable, TIMESTAMP, to insert the time of day. You cannot change or remove the TIMESTAMP CLI variable.

You must remove a CLI variable before you can change its definition.

## Examples

This example shows how to define a CLI variable:

```
n1000v# cli var name testinterface interface 2/3
```

This example shows how to reference the TIMESTAMP variable:

```
n1000v# copy running-config > bootflash:run-config-$(TIMESTAMP).cnfg
```

This example shows how to remove a CLI variable:

```
n1000v# cli no var name testinterface interface 2/3
```

**Related Commands**

| Command | Description |
|---|---|
| **show cli variables** | Displays the CLI variables. |

# clock set

To manually set the clock, use the **clock set** command.

**clock set** *time day month year*

## Syntax Description

| | |
|---|---|
| *time* | Time of day. The format is *HH*:*MM*:*SS*. |
| *day* | Day of the month. The range is from 1 to 31. |
| *month* | Month of the year. The values are **January**, **February**, **March**, **April**, **May**, **June**, **July**, **August**, **September**, **October**, **November**, and **December**. |
| *year* | Year. The range is from 2000 to 2030. |

## Defaults

None

## Command Modes

Any

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

Use this command when you cannot synchronize your device with an outside clock source, such as NTP.

## Examples

This example shows how to manually set the clock:

```
n1000v# clock set 9:00:00 1 June 2008
```

## Related Commands

| Command | Description |
|---|---|
| **show clock** | Displays the clock time. |

# clock summer-time

To configure the summer-time (daylight saving time) offset, use the **clock summer-time** command. To revert to the default, use the **no** form of this command.

**clock summer-time** *zone-name start-week start-day start-month start-time end-week end-day end-month end-time offset-minutes*

**no clock summer-time**

## Syntax Description

| | |
|---|---|
| *zone-name* | Time zone string. The time zone string is a three-character string. |
| *start-week* | Week of the month to start the summer-time offset. The range is from 1 to 5. |
| *start-day* | Day of the month to start the summer-time offset. Valid values are **Monday**, **Tuesday**, **Wednesday**, **Thursday**, **Friday**, **Saturday**, or **Sunday**. |
| *start-month* | Month to start the summer-time offset. Valid values are **January**, **February**, **March**, **April**, **May**, **June**, **July**, **August**, **September**, **October**, **November**, and **December**. |
| *start-time* | Time to start the summer-time offset. The format is *hh*:*mm*. |
| *end-week* | Week of the month to end the summer-time offset. The range is from 1 to 5. |
| *end-day* | Day of the month to end the summer-time offset. Valid values are **Monday**, **Tuesday**, **Wednesday**, **Thursday**, **Friday**, **Saturday**, or **Sunday**. |
| *end-month* | Month to end the summer-time offset. Valid values are **January**, **February**, **March**, **April**, **May**, **June**, **July**, **August**, **September**, **October**, **November**, and **December**. |
| *end-time* | Time to end the summer-time offset. The format is *hh*:*mm*. |
| *offset-minutes* | Number of minutes to offset the clock. The range is from 1 to 1440. |

## 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 configure the offset for summer-time or daylight saving time:

```
n1000v# configure terminal
n1000v(config)# clock summer-time PDT 1 Sunday March 02:00 1 Sunday November 02:00 60
```

This example shows how to remove the summer-time offset:

```
n1000v# configure terminal
n1000v(config)# no clock summer-time
```

**Related Commands**

| Command | Description |
|---|---|
| **show clock** | Displays clock summer-time offset configuration. |

# clock timezone

To configure the time zone offset from Coordinated Universal Time (UTC), use the **clock timezone** command. To revert to the default, use the **no** form of this command.

**clock timezone** *zone-name offset-hours offset-minutes*

**no clock timezone**

## Syntax Description

| | |
|---|---|
| *zone-name* | Zone name. The name is a 3-character string for the time zone acronym (for example, PST or EST). |
| *offset-hours* | Number of hours offset from UTC. The range is from –23 to 23. |
| *offset-minutes* | Number of minutes offset from UTC. The range is from 0 to 59. |

## Defaults

None

## 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 configure the time zone offset from UTC:

```
n1000v# clock timezone EST 5 0
```

This example shows how to remove the time zone offset:

```
n1000v# no clock timezone
```

## Related Commands

| Command | Description |
|---|---|
| **show clock** | Displays the clock time. |

# collect counter

To configure the number of bytes or packets in a flow as a non-key field and collect the number of bytes or packets seen for a Flexible NetFlow flow record, use the **collect counter** command. To disable the counters, use the **no** form of this command.

**collect counter** {**bytes** [**long**] | **packets** [**long**]}

**no collect counter** {**bytes** [**long**] | **packets** [**long**]}

## Syntax Description

| | |
|---|---|
| **bytes** | Configures the number of bytes or packets seen in a flow as a non-key field and enables collecting the total number of bytes from the flow. |
| **long** | (Optional) Enables collecting the total number of bytes from the flow using a 64 bit counter. |
| **packets** | Configures the number of bytes seen in a flow as a non-key field and enables collecting the total number of packets from the flow. |

## Command Default

This command is not enabled by default.

## Command Modes

Flow record configuration (config-flow-record)

## SupportedUserRoles

network-admin

## Command History

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

## Examples

The following example enables collecting the total number of bytes from the flows as a non-key field:

```
n1000v(config)# flow record FLOW-RECORD-1
n1000v(config-flow-record)# collect counter bytes
```

The following example enables collecting the total number of bytes from the flows as a non-key field using a 64 bit counter:

```
n1000v(config)# flow record FLOW-RECORD-1
n1000v(config-flow-record)# collect counter bytes long
```

The following example enables collecting the total number of packets from the flows as a non-key field:

```
n1000v(config)# flow record FLOW-RECORD-1
n1000v(config-flow-record)# collect counter packets
```

The following example enables collecting the total number of packets from the flows as a non-key field using a 64 bit counter:

```
n1000v(config)# flow record FLOW-RECORD-1
n1000v(config-flow-record)# collect counter packets long
```

## Related Commands

| Command | Description |
|---|---|
| **collect counter** | Configures the counters as a non-key field and collects the counter values. |
| **flow record** | Creates a flow record. |
| **show flow record** | Displays flow record status and statistics. |

# collect timestamp sys-uptime

To collect the TIMESTAMP SYS-UPTIME for a NetFlow flow record, use the **collect timestamp sys-uptime** command. To disable the collection, use the **no** form of this command.

**collect timestamp sys-uptime** {**first** | **last**}

**no collect timestamp sys-uptime** {**first** | **last**}

## Syntax Description

| | |
|---|---|
| **first** | Configures the sys-uptime for the time the first packet was seen from the flows as a non-key field and enables collecting time stamps based on the sys-uptime for the time the first packet was seen from the flows. |
| **last** | Configures the sys-uptime for the time the last packet was seen from the flows as a non-key field and enables collecting time stamps based on the sys-uptime for the time the most recent packet was seen from the flows. |

## Command Default

This command is not enabled by default.

## Command Modes

Flow record configuration (config-flow-record)

## SupportedUserRoles

network-admin

## Command History

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

## Examples

The following example enables collecting the sys-uptime for the time the first packet was seen from the flows:

```
n1000v(config)# flow record FLOW-RECORD-1
n1000v(config-flow-record)# collect timestamp sys-uptime first
```

The following example enables collecting the sys-uptime for the time the most recent packet was seen from the flows:

```
n1000v(config)# flow record FLOW-RECORD-1
n1000v(config-flow-record)# collect timestamp sys-uptime last
```

## Related Commands

| Command | Description |
|---|---|
| **flow record** | Creates a flow record. |
| **show flow record** | Displays flow record status and statistics. |

# collect transport tcp flags

To collect a Transmission Control Protocol (TCP) flags for a NetFlow flow record, use the **collect transport tcp flags** command. To disable the collection, use the **no** form of this command.

**collect transport tcp flags**

**no collect transport tcp flags**

## Syntax Description

This command has no arguments or keywords

## Command Default

This command is not enabled by default.

## Command Modes

Flow record configuration (config-flow-record)

## SupportedUserRoles

network-admin

## Command History

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

## Examples

The following example collects the TCP flags:

```
n1000v(config)# flow record FLOW-RECORD-1
n1000v(config-flow-record)# collect transport tcp flags
```

## Related Commands

| Command | Description |
|---|---|
| **flow record** | Creates a flow record. |
| **show flow record** | Displays flow record status and statistics. |

# configure terminal

To access configuration commands in the CLI global configuration mode, use the **configure terminal** command.

**configure terminal**

## 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

The configuration changes you make in the global configuration mode are saved in the running configuration file. To save these changes persistently across reboots and restarts, you must copy them to the startup configuration file using the **copy running-config startup-config** command.

## Examples

This example shows how to access configuration commands in the CLI global configuration mode:

```
n1000v# configure terminal
n1000v(config)#
```

## Related Commands

| Command | Description |
|---|---|
| **where** | Displays the current configuration mode context. |
| **pwd** | Displays the name of the present working directory. |
| **copy run start** | Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration. |

# connect

To initiate a connection with vCenter, use the **connect** command. To disconnect from vCenter, use the **no** form of this command.

**connect**

**no connect**

## Syntax Description

This command has no arguments or keywords.

## Defaults

no connect

## Command Modes

SVS connect configuration (config-svs-conn)

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

Upon connection to vCenter, if a username and password have not been configured for this connection, you are prompted to enter them.

There can be only one active connection at a time. If a previously-defined connection is up, an error message displays and the **connect** command is rejected until the previous connection is closed by entering **no connect**.

## Examples

This example shows how to connect to vCenter:

```
n1000v(config#) svs connection vcWest
n1000v(config-svs-conn#) protocol vmware-vim
n1000v(config-svs-conn#) remote hostname vcMain
n1000v(config-svs-conn#) vmware dvs datacenter-name HamiltonDC
n1000v(config-svs-conn#) connect
```

This example shows how to disconnect from vCenter:

```
n1000v(config#) svs connection vcWest
n1000v(config-svs-conn#) no connect
```

## Related Commands

| Command | Description |
|---|---|
| **show svs connections** | Displays the current connections to the Cisco Nexus 1000V. |

# control vlan

To assign a control VLAN to the Cisco Nexus 1000V domain, use the **control vlan** command. To remove the control VLAN, use the **no** form of this command.

**control vlan** *number*

**no control vlan**

## Syntax Description

| | |
|---|---|
| *number* | control VLAN number. |

## Defaults

None

## Command Modes

SVS domain configuration (config-svs-domain)

## Supported User Roles

network-admin

## Command History

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

## Usage Guidelines

Newly-created VLANs remain unused until Layer 2 ports are assigned to them.

If you enter a VLAN ID that is assigned to an internally allocated VLAN, the CLI returns an error message.

## Examples

This example shows how to configure control VLAN 70 for domain ID 32:

```
n1000v# config t
n1000v(config)# svs-domain
n1000v(config-svs-domain)# domain id 32
n1000v(config-svs-domain)# control vlan 70
n1000v(config-svs-domain)#
```

This example shows how to remove control VLAN 70 from domain ID 32:

```
n1000v# config t
n1000v(config)# svs-domain
n1000v(config-svs-domain)# domain id 32
n1000v(config-svs-domain)# no control vlan 70
n1000v(config-svs-domain)#
```

## Related Commands

| Command | Description |
|---|---|
| **show vlan-id** | Displays the configuration for the specified VLAN. |
| **svs-domain** | Creates the domain and places you into CLI SVS domain configuration mode. |
| **domain id** | Assigns a domain ID to the domain. |
| **packet vlan** | Assigns a packet VLAN to the domain. |
| **show svs-domain** | Displays the domain configuration. |

# copy

To copy a file from a source to a destination, use the **copy** command.

**copy** *source-url destination-url*

## Syntax Description

| | |
|---|---|
| *source-url* | Location URL (or variable) of the source file or directory to be copied. The source can be either local or remote, depending upon whether the file is being downloaded or uploaded. |
| *destination-url* | Destination URL (or variable) of the copied file or directory. The destination can be either local or remote, depending upon whether the file is being downloaded or uploaded. |

The format of the source and destination URLs varies according to the file or directory location. You may enter either a command-line interface (CLI) variable for a directory or a filename that follows the Cisco NX-OS file system syntax (*filesystem*:[*/directory*][*/filename*]).

The following tables list URL prefix keywords by the file system type. If you do not specify a URL prefix keyword, the device looks for the file in the current directory.

Table 1 lists URL prefix keywords for bootflash and remote writable storage file systems.

***Table 1 URL Prefix Keywords for Storage File Systems***

| Keyword | Source or Destination |
|---|---|
| **bootflash:**[*//module/*] | Source or destination URL for boot flash memory. The *module* argument value is **sup-active**, **sup-local**, **sup-remote**, or **sup-standby**. |
| **ftp:** | Source or destination URL for a FTP network server. The syntax for this alias is as follows:<br>**ftp:**[*//server*][*/path*]*/filename* |
| **scp:** | Source or destination URL for a network server that supports Secure Shell (SSH) and accepts copies of files using the secure copy protocol (scp). The syntax for this alias is as follows:<br>**scp:**[*//*[*username@*]*server*][*/path*]*/filename* |
| **sftp:** | Source or destination URL for an SSH FTP (SFTP) network server. The syntax for this alias is as follows:<br>**sftp:**[*//*[*username@*]*server*][*/path*]*/filename* |
| **tftp:** | Source or destination URL for a TFTP network server. The syntax for this alias is as follows:<br>**tftp:**[*//server*[**:***port*]][*/path*]*/filename* |

Table 2 lists the URL prefix keywords for nonwritable file systems.

*Table 2 URL Prefix Keywords for Special File Systems*

| Keyword | Source or Destination |
|---|---|
| **core:** | Local memory for core files. You can copy core files from the core: file system. |
| **debug:** | Local memory for debug files. You can copy core files from the debug: file system. |
| **log:** | Local memory for log files. You can copy log files from the log: file system. |
| **system:** | Local system memory. You can copy the running configuration to or from the system: file system. The system: file system is optional when referencing the running-config file in a command. |
| **volatile:** | Local volatile memory. You can copy files to or from the volatile: file system. All files in the volatile: memory are lost when the physical device reloads. |

## Defaults

The default name for the destination file is the source filename.

## Command Modes

Any

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

The entire copying process may take several minutes, depending on the network conditions and the size of the file, and differs from protocol to protocol and from network to network.

The colon character (**:**) is required after the file system URL prefix keywords (such as **bootflash**).

In the URL syntax for **ftp:**, **scp:**, **sftp:**, and **tftp:**, the server is either an IP address or a host name.

## Examples

This example shows how to copy a file within the same directory:

```
n1000v# copy file1 file2
```

This example shows how to copy a file to another directory:

```
n1000v# copy file1 my_files:file2
```

This example shows how to copy a file to another supervisor module:

```
n1000v# copy file1 bootflash://sup-remote/file1.bak
```

This example shows how to copy a file from a remote server:

```
n1000v# copy scp://10.10.1.1/image-file.bin bootflash:image-file.bin
```

## Related Commands

| Command | Description |
|---|---|
| **cd** | Changes the current working directory. |
| **cli var name** | Configures CLI variables for the session. |
| **dir** | Displays the directory contents. |
| **move** | Moves a file. |
| **pwd** | Displays the name of the current working directory. |

# copy running-config startup-config

To copy the running configuration to the startup configuration, use the **copy running-config startup-config** command.

**copy running-config startup-config**

## 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

Use this command to save configuration changes in the running configuration to the startup configuration in persistent memory. When a device reload or switchover occurs, the saved configuration is applied.

## Examples

This example shows how to save the running configuration to the startup configuration:

```
n1000v# copy running-config startup-config
[########################################] 100%
```

## Related Commands

| Command | Description |
|---|---|
| **show running-config** | Displays the running configuration. |
| **show running-config diff** | Displays the differences between the running configuration and the startup configuration. |
| **show startup-config** | Displays the startup configuration. |
| **write erase** | Erases the startup configuration in the persistent memory. |

# D Commands

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

## deadtime

To configure the duration of time for which a non-reachable RADIUS or TACACS+ server is skipped, use the **deadtime** command. To revert to the default, use the **no** form of this command.

**deadtime** *minutes*

**no deadtime** *minutes*

**Syntax Description**

| | |
|---|---|
| *minutes* | Number of minutes, from 0 to 1440, for the interval. |

**Defaults**

0 minutes

**Command Modes**

RADIUS server group configuration (`config-radius`)
TACACS+ server group configuration (`config-tacacs+`)
Global configuration (**config**)

**SupportedUserRoles**

network-admin

**Command History**

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

**Usage Guidelines**

Before you can configure it, you must enable TACACS+ using the **tacacs+ enable** command.

The dead-time can be configured either globally and applied to all RADIUS or TACACS+ servers; or per server group.

If the dead-time interval for a RADIUS or TACACS+ server group is greater than zero (0), that value takes precedence over the global dead-time value.

Setting the dead-time interval to 0 disables the timer.

When the dead-time interval is 0 minutes, RADIUS and TACACS+ servers are not marked as dead even if they are not responding.

## Examples

This example shows how to set the dead-time interval to 2 minutes for a RADIUS server group:

```
n1000v# config t
n1000v(config)# aaa group server radius RadServer
n1000v(config-radius)# deadtime 2
```

This example shows how to set a global dead-time interval to 5 minutes for all TACACS+ servers and server groups:

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

This example shows how to set the dead-time interval to 5 minutes for a TACACS+ server group:

```
n1000v# config t
n1000v(config)# aaa group server tacacs+ TacServer
n1000v(config-tacacs+)# deadtime 5
```

This example shows how to revert to the dead-time interval default:

```
n1000v# config t
n1000v(config)# feature tacacs+
n1000v(config)# aaa group server tacacs+ TacServer
n1000v(config-tacacs+)# no deadtime 5
```

## Related Commands

| Command | Description |
|---|---|
| **aaa group server** | Configures AAA server groups. |
| **radius-server host** | Configures a RADIUS server. |
| **show radius-server groups** | Displays RADIUS server group information. |
| **show tacacs-server groups** | Displays TACACS+ server group information. |
| **tacacs+ enable** | Enables TACACS+. |
| **tacacs-server host** | Configures a TACACS+ server. |

# debug logfile

To direct the output of the **debug** commands to a specified file, use the **debug logfile** command. To revert to the default, use the **no** form of this command.

**debug logfile** *filename* [**size** *bytes*]

**no debug logfile** *filename* [**size** *bytes*]

## Syntax Description

| | |
|---|---|
| *filename* | Name of the file for **debug** command output. The filename is alphanumeric, case sensitive, and has a maximum of 64 characters. |
| **size** *bytes* | (Optional) Specifies the size of the logfile in bytes. The range is from 4096 to 4194304. |

## Defaults

Default filename: syslogd_debugs

Default file size: 4194304 bytes

## Command Modes

Any

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

The logfile is created in the log: file system root directory.

Use the **dir log:** command to display the log files.

## Examples

This example shows how to specify a debug logfile:

```
n1000v# debug logfile debug_log
```

This example shows how to revert to the default debug logfile:

```
n1000v# no debug logfile debug_log
```

## Related Commands

| Command | Description |
|---|---|
| **dir** | Displays the contents of a directory. |
| **show debug** | Displays the debug configuration. |
| **show debug logfile** | Displays the debug logfile contents. |

# debug logging

To enable **debug** command output logging, use the **debug logging** command. To disable debug logging, use the **no** form of this command.

**debug logging**

**no debug logging**

## Syntax Description

This command has no arguments or keywords.

## Defaults

Disabled

## 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 enable the output logging for the **debug** command:

```
n1000v# debug logging
```

This example shows how to disable the output logging for the **debug** command:

```
n1000v# no debug logging
```

## Related Commands

| Command | Description |
|---|---|
| **debug logfile** | Configures the logfile for the **debug** command output. |

# default switchport (port profile)

To remove a particular switchport characteristc from a port profile, use the **default switchport** command.

**default switchport** {**mode** | **access vlan** | **trunk** {**native** | **allowed**} **vlan** | **private-vlan** {**host-association** | **mapping** [**trunk**]} | **port-security**}

## Syntax Description

| | |
|---|---|
| **mode** | Removes the port mode characteristic from a port profile, which causes the port mode to revert to global or interface defaults (access mode). This is equivalent to executing the **no switchport mode port-profile** command. |
| **access vlan** | Removes an access VLAN configuration. |
| **trunk allowedvlan** | Removes trunking allowed VLAN characteristics. |
| **trunk native vlan** | Removes trunking native VLAN characteristics. |
| **private-vlan host-association** | Removes PVLAN host-association. |
| **private-vlan mapping** | Removes PVLAN mapping. |
| **port-security** | Removes port-security characteristics. |

## Defaults

None

## Command Modes

Port profile configuration (**config-port-prof**)

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

The functionally of this command is equivalent to using the no form of a specific switchport command. For example, the effect of the following commands is the same:

- **default switchport mode** command = **no switchport mode** command
- **default switchport access vlan** command = **no switchport access vlan** command
- **default switchport trunk native vlan** command= **no switchport trunk native vlan** command

## Examples

This example shows how to revert port profile ports to switch access ports.

```
n1000v(config-port-prof)# default switchport mode
```

This example shows how to remove the trunking allowed VLAN characteristics of a port profile.

```
n1000v(config-port-prof)# default switchport trunk allowed vlan
```

This example shows how toremove the private VLAN host association of a port profile.

```
n1000v(config-port-prof)# default switchport private-vlan host-association
```

This example shows how to remove port security characteristics of a port profile.

```
n1000v(config-port-prof)# default switchport port-security
```

**Related Commands**

| Command | Description |
|---|---|
| **show port-profile** | Displays information about port profile(s). |

# default shutdown (port profile)

To remove the admin status characteristic (config attribute) from a port-profile, use the **default shutdown** command. This will set the admin status of the interfaces inheriting this port-profile to the global or interface default (usually, the default admin status is shutdown).

**default shutdown**

## Syntax Description

This command has no arguments or keywords.

## Defaults

None

## Command Modes

Port profile configuration (**config- port-prof**)

## SupportedUserRoles

network-admin

## Command History

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

## Examples

This example shows how to change the ports in a port profile to the shutdown state:

```
n1000v# config t
n1000v# port-profile DataProfile
n1000v(config-port-prof)# default shutdown
n1000v(config-port-prof)# show port-profile name DataProfile
port-profile DataProfile
  description:
  status: enabled
  capability uplink: no
  capability l3control: no
  system vlans: none
  port-group: DataProfile
  max-ports: 32
  inherit:
  config attributes:
    switchport mode access
  evaluated config attributes:
    switchport mode access
  assigned interfaces:
    Vethernet1switch(config-port-prof)#
```

## Related Commands

| Command | Description |
|---|---|
| **show port-profile** | Displays the configuration for a port profile. |

# default shutdown (interface)

To remove any interface-level override for the admin status, use the **default shutdown** command. This command removes any configuration for admin status entered previously. This allows the port-profile config to take effect.

**default shutdown**

## Syntax Description

This command has no arguments or keywords.

## Defaults

None

## Command Modes

Interface configuration (**config- if**)

## SupportedUserRoles

network-admin

## Command History

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

## Examples

This example shows how to change the ports to the shutdown state:

```
n1000v# config t
n1000v(config)# interface ethernet 3/2
n1000v(config-if)# default shutdown
n1000v(config-if)#
```

## Related Commands

| Command | Description |
|---|---|
| **show running-config interface** | Displays the configuration of an interface. |

# default switchport port-security (VEthernet)

To remove any user configuration for the switchport port-security characteristic from a VEthernet interface, use the **default switchport port-security** command. This has the effect of setting the default (disabled) for port-security for that interface.

**default switchport port-security**

## Syntax Description

This command has no arguments or keywords.

## Defaults

Disabled

## Command Modes

Interface configuration (**config-if**)

## SupportedUserRoles

network-admin

## Command History

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

## Examples

This example shows how to disable port security on VEthernet 2:

```
n1000v# config t
n1000v(config)# interface veth 2
n1000v(config-if)# default switchport port-security
n1000v(config-if)#
```

## Related Commands

| Command | Description |
|---|---|
| **show running-config port-security** | Displays the port security configuration. |
| **show port-security** | Displays the port security status. |

# delay

To assign an informational throughput delay value to an Ethernet interface, use the **delay** command. To remove delay value, use the **no** form of this command.

**delay** *value*

**no delay** [*value*]

## Syntax Description

| | |
|---|---|
| *delay_val* | Specifies the throughput delay time in tens of microseconds.<br>Allowable values are between 1 and 16777215. |

## Defaults

None

## Command Modes

Interface configuration (config-if)

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

The actual Ethernet interface throughput delay time does not change when you set this value—the setting is for informational purposes only.

## Examples

This example shows how to assign the delay time to an Ethernet slot 3 port 1 interface:

```
n1000v# config t
n1000v(config)# interface ethernet 3/1
n1000v(config-if)# delay 10000
n1000v(config-if)#
```

This example shows how to remove the delay time configuration:

```
n1000v# config t
n1000v(config)# interface ethernet 3/1
n1000v(config-if)# no delay 10000
n1000v(config-if)#
```

## Related Commands

| Command | Description |
|---|---|
| **show interface** | Displays configuration information for an interface. |

# delete

To delete a file, use the **delete** command.

**delete** [*filesystem*:[*//directory/*] | *directory/*]*filename*

## Syntax Description

| | |
|---|---|
| *filesystem*: | (Optional) Name of the file system. Valid values are **bootflash** or **volatile**. |
| *//directory/* | (Optional) Name of the directory. The directory name is case sensitive. |
| *filename* | Name of the file. The name is case sensitive. |

## Defaults

None

## Command Modes

Any

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

Use the **dir** command to locate the file you that want to delete.

## Examples

This example shows how to delete a file:

```
n1000v# delete bootflash:old_config.cfg
```

## Related Commands

| Command | Description |
|---|---|
| **dir** | Displays the contents of a directory. |

# deny (IPv4)

To create an IPv4 ACL rule that denies traffic matching its conditions, use the **deny** command. To remove a rule, use the **no** form of this command.

### General Syntax

[*sequence-number*] **deny** *protocol source destination* [**dscp** *dscp* | **precedence** *precedence*]

**no deny** *protocol source destination* [**dscp** *dscp* | **precedence** *precedence*]

**no** *sequence-number*

### Internet Control Message Protocol

[*sequence-number*] **deny icmp** *source destination* [*icmp-message*] [**dscp** *dscp* | **precedence** *precedence*]

### Internet Group Management Protocol

[*sequence-number*] **deny igmp** *source destination* [*igmp-message*] [**dscp** *dscp* | **precedence** *precedence*]

### Internet Protocol v4

[*sequence-number*] **deny ip** *source destination* [**dscp** *dscp* | **precedence** *precedence*]

### Transmission Control Protocol

[*sequence-number*] **deny tcp** *source* [*operator port* [*port*] | **portgroup** *portgroup*] *destination* [*operator port* [*port*] | **portgroup** *portgroup*] [**dscp** *dscp* | **precedence** *precedence*] [**fragments**] [**log**] [**time-range** *time-range-name*] [*flags*] [**established**]

### User Datagram Protocol

[*sequence-number*] **deny udp** *source operator port* [*port*] *destination* [*operator port* [*port*] [**dscp** *dscp* | **precedence** *precedence*]

## Syntax Description

| | |
|---|---|
| *sequence-number* | (Optional) Sequence number of the **deny** 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.<br><br>A sequence number can be any integer between 1 and 4294967295.<br><br>By default, the first rule in an ACL has a sequence number of 10.<br><br>If you do not specify a sequence number, the device adds the rule to the end of the ACL and assigns a sequence number that is 10 greater than the sequence number of the preceding rule.<br><br>Use the **resequence** command to reassign sequence numbers to rules. |
| *protocol* | Name or number of the protocol of packets that the rule matches. Valid numbers are from 0 to 255. Valid protocol names are the following keywords:<br><br>• **icmp**—Specifies that the rule applies to ICMP traffic only. When you use this keyword, the *icmp-message* argument is available, in addition to the keywords that are available for all valid values of the *protocol* argument.<br><br>• **igmp**—Specifies that the rule applies to IGMP traffic only. When you use this keyword, the *igmp-type* argument is available, in addition to the keywords that are available for all valid values of the *protocol* argument.<br><br>• **ip**—Specifies that the rule applies to all IPv4 traffic. When you use this keyword, only the other keywords and arguments that apply to all IPv4 protocols are available. They include the following:<br><br>– **dscp**<br><br>– **precedence**<br><br>• **tcp**—Specifies that the rule applies to TCP traffic only. When you use this keyword, the *flags* and *operator* arguments are available, in addition to the keywords that are available for all valid values of the *protocol* argument.<br><br>• **udp**—Specifies that the rule applies to UDP traffic only. When you use this keyword, the *operator* argument is available, in addition to the keywords that are available for all valid values of the *protocol* argument. |
| *source* | Source IPv4 addresses that the rule matches. For details about the methods that you can use to specify this argument, see “Source and Destination” in the “Usage Guidelines” section. |
| *destination* | Destination IPv4 addresses that the rule matches. For details about the methods that you can use to specify this argument, see “Source and Destination” in the “Usage Guidelines” section. |

| | |
|---|---|
| **dscp** *dscp* | (Optional) Specifies that the rule matches only those packets with the specified 6-bit differentiated services value in the DSCP field of the IP header. The *dscp* argument can be one of the following numbers or keywords:<br>• 0–63—The decimal equivalent of the 6 bits of the DSCP field. For example, if you specify 10, the rule matches only those packets that have the following bits in the DSCP field: 001010.<br>• **af11**—Assured Forwarding (AF) class 1, low drop probability (001010)<br>• **af12**—AF class 1, medium drop probability (001100)<br>• **af13**—AF class 1, high drop probability (001110)<br>• **af21**—AF class 2, low drop probability (010010)<br>• **af22**—AF class 2, medium drop probability (010100)<br>• **af23**—AF class 2, high drop probability (010110)<br>• **af31**—AF class 3, low drop probability (011010)<br>• **af32**—AF class 3, medium drop probability (011100)<br>• **af33**—AF class 3, high drop probability (011110)<br>• **af41**—AF class 4, low drop probability (100010)<br>• **af42**—AF class 4, medium drop probability (100100)<br>• **af43**—AF class 4, high drop probability (100110)<br>• **cs1**—Class-selector (CS) 1, precedence 1 (001000)<br>• **cs2**—CS2, precedence 2 (010000)<br>• **cs3**—CS3, precedence 3 (011000)<br>• **cs4**—CS4, precedence 4 (100000)<br>• **cs5**—CS5, precedence 5 (101000)<br>• **cs6**—CS6, precedence 6 (110000)<br>• **cs7**—CS7, precedence 7 (111000)<br>• **default**—Default DSCP value (000000)<br>• **ef**—Expedited Forwarding (101110) |

| | |
|---|---|
| **precedence** *precedence* | (Optional) Specifies that the rule matches only packets that have an IP Precedence field with the value specified by the *precedence* argument. The *precedence* argument can be a number or a keyword, as follows:<br>• 0–7—Decimal equivalent of the 3 bits of the IP Precedence field. For example, if you specify 3, the rule matches only packets that have the following bits in the DSCP field: 011.<br>• **critical**—Precedence 5 (101)<br>• **flash**—Precedence 3 (011)<br>• **flash-override**—Precedence 4 (100)<br>• **immediate**—Precedence 2 (010)<br>• **internet**—Precedence 6 (110)<br>• **network**—Precedence 7 (111)<br>• **priority**—Precedence 1 (001)<br>• **routine**—Precedence 0 (000) |
| *icmp-message* | (ICMP only: Optional) ICMP message type that the rule matches. This argument can be an integer from 0 to 255 or one of the keywords listed under "ICMP Message Types" in the "Usage Guidelines" section. |
| *igmp-message* | (IGMP only: Optional) IGMP message type that the rule matches. The *igmp-message* argument can be the IGMP message number, which is an integer from 0 to 15. It can also be one of the following keywords:<br>• **dvmrp**—Distance Vector Multicast Routing Protocol<br>• **host-query**—Host query<br>• **host-report**—Host report<br>• **pim**—Protocol Independent Multicast<br>• **trace**—Multicast trace |

| | |
|---|---|
| *operator port* [*port*] | (Optional; TCP and UDP only) Rule matches only packets that are from a source port or sent to a destination port that satisfies the conditions of the *operator* and *port* arguments. Whether these arguments apply to a source port or a destination port depends upon whether you specify them after the *source* argument or after the *destination* argument.<br><br>The *port* argument can be the name or the number of a TCP or UDP port. Valid numbers are integers from 0 to 65535. For listings of valid port names, see "TCP Port Names" and "UDP Port Names" in the "Usage Guidelines" section.<br><br>A second *port* argument is required only when the *operator* argument is a range.<br><br>The *operator* argument must be one of the following keywords:<br>• **eq**—Matches only if the port in the packet is equal to the *port* argument.<br>• **gt**—Matches only if the port in the packet is greater than and not equal to the *port* argument.<br>• **lt**—Matches only if the port in the packet is less than and not equal to the *port* argument.<br>• **neq**—Matches only if the port in the packet is not equal to the *port* argument.<br>• **range**—Requires two *port* arguments and matches only if the port in the packet is equal to or greater than the first *port* argument and equal to or less than the second *port* argument. |
| *flags* | (TCP only; Optional) TCP control bit flags that the rule matches. The value of the *flags* argument must be one or more of the following keywords:<br>• **ack**<br>• **fin**<br>• **psh**<br>• **rst**<br>• **syn**<br>• **urg** |

## Defaults

A newly created IPv4 ACL contains no rules.

If you do not specify a sequence number, the device assigns the rule a sequence number that is 10 greater than the last rule in the ACL.

## Command Modes

IPv4 ACL configuration (config-acl)

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

When the device applies an IPv4 ACL to a packet, it evaluates the packet with every rule in the ACL. The device enforces the first rule that has conditions that are satisfied by the packet. When the conditions of more than one rule are satisfied, the device enforces the rule with the lowest sequence number.

### Source and Destination

You can specify the *source* and *destination* arguments in one of several ways. In each rule, the method that you use to specify one of these arguments does not affect how you specify the other argument. When you configure a rule, use the following methods to specify the *source* and *destination* arguments:

- Address and network wildcard—You can use an IPv4 address followed by a network wildcard to specify a host or a network as a source or destination. The syntax is as follows:

  *IPv4-address network-wildcard*

  The following example shows how to specify the *source* argument with the IPv4 address and network wildcard for the 192.168.67.0 subnet:

  ```
  n1000v(config-acl)# deny tcp 192.168.67.0 0.0.0.255 any
  ```

- Address and variable-length subnet mask—You can use an IPv4 address followed by a variable-length subnet mask (VLSM) to specify a host or a network as a source or destination. The syntax is as follows:

  *IPv4-address/prefix-len*

  The following example shows how to specify the *source* argument with the IPv4 address and VLSM for the 192.168.67.0 subnet:

  ```
  n1000v(config-acl)# deny udp 192.168.67.0/24 any
  ```

- Host address—You can use the **host** keyword and an IPv4 address to specify a host as a source or destination. The syntax is as follows:

  **host** *IPv4-address*

  This syntax is equivalent to *IPv4-address*/32 and *IPv4-address* 0.0.0.0.

  The following example shows how to specify the *source* argument with the **host** keyword and the 192.168.67.132 IPv4 address:

  ```
  n1000v(config-acl)# deny icmp host 192.168.67.132 any
  ```

- Any address—You can use the **any** keyword to specify that a source or destination is any IPv4 address. For examples of the use of the **any** keyword, see the examples in this section. Each example shows how to specify a source or destination by using the **any** keyword.

### ICMP Message Types

The *icmp-message* argument can be the ICMP message number, which is an integer from 0 to 255. It can also be one of the following keywords:

- **administratively-prohibited**—Administratively prohibited
- **alternate-address**—Alternate address
- **conversion-error**—Datagram conversion
- **dod-host-prohibited**—Host prohibited
- **dod-net-prohibited**—Net prohibited
- **echo**—Echo (ping)
- **echo-reply**—Echo reply

- **general-parameter-problem**—Parameter problem
- **host-isolated**—Host isolated
- **host-precedence-unreachable**—Host unreachable for precedence
- **host-redirect**—Host redirect
- **host-tos-redirect**—Host redirect for ToS
- **host-tos-unreachable**—Host unreachable for ToS
- **host-unknown**—Host unknown
- **host-unreachable**—Host unreachable
- **information-reply**—Information replies
- **information-request**—Information requests
- **mask-reply**—Mask replies
- **mask-request**—Mask requests
- **mobile-redirect**—Mobile host redirect
- **net-redirect**—Network redirect
- **net-tos-redirect**—Net redirect for ToS
- **net-tos-unreachable**—Network unreachable for ToS
- **net-unreachable**—Net unreachable
- **network-unknown**—Network unknown
- **no-room-for-option**—Parameter required but no room
- **option-missing**—Parameter required but not present
- **packet-too-big**—Fragmentation needed and DF set
- **parameter-problem**—All parameter problems
- **port-unreachable**—Port unreachable
- **precedence-unreachable**—Precedence cutoff
- **protocol-unreachable**—Protocol unreachable
- **reassembly-timeout**—Reassembly timeout
- **redirect**—All redirects
- **router-advertisement**—Router discovery advertisements
- **router-solicitation**—Router discovery solicitations
- **source-quench**—Source quenches
- **source-route-failed**—Source route failed
- **time-exceeded**—All time-exceeded messages
- **timestamp-reply**—Time-stamp replies
- **timestamp-request**—Time-stamp requests
- **traceroute**—Traceroute
- **ttl-exceeded**—TTL exceeded
- **unreachable**—All unreachables

### TCP Port Names

When you specify the *protocol* argument as **tcp**, the *port* argument can be a TCP port number, which is an integer from 0 to 65535. It can also be one of the following keywords:

**bgp**—Border Gateway Protocol (179)

**chargen**—Character generator (19)

**cmd**—Remote commands (rcmd, 514)

**daytime**—Daytime (13)

**discard**—Discard (9)

**domain**—Domain Name Service (53)

**drip**—Dynamic Routing Information Protocol (3949)

**echo**—Echo (7)

**exec**—EXEC (rsh, 512)

**finger**—Finger (79)

**ftp**—File Transfer Protocol (21)

**ftp-data**—FTP data connections (2)

**gopher**—Gopher (7)

**hostname**—NIC hostname server (11)

**ident**—Ident Protocol (113)

**irc**—Internet Relay Chat (194)

**klogin**—Kerberos login (543)

**kshell**—Kerberos shell (544)

**login**—Login (rlogin, 513)

**lpd**—Printer service (515)

**nntp**—Network News Transport Protocol (119)

**pim-auto-rp**—PIM Auto-RP (496)

**pop2**—Post Office Protocol v2 (19)

**pop3**—Post Office Protocol v3 (11)

**smtp**—Simple Mail Transport Protocol (25)

**sunrpc**—Sun Remote Procedure Call (111)

**tacacs**—TAC Access Control System (49)

**talk**—Talk (517)

**telnet**—Telnet (23)

**time**—Time (37)

**uucp**—UNIX-to-UNIX Copy Program (54)

**whois**—WHOIS/NICNAME (43)

**www**—World Wide Web (HTTP, 8)

### UDP Port Names

When you specify the *protocol* argument as **udp**, the *port* argument can be a UDP port number, which is an integer from 0 to 65535. It can also be one of the following keywords:

**biff**—Biff (mail notification, comsat, 512)

**bootpc**—Bootstrap Protocol (BOOTP) client (68)

**bootps**—Bootstrap Protocol (BOOTP) server (67)

**discard**—Discard (9)

**dnsix**—DNSIX security protocol auditing (195)

**domain**—Domain Name Service (DNS, 53)

**echo**—Echo (7)

**isakmp**—Internet Security Association and Key Management Protocol (5)

**mobile-ip**—Mobile IP registration (434)

**nameserver**—IEN116 name service (obsolete, 42)

**netbios-dgm**—NetBIOS datagram service (138)

**netbios-ns**—NetBIOS name service (137)

**netbios-ss**—NetBIOS session service (139)

**non500-isakmp**—Internet Security Association and Key Management Protocol (45)

**ntp**—Network Time Protocol (123)

**pim-auto-rp**—PIM Auto-RP (496)

**rip**—Routing Information Protocol (router, in.routed, 52)

**snmp**—Simple Network Management Protocol (161)

**snmptrap**—SNMP Traps (162)

**sunrpc**—Sun Remote Procedure Call (111)

**syslog**—System Logger (514)

**tacacs**—TAC Access Control System (49)

**talk**—Talk (517)

**tftp**—Trivial File Transfer Protocol (69)

**time**—Time (37)

**who**—Who service (rwho, 513)

**xdmcp**—X Display Manager Control Protocol (177)

## Examples

This example shows how to configure an IPv4 ACL named acl-lab-01 with rules that deny all TCP and UDP traffic from the 10.23.0.0 and 192.168.37.0 networks to the 10.176.0.0 network and a final rule that permits all other IPv4 traffic:

```
n1000v# config t
n1000v(config)# ip access-list acl-lab-01
n1000v(config-acl)# deny tcp 10.23.0.0/16 10.176.0.0/16
n1000v(config-acl)# deny udp 10.23.0.0/16 10.176.0.0/16
n1000v(config-acl)# deny tcp 192.168.37.0/16 10.176.0.0/16
n1000v(config-acl)# deny udp 192.168.37.0/16 10.176.0.0/16
```

```
n1000v(config-acl)# permit ip any any
```

## Related Commands

| Command | Description |
|---|---|
| **ip access-list** | Configures an IPv4 ACL. |
| **permit (IPv4)** | Configures a permit rule in an IPv4 ACL. |
| **remark** | Configures a remark in an IPv4 ACL. |
| **show ip access-list** | Displays all IPv4 ACLs or one IPv4 ACL. |
| **statistics per-entry** | Enables collection of statistics for each entry in an ACL. |

# deny (MAC)

To create a MAC access control list (ACL)+ rule that denies traffic matching its conditions, use the **deny** command. To remove a rule, use the **no** form of this command.

[*sequence-number*] **deny** *source destination* [*protocol*] [**cos** *cos-value*] [**vlan** *VLAN-ID*]

**no deny** *source destination* [*protocol*] [**cos** *cos-value*] [**vlan** *VLAN-ID*]

**no** *sequence-number*

## Syntax Description

| | |
|---|---|
| *sequence-number* | (Optional) Sequence number of the **deny** 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.<br>A sequence number can be any integer between 1 and 4294967295.<br>By default, the first rule in an ACL has a sequence number of 10.<br>If you do not specify a sequence number, the device adds the rule to the end of the ACL and assigns a sequence number that is 10 greater than the sequence number of the preceding rule.<br>Use the **resequence** command to reassign sequence numbers to rules. |
| *source* | Source MAC addresses that the rule matches. For details about the methods that you can use to specify this argument, see “Source and Destination” in the “Usage Guidelines” section. |
| *destination* | Destination MAC addresses that the rule matches. For details about the methods that you can use to specify this argument, see “Source and Destination” in the “Usage Guidelines” section. |
| *protocol* | (Optional) Protocol number that the rule matches. Valid protocol numbers are 0x0 to 0xffff. For listings of valid protocol names, see “MAC Protocols” in the “Usage Guidelines” section. |
| **cos** *cos-value* | (Optional) Specifies that the rule matches only packets with an IEEE 802.1Q header that contains the Class of Service (CoS) value given in the *cos-value* argument. The *cos-value* argument can be an integer from 0 to 7. |
| **vlan** *VLAN-ID* | (Optional) Specifies that the rule matches only packets with an IEEE 802.1Q header that contains the VLAN ID given. The *VLAN-ID* argument can be an integer from 1 to 4094. |

## Defaults

A newly created MAC ACL contains no rules.

If you do not specify a sequence number, the device assigns the rule a sequence number that is 10 greater than the last rule in the ACL.

## Command Modes

MAC ACL configuration (**config-mac-acl**)

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

When the device applies a MAC ACL to a packet, it evaluates the packet with every rule in the ACL. The device enforces the first rule that has conditions that are satisfied by the packet. When the conditions of more than one rule are satisfied, the device enforces the rule with the lowest sequence number.

### Source and Destination

You can specify the *source* and *destination* arguments in one of two ways. In each rule, the method that you use to specify one of these arguments does not affect how you specify the other argument. When you configure a rule, use the following methods to specify the *source* and *destination* arguments:

- Address and mask—You can use a MAC address followed by a mask to specify a single address or a group of addresses. The syntax is as follows:

  ```
  MAC-address MAC-mask
  ```

  The following example specifies the *source* argument with the MAC address 00c0.4f03.0a72:

  ```
  n1000v(config-acl)# deny 00c0.4f03.0a72 0000.0000.0000 any
  ```

  The following example specifies the *destination* argument with a MAC address for all hosts with a MAC vendor code of 00603e:

  ```
  n1000v(config-acl)# deny any 0060.3e00.0000 0000.0000.0000
  ```

- Any address—You can use the **any** keyword to specify that a source or destination is any MAC address. For examples of the use of the **any** keyword, see the examples in this section. Each of the examples shows how to specify a source or destination by using the **any** keyword.

### MAC Protocols

The *protocol* argument can be the MAC protocol number or a keyword. The protocol number is a four-byte hexadecimal number prefixed with 0x. Valid protocol numbers are from 0x0 to 0xffff. Valid keywords are the following:

- **aarp**—Appletalk ARP (0x80f3)
- **appletalk**—Appletalk (0x809b)
- **decnet-iv**—DECnet Phase IV (0x6003)
- **diagnostic**—DEC Diagnostic Protocol (0x6005)
- **etype-6000**—EtherType 0x6000 (0x6000)
- **etype-8042**—EtherType 0x8042 (0x8042)
- **ip**—Internet Protocol v4 (0x0800)
- **lat**—DEC LAT (0x6004)
- **lavc-sca**—DEC LAVC, SCA (0x6007)
- **mop-console**—DEC MOP Remote console (0x6002)
- **mop-dump**—DEC MOP dump (0x6001)
- **vines-echo**—VINES Echo (0x0baf)

## Examples

This example shows how to configure a MAC ACL named mac-ip-filter with rules that permit any non-IPv4 traffic between two groups of MAC addresses:

```
n1000v# config t
n1000v(config)# mac access-list mac-ip-filter
n1000v(config-mac-acl)# deny 00c0.4f00.0000 0000.00ff.ffff 0060.3e00.0000 0000.00ff.ffff
ip
n1000v(config-mac-acl)# permit any any
```

## Related Commands

| Command | Description |
|---|---|
| **mac access-list** | Configures a MAC ACL. |
| **permit (MAC)** | Configures a deny rule in a MAC ACL. |
| **remark** | Configures a remark in an ACL. |
| **show mac access-list** | Displays all MAC ACLs or one MAC ACL. |
| **statistics per-entry** | Enables collection of statistics for each entry in an ACL. |

# description (interface)

To do add a description for the interface and save it in the running configuration, use the **description** command. To remove the interface description, use the **no** form of this command.

**description** *text*

**no description**

## Syntax Description

| | |
|---|---|
| *text* | Describes the interface. The maximum number of characters is 80. |

## Defaults

None

## Command Modes

Interface configuration (config-if)

## SupportedUserRoles

network-admin

## Command History

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

## Examples

This example shows how to add the description for the interface and save it in the running configuration.:

```
n1000v(config-if)# description Ethernet port 3 on module 1
```

This example shows how to remove the interface description.

```
n1000v(config-if)# no description Ethernet port 3 on module 1
```

## Related Commands

| Command | Description |
|---|---|
| **interface vethernet** | Creates a virtual Ethernet interface. |
| **interface port-channel** | Creates a port-channel interface. |
| **interface ethernet** | Creates an Ethernet interface. |
| **interface mgmt** | Configure the management interface. |
| **show interface** | Displays the interface status, including the description. |

# description (NetFlow)

To add a description to a flow record, flow monitor, or flow exporter, use the **description** command. To remove the description, use the **no** form of this command.

**description** *line*

**no description**

## Syntax Description

| | |
|---|---|
| *line* | Description of up to 63 characters. |

## Defaults

None

## Command Modes

NetFlow flow record (config-flow-record)

NetFlow flow exporter (config-flow-exporter)

Netflow flow monitor (config-flow-monitor)

## SupportedUserRoles

network-admin

## Command History

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

## Examples

This example shows how to add a description to a flow record:

```
n1000v(config)# flow record RecordTest
n1000v(config-flow-record)# description Ipv4flow
```

This example shows how to add a description to a flow exporter:

```
n1000v# config t
n1000v(config)# flow exporter ExportTest
n1000v(config-flow-exporter)# description ExportHamilton
```

This example shows how to add a description to a flow monitor:

```
n1000v# config t
n1000v(config)# flow monitor MonitorTest
n1000v(config-flow-monitor)# description Ipv4Monitor
```

## Related Commands

| Command | Description |
|---|---|
| **flow exporter** | Creates a Flexible NetFlow flow exporter. |
| **flow record** | Creates a Flexible NetFlow flow record. |

| Command | Description |
|---|---|
| **flow monitor** | Creates a Flexible NetFlow flow monitor. |
| **show flow exporter** | Displays information about the NetFlow flow exporter. |
| **show flow record** | Displays information about NetFlow flow records. |
| **show flow monitor** | Displays information about the NetFlow flow monitor. |

# description (QoS)

To add a description to a QoS class map, policy map, use the **description** command. To remove the description, use the **no** form of this command.

**description** *text*

**no description** *text*

## Syntax Description

| | |
|---|---|
| *text* | Description, of up to 200 characters, for the class map or policy map. |

## Defaults

None

## Command Modes

QoS class map configuration (**config-cmap-qo**s)
QoS policy map configuration (**config-pmap-qos**)

## SupportedUserRoles

network-admin

## Command History

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

## Examples

This example shows how to add a description to a policy map:

```
n1000v(config)# policy-map my_policy1
n1000v(config-pmap)# description this policy applies to input packets
n1000v(config-pmap)#
```

## Related Commands

| Command | Description |
|---|---|
| **class-map** | Creates or modifies a class map. |
| **policy-map** | Creates or modifies a policy map. |

# description (role)

To add a description for a role, use the **description** command. To remove a description of a role, use the **no** form of this command.

**description** *string*

**no description**

## Syntax Description

| | |
|---|---|
| *string* | Describes the role. The string can include spaces. |

## Defaults

None

## Command Modes

Role configuration (**config-role**)

## SupportedUserRoles

network-admin

## Command History

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

## Examples

This example shows how to add a description to a role:

```
n1000v(config-role)# description admin
```

This example shows how to remove the role description:

```
n1000v(config-role)# no description admin
```

## Related Commands

| Command | Description |
|---|---|
| **username** | Creates a user account including the assignment of a role. |
| **show role** | Displays a role configuration. |

# description (SPAN)

To add a description to a SPAN session, use the **description** command. To remove the description, use the **no** form of this command.

**description** *string*

**no description**

## Syntax Description

| | |
|---|---|
| *string* | Specifies a description of up to 32 alphanumeric characters. |

## Defaults

Blank (no description)

## Command Modes

SPAN monitor configuration (config-monitor)

## SupportedUserRoles

network-admin

## Command History

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

## Examples

This example shows how to add a description to a SPAN session:

```
n1000v# config t
n1000v(config)# monitor session 8
n1000v(config-monitor)# description span_session_8a
n1000v(config-monitor)#
```

This example shows how to remove a description from a SPAN session:

```
n1000v# config t
n1000v(config)# monitor session 8
n1000v(config)# no description span_session_8a
n1000v(config-monitor)#
```

## Related Commands

| Command | Description |
|---|---|
| **show monitor session** | Displays session information. |

# destination (NetFlow)

To add a destination IP address or VRF to a NetFlow flow exporter, use the **destination** command. To remove the IP address or VRF, use the **no** form of this command.

**destination** {*ipaddr* | *ipv6addr*} [**use-vrf** *vrf_name*]

**no destination**

## Syntax Description

| | |
|---|---|
| *ipaddr* | Destination IP address for collector. |
| *ipv6addr* | Destination IPv6 address for collector. |
| **use-vrf** *vrf_name* | (Optional) Optional VRF label. |

## Defaults

None

## Command Modes

NetFlow flow exporter configuration (config-flow-exporter)

## SupportedUserRoles

network-admin

## Command History

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

## Examples

This example shows how to add a destination IP address to a Netflow flow exporter:

```
n1000v# config t
n1000v(config)# flow exporter ExportTest
n1000v(config-flow-exporter)# destination 192.0.2.1
```

This example shows how to remove the IP address from a flow exporter:

```
n1000v# config t
n1000v(config)# flow exporter ExportTest
n1000v(config-flow-exporter)# no destination 192.0.2.1
```

## Related Commands

| Command | Description |
|---|---|
| **flow exporter** | Creates a Flexible NetFlow flow exporter. |
| **flow record** | Creates a Flexible NetFlow flow record. |
| **flow monitor** | Creates a Flexible NetFlow flow monitor. |
| **show flow exporter** | Displays information about the NetFlow flow exporter. |
| **show flow record** | Displays information about NetFlow flow records. |
| **show flow monitor** | Displays information about the NetFlow flow monitor. |

# destination interface (SPAN)

To configures the port(s) in a SPAN session to act as destination(s) for copied source packets, use the **destination interface** command. To remove the destination interface, use the **no** form of this command.

**destination interface** *type number(s)_or_range*

**no destination interface** *type number(s)_or_range*

## Syntax Description

| | |
|---|---|
| **ethernet** *slot/port_or_range* | Designates the SPAN destination(s) Ethernet interface(s). |
| **port-channel** *number(s)_or_range* | Designates the SPAN destination(s) port channel(s). |
| **vethernet** *number(s)_or_range* | Designates the SPAN destination(s) virtual Ethernet interface(s). |

## Defaults

None

## Command Modes

SPAN monitor configuration (**config-monitor**)

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

SPAN destination ports must already be configured as either access or trunk ports.

SPAN sessions are created in the shut state by default.

When you create a SPAN session that already exists, any additional configuration is added to that session. To make sure the session is cleared of any previous configuration, you can delete the session first using the command, **no monitor session**.

## Examples

This example shows how to configure ethernet interfaces 2/5 and 3/7 in a SPAN session to act as destination(s) for copied source packets:

```
n1000v# config t
n1000v(config)# monitor session 8
n1000v(config-monitor)# destination interface ethernet 2/5, ethernet 3/7
```

This example shows how to remove the SPAN configuration from destination interface ethernet 2/5:

```
n1000v# config t
n1000v(config)# monitor session 8
n1000v(config-monitor)# no destination interface ethernet 2/5
```

## Related Commands

| Command | Description |
|---|---|
| **show interface** | Displays the interface trunking configuration for the specified destination interface. |
| **show monitor** | Displays Ethernet SPAN information. |
| **monitor session** | Starts the specified SPAN monitor session(s). |

# dir

To display the contents of a directory or file, use the **dir** command.

**dir** [**bootflash: | debug: | log: | volatile:**]

## Syntax Description

| | |
|---|---|
| **bootflash:** | (Optional) Directory or filename. |
| **debug:** | (Optional) Directory or filename on expansion flash. |
| **log:** | (Optional) Directory or filename on log flash. |
| **volatile:** | (Optional) Directory or filename on volatile flash. |

## 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

Use the **pwd** command to identify the directory you are currently working in.

Use the **cd** command to change the directory you are currently working in.

## Examples

This example shows how to display the contents of the bootflash: directory

```
n1000v# dir bootflash:
```

## Related Commands

| Command | Description |
|---|---|
| **cd** | Changes the current working directory. |
| **pwd** | Displays the current working directory. |

# domain id

To assign a domain-id, use the **domain id** command. To remove a domain-id, use the **no** form of this command.

**domain id** *number*

**no domain id**

## Syntax Description

| | |
|---|---|
| *number* | Specifies the domain-id number. The allowable domain IDs are 1 to 4095. |

## Defaults

None

## Command Modes

Domain configuration (config-svs-domain)

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

During installation of the Cisco Nexus 1000V the setup utility prompts you to configure a domain, including the domain ID and control and packet VLANs.

## Examples

This example shows how to assign a domain id:

```
n1000v# config t
n1000v(config)# sve-domain
n1000v(config-svs-domain)# domain-id number 32
n1000v(config-svs-domain)#
```

This example shows how to remove the domain-id:

```
n1000v# config t
n1000v(config)# sve-domain
n1000v(config-svs-domain)# no domain-id number 32
n1000v(config-svs-domain)#
```

## Related Commands

| Command | Description |
|---|---|
| **show svs domain** | Displays domain configuration. |

# dscp (NetFlow)

To add a differentiated services codepoint (DSCP) to a NetFlow flow exporter, use the **dscp** command. To remove the DSCP, use the **no** form of this command.

**dscp** *value*

**no dscp**

## Syntax Description

| | |
|---|---|
| *value* | Specifies a DSCP between 0 and 63. |

## Defaults

None

## Command Modes

NetFlow flow exporter configuration (config-flow-exporter)

## SupportedUserRoles

network-admin

## Command History

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

## Examples

This example shows how to configure DSCP for a NetFlow flow exporter:

```
n1000v# config t
n1000v(config)# flow exporter ExportTest
n1000v(config-flow-exporter)# dscp 2
n1000v(config-flow-exporter)#
```

This example shows how to remove DSCP from the NetFlow flow exporter:

```
n1000v# config t
n1000v(config)# flow exporter ExportTest
n1000v(config-flow-exporter)# no dscp 2
n1000v(config-flow-exporter)#
```

## Related Commands

| Command | Description |
|---|---|
| **flow exporter** | Creates a Flexible NetFlow flow exporter. |
| **flow record** | Creates a Flexible NetFlow flow record. |
| **flow monitor** | Creates a Flexible NetFlow flow monitor. |
| **show flow exporter** | Displays information about the NetFlow flow exporter. |
| **show flow record** | Displays information about NetFlow flow records. |
| **show flow monitor** | Displays information about the NetFlow flow monitor. |

# duplex

To set the duplex mode for an interface as full, half, or autonegotiate, use the **duplex** command. To revert back to the default setting, use the **no** form of this command.

**duplex** {**full** | **half** | **auto**}

**no duplex** [**full** | **half** | **auto**]

## Syntax Description

| | |
|---|---|
| **full** | Specifies full-duplex mode for the interface. |
| **half** | Specifies half-duplex mode for the interface. |
| **auto** | Sets the duplex mode on the interface to autonegotiate with the connecting port. |

## Defaults

None

## Command Modes

Interface configuration (config-if)

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

When you use the no form of this command, an argument (such as full, half, or auto) is optional. To return to the default duplex setting, you can use either of the following commands (if, for example, the setting had been changed to full):

```
n1000v(config-if)# no duplex

n1000v(config-if)# no duplex full
```

## Examples

This example shows how to set the Ethernet port 1 on the module in slot 3 to full-duplex mode:

```
n1000v# config t
n1000v(config)# interface ethernet 2/1
n1000v(config-if)# duplex full
```

This example shows how to revert to the default duplex setting for the Ethernet port 1 on the module in slot 3:

```
n1000v# config t
n1000v(config)# interface ethernet 2/1
n1000v(config-if)# no duplex
```

**Related Commands**

| Command | Description |
|---|---|
| **interface** | Specifies the interface that you are configuring. |
| **speed** | Sets the speed for the port channel interface. |
| **show interface** | Displays the interface status, which includes the speed and duplex mode parameters. |

# 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. |
| *text* | (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. |

## 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. |

# 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 modee:

```
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

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. |

# errdisable recovery cause

To enable an application to automatically recover an interface from the error-disabled (errdisable), 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

| 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)#
```

**Related Commands**

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

# errdisable recovery interval

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

**errdisable recovery interval** *interval*

## Syntax Description

| | |
|---|---|
| *interval* | 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:

```
n1000v(config)# errdisable recovery interval 32
n1000v(config)#
```

## Related Commands

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

# 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

| | |
|---|---|
| *flow_id* | 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

| 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

This example shows how to add ERSPAN ID 51 to the session configuration and save it in the running configuration:

```
n1000v# config t
n1000v(config)# monitor session type erspan-source
n1000v(config-erspan-src)# erspan_id 51
n1000v(config-erspan-src)#
```

## Related Commands

| 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 |
|---|---|
| **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

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.<br>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 *time* 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)#
```

**Related Commands**

| Command | Description |
|---|---|
| **show terminal** | Displays the terminal configuration, including the timeout value. |
| **show users** | Displays the currently active user sessions. |

# 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. |

# 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

| | |
|---|---|
| *name* | 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

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

## Examples

This example shows how to add the flow exporter called Exportv9 and save it in the running configuration:

```
n1000v# config t
n1000v(config)# flow monitor MonitorTest
n1000v(config-flow-monitor)# exporter Exportv9
n1000v(config-flow-monitor)#
```

This example shows how to remove the flow exporter called Exportv9:

```
n1000v# config t
n1000v(config)# flow monitor MonitorTest
n1000v(config-flow-monitor)# no exporter Exportv9
n1000v(config-flow-monitor)#
```

## Related Commands

| 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 |
|---|---|
| **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 specifed monitor and saves it in the running configuration. |

# F Commands

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

## filter vlan

To configure a filter from the source VLANs for a specified Switch Port Analyzer (SPAN) session, use the **filter vlan** command. To remove the filter, use the **no** form of this command.

**filter vlan** {*number* | *range*}

**no filter vlan** {*number* | *range*}

**Syntax Description**

| | |
|---|---|
| *number* | Number of the VLAN associated with this filter. |
| *range* | Range of VLANs associated with this filter. |

**Defaults**

None

**Command Modes**

CLI monitor configuration (config-monitor)

**SupportedUserRoles**

network-admin

**Command History**

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

**Examples**

This example shows how to configure the filter for VLAN IDs, 3, 4, 5, and 7:

```
n1000v# config t
n1000v(config)# monitor session 3
n1000v(config-monitor)# filter vlan 3-5, 7
n1000v(config-monitor)#
```

This example shows how to remove the filter for VLAN ID 7:

```
n1000v# config t
n1000v(config)# monitor session 3
n1000v(config-monitor)# no filter vlan 7
n1000v(config-monitor)#
```

## Related Commands

| Command | Description |
|---|---|
| **monitor session** | Creates a session with the given session number and places you in the CLI monitor configuration mode to further configure the session. |
| **description** | For the specified SPAN session, adds a description. |
| **source** | For the specified session, configures the sources and the direction of traffic to monitor. |
| **destination interface** | Configures the ports, for the specified session, to act as destinations for copied source packets. |
| **no shut** | Enables the SPAN session. |
| **interface ethernet** | Places you in CLI interface configuration mode for the specified interface. |
| **switchport trunk allowed vlan** | For the specified interface, configures the range of VLANs that are allowed on the interface. |
| **show interface ethernet** | Displays the interface trunking configuration for the selected slot and port or range of ports. |

# find

To find filenames beginning with a character string, use the **find** command.

**find** *filename-prefix*

## Syntax Description

| | |
|---|---|
| *filename-prefix* | First part or all of a filename. The filename prefix is case sensitive. |

## Defaults

None

## Command Modes

Any

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

The **find** command searches all subdirectories under the current working directory. You can use the **cd** and **pwd** commands to navigate to the starting directory.

## Examples

This example shows how to display filenames beginning with ospf:

```
n1000v# find ospf
/usr/bin/find: ./lost+found: Permission denied
./ospf-gr.cfg
./ospfgrconfig
./ospf-gr.conf
```

## Related Commands

| Command | Description |
|---|---|
| **cd** | Changes the current working directory. |
| **pwd** | Displays the name of the current working directory. |

# flow exporter

To create or modify a Flexible NetFlow flow exporter defining where and how Flow Records are exported to the NetFlow Collector Server, use the **flow exporter** command. To remove a flow exporter, use the **no** form of this command.

**flow exporter** *exporter-name*

**no flow exporter** *exporter-name*

## Syntax Description

| | |
|---|---|
| *exporter-name* | Name of the flow exporter that is created or modified. |

## Defaults

Flow exporters are not present in the configuration until you create them.

## Command Modes

Global configuration (config)

## SupportedUserRoles

network-admin

## Command History

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

## Examples

The following example shows how to create and configure FLOW-EXPORTER-1:

```
n1000v(config)# flow exporter FLOW-EXPORTER-1
n1000v(config-flow-exporter)# description located in Pahrump, NV
n1000v(config-flow-exporter)# destination A.B.C.D
n1000v(config-flow-monitor)# dscp 32
n1000v(config-flow-monitor)# source mgmt0
n1000v(config-flow-monitor)# transport udp 59
n1000v(config-flow-monitor)# version 9
```

The following example shows how to remove FLOW-EXPORTER-1:

```
n1000v(config)# no flow exporter FLOW-EXPORTER-1
n1000v(config)#
```

## Related Commands

| Command | Description |
|---|---|
| **clear flow exporter** | Clears the flow monitor. |
| **show flow exporter** | Displays flow monitor status and statistics. |
| **description** | Adds a description to a flow record, flow monitor, or flow exporter. |
| **destination** | Adds a destination IP address to a NetFlow flow exporter. |
| **dscp** | Adds a differentiated services codepoint (DSCP) to a flow exporter. |

| Command | Description |
|---|---|
| **source mgmt** | Adds the management interface to a flow exporter designating it as the source for NetFlow flow records. |
| **transport udp** | Adds a destination UDP port used to reach the NetFlow collector to a flow exporter. |
| **version 9** | Designates NetFlow export version 9 in the NetFlow exporter. |

# flow monitor

To create a Flexible NetFlow flow monitor, or to modify an existing Flexible NetFlow flow monitor, and enter Flexible NetFlow flow monitor configuration mode, use the **flow monitor** command. To remove a Flexible NetFlow flow monitor, use the **no** form of this command.

**flow monitor** *monitor-name*

**no flow monitor** *monitor-name*

## Syntax Description

| | |
|---|---|
| *monitor-name* | Name of the flow monitor that is created or modified. |

## Defaults

Flow monitors are not present in the configuration until you create them.

## Command Modes

Global configuration (config)

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

Flow monitors are the Flexible NetFlow component that is applied to interfaces to perform network traffic monitoring. Flow monitors consist of a record that you add to the flow monitor after you create the flow monitor, and a cache that is automatically created at the time the flow monitor is applied to the first interface. Flow data is collected from the network traffic during the monitoring process based on the key and non-key fields in the record which is configured for the flow monitor and stored in the flow monitor cache.

Once you enter the flow monitor configuration mode, the prompt changes to the following:

```
n1000v(config-flow-monitor)#
```

Within the flow monitor configuration mode, the following keywords and arguments are available to configure the flow monitor:

- **cache—**Specifies the cache size, from 256 to 16384 entries.
- **description** *description*—Provides a description for this flow monitor; maximum of 63 characters.
- **exit**—Exits from the current configuration mode.
- **exporter** *name*—Specifies the name of an exporter to export records.
- **no**—Negates a command or sets its defaults.
- **record** {*record-name* | **netflow ipv4** *collection-type* | **netflow-original**}—Specifies a flow record to use as follows:
  - *record-name*—Name of a record.

  - **netflow ipv4** *collection-type*—Specifies the traditional IPv4 NetFlow collection schemes as follows:

    **original-input**—Specifies the traditional IPv4 input NetFlow.

    **original-output**—Specifies the traditional IPv4 output NetFlow

    **protocol-port**—Specifies the protocol and ports aggregation scheme.
  - **netflow-original**—Specifies the traditional IPv4 input NetFlow with origin autonomous systems.
- **timeout** {**active** | **inactive**}—Specifies a flow timeout period as follows:
  - **active**—Specifies an active or long timeout in the range of 60 to 4092 seconds.
  - **inactive**—Specifies an inactive or normal timeout in the range of 15 to 4092 seconds.

The **netflow-original** and **original-input** keywords are the same and are equivalent to the following commands:

- **match ipv4 source address**
- **match ipv4 destination address**
- **match ip tos**
- **match ip protocol**
- **match transport source-port**
- **match transport destination-port**
- **match interface input**
- **collect counter bytes**
- **collect counter packet**
- **collect timestamp sys-uptime first**
- **collect timestamp sys-uptime last**
- **collect interface output**
- **collect transport tcp flags**

The **original-output** keywords are the same as **original-input** keywords except for the following:

- **match interface output** (instead of match interface input)
- **collect interface input** (instead of collect interface output)

## Examples

The following examples creates and configures a flow monitor named FLOW-MONITOR-1:

```
n1000v(config)# flow monitor FLOW-MONITOR-1
n1000v(config-flow-monitor)# description monitor location las vegas, NV
n1000v(config-flow-monitor)# exporter exporter-name1
n1000v(config-flow-monitor)# record test-record
n1000v(config-flow-monitor)# netflow ipv4 original-input
```

## Related Commands

| Command | Description |
|---|---|
| **clear flow monitor** | Clears the flow monitor. |
| **show flow monitor** | Displays flow monitor status and statistics. |

# flow record

To create a Flexible NetFlow flow record, or to modify an existing Flexible NetFlow flow record, and enter Flexible NetFlow flow record configuration mode, use the **flow record** command. To remove a Flexible NetFlow flow record, use the **no** form of this command.

**flow record** *record-name*

**no flow record** *record-name*

## Syntax Description

| | |
|---|---|
| *record-name* | Name of the flow record that is created or modified. |

## Defaults

Flow records are not present in the configuration until you create them.

## Command Modes

Global configuration (config)

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

Flexible NetFlow uses key and non-key fields just as original NetFlow does to create and populate flows in a cache. In Flexible NetFlow a combination of key and non-key fields is called a record. Original NetFlow and Flexible NetFlow both use the values in key fields in IP datagrams, such as the IP source or destination address and the source or destination transport protocol port, as the criteria for determining when a new flow must be created in the cache while network traffic is being monitored. A flow is defined as a stream of packets between a given source and a given destination. New flows are created whenever NetFlow analyzes a packet that has a unique value in one of the key fields.

Once you enter the flow record configuration mode, the prompt changes to the following:

```
n1000v(config-flow-record)#
```

Within the flow record configuration mode, the following keywords and arguments are available to configure the flow record:

- **collect**—Specifies a non-key field. See the **collect** command for additional information.
- **description** *description*—Provides a description for this flow record; maximum of 63 characters.
- **exit**—Exits from the current configuration mode.
- **match**—Specifies a key field. See the **match** command for additional information.
- **no**—Negates a command or sets its defaults.

Cisco NX-OS enables the following match fields by default when you create a flow record:

- **match interface input**

- **match interface output**
- **match flow direction**

## Examples

The following example creates a flow record named FLOW-RECORD-1, and enters Flexible NetFlow flow record configuration mode:

```
n1000v(config)# flow record FLOW-RECORD-1
n1000v(config-flow-record)#
```

## Related Commands

| Command | Description |
|---|---|
| **clear flow monitor** | Clears the flow monitor. |
| **flow monitor** | Creates a flow monitor. |
| **show flow monitor** | Displays flow monitor status and statistics. |

# format

To format an external Flash device to erase the contents and restore it to its factory-shipped state, use the **format** command.

**format** *filesystem***:**

## Syntax Description

| | |
|---|---|
| *filesystem***:** | Name of the file system. The valid values are **bootflash, logflash, slot0**, **usb1**, or **usb2**. |

## Defaults

None

## 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 format an external Flash device:

```
n1000v# format slot0:
```

## Related Commands

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

# from (table map)

To specify a set of mappings of input field values to output field values in a table map, use the **from** command.

**from** *source-value* **to** *dest-value*

## Syntax Description

| | |
|---|---|
| *source-value* | Specifies the source value in the range from 0 to 63. |
| *dest-value* | Specifies the destination value in the range from 0 to 63. |

## Defaults

None

## Command Modes

Table map configuration

## SupportedUserRoles

network-admin

## Command History

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

## Examples

This example shows how to create a mapping from three source values to the corresponding destination values:

```
n1000v(config)# table-map cir-markdown-map
n1000v(config-tmap)# from 0 to 7
n1000v(config-tmap)# from 1 to 6
n1000v(config-tmap)# from 2 to 5
```

## Related Commands

| Command | Description |
|---|---|
| **show table-map** | Displays table maps. |

# G Commands

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

## gunzip

To uncompress a compressed file, use the **gunzip** command.

**gunzip** *filename*

**Syntax Description**

| | |
|---|---|
| *filename* | Name of a file. The filename is case sensitive. |

**Defaults**

None

**Command Modes**

Any

**SupportedUserRoles**

network-admin

**Command History**

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

**Usage Guidelines**

The compressed filename must have the .gz extension.

You do not have to enter the .gz extension as part of the filename.

The Cisco NX-OS software uses Lempel-Ziv 1977 (LZ77) coding for compression.

**Examples**

This example shows how to uncompress a compressed file:

```
n1000v# gunzip run_cnfg.cfg
```

**Related Commands**

| Command | Description |
|---|---|
| **dir** | Displays the directory contents. |
| **gzip** | Compresses a file. |

# gzip

To compress a file, use the **gzip** command.

**gzip** *filename*

## Syntax Description

| | |
|---|---|
| *filename* | Name of a file. The filename is case sensitive. |

## Defaults

None

## Command Modes

Any

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

After you use this command, the file is replaced with the compressed filename that has the .gz extension. The Cisco NX-OS software uses Lempel-Ziv 1977 (LZ77) coding for compression.

## Examples

This example shows how to compress a file:

```
n1000v# gzip run_cnfg.cfg
```

## Related Commands

| Command | Description |
|---|---|
| **dir** | Displays the directory contents. |
| **gunzip** | Uncompresses a compressed file. |

# I Commands

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

## inherit port-profile

To add the inherited configuration to the new port profile as a default configuration, use the **inherit port-profile** command. To remove the inherited policies, use the **no** form of this command.

**inherit port-profile** *name*

**no inherit port-profile**

**Syntax Description**

| | |
|---|---|
| *name* | Name for the port profile whose policies are inherited. The name can be up to 80 characters and must be unique for each port profile on the Cisco Nexus 1000V. |

**Defaults**

None

**Command Modes**

Port profie configuration (config-port-prof)

**SupportedUserRoles**

network-admin

**Command History**

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

**Usage Guidelines**

Any inherited setting, except the port profile type, can be changed using the CLI.

When you use the **no** form of the command, the port profile settings are returned to the defaults, except for the port profile type and any settings that were explicitly configured independent of those inherited.

## Examples

This example shows how to designate *AllAccess1* as the port profile whose policies will be inherited:

```
n1000v# config t
n1000v(config)# port-profile type vethernet AllAccess2
n1000v(config-port-prof)# inherit port-profile AllAccess1
```

This example shows how to remove the inherited policies:

```
n1000v# config t
n1000v(config)# port-profile type vethernet AllAccess2
n1000v(config-port-prof)# no port-profile inherit
```

## Related Commands

| Command | Description |
|---|---|
| **show port-profile** | Displays the port profile inherited by the current port profile. |
| **port-profile** | Places you into port profile configuration mode and defines the port profile. |

# install certificate

To install a certificate, use the **install certificate** command. To remove a certificate, use the **no** form of this command.

**install certificate** {**bootflash:** | **default**}

**no install certificate**

## Syntax Description

| | |
|---|---|
| **bootflash:** | Specifies the path. |
| **default** | Specifies the default certificate. |

## Defaults

No certificate is installed.

## Command Modes

SVS connection configuration (config-svs-conn)

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

Only one SVS connection can be created.

## Examples

This example shows how to install a certificate:

```
n1000v# configure terminal
n1000v(config)# svs connect s1
n1000v(config-svs-conn)# install certificate default
n1000v(config-svs-conn)#
```

This example shows how to remove a certificate:

```
n1000v# configure terminal
n1000v(config)# svs connect s1
n1000v(config-svs-conn)# no install certificate default
n1000v(config-svs-conn)#
```

## Related Commands

| Command | Description |
|---|---|
| **show svs** | Displays SVS information. |

# install license bootflash:

To install a license file(s) on a VSM, use the **install license bootflash:** command.

**install license bootflash:** *filename*

## Syntax Description

| | |
|---|---|
| *filename* | (Optional) Specify a name for the license file. If you do not specify a name, then the license is installed using the default name. |

## 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

- You must first uninstall an evaluation license if one is present on your VSM. For more information, see the *Cisco Nexus 1000V License Configuration Guide, Release 4.0(4)SV1(3)*.
- You must be logged in to the active VSM console port.
- This command installs the license file using the name, license_file.lic. You can specify a different name.
- If you are installing multiple licenses for the same VSM, also called license stacking, make sure that each license key file name is unique.
- Repeat this procedure for each additional license file you are installing, or stacking, on the VSM.

## Examples

This example shows how to install a license to bootflash on a VSM and then display the installed file:

```
n1000v# install license bootflash:license_file.lic
Installing license ..done
n1000v# show license file license.lic
SERVER this_host ANY
VENDOR cisco
INCREMENT NEXUS1000V_LAN_SERVICES_PKG cisco 1.0 permanent 1 \
        HOSTID=VDH=1575337335122974806 \
        NOTICE="<LicFileID>license.lic</LicFileID><LicLineID>0</LicLineID> \
        <PAK>PAK12345678</PAK>" SIGN=3AF5C2D26E1A
n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **show license file** | Verifies the license installation by displaying the license configured for the VSM. |
| **clear license** | Uninstalls a license, that is, removes it from the VSM and shuts down the Ethernet interfaces to the VEMs covered by that license. |
| **logging level license** | Designates the level of severity at which license messages should be logged. |
| **install license** | Installs a license file(s) on a VSM |
| **svs license transfer src-vem** | Transfers licenses from a source VEM to another VEM, or to the VSM pool of available licenses. |

# interface control

To configure the control interface and enter interface configuration mode, use the **interface control** command.

**interface control0**

## Syntax Description

This command has no arguments or keywords.

## Defaults

None

## Command Modes

Global configuration (config)
Interface configuration (config-if)

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

## Examples

This example shows how to enter the interface configuration mode to configure the control interface:

```
n1000v(config)# interface control0
n1000v(config-if)#
```

## Related Commands

| Command | Description |
|---|---|
| **show interface control0** | Displays information about the traffic on the control interface. |

# interface ethernet

To configure an Ethernet interface, use the **interface ethernet** command.

**interface ethernet** *slot/port*

## Syntax Description

| | |
|---|---|
| *slot/port* | Specifies the slot number and port number for the Ethernet interface. |

## Defaults

None

## Command Modes

Global configuration (config)

Interface configuration (config-if)

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

## Examples

This example shows how to access the interface command mode for configuring the Ethernet interface on slot 2, port 1:

```
n1000v# config t
n1000v(config)# interface ethernet 2/1
n1000v(config-if)#
```

## Related Commands

| Command | Description |
|---|---|
| **show interface ethernet** *slot/port* | Displays information about the Ethernet interface. |

# interface loopback

To create and configure a loopback interface, use the **interface loopback** command. To remove a loopback interface, use the **no** form of this command.

**interface loopback** *number*

**no interface loopback** *number*

## Syntax Description

| | |
|---|---|
| *number* | Identifying interface number; valid values are from 0 to 1023. |

## Defaults

None

## Command Modes

Global configuration (config)
Interface configuration (config-if)

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

## Examples

This example shows how to create a loopback interface:

```
n1000v(config)# interface loopback 50
n1000v(config-if)#
```

## Related Commands

| Command | Description |
|---|---|
| **show interface loopback** | Displays information about the traffic on the specified loopback interface. |

# interface mgmt

To configure the management interface and enter interface configuration mode, use the **interface management** command.

**interface mgmt0**

## Syntax Description

This command has no arguments or keywords.

## Defaults

None

## Command Modes

Global configuration (config)
Interface configuration (config-if)

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

## Examples

This example shows how to enter the interface configuration mode to configure the management interface:

```
n1000v(config)# interface mgmt0
n1000v(config-if)#
```

## Related Commands

| Command | Description |
|---|---|
| **show interface mgmt0** | Displays information about the traffic on the management interface. |

# interface port-channel

To create a port-channel interface and enter interface configuration mode, use the **interface port-channel** command. To remove a logical port-channel interface or subinterface, use the **no** form of this command.

**interface port-channel** *channel-number*

**no interface port-channel** *channel-number*

## Syntax Description

| | |
|---|---|
| *channel-number* | Channel number that is assigned to this port-channel logical interface. The range of valid values is from 1 to 4096. |

## Defaults

None

## Command Modes

Global configuration (config)
Interface configuration (config-if)

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

Use the **interface port-channel** command to create or delete port-channel groups and to enter the interface configuration mode for the port channel.

A port can belong to only one channel group.

When you use the **interface port-channel** command, follow these guidelines:

- If you are using CDP, you must configure it only on the physical interface and not on the port-channel interface.
- If you do not assign a static MAC address on the port-channel interface, a MAC address is automatically assigned. If you assign a static MAC address and then later remove it, the MAC address is automatically assigned.
- The MAC address of the port channel is the address of the first operational port added to the channel group. If this first-added port is removed from the channel, the MAC address comes from the next operational port added, if there is one.

## Examples

This example shows how to create a port-channel group interface with channel-group number 50:

```
n1000v(config)# interface port-channel 50
n1000v(config-if)#
```

**Related Commands**

| Command | Description |
|---|---|
| **show interface port-channel** | Displays information on traffic on the specified port-channel interface. |
| **show port-channel summary** | Displays information on the port channels. |

# interface vethernet

To create a virtual Ethernet interface and enter interface configuration mode, use the **interface vethernet** command. To remove a virtual Ethernet interface, use the **no** form of this command.

**interface vethernet** *number*

**no interface vethernet** *number*

## Syntax Description

| | |
|---|---|
| *number* | Identifying interface number; valid values are from 1 to 1048575. |

## Defaults

None

## Command Modes

Global configuration (config)
Interface configuration (config-if)

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

## Examples

This example shows how to create a virtual Ethernet interface:

```
n1000v(config)# interface vethernet 50
n1000v(config-if)#
```

## Related Commands

| Command | Description |
|---|---|
| **show interface vethernet** *number* | Displays information about the traffic on the specified virtual Ethernet interface. |

# ip access-list

To create an access list, use the **ip access-list** command. To remove an access list, use the **no** form of this command.

**ip access-list** {*name* | **match-local-traffic**}

**no ip access-list** {*name* | **match-local-traffic**}

## Syntax Description

| | |
|---|---|
| *name* | List name. |
| **match-local-traffic** | Enables access list matching for locally generated traffic. |

## Defaults

No access list exists.

## 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 an access list:

```
n1000v(config)# configure terminal
n1000v(config)# ip access-list acl1
n1000v(config)#
```

## Related Commands

| Command | Description |
|---|---|
| **show access-lists** | Displays access lists. |

# ip address

To create an IP route, use the **ip address** command. To remove an IP address, use the **no** form of this command.

**ip address** {*address mask* | *prefix*} {*next-hop* | *next-hop-prefix* | *interface-type interface-number*} [**tag** *tag-value* | *preference*]

**no ip address** {*address mask* | *prefix*} {*next-hop* | *next-hop-prefix* | *interface-type interface-number*} [**secondary** | **tag** *tag-value* | *preference*]

## Syntax Description

| | |
|---|---|
| *address* | IP address, in format A.B.C.D. |
| *mask* | IP network mask, in format A.B.C.D. |
| *prefix* | IP prefix and network mask length, in format A.B.C.D/LEN. |
| *next-hop* | IP next-hop address, in format A.B.C.D. |
| *next-hop-prefix* | IP next-hop prefix in format A.B.C.D./LEN. |
| *interface-type* | Interface type. |
| *interface-number* | Interface or subinterface number. |
| **secondary** | (Optional) Configures additional IP addresses on the interface. |
| **tag** | (Optional) Specifies a supply tag. |
| *tag-value* | Supply tag value. The range of valid values is 0 to 4294967295. The default is 0. |
| *preference* | (Optional) Route preference. |

## 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 an IP address:

```
n1000v(config)# configure terminal
n1000v(config)# ip address 209.165.200.225 255.255.255.224 x
n1000v(config)#
```

**Related Commands**

| Command | Description |
|---|---|
| **show ip interface A.B.C.D.** | Displays interfaces for local IP addresses. |

# ip arp inspection limit

To set the rate limit of ARP requests and responses, use the **ip arp inspection limit** command. To remove this setting, use the **no** form of this command. To set the rate limit to its default, use the **default** form of this command.

**ip arp inspection limit** {**rate** *pps* [**burst interval** *bint*] | **none**}

**no ip arp inspection limit** {**rate** *pps* [**burst interval** *bint*] | **none**}

**default ip arp inspection limit** {**rate** *pps* [**burst interval** *bint*] | **none**}

## Syntax Description

| | |
|---|---|
| **rate** *pps* | Specifies the rate limit in packets per second. |
| **burst interval** | (Optional) Specifies the burst interval. |
| *bint* | (Optional) Burst interval in seconds. |
| **none** | Specifies that there is no limit. |

## Defaults

None

## Command Modes

Inteface configuration (config-if)
Port profile configuration (config-port-prof)

## SupportedUserRoles

network-admin

## Command History

| Release | Modification |
|---|---|
| 4.0(4)SV1(2) | This command was introduced. |

## Examples

This example shows how to set the rate limit of ARP requests to 20 pps:

```
n1000v(config)# ip arp inspection limit rate 20
```

This example shows how to remove the configuration:

```
n1000v(config)# no arp inspection limit rate 20
```

## Related Commands

| Command | Description |
|---|---|
| **show ip arp inspection interface interface** | Displays the trust state and the ARP packet rate for a specified interface. |

# ip arp inspection trust

To configure a Layer 2 interface as a trusted ARP interface, use the **ip arp inspection trust** command. To configure a Layer 2 interface as an untrusted ARP interface, use the **no** form of this command. To return a Layer 2 interface to its default, use the **default** form of this command.

**ip arp inspection trust**

**no ip arp inspection trust**

**default ip arp inspection trust**

## Syntax Description

This command has no arguments or keywords.

## Defaults

By default, all interfaces are untrusted ARP interfaces.

## Command Modes

Interface configuration (config-if)
Port profile configuration (config-port-prof)

## SupportedUserRoles

network-admin

## Command History

| Release | Modification |
|---|---|
| 4.0(4)SV1(2) | This command was introduced. |

## Usage Guidelines

You can configure only Layer 2 virtual Ethernet interfaces as trusted ARP interfaces.

## Examples

This example shows how to configure a Layer 2 interface as a trusted ARP interface:

```
n1000v# configure terminal
n1000v(config)# interface vethernet 2
n1000v(config-if)# ip arp inspection trust
n1000v(config-if)#
```

## Related Commands

| Command | Description |
|---|---|
| **show ip arp inspection interface** | Displays the trust state and the ARP packet rate for a specified interface. |

# ip arp inspection validate

To enable additional Dynamic ARP Inspection (DAI) validation, use the **ip arp inspection validate** command. To disable additional DAI, use the **no** form of this command.

**ip arp inspection validate {dst-mac [ip] [src-mac] | ip [dst-mac] [src-mac] | src-mac [dst-mac] [ip]}**

**no ip arp inspection validate {dst-mac [ip] [src-mac] | ip [dst-mac] [src-mac] | src-mac [dst-mac] [ip]}**

## Syntax Description

| | |
|---|---|
| **dst-mac** | (Optional) Enables validation of the destination MAC address in the Ethernet header against the target MAC address in the ARP body for ARP responses. The device classifies packets with different MAC addresses as invalid and drops them. |
| **ip** | (Optional) Enables validation of the ARP body for invalid and unexpected IP addresses. Addresses include 0.0.0.0, 255.255.255.255, and all IP multicast addresses. The device checks the sender IP addresses in all ARP requests and responses and checks the target IP addresses only in ARP responses. |
| **src-mac** | (Optional) Enables validation of the source MAC address in the Ethernet header against the sender MAC address in the ARP body for ARP requests and responses. The devices classifies packets with different MAC addresses as invalid and drops them. |

## Defaults

None

## Command Modes

Global configuration (config)

## SupportedUserRoles

network-admin

## Command History

| Release | Modification |
|---|---|
| 4.0(4)SV1(2) | This command was introduced. |

## Usage Guidelines

You must specify at least one keyword. If you specify more than one keyword, the order is irrelevant.

## Examples

This example shows how to enable additional DAI validation:

```
n1000v# configure terminal
n1000v(config)# ip arp inspection validate src-mac dst-mac ip
n1000v(config)#
```

**Related Commands**

| Command | Description |
|---|---|
| **show ip arp inspection** | Displays the DAI configuration status. |

# ip arp inspection vlan

To enable Dynamic ARP Inspection (DAI) for a list of VLANs, use the **ip arp inspection vlan** command. To disable DAI for a list of VLANs, use the **no** form of this command.

**ip arp inspection vlan** *vlan-list*

**no ip arp inspection vlan** *vlan-list*

## Syntax Description

| | |
|---|---|
| *vlan-list* | VLANs on which DAI is active. The *vlan-list* argument allows you to specify a single VLAN ID, a range of VLAN IDs, or comma-separated IDs and ranges (see the “Examples” section). Valid VLAN IDs are from 1 to 4096. |

## Defaults

None

## Command Modes

Global configuration (config)

## SupportedUserRoles

network-admin

## Command History

| Release | Modification |
|---|---|
| 4.0(4)SV1(2) | This command was introduced. |

## Usage Guidelines

By default, the device does not log packets inspected by DAI.

## Examples

This example shows how to enable DAI on VLANs 13, 15, and 17 through 23:

```
n1000v# configure terminal
n1000v(config)# ip arp inspection vlan 13,15,17-23
n1000v(config)#
```

## Related Commands

| Command | Description |
|---|---|
| **ip arp inspection validate** | Enables additional DAI validation. |
| **show ip arp inspection vlan** | Displays the DAI status for a specified list of VLANs. |

# ip dscp

To specify the IP DSCP value for the packets in the ERSPAN traffic and save it in the running configuration, use the **ip dscp** command.

**ip dscp** *dscp_value*

## Syntax Description

| | |
|---|---|
| *dscp_value* | DSCP value, in seconds, for ERSPAN traffic packets. The value can range from 0–63. |

## Defaults

The default DSCP value is 0.

## Command Modes

CLI ERSPAN source configuration (config-erspan-src)

## SupportedUserRoles

network-admin

## Command History

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

## Examples

This example shows how to specify the DSCP value of 25 for packets in the ERSPAN traffic:

```
n1000v# config t
n1000v(config)# monitor session 3 type erspa
n1000v(config-erspan-src)# ip dscp 25
n1000v(config-erspan-src)#
```

## Related Commands

| Command | Description |
|---|---|
| **monitor session type erspan-source** | Creates a session with the given session number and places you in the CLI ERSPAN source configuration mode. |
| **description** | For the specified ERSPAN session, adds a description and saves it in the running configuration. |
| **source** | Configures the sources and the direction of traffic to monitor for the specified session, and saves the information in the running configuration. |
| **filter vlan** | Configures the VLANs, VLAN lists, or VLAN ranges to be monitored for the specified session; and saves this information in the running configuration. |
| **destination ip** | Configures the IP address of the host to which the encapsulated traffic is sent and saves it in the running configuration. |
| **ip ttl** | Specifies the IP time-to-live value for the packets in the ERSPAN traffic, and saves it in the running configuration. |

| Command | Description |
|---|---|
| **ip prec** | Specifies the IP precedence value for the packets in the ERSPAN traffic, and saves it in the running configuration. |
| **mtu** | Specifies a maximum transmission unit (MTU) size for the ERSPAN traffic, and saves it in the running configuration. |
| **erspan-id** | Adds an ERSPAN ID to the session configuration and saves it in the running configuration. |
| **no shut** | Enables the ERSPAN session and saves it in the running configuration. |
| **show monitor session** *session_id* | Displays the ERSPAN session configuration as it exists in the running configuration. |

# ip dhcp snooping

To globally enable DHCP snooping on the device, use the **ip dhcp snooping** command. To globally disable DHCP snooping, use the **no** form of this command.

**ip dhcp snooping**

**no ip dhcp snooping**

## Syntax Description

This command has no arguments or keywords.

## Defaults

By default, DHCP snooping is globally disabled.

## Command Modes

Global configuration (config)

## SupportedUserRoles

network-admin

## Command History

| Release | Modification |
|---|---|
| 4.0(4)SV1(2) | This command was introduced. |

## Usage Guidelines

To use this command, you must enable the DHCP snooping feature (see the **feature dhcp** command).

The device preserves DHCP snooping configuration when you disable DHCP snooping with the **no ip dhcp snooping** command.

## Examples

This example shows how to globally enable DHCP snooping:

```
n1000v# configure terminal
n1000v(config)# ip dhcp snooping
n1000v(config)#
```

## Related Commands

| Command | Description |
|---|---|
| **feature dhcp** | Enables the DHCP snooping feature on the device. |
| **ip dhcp snooping trust** | Configures an interface as a trusted source of DHCP messages. |
| **ip dhcp snooping vlan** | Enables DHCP snooping on the specified VLANs. |
| **show ip dhcp snooping** | Displays general information about DHCP snooping. |

# ip dhcp snooping limit rate

To configure a rate limit for DHCP packets that are received on a port, use the **ip dhcp snooping limit rate** command. To remove the rate limit for DHCP packets that are received on each port, use the **no** form of this command.

**ip dhcp snooping limit rate** *rate*

**no ip dhcp snooping limit rate**

## Syntax Description

| | |
|---|---|
| *rate* | Number of DHCP packets per second. The range is from 1 to 2048. |

## Defaults

None

## Command Modes

Interface configuration (config-if)
Port profile configuration (config-port-prof)

## SupportedUserRoles

network-admin

## Command History

| Release | Modification |
|---|---|
| 4.0(4)SV1(2) | This command was introduced. |

## Examples

This example shows how to limit the rate of DHCP packets to 30 pps on vEthernet interface 3:

```
n1000v# configure terminal
n1000v(config)# interface vethernet 3
n1000v(config-if)# ip dhcp snooping limit rate 30
```

## Related Commands

| Command | Description |
|---|---|
| **show ip dhcp snooping** | Displays general information about DHCP snooping. |

# ip dhcp snooping trust

To configure an interface as a trusted source of DHCP messages, use the **ip dhcp snooping trust** command. To configure an interface as an untrusted source of DHCP messages, use the **no** form of this command.

**ip dhcp snooping trust**

**no ip dhcp snooping trust**

## Syntax Description

This command has no arguments or keywords.

## Defaults

By default, no interface is a trusted source of DHCP messages.

## Command Modes

Interface configuration (config-if)
Port profile configuration (config-port-prof)

## SupportedUserRoles

network-admin

## Command History

| Release | Modification |
|---|---|
| 4.0(4)SV1(2) | This command was introduced. |

## Usage Guidelines

You can configure DHCP trust on the following types of interfaces:

- Layer 2 vEthernet interfaces
- Private VLAN interfaces

## Examples

This example shows how to configure an interface as a trusted source of DHCP messages:

```
n1000v# configure terminal
n1000v(config)# interface vethernet 2
n1000v(config-if)# ip dhcp snooping trust
n1000v(config-if)#
```

## Related Commands

| Command | Description |
|---|---|
| **ip dhcp snooping** | Globally enables DHCP snooping on the device. |
| **ip dhcp snooping verify mac-address** | Enables MAC address verification as part of DHCP snooping. |
| **ip dhcp snooping vlan** | Enables DHCP snooping on the specified VLANs. |
| **show ip dhcp snooping** | Displays general information about DHCP snooping. |

# ip dhcp snooping verify mac-address

To enable DHCP snooping MAC address verification, use the **ip dhcp snooping verify mac-address** command. To disable MAC address verification, use the **no** form of this command.

**ip dhcp snooping verify mac-address**

**no ip dhcp snooping verify mac-address**

## Syntax Description

This command has no arguments or keywords.

## 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 enable DHCP snooping MAC address verification:

```
n1000v(config)# config t
n1000v(config)# ip dhcp snooping verify mac-address
n1000v(config)#
```

This example shows how to disable DHCP snooping MAC address verification:

```
n1000v(config)# config t
n1000v(config)# no ip dhcp snooping verify mac-address
n1000v(config)#
```

## Related Commands

| Command | Description |
|---|---|
| **show running-config dhcp** | Displays the DHCP snooping configuration. |
| **ip dhcp snooping** | Enables DHCP snooping globally. |
| **ip dhcp snooping vlan** | Enables DHCP snooping on the VLANs specified by *vlan-list*. |
| **clear ip dhcp snooping binding** | Clears dynamically added entries from the DHCP snooping binding database. |

| Command | Description |
|---|---|
| **ip dhcp snooping trust** | Configures the interface as a trusted interface for DHCP snooping. |
| **ip dhcp snooping limit rate** | Configures the DHCP limit rate. |

# ip dhcp snooping vlan

To enable DHCP snooping on one or more VLANs, use the **ip dhcp snooping vlan** command. To disable DHCP snooping on one or more VLANs, use the **no** form of this command.

**ip dhcp snooping vlan** *vlan-list*

**no ip dhcp snooping vlan** *vlan-list*

## Syntax Description

| | |
|---|---|
| *vlan-list* | Range of VLANs on which to enable DHCP snooping. The *vlan-list* argument allows you to specify a single VLAN ID, a range of VLAN IDs, or comma-separated IDs and ranges (see the "Examples" section). Valid VLAN IDs are from 1 to 4096. |

## Defaults

By default, DHCP snooping is not enabled on any VLAN.

## Command Modes

Global configuration (config)

## SupportedUserRoles

network-admin

## Command History

| Release | Modification |
|---|---|
| 4.0(4)SV1(2) | This command was introduced. |

## Examples

This example shows how to enable DHCP snooping on VLANs 100, 200, and 250 through 252:

```
n1000v# configure terminal
n1000v(config)# ip dhcp snooping vlan 100,200,250-252
n1000v(config)#
```

## Related Commands

| Command | Description |
|---|---|
| **ip dhcp snooping** | Globally enables DHCP snooping on the device. |
| **ip dhcp snooping trust** | Configures an interface as a trusted source of DHCP messages. |
| **show ip dhcp snooping** | Displays general information about DHCP snooping. |

# ip directed-broadcast

To enable IP directed broadcast, use the **ip directed-broadcast** command. To disable IP directed broadcast, use the **no** form of this command.

**ip directed-broadcast**

**no ip directed-broadcast**

## Syntax Description

This command has no arguments or keywords.

## Defaults

None

## Command Modes

Interface configuration (config-if)

## SupportedUserRoles

network-admin

## Command History

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

## Examples

This example shows how to enable IP directed broadcast:

```
n1000v# configure terminal
n1000v(config)# interface mgmt 0
n1000v(config-if)# ip directed-broadcast
n1000v(config-if)#
```

## Related Commands

| Command | Description |
|---|---|
| **show ip interface** | Displays IP interface information. |

# ip flow monitor

To enable a Flexible NetFlow flow monitor for traffic that the router is receiving or forwarding, use the **ip flow monitor** interface configuration mode command. To disable a Flexible NetFlow flow monitor, use the **no** form of this command.

**ip flow monitor** *monitor-name* {**input** | **output**}

**no ip flow monitor** *monitor-name* {**input** | **output**}

## Syntax Description

| | |
|---|---|
| *monitor-name* | Name of a flow monitor that you previously configured. |
| **input** | Monitors traffic that the routers is receiving on the interface. |
| **output** | Monitors traffic that the routers is transmitting on the interface. |

## Defaults

Disabled.

## Command Modes

Interface configuration (config-if)

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

You must have already created a flow monitor by using the **flow monitor** command before you can apply the flow monitor to an interface with the **ip flow monitor** command to enable traffic monitoring with Flexible NetFlow.

## Examples

The following example enables a flow monitor for monitoring input traffic:

```
n1000v(config)# interface ethernet0/0
n1000v(config-if)# ip flow monitor FLOW-MONITOR-1 input
```

The following example enables a flow monitor for monitoring output traffic:

```
n1000v(config)# interface ethernet0/0
n1000v(config-if)# ip flow monitor FLOW-MONITOR-1 output
```

The following example enables the same flow monitor on the same interface for monitoring input and output traffic:

```
n1000v(config)# interface ethernet0/0
n1000v(config-if)# ip flow monitor FLOW-MONITOR-1 input
n1000v(config-if)# ip flow monitor FLOW-MONITOR-1 output
```

The following example enables two different flow monitors on the same interface for monitoring input and output traffic:

```
n1000v(config)# interface ethernet0/0
n1000v(config-if)# ip flow monitor FLOW-MONITOR-1 input
n1000v(config-if)# ip flow monitor FLOW-MONITOR-2 output
```

The following example enables the same flow monitor on two different interfaces for monitoring input and output traffic:

```
n1000v(config)# interface ethernet0/0
n1000v(config-if)# ip flow monitor FLOW-MONITOR-1 input
n1000v(config)# interface ethernet1/0
n1000v(config-if)# ip flow monitor FLOW-MONITOR-1 output
```

The following example enables two different flow monitors on two different interfaces for monitoring input and output traffic:

```
n1000v(config)# interface ethernet0/0
n1000v(config-if)# ip flow monitor FLOW-MONITOR-1 input
n1000v(config)# interface ethernet1/0
n1000v(config-if)# ip flow monitor FLOW-MONITOR-2 output
```

## Related Commands

| Command | Description |
|---|---|
| **flow exporter** | Creates a flow exporter. |
| **flow monitor** | Creates a flow monitor. |
| **flow record** | Creates a flow record. |

# ip igmp snooping (Global)

To enable IGMP snooping, use the **ip igmp snooping** command. To disable IGMP snooping, use the **no** form of this command.

**ip igmp snooping**

**no ip igmp snooping**

## Syntax Description

This command has no arguments or keywords.

## Defaults

Enabled

## Command Modes

Global configuration (config)

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

If the global configuration of IGMP snooping is disabled, then all VLANs are treated as disabled, whether they are enabled or not.

## Examples

This example shows how to enable IGMP snooping:

```
n1000v(config)# ip igmp snooping
n1000v(config)#
```

This example shows how to disable IGMP snooping:

```
n1000v(config)# no ip igmp snooping
n1000v(config)#
```

## Related Commands

| Command | Description |
|---|---|
| **show ip igmp snooping** | Displays IGMP snooping information. |

# ip igmp snooping (VLAN)

To enable IGMP snooping on a VLAN interface, use the **ip igmp snooping** command. To disable IGMP snooping on the interface, use the **no** form of this command.

**ip igmp snooping**

**no ip igmp snooping**

## Syntax Description

This command has no arguments or keywords.

## Defaults

Enabled

## Command Modes

VLAN configuration (config-vlan)

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

If the global configuration of IGMP snooping is disabled, then all VLANs are treated as disabled, whether they are enabled or not.

## Examples

This example shows how to enable IGMP snooping on a VLAN interface:

```
n1000v(config)# vlan 1
n1000v(config-vlan)# ip igmp snooping
n1000v(config-vlan)#
```

This example shows how to disable IGMP snooping on a VLAN interface:

```
n1000v(config)# vlan 1
n1000v(config-vlan)# no ip igmp snooping
n1000v(config-vlan)#
```

## Related Commands

| Command | Description |
|---|---|
| **show ip igmp snooping** | Displays IGMP snooping information. |

# ip igmp snooping explicit-tracking

To enable tracking of IGMPv3 membership reports from individual hosts for each port on a per-VLAN basis, use the **ip igmp snooping explicit-tracking** command. To disable tracking, use the **no** form of this command.

**ip igmp snooping explicit-tracking**

**no ip igmp snooping explicit-tracking**

## Syntax Description

This command has no arguments or keywords.

## Defaults

Enabled

## Command Modes

VLAN configuration (config-vlan)

## SupportedUserRoles

network-admin

## Command History

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

## Examples

This example shows how to enable tracking of IGMPv3 membership reports on a VLAN interface:

```
n1000v(config)# vlan 1
n1000v(config-vlan)# ip igmp snooping explicit-tracking
n1000v(config-vlan)#
```

This example shows how to disable IGMP snooping on a VLAN interface:

```
n1000v(config)# vlan 1
n1000v(config-vlan)# no ip igmp snooping explicit-tracking
n1000v(config-vlan)#
```

## Related Commands

| Command | Description |
|---|---|
| **show ip igmp snooping** | Displays IGMP snooping information. |

# ip igmp snooping fast-leave

To enable support of IGMPv2 hosts that cannot be explicitly tracked because of the host report suppression mechanism of the IGMPv2 protocol, use the **ip igmp snooping fast-leave** command. To disable support of IGMPv2 hosts, use the **no** form of this command.

**ip igmp snooping fast-leave**

**no ip igmp snooping fast-leave**

## Syntax Description

This command has no arguments or keywords.

## Defaults

Disabled

## Command Modes

VLAN configuration (config-vlan)

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

When you enable fast leave, the IGMP software assumes that no more than one host is present on each VLAN port.

## Examples

This example shows how to enable support of IGMPv2 hosts:

```
n1000v(config)# vlan 1
n1000v(config-vlan)# ip igmp snooping fast-leave
n1000v(config-vlan)#
```

This example shows how to disable support of IGMPv2 hosts:

```
n1000v(config)# vlan 1
n1000v(config-vlan)# no ip igmp snooping fast-leave
n1000v(config-vlan)#
```

## Related Commands

| Command | Description |
|---|---|
| **show ip igmp snooping** | Displays IGMP snooping information. |

# ip igmp snooping last-member-query-interval

To configure a query interval in which the software removes a group, use the **ip igmp snooping last-member-query-interval** command. To reset the query interval to the default, use the **no** form of this command.

**ip igmp snooping last-member-query-interval** *interval*

**no ip igmp snooping last-member-query-interval** [*interval*]

## Syntax Description

| | |
|---|---|
| *interval* | Query interval in seconds. The range is from 1 to 25. The default is 1. |

## Defaults

The query interval is 1.

## Command Modes

VLAN configuration (config-vlan)

## SupportedUserRoles

network-admin

## Command History

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

## Examples

This example shows how to configure a query interval in which the software removes a group:

```
n1000v(config)# vlan 1
n1000v(config-vlan)# ip igmp snooping last-member-query-interval 3
n1000v(config-vlan)#
```

This example shows how to reset a query interval to the default:

```
n1000v(config)# vlan 1
n1000v(config-vlan)# no ip igmp snooping last-member-query-interval
n1000v(config-vlan)#
```

## Related Commands

| Command | Description |
|---|---|
| **show ip igmp snooping** | Displays IGMP snooping information. |

# ip igmp snooping mrouter interface

To configure a static connection to a multicast router, use the **ip igmp snooping mrouter interface** command. To remove the static connection, use the **no** form of this command.

**ip igmp snooping mrouter interface** *if-type if-number*

**no ip igmp snooping mrouter interface** *if-type if-number*

## Syntax Description

| | |
|---|---|
| *if-type* | Interface type. For more information, use the question mark (?) online help function. |
| *if-number* | Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function. |

## Defaults

None

## Command Modes

VLAN configuration (config-vlan)

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

The interface to the router must be in the selected VLAN.

## Examples

This example shows how to configure a static connection to a multicast router:

```
n1000v(config)# vlan 1
n1000v(config-vlan)# ip igmp snooping mrouter interface ethernet 2/1
n1000v(config-vlan)#
```

This example shows how to remove a static connection to a multicast router:

```
n1000v(config)# vlan 1
n1000v(config-vlan)# no ip igmp snooping mrouter interface ethernet 2/1
n1000v(config-vlan)#
```

## Related Commands

| Command | Description |
|---|---|
| **show ip igmp snooping** | Displays IGMP snooping information. |

# ip igmp snooping report-suppression (Global)

To configure IGMPv1 or GMPv2 report suppression for VLANs, use the **ip igmp snooping report-suppression** command. To remove IGMPv1 or GMPv2 report suppression, use the **no** form of this command.

**ip igmp snooping report-suppression**

**no ip igmp snooping report-suppression**

## Syntax Description

This command has no arguments or keywords.

## Defaults

Enabled

## 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 IGMPv1 or GMPv2 report suppression for VLANs:

```
n1000v(config)# ip igmp snooping report-suppression
```

This example shows how to remove IGMPv1 or GMPv2 report suppression:

```
n1000v(config)# no ip igmp snooping report-suppression
```

## Related Commands

| Command | Description |
|---|---|
| **show ip igmp snooping** | Displays IGMP snooping information. |

# ip igmp snooping report-suppression (VLAN)

To configure IGMPv1 or GMPv2 report suppression for VLANs, use the **ip igmp snooping report-suppression** command. To remove IGMPv1 or GMPv2 report suppression, use the **no** form of this command.

**ip igmp snooping report-suppression**

**no ip igmp snooping report-suppression**

## Syntax Description

This command has no arguments or keywords.

## Defaults

Enabled

## Command Modes

VLAN configuration (config-vlan)

## SupportedUserRoles

network-admin

## Command History

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

## Examples

This example shows how to configure IGMPv1 or GMPv2 report suppression for VLANs:

```
n1000v(config)# vlan 1
n1000v(config-vlan)# ip igmp snooping report-suppression
n1000v(config-vlan)#
```

This example shows how to remove IGMPv1 or GMPv2 report suppression:

```
n1000v(config)# vlan 1
n1000v(config-vlan)# no ip igmp snooping report-suppression
n1000v(config-vlan)#
```

## Related Commands

| Command | Description |
|---|---|
| **show ip igmp snooping** | Displays IGMP snooping information. |

# ip igmp snooping static-group

To configure a Layer 2 port of a VLAN as a static member of a multicast group, use the **ip igmp snooping static-group** command. To remove the static member, use the **no** form of this command.

**ip igmp snooping static-group** *group* **interface** *if-type if-number*

**no ip igmp snooping static-group** *group* **interface** *if-type if-number*

## Syntax Description

| | |
|---|---|
| *group* | Group IP address. |
| **interface** | Specifies interface for static group. |
| *if-type* | Interface type. For more information, use the question mark (?) online help function. |
| *if-number* | Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function. |

## Defaults

None

## Command Modes

VLAN configuration (config-vlan)

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

You can specify the interface by the type and the number, such as ethernet slot/port.

## Examples

This example shows how to configure a static member of a multicast group:

```
n1000v(config)# vlan 1
n1000v(config-vlan)# ip igmp snooping static-group 230.0.0.1 interface ethernet 2/1
n1000v(config-vlan)#
```

This example shows how to remove a static member of a multicast group:

```
n1000v(config)# vlan 1
n1000v(config-vlan)# no ip igmp snooping static-group 230.0.0.1 interface ethernet 2/1
n1000v(config-vlan)#
```

## Related Commands

| Command | Description |
|---|---|
| **show ip igmp snooping** | Displays IGMP snooping information. |

# ip igmp snooping v3-report-suppression (Global)

To configure IGMPv3 report suppression and proxy reporting, use the **ip igmp snooping v3-report-suppression** command. To remove IGMPv3 report suppression and proxy reporting, use the **no** form of this command.

**ip igmp snooping v3-report-suppression**

**no ip igmp snooping v3-report-suppression**

## 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. |

## Examples

This example shows how to configure IGMPv3 report suppression and proxy reporting:

```
n1000v(config)# ip igmp snooping v3-report-suppression
```

This example shows how to remove IGMPv3 report suppression and proxy reporting:

```
n1000v(config)# no ip igmp snooping v3-report-suppression
```

## Related Commands

| Command | Description |
|---|---|
| **show ip igmp snooping** | Displays IGMP snooping information. |

# ip igmp snooping v3-report-suppression (VLAN)

To configure IGMPv3 report suppression and proxy reporting for VLANs, use the **ip igmp snooping v3-report-suppression** command. To remove IGMPv3 report suppression, use the **no** form of this command.

**ip igmp snooping v3-report-suppression**

**no ip igmp snooping v3-report-suppression**

## Syntax Description

This command has no arguments or keywords.

## Defaults

Disabled

## Command Modes

VLAN configuration (config-vlan)

## SupportedUserRoles

network-admin

## Command History

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

## Examples

This example shows how to configure IGMPv3 report suppression and proxy reporting for VLANs:

```
n1000v(config)# vlan 1
n1000v(config-vlan)# ip igmp snooping v3-report-suppression
n1000v(config-vlan)#
```

This example shows how to remove IGMPv3 report suppression and proxy reporting for VLANs:

```
n1000v(config)# vlan 1
n1000v(config-vlan)# no ip igmp snooping v3-report-suppression
n1000v(config-vlan)#
```

## Related Commands

| Command | Description |
|---|---|
| **show ip igmp snooping** | Displays IGMP snooping information. |

# ip port access-group

To create an access group, use the **ip port access-group** command. To remove access control, use the **no** form of this command.

**ip port access-group** *name* {**in** | **out**}

**no ip port access-group** *name* {**in** | **out**}

**Related Commands**

| | |
|---|---|
| *name* | Group name. The range of valid values is 1 to 64. |
| **in** | Specifies inbound traffic. |
| **out** | Specifies outbound traffic. |

**Defaults**

No access group exists.

**Command Modes**

Port profile configuration (config-port-prof)

**SupportedUserRoles**

network-admin

**Command History**

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

**Usage Guidelines**

You create an access group to specify in an ACL the access control of packets.

**Examples**

This example shows how to create an access group:

```
n1000v# configure terminal
n1000v(config)# port-profile 1
n1000v(config-port-prof)# ip port access-group group1 in
n1000v(config-port-prof)#
```

**Related Commands**

| Command | Description |
|---|---|
| **show access-lists** | Displays access lists. |
| **show port-profile** | Displays port profile information. |

# ip prec

To specify the IP precedence value for the packets in the ERSPAN traffic and save it in the running configuration, use the **ip prec** command.

**ip prec** *precedence_value*

## SyntaxDescription

| | |
|---|---|
| *precedence_value* | IP precedence value for the ERSPAN traffic packets. The range is 0–7. |

## Defaults

None

## Command Modes

CLI ERSPAN source configuration (config-monitor-erspan-src)

## SupportedUserRoles

network-admin

## Command History

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

## Examples

This example shows how to specify the IP precedence value as 1 for the packets in the ERSPAN traffic and save it in the running configuration:

```
n1000v# config t
n1000v(config)# monitor session 3 type erspa
n1000v(config-erspan-src)# destination ip 10.54.54.1
n1000v(config-monitor-erspan-src)# ip prec 1
n1000v(config-monitor-erspan-src)#
```

## Related Commands

| Command | Description |
|---|---|
| **monitor session type erspan-source** | Creates a session with the given session number and places you in the CLI ERSPAN source configuration mode. |
| **description** | For the specified ERSPAN session, adds a description and saves it in the running configuration. |
| **source** | Configures the sources and the direction of traffic to monitor for the specified session, and saves the information in the running configuration. |
| **filter vlan** | Configures the VLANs, VLAN lists, or VLAN ranges to be monitored for the specified session; and saves this information in the running configuration. |
| **destination ip** | Configures the IP address of the host to which the encapsulated traffic is sent and saves it in the running configuration. |

| Command | Description |
|---|---|
| **ip ttl** | Specifies the IP time-to-live value for the packets in the ERSPAN traffic, and saves it in the running configuration. |
| **ip dscp** | Specifies the IP DSCP value for the packets in the ERSPAN traffic, and saves it in the running configuration. |
| **mtu** | Specifies a maximum transmission unit (MTU) size for the ERSPAN traffic, and saves it in the running configuration. |
| **erspan-id** | Adds an ERSPAN ID to the session configuration and saves it in the running configuration. |
| **no shut** | Enables the ERSPAN session and saves it in the running configuration. |
| **show monitor session session_id** | Displays the ERSPAN session configuration as it exists in the running configuration. |

# ip source binding

To create a static IP source entry for a Layer 2 vEthernet interface, use the **ip source binding** command. To disable the static IP source entry, use the **no** form of this command.

**ip source binding** *IP-address MAC-address* **vlan** *vlan-id* **interface vethernet** *interface-number*

**no ip source binding** *IP-address MAC-address* **vlan** *vlan-id* **interface vethernet** *interface-number*

## Syntax Description

| | |
|---|---|
| *IP-address* | IPv4 address to be used on the specified interface. Valid entries are in dotted-decimal format. |
| *MAC-address* | MAC address to be used on the specified interface. Valid entries are in dotted-hexadecimal format. |
| **vlan** *vlan-id* | Specifies the VLAN associated with the IP source entry. |
| **interface vethernet** *interface-number* | Specifies the Layer 2 vEthernet interface associated with the static IP entry. |

## Defaults

None

## Command Modes

Global configuration (config)

## SupportedUserRoles

network-admin

## Command History

| Release | Modification |
|---|---|
| 4.0(4)SV1(2) | This command was introduced. |

## Usage Guidelines

By default, there are no static IP source entries.

## Examples

This example shows how to create a static IP source entry that is associated with VLAN 100 on vEthernet interface 3:

```
n1000v# configure terminal
n1000v(config)# ip source binding 10.5.22.7 001f.28bd.0013 vlan 100 interface vethernet 3
n1000v(config)#
```

## Related Commands

| Command | Description |
|---|---|
| **ip verify source dhcp-snooping-vlan** | Enables IP Source Guard on an interface. |
| **show ip verify source** | Displays IP-to-MAC address bindings. |

# ip source-route

To enable an IP source route, use the **ip source-route** command. To disable an IP source route, use the **no** form of this command.

**ip source-route**

**no ip source-route**

## Syntax Description

This command has no arguments or keywords.

## 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 enable an IP source route:

```
n1000v(config)# configure terminal
n1000v(config)# ip source-route
n1000v(config)#
```

## Related Commands

| Command | Description |
|---|---|
| **show ip static-route** | Displays static routes. |

# ip ttl

To specify the IP time-to-live value for the packets in the Encapsulated Remote Switch Port Analyzer (ERSPAN) traffic and save it in the running configuration, use the **ip ttl** command.

**ip ttl** *ttl_value*

## Syntax Description

| | |
|---|---|
| *ttl_value* | Time-to-live value, in seconds, from 1–255. |

## Defaults

None

## Command Modes

CLI ERSPAN source configuration (config-monitor-erspan-src)

## SupportedUserRoles

network-admin

## Command History

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

## Examples

This example shows how to specify the time-to-live value of 64 seconds for packets in the ERSPAN traffic:

```
n1000v# config t
n1000v(config)# monitor session 3 type erspa
n1000v(config-erspan-src)# destination ip 10.54.54.1
nn1000v(config-monitor-erspan-src)# ip ttl 64
n1000v(config-monitor-erspan-src)#
```

## Related Commands

| Command | Description |
|---|---|
| **monitor session type erspan-source** | Creates a session with the given session number and places you in the CLI ERSPAN source configuration mode. |
| **description** | For the specified ERSPAN session, adds a description and saves it in the running configuration. |
| **source** | Configures the sources and the direction of traffic to monitor for the specified session, and saves the information in the running configuration. |
| **filter vlan** | Configures the VLANs, VLAN lists, or VLAN ranges to be monitored for the specified session; and saves this information in the running configuration. |
| **destination ip** | Configures the IP address of the host to which the encapsulated traffic is sent and saves it in the running configuration. |

| Command | Description |
|---|---|
| **ip prec** | Specifies the IP precedence value for the packets in the ERSPAN traffic, and saves it in the running configuration. |
| **ip dscp** | Specifies the IP DSCP value for the packets in the ERSPAN traffic, and saves it in the running configuration. |
| **mtu** | Specifies a maximum transmission unit (MTU) size for the ERSPAN traffic, and saves it in the running configuration. |
| **erspan-id** | Adds an ERSPAN ID to the session configuration and saves it in the running configuration. |
| **no shut** | Enables the ERSPAN session and saves it in the running configuration. |
| **show monitor session session_id** | Displays the ERSPAN session configuration as it exists in the running configuration. |

# ip verify source dhcp-snooping-vlan

To enable IP Source Guard on a Layer 2 vEthernet interface, use the **ip verify source dhcp-snooping-vlan** command. To disable IP Source Guard on an interface, use the **no** form of this command.

**ip verify source dhcp-snooping-vlan**

**no ip verify source dhcp-snooping-vlan**

## Syntax Description

This command has no arguments or keywords.

## Defaults

None

## Command Modes

Interface configuration (config-if)
Port profile configuration (config-port-prof)

## SupportedUserRoles

network-admin

## Command History

| Release | Modification |
|---|---|
| 4.0(4)SV1(2) | This command was introduced. |

## Usage Guidelines

By default, IP Source Guard is not enabled on any interface.

## Examples

This example shows how to enable IP Source Guard on an interface:

```
n1000v# configure terminal
n1000v(config)# interface vethernet 2
n1000v(config-if)# ip verify source dhcp-snooping-vlan
n1000v(config-if)#
```

## Related Commands

| Command | Description |
|---|---|
| **ip source binding** | Creates a static IP source entry for the specified vEthernet interface. |
| **show ip verify source** | Displays IP-to-MAC address bindings. |

# L Commands

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

## limit-resource erspan-flow-id minimum

To configure the range of allowed ERSPAN flow IDs, use the **limit-resource erspan-flow-id minimum** command. To remove the configuration, use the **no** form of this command.

**limit-resource erspan-flow-id minimum** *min-val* **maximum** *max-val*

**no limit-resource erspan-flow-id**

**Syntax Description**

| | |
|---|---|
| *min-val* | Minimum ERSPAN flow ID number allowed. |
| **maximum** | Configures the maximum range value for ERSPAN flow IDs. |
| *max-val* | Maximum ERSPAN flow ID number allowed. |

**Defaults**

None

**Command Modes**

Global configuration (config)

**SupportedUserRoles**

network-admin

**Command History**

| Release | Modification |
|---|---|
| 4.0(4)SV1(2) | This command was introduced. |

**Examples**

This example shows how to restrice the range of allowed ERSPAN flow IDs to the range, 1-80:

```
n1000v(config)# limit-resource erspan-flow-id minimum 1 maximum 80
```

This example shows how to restore the default range of ERSPAN flow IDs:

```
n1000v(config)# no limit-resource erspan-flow-id
```

## Related Commands

| Command | Description |
|---|---|
| **erspan-id** | Adds an ERSPAN ID (1-1023) to the session configuration and saves it in the running configuration. |
| **show monitor session** | Displays the ERSPAN session configuration as it exists in the running configuration. |
| **monitor session** | Creates an ERSPAN session. |

# line console

To enter console configuration mode, use the **line console** command. To exit console configuration mode, use the **no** form of this command.

**line console**

**no line console**

## Syntax Description

This command has no arguments or keywords.

## 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 enter console configuration mode:

```
n1000v# configure terminal
n1000v(config)# line console
n1000v(config-console)#
```

# line vty

To enter line configuration mode, use the **line vty** command. To exit line configuration mode, use the **no** form of this command.

**line vty**

**no line vty**

## Syntax Description

This command has no arguments or keywords.

## 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 enter line configuration mode:

```
n1000v# configure terminal
n1000v(config)# line vty
n1000v(config-line)#
```

# logging console

Use the **logging console** command to enable logging messages to the console session.

To disable logging messages to the console session, use the **no** form of this command.

**logging console** [*severity-level*]

**no logging console**

## Syntax Description

*severity-level* — The severity level at which you want messages to be logged. When you set a severity level, for example 4, then messages at that severity level and higher (0 through 4) are logged.

Severity levels are as follows:

| Level | Designation | Definition |
|---|---|---|
| 0 | Emergency | System unusable *__the highest level__* |
| 1 | Alert | Immediate action needed |
| 2 | Critical | Critical condition—default level |
| 3 | Error | Error condition |
| 4 | Warning | Warning condition |
| 5 | Notification | Normal but significant condition |
| 6 | Informational | Informational message only |
| 7 | Debugging | Appears during debugging only |

## 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 enable logging messages with a severity level of 4 (warning) or higher to the console session:

```
n1000v# configure terminal
n1000v(config)# logging console 4
n1000v(config)#
```

**Related Commands**

| Command | Description |
|---|---|
| **show logging console** | Displays the console logging configuration. |

# logging event

Use the **logging event** command to log interface events.

**logging event {link-status | trunk-status} {enable | default}**

**no logging event {link-status | trunk-status} {enable | default}**

## Syntax Description

| | |
|---|---|
| **link-status** | Log all up/down and change status messages. |
| **trunk-status** | Log all trunk status messages. |
| **default** | The default logging configuration is used. |
| **enable** | Enables interface logging to override the port level logging configuration. |

## 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 log interface events:

```
n1000v# configure terminal
n1000v(config)# logging event link-status default
n1000v(config)#
```

## Related Commands

| Command | Description |
|---|---|
| **show logging** | Displays the logging configuration and contents of logfile. |

# logging level

Use the **logging level** command to enable the logging of messages as follows:

- from a named facility (such as license or aaa)
- of a specified severity level or higher

To disable the logging of messages, use the **no** form of this command.

**logging level** *facility severity-level*

**no logging level** *facility severity-level*

## Syntax Description

| | |
|---|---|
| *facility* | Names the *facility.* |
| *severity-level* | The severity level at which you want messages to be logged. When you set a severity level, for example 4, then messages at that severity level and higher (0 through 4) are logged.<br>Severity levels are as follows: |

| Level | Designation | Definition |
|---|---|---|
| 0 | Emergency | System unusable *__the highest level__* |
| 1 | Alert | Immediate action needed |
| 2 | Critical | Critical condition—default level |
| 3 | Error | Error condition |
| 4 | Warning | Warning condition |
| 5 | Notification | Normal but significant condition |
| 6 | Informational | Informational message only |
| 7 | Debugging | Appears during debugging only |

## Defaults

None

## Command Modes

Global configuration (config)

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

To apply the same severity level to all facilities, use the following command:

- **logging level all** *level_number*

To list the available facilities for which messages can be logged, use the following command:

- **logging level ?**

## Examples

This example shows how to enable logging messages from the AAA facility that have a severity level of 0 through 2:

```
n1000v# configure terminal
n1000v(config)# logging level aaa 2
n1000v(config)#
```

This example shows how to enable logging messages from the license facility with a severity level of 0 through 4; and then display the license logging configuration:

```
n1000v# configure terminal
n1000v(config)# logging level license 4
n1000v(config)# show logging level license
Facility        Default Severity        Current Session Severity
--------        ----------------        ------------------------
licmgr                  6                       4

0(emergencies)          1(alerts)       2(critical)
3(errors)               4(warnings)     5(notifications)
6(information)          7(debugging)

n1000v(config)#
```

## Related Commands

| Command | Description |
|---|---|
| **show logging level** | Displays the facility logging level configuration. |
| **logging level ?** | Lists the available facilities for which messages can be logged. |

# logging logfile

Use the **logging logfile** command to configure the log file used to store system messages.

To remove a configuration, use the **no** form of this command.

**logging logfile** *logfile-name severity-level* **[size** *bytes***]**

**no logging logfile [***logfile-name severity-level* **[size** *bytes***]]]**

## Syntax Description

| | |
|---|---|
| *logfile-name* | Specifies the name of the log file that stores system messages. |
| *severity-level* | The severity level at which you want messages to be logged. When you set a severity level, for example 4, then messages at that severity level and higher (0 through 4) are logged.<br>Severity levels are as follows: |

| Level | Designation | Definition |
|---|---|---|
| 0 | Emergency | System unusable *__the highest level__* |
| 1 | Alert | Immediate action needed |
| 2 | Critical | Critical condition—default level |
| 3 | Error | Error condition |
| 4 | Warning | Warning condition |
| 5 | Notification | Normal but significant condition |
| 6 | Informational | Informational message only |
| 7 | Debugging | Appears during debugging only |

| | |
|---|---|
| **size** *bytes* | (Optional) Specifies the log file size in bytes, from 4096 to 10485760 bytes.<br>The default file size is 10485760 bytes. |

## 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 configure a log file named LogFile to store system messages and set its severity level to 4:

```
n1000v# config t
n1000v(config)# logging logfile LogFile 4
```

```
n1000v(config)#
```

**Related Commands**

| Command | Description |
|---|---|
| **show logging logfile** | Displays the contents of the log file. |

# logging module

To start logging of module messages to the log file, use the **logging module** command. To stop module log messages, use the **no** form of this command.

**logging module** [*severity*]

**no logging module** [*severity*]

## Syntax Description

*severity-level* — The severity level at which you want messages to be logged. If you do not specify a severity level, the default is used. When you set a severity level, for example 4, then messages at that severity level and higher (0 through 4) are logged.

Severity levels are as follows:

| Level | Designation | Definition |
|---|---|---|
| 0 | Emergency | System unusable *__the highest level__* |
| 1 | Alert | Immediate action needed |
| 2 | Critical | Critical condition—default level |
| 3 | Error | Error condition |
| 4 | Warning | Warning condition |
| 5 | Notification | Normal but significant condition (the default) |
| 6 | Informational | Informational message only |
| 7 | Debugging | Appears during debugging only |

## Defaults

Disabled

If you start logging of module messages, and do not specify a severity, then the default is used, Notification (5).

## 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 start logging of module messages to the log file at the default severity level (severity 4):

```
n1000v# configure terminal
n1000v(config)# logging module
n1000v(config)#
```

This example shows how to stop the logging of module messages to the log file:

```
n1000v# configure terminal
n1000v(config)# no logging module
n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **show logging module** | Displays the current configuration for logging module messages to the log file. |

# logging monitor

Use the **logging monitor** command to enable the logging of messages to the monitor (terminal line). This configuration applies to telnet and Secure Shell (SSH) sessions.

To disable monitor logging, use the **no** form of this command.

**logging monitor** [*severity-level*]

**no logging monitor**

## Syntax Description

*severity-level* — The severity level at which you want messages to be logged. If you do not specify a severity level, the default is used. When you set a severity level, for example 4, then messages at that severity level and higher (0 through 4) are logged.

Severity levels are as follows:

| Level | Designation | Definition |
|---|---|---|
| 0 | Emergency | System unusable *__the highest level__* |
| 1 | Alert | Immediate action needed |
| 2 | Critical | Critical condition—default level |
| 3 | Error | Error condition |
| 4 | Warning | Warning condition |
| 5 | Notification | Normal but significant condition (the default) |
| 6 | Informational | Informational message only |
| 7 | Debugging | Appears during debugging only |

## 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 enable monitor log messages:

```
n1000v# configure terminal
n1000v(config)# logging monitor
n1000v(config)#
```

**Related Commands**

| Command | Description |
|---|---|
| **show logging monitor** | Displays the monitor logging configuration. |

# logging server

Use the **logging server** command to designate and configure a remote server for logging system messages. Use the **no** form of this command to remove or change the configuration,

**logging server** *host0* [*i1* [**use-vrf** *s0* [**facility** {**auth** | **authpriv** | **cron** | **daemon** | **ftp** | **kernel** | **local0** | **local1** | **local2** | **local3** | **local4** | **local5** | **local6** | **local7** | **lpr** | **mail** | **news** | **syslog** | **user** | **uucp**}]]]

**no logging server** *host0* [*i1* [**use-vrf** *s0* [**facility** {**auth** | **authpriv** | **cron** | **daemon** | **ftp** | **kernel** | **local0** | **local1** | **local2** | **local3** | **local4** | **local5** | **local6** | **local7** | **lpr** | **mail** | **news** | **syslog** | **user** | **uucp**}]]]

## Syntax Description

| | |
|---|---|
| *host0* | Hostname/IPv4/IPv6 address of the Remote Syslog Server. |
| *i1* | (Optional) 0-emerg;1-alert;2-crit;3-err;4-warn;5-notif;6-inform;7-debug. |
| **use-vrf** *s0* | (Optional) Enter VRF name, default is management + VRF name,default management. |
| **facility** | (Optional) Facility to use when forwarding to server. |
| **auth** | Use auth facility. |
| **authpriv** | Use authpriv facility. |
| **cron** | Use Cron/at facility. |
| **daemon** | Use daemon facility. |
| **ftp** | Use file transfer system facility. |
| **kernel** | Use kernel facility. |
| **local0** | Use local0 facility. |
| **local1** | Use local1 facility. |
| **local2** | Use local2 facility. |
| **local3** | Use local3 facility. |
| **local4** | Use local4 facility. |
| **local5** | Use local5 facility. |
| **local6** | Use local6 facility. |
| **local7** | Use local7 facility. |
| **lpr** | Use lpr facility. |
| **mail** | Use mail facility. |
| **news** | Use USENET news facility. |
| **syslog** | Use syslog facility. |
| **user** | Use user facility. |
| **uucp** | Use Unix-to-Unix copy system facility. |

## 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 configure a remote syslog server at a specified IPv4 address, using the default outgoing facility:

```
n1000v# configure terminal
n1000v(config)# logging server 172.28.254.253
n1000v(config)#
```

This example shows how to configure a remote syslog server at a specified host name, with severity level 5 or higher:

```
n1000v# configure terminal
n1000v(config)# logging server syslogA 5
n1000v(config)#
```

**Related Commands**

| Command | Description |
|---|---|
| **show logging server** | Displays the current server configuration for logging system messages. |

# logging timestamp

To set the unit of measure for the system messages timestamp, use the **logging timestamp** command. To restore the default unit of measure, use the **no** form of this command.

**logging timestamp** {**microseconds** | **milliseconds** | **seconds**}

**no logging timestamp** {**microseconds** | **milliseconds** | **seconds**}

## Syntax Description

| | |
|---|---|
| **microseconds** | Timestamp in micro-seconds. |
| **milliseconds** | Timestamp in milli-seconds. |
| **seconds** | Timestamp in seconds (Default). |

## Defaults

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 set microseconds as the unit of measure for the system messages timestamp:

```
n1000v# configure terminal
n1000v(config)# logging timestamp microseconds
n1000v(config)#
```

## Related Commands

| Command | Description |
|---|---|
| **show logging timestamp** | Displays the logging timestamp configuration. |

# M Commands

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

## mac access-list

To create a MAC ACL, use the **mac access-list** command. To remove the MAC ACL, use the **no** form of this command.

**mac access-list** *name*

**no mac access-list** *name*

**Syntax Description**

| | |
|---|---|
| *name* | List name. The range of valid values is 1 to 64. |

**Defaults**

The MAC ACL does not exist.

**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 MAC ACL:

```
n1000v# configure terminal
n1000v(config)# mac access-list aL1
n1000v(config)#
```

**Related Commands**

| Command | Description |
|---|---|
| **show access-list** | Displays access list information. |

# mac address-table aging-time

To configure the aging time for entries in the Layer 2 table, use the **mac address-table aging-time** command. To return to the default settings, use the **no** form of this command.

**mac address-table aging-time** *seconds* [**vlan** *vlan-id*]

**no mac address-table aging-time** [**vlan** *vlan-id*]

## Syntax Description

| | |
|---|---|
| *seconds* | Aging time for MAC table entries for Layer 2. The range is from 120 to 918000 seconds. The default is 1800 seconds. Entering 0 disables the aging time. |
| **vlan** *vlan-id* | (Optional) Specifies the VLAN to apply the changed aging time. |

## Defaults

1800 seconds

## Command Modes

Global configuration (config)

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

Enter **0** seconds to disable the aging process.

The age value may be rounded off to the nearest multiple of 5 seconds. If the system rounds the value to a different value from that specified by the user (from the rounding process), the system returns an informational message.

When you use this command in the global configuration mode, the age values of all VLANs for which a configuration has not been specified are modified and those VLANs with specifically modified aging times are not modified. When you use the **no** form of this command without the VLAN parameter, only those VLANs that have not been specifically configured for the aging time reset to the default value. Those VLANs with specifically modified aging times are not modified.

When you use this command and specify a VLAN, the aging time for only the specified VLAN is modified. When you use the **no** form of this command and specify a VLAN, the aging time for the VLAN is returned to the current *global* configuration for the aging time, which may or may not be the default value of 300 seconds depending if the global configuration of the device for aging time has been changed.

Aging time is counted from the last time that the switch detected the MAC address.

## Examples

This example shows how to change the length of time an entry remains in the MAC address table to 500 seconds for the entire device:

```
n1000v(config)# mac address-table aging-time 500
n1000v(config)#
```

## Related Commands

| Command | Description |
|---|---|
| **show mac address-table** | Displays information about the MAC address table. |
| **clear mac address-table aging-time** | Displays information about the MAC address aging time. |

# mac address-table static

To configure a static entry for the Layer 2 MAC address table, use the **mac address-table static** command. To delete the static entry, use the **no** form of this command.

**mac address-table static** *mac-address* **vlan** *vlan-id* {[**drop** | **interface** {*type slot/port* | **port-channel** *number*]}

**no mac address-table static** {**address** *mac_addr*} {**vlan** *vlan-id*}

## Syntax Description

| | |
|---|---|
| *mac-address* | Specifies the MAC address to add to the table. Use the format XXXX.XXXX.XXXX. |
| **vlan** *vlan-id* | Specifies the VLAN to apply static MAC address; valid values are from 1 to 4094. |
| **drop** | Drops all traffic that is received from and going to the configured MAC address in the specified VLAN. |
| *type slot/port* | (Optional) Specifies the interface. Use the type of interface, the slot number, and the port number. |
| **port-channel** *number* | (Optional) Specifies the interface. Use the port-channel number. |

## Defaults

None

## Command Modes

Global configuration (config)

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

You cannot apply the **mac address-table static** *mac-address* **vlan** *vlan-id* **drop** command to a multicast MAC address.

The output interface specified cannot be a VLAN interface or a Switched Virtual Interface (SVI).

Use the **no** form to remove entries that are profiled by the combination of specified entry information.

## Examples

This example shows how to add a static entry to the MAC address table:

```
n1000v(config)# mac address-table static 0050.3e8d.6400 vlan 3 interface ethernet 2/1
n1000v(config)#
```

## Related Commands

| Command | Description |
|---|---|
| **show mac address-table** | Displays information about MAC address table. |

# mac port access-group

To enable access control for port groups, use the **mac port access-group** command. To disable access control for port groups, use the **no** form of this command.

**mac port access-group** *name* {**in** | **out**}

**no mac port access-group** *name* {**in** | **out**}

## Syntax Description

| | |
|---|---|
| *name* | Group name. The range of valid values is 1 to 64. |
| **in** | Specifies inbound traffic. |
| **out** | Specifies outbound traffic. |

## Defaults

Access control for packets is not specified.

## Command Modes

Port profile configuration (config-port-prof)

## SupportedUserRoles

network-admin

## Command History

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

## Examples

This example shows how to enable access control for port groups:

```
n1000v# configure terminal
n1000v(config)# port-profile 1
n1000v(config-port-prof)# mac port access-group groupOne in
n1000v(config-port-prof)#
```

## Related Commands

| Command | Description |
|---|---|
| **show mac** | Displays MAC information. |

# match (ACL)

To define ACL matching criteria, use the **match** command. To remove matching criteria, use the **no** form of this command.

**match** {{**access-group name** *name*} | {[**not**] **cos** *cos-list*} | {[**not**] **dscp** {*dscp-list* | *dscp-enum*}**+**} | {[**not**] **precedence** {*precedence-list* | *prec-enum*}**+**} | {[**not**] **discard-class** *discard-class-list*} | {[**not**] **qos-group** *qos-group-list*} | {[**not**] **class-map** *cmap-name*} | {[**not**] **packet length** *len-list*} | {[**not**] **ip rtp** *port-list*}}

**no match** {{**access-group name** *acl-name*} | {[**not**] **cos** *cos-list*} | {[**not**] **dscp** {*dscp-list* | *dscp-enum*}**+**} | {[**not**] **precedence** {*precedence-list* | *prec-enum*}**+**} | {[**not**] **discard-class** *discard-class-list*} | {[**not**] **qos-group** *qos-group-list*} | {[**not**] **class-map** *cmap-name*} | {[**not**] **packet length** *len-list*} | {[**not**] **ip rtp** *port-list*}}

## Syntax Description

| | |
|---|---|
| **access-group** | Specifies the access group. |
| **name** | Specifies the ACL name. |
| *name* | ACL name. The range of valid values is 1 to 64. |
| **not** | (Optional) Negates the match result. |
| **cos** | IEEE 802.1Q CoS (Class of Service). |
| *cos-list* | List of CoS values. The range of valid values is 0 to 7. |
| **dscp** | DSCP in IP(v4) and IPv6 packets. |
| *dscp-list* | List of DSCP values. |
| *dscp-enum* | . |
| **precedence** | Precedence in IP(v4) and IPv6 packets. |
| *precedence-list* | List of precedence values. |
| *prec-enum* | . |
| **discard-class** *discard-class-list* | Discard class + List of discard-class values. |
| **qos-group** *qos-group-list* | Qos-group + List of qos-group values. |
| **class-map** *cmap-name* | Class map + Match class-map name. |
| **packet** | Packet. |
| **length** | Length of IP datagram. |
| *len-list* | list of IP packet length. |
| **ip** | IP. |
| **rtp** | Real Time Protocol. |
| *port-list* | UDP port list that are using RTP. |

## Defaults

None

**Command Modes** Class map configuration (config-cmap-qos

**SupportedUserRoles** network-admin

**Command History**

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

**Examples**

This example shows how to configure a class-map match criteria:

```
n1000v(config)# class-map cl_map1
n1000v(config-cmap-qos)# match access-group name ac_gr1
n1000v(config-cmap-qos)#
```

This example shows how to remove the class-map match criteria:

```
n1000v(config)# class-map cl_map1
n1000v(config-cmap-qos)# no match access-group name ac_gr1
n1000v(config-cmap-qos)#
```

**Related Commands**

| Command | Description |
|---|---|
| **show class map** | Displays class map information. |

# match ip (NetFlow)

To define IP matching criteria for a NetFlow flow record, use the **match ip** command. To remove the matching criteria, use the **no** form of this command.

**match ip** {**protocol** | **tos**}

**no match ip** {**protocol** | **tos**}

## Syntax Description

| | |
|---|---|
| **protocol** | Protocol. |
| **tos** | Type of service. |

## Defaults

None

## Command Modes

Flow record configuration (config-flow-record)

## SupportedUserRoles

network-admin

## Command History

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

## Examples

This example shows how to configure IP matching criteria for a NetFlow flow record and then display the result:

```
n1000v# config t
n1000v(config)# flow record RecordTest
n1000v(config-flow-record)# match ip protocol
n1000v(config-flow-record)# show flow record
Flow record RecordTest:
    No. of users: 0
    Template ID: 0
    Fields:
        match ip protocol
        match interface input
        match interface output
        match flow direction
doc-n1000v(config-flow-record)#
```

This example shows how to remove the IP matching criteria for a NetFlow flow record a and then display the result:

```
n1000v# config t
n1000v(config)# flow record RecordTest
n1000v(config-flow-record)# no match ip protocol
n1000v(config-flow-record)# show flow record
Flow record RecordTest:
    No. of users: 0
```

```
    Template ID: 0
    Fields:
        match interface input
        match interface output
        match flow direction
doc-n1000v(config-flow-record)#
```

## Related Commands

| Command | Description |
|---|---|
| **show flow record** [*name*] | Displays a NetFlow flow record configuration. |
| **match ipv4** | Defines IPv4 matching criteria for a NetFlow flow record. |
| **match transport** | Defines transport matching criteria for a NetFlow flow record. |

# match ipv4 (NetFlow)

To define IPv4 matching criteria for a NetFlow flow record, use the **match ipv4** command. To remove the matching criteria, use the **no** form of this command.

**match ipv4** {**source** | **destination**} **address**

**no match ipv4** {**source** | **destination**} **address**

## Syntax Description

| | |
|---|---|
| **source** | Source Address. |
| **destination** | Destination Address. |
| **address** | Address. |

## Defaults

None

## Command Modes

Flow record configuration (config-flow-record)

## SupportedUserRoles

network-admin

## Command History

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

## Examples

This example shows how to configure IPv4 matching criteria for a NetFlow flow record and then display the result:

```
n1000v# config t
n1000v(config)# flow record RecordTest
n1000v(config-flow-record)# match ipv4 destination address
n1000v(config-flow-record)# show flow record
Flow record RecordTest:
    Description: Ipv4flow
    No. of users: 0
    Template ID: 0
    Fields:
        match ipv4 destination address
        match interface input
        match interface output
        match flow direction
        collect counter packets
n1000v(config-flow-record)#
```

This example shows how to remove the IPv4 matching criteria for a NetFlow flow record a and then display the result:

```
n1000v# config t
n1000v(config)# flow record RecordTest
n1000v(config-flow-record)# no match ipv4 destination address
```

```
n1000v(config-flow-record)# show flow record
Flow record RecordTest:
    No. of users: 0
    Template ID: 0
    Fields:
        match interface input
        match interface output
        match flow direction
doc-n1000v(config-flow-record)#
```

## Related Commands

| Command | Description |
|---|---|
| **show flow record** [*name*] | Displays a NetFlow flow record configuration. |
| **match ip** | Defines IP matching criteria for a NetFlow flow record. |
| **match transport** | Defines transport matching criteria for a NetFlow flow record. |

# match transport (NetFlow)

To define transport matching criteria for a NetFlow flow record, use the **match transport** command. To remove the matching criteria, use the **no** form of this command.

**match transport** {**destination-port** | **source-port**}

**no match transport** {**destination-port** | **source-port**}

## Syntax Description

| | |
|---|---|
| **destination-port** | Transport destination port. |
| **source-port** | Transport source port. |

## Defaults

None

## Command Modes

Flow Record configuration (config-flow-record)

## SupportedUserRoles

network-admin

## Command History

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

## Examples

This example shows how to configure transport matching criteria for a NetFlow flow record and then display the result:

```
n1000v# config t
n1000v(config)# flow record RecordTest
n1000v(config-flow-record)# match transport destination-port
n1000v(config-flow-record)# show flow record
Flow record RecordTest:
    Description: Ipv4flow
    No. of users: 0
    Template ID: 0
    Fields:
        match ipv4 destination-port
        match interface input
        match interface output
        match flow direction
        collect counter packets
n1000v(config-flow-record)#
```

This example shows how to remove the transport matching criteria for a NetFlow flow record a and then display the result:

```
n1000v# config t
n1000v(config)# flow record RecordTest
n1000v(config-flow-record)# no match transport destination-port
n1000v(config-flow-record)# show flow record
```

```
Flow record RecordTest:
    No. of users: 0
    Template ID: 0
    Fields:
        match interface input
        match interface output
        match flow direction
doc-n1000v(config-flow-record)#
```

## Related Commands

| Command | Description |
|---|---|
| **show flow record** [*name*] | Displays a NetFlow flow record configuration. |
| **match ip** | Defines IP matching criteria for a NetFlow flow record. |
| **match ipv4** | Defines IPv4 matching criteria for a NetFlow flow record. |

# media

To specify the media type of a VLAN as Ethernet, use the **media** command. To remove the type, use the **no** form of this command.

**media ethernet**

**no media**

## Syntax Description

| | |
|---|---|
| **ethernet** | Specifies Ethernet media type. |

## Defaults

None

## Command Modes

VLAN configuration (config-vlan)

## SupportedUserRoles

network-admin

## Command History

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

## Examples

This example shows how to configure media type:

```
n1000v# configure terminal
n1000v(config)# media ethernet
n1000v(config)#
```

## Related Commands

| Command | Description |
|---|---|
| **show vlan** | Displays VLAN information. |

# mkdir

To create a new directory, use the **mkdir** command.

**mkdir {bootflash: | debug: | volatile:}**

## Syntax Description

| | |
|---|---|
| **bootflash:** | Specifies bootflash as the directory name. |
| **debug:** | Specifies debug as the directory name. |
| **volatile:** | Specifies volatile as the directory name. |

## Defaults

None

## 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 create the bootflash: directory:

```
n1000v# mkdir bootflash:
```

## Related Commands

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

# module vem

To enter commands on the VEM remotely from the Cisco Nexus 1000V, use the **module vem** command.

**module vem** *module-number* **execute** *line* [*line*]

## Syntax Description

| | |
|---|---|
| *module-number* | Specifies the module number. The range is 3 to 66. |
| **execute** | Specifies the command to execute on the VEM. |
| *line* | (Optional)The syntax of the command to be sent to the VEM. |

## Defaults

None

## Command Modes

EXEC

## SupportedUserRoles

network-admin

## Command History

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

## Examples

This example shows how to display the VEM port profile configuration remotely from the Cisco Nexus 1000V:

```
n1000v# module vem 3 execute vemcmd show port-profile
```

This example shows how to display the VEM VSD configuration remotely from the Cisco Nexus 1000V:

```
n1000v# module vem 3 execute vemcmd show vsd
 ID  Def_Act ILTL  OLTL  NMLTL  State    Member LTLs
  1   DROP    48    49     4     ENA    54,52,55,53
  2   FRWD    50    51     0     ENA
vsim-cp# module vem 3 execute vemcmd show vsd ports
  LTL   IfIndex    VSD_ID     VSD_PORT_TYPE
   48   1b020000     1          INSIDE
   49   1b020010     1          OUTSIDE
   50   1b020020     2          INSIDE
   51   1b020030     2          OUTSIDE
   52   1b020040     1          REGULAR
   53   1b020050     1          REGULAR
   54   1b020060     1          REGULAR
   55   1b020070     1          REGULAR
n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **show module vem** | Displays Virtual Ethernet Module information. |

# monitor session

To enter the monitor configuration mode for configuring an Ethernet switch port analyzer (SPAN) session for analyzing traffic between ports, use the monitor session command.

To disable monitoring a SPAN session(s), use the no form of this command.

**monitor session {***session-number* [**shut | type erspan-source**] **| all shut**}

**no monitor session {***session-number* [**shut | type erspan-source**] **| all shut**}

## Syntax Description

| | |
|---|---|
| *session-number* | Specifies the session number for monitoring a switched port. SPAN sessions are numbered from 1 to 64. |
| **shut** | (Optional) Shuts the selected session. |
| **type** | (Optional) Specifies a session type. |
| **erspan-source** | (Optional) Creates an erspan source session |
| **all** | Specify all sessions for monitoring a switched port. |

## 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 enter the monitor configuration mode for configuring SPAN session number 2 for analyzing traffic between ports:

```
n1000v# configuration t
n1000v(config)# monitor session 2
n1000v(config-monitor)#
```

This example shows how to remove the configuration for SPAN session 2 for analyzing traffic between ports:

```
n1000v# configuration t
n1000v(config)# no monitor session 2
n1000v(config)#
```

## Related Commands

| Command | Description |
|---|---|
| **show monitor** | Displays Ethernet SPAN information. |

# move

To move a file from one directory to another, use the **move** command.

**move** [*filesystem*:[*//module/*][*directory/*] | *directory/*]*source-filename*
{{*filesystem*:[*//module/*][*directory/*] | *directory/*}[*destination-filename*] | *target-filename*}

## 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/* | (Optional) Name of a directory. The name is case sensitive. |
| *source-filename* | Name of the file to move. The name is case sensitive. |
| *destination-filename* | (Optional) Name of the destination file. The name is alphanumeric, case sensitive, and has a maximum of 64 characters. |

## Defaults

The default name for the destination file is the same as the source filename.

## Command Modes

Any

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

You can make a copy of a file by using the **copy** command.

**Tip** You can rename a file by moving it within the same directory.

## Examples

This example shows how to move a file to another directory:

```
n1000v# move file1 my_files:file2
```

This example shows how to move a file to another file system:

```
n1000v# move file1 slot0:
```

This example shows how to move a file to another supervisor module:

```
n1000v# move file1 bootflash://sup-remote/file1.bak
```

## Related Commands

| Command | Description |
|---|---|
| **cd** | Changes the current working directory. |
| **copy** | Makes a copy of a file. |
| **dir** | Displays the directory contents. |
| **pwd** | Displays the name of the current working directory. |

# mtu

To configure the maximum transmission unit (MTU) size for an interface, use the **mtu** command. To remove the configured MTU size from the interface, use the **no** form of this command.

**mtu** *size*

**no mtu** *size*

## Syntax Description

| | |
|---|---|
| *size* | Specifies the MTU size. The range is 1500 to 9000. |

## Defaults

1500 Bytes

## Command Modes

Interface configuration (config-if)

## SupportedUserRoles

network-admin

## Command History

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

## Examples

This example shows how to set the MTU size to 2000:

```
n1000v# configure terminal
n1000v(config)# interface port-channel 2
n1000v(config-if)# mtu 2000
```

## Related Commands

| Command | Description |
|---|---|
| **show interface** | Displays information about the interface, which includes MTU size. |

# N Commands

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

## name

To name a VLAN, use the **name** command. To remove a VLAN name, use the **no** form of this command.

**name** *name*

**no name**

**Syntax Description**

| | |
|---|---|
| *name* | VLAN name. The range of valid values is 1 to 32. |

**Defaults**

The VLAN has no name.

**Command Modes**

VLAN configuration (config-vlan)

**SupportedUserRoles**

network-admin

**Command History**

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

**Examples**

This example shows how to name a VLAN:

```
n1000v# configure terminal
n1000v(config)# vlan 10
n1000v(config-vlan)# name v10
(config-vlan)#
```

**Related Commands**

| Command | Description |
|---|---|
| **show vlan** | Displays VLAN information. |

# ntp enable

To enable NTP, use the **ntp enable** command. To disable, use the **no** command form.

**ntp enable**

**no ntp enable**

## Syntax Description

This command has no arguments or keywords.

## Defaults

Enabled

## 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 enable NTP:

```
n1000v# ntp enable
```

This example shows how to disable NTP:

```
n1000v# no ntp enable
```

## Related Commands

| Command | Description |
|---|---|
| **ntp server** | Configures a remote NTP server.. |

# ntp peer

To do configure the Network Time Protocol peer, use the **ntp peer** command. To remove the peer, use the **no** form of this command.

**ntp peer** *host [prefer]* [**use-vrf** *vrf*]

**no ntp peer** *host* [**prefer**] [**use-vrf** *vrf*]

## Syntax Description

| | |
|---|---|
| *host* | Hostname or IP address of the NTP peer. |
| **prefer** | (Optional) Specifies this peer as the preferred peer. |
| **use-vrf** *vrf* | (Optional) Specifies the virtual routing and forwarding (VRF) used to reach this peer. |

## 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 configure an NTP peer:

```
n1000v(config)# ntp peer 192.0.2.2
```

## Related Commands

| Command | Description |
|---|---|
| **show ntp peer** | Displays information about the NTP peer. |

# ntp server

To do configure a Network Time Protocol server, use the **ntp server** command. To remove the server, use the **no** form of this command.

**ntp server** *host* [**prefer**] [**use-vrf** *vrf*]

**no ntp server** *host* [**prefer**] [**use-vrf** *vrf*]

## Syntax Description

| | |
|---|---|
| *host* | Hostname or IP address of the NTP server. |
| **prefer** | (Optional) Specifies this server as the preferred server. |
| **use-vrf** *vrf* | (Optional) Specifies the virtual routing and forwarding (VRF) used to reach this peer. |

## 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 configure an NTP server:

```
n1000v(config)# ntp server 192.0.2.2
```

## Related Commands

| Command | Description |
|---|---|
| **show ntp peer** | Displays information about the NTP peer. |

# ntp source

To do configure the Network Time Protocol source, use the **ntp source** command. To remove the NTP source, use the **no** form of this command.

**ntp source** *addr*

**no ntp source** *addr*

## Syntax Description

| | |
|---|---|
| *addr* | IPv4 or IPv6 address of the source. The IPv4 address format is dotted decimal, x.x.x.x. The IPv6 address format is hex A:B::C:D. |

## 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 configure the NTP source:

```
n1000v(config)# ntp source 192.0.2.3
```

This example shows how to remove the NTP source:

```
n1000v(config)# no ntp source 192.0.2.3
```

## Related Commands

| Command | Description |
|---|---|
| **show ntp source** | Displays information about the NTP source. |

# O Commands

This chapter describes theCisco Nexus 1000V commands that begin with the letter O.

## option exporter-stats timeout

To specify a timeout period for resending NetFlow flow exporter data, use the **option exporter-stats timeout** command. To remove the timeout period, use the **no** form of this command.

**option exporter-stats timeout** *time*

**no option exporter-stats timeout**

**Syntax Description**

| | |
|---|---|
| *time* | A time period between 1 and 86400 seconds. |

**Defaults**

None

**Command Modes**

Netflow flow exporter version 9 configuration (**config-flow-exporter-version-9**)

**SupportedUserRoles**

network-admin

**Command History**

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

**Examples**

This example shows how to configure a 3600-second timeout period for resending NetFlow flow exporter data:

```
n1000v# config t
n1000v(config)# flow exporter ExportTest
n1000v(config-flow-exporter)# version 9
n1000v(config-flow-exporter-version-9)# option exporter-stats timeout 3600
```

This example shows how to remove the timeout period for resending NetFlow flow exporter data:

```
n1000v# config t
n1000v(config)# flow exporter ExportTest
n1000v(config-flow-exporter)# version 9
n1000v(config-flow-exporter-version-9)# no option exporter-stats timeout
n1000v(config-flow-exporter)#
```

## Related Commands

| Command | Description |
|---|---|
| **version 9** | Designates NetFlow export version 9 in the NetFlow exporter. |
| **option interface-table timeout** | Specifies a timeout period for resending the NetFlow flow exporter interface table. |
| **template data timeout** | Specifies a timeout period for resending NetFlow flow exporter template data. |
| **flow exporter** | Creates a Flexible NetFlow flow exporter. |
| **flow record** | Creates a Flexible NetFlow flow record. |
| **flow monitor** | Creates a Flexible NetFlow flow monitor. |
| **show flow exporter** | Displays information about the NetFlow flow exporter. |
| **show flow record** | Displays information about NetFlow flow records. |
| **show flow monitor** | Displays information about the NetFlow flow monitor. |

# option interface-table timeout

To specify the timeout period for resending the NetFlow flow exporter interface table, use the **option interface-table timeout** command. To remove the timeout period, use the **no** form of this command.

**option interface-table timeout** *time*

**no option interface-table timeout**

## Syntax Description

| | |
|---|---|
| *time* | A time period between 1 and 86400 seconds. |

## Defaults

None

## Command Modes

Netflow flow exporter version 9 configuratio (config-flow-exporter-version-9)

## SupportedUserRoles

network-admin

## Command History

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

## Examples

This example shows how to configure a 3600 second timeout period for resending the NetFlow flow exporter interface table:

```
n1000v# config t
n1000v(config)# flow exporter ExportTest
n1000v(config-flow-exporter)# version 9
n1000v(config-flow-exporter-version-9)# option exporter-stats timeout 3600
```

This example shows how to remove the timeout period for resending the NetFlow flow exporter interface table:

```
n1000v# config t
n1000v(config)# flow exporter ExportTest
n1000v(config-flow-exporter)# version 9
n1000v(config-flow-exporter-version-9)# no option exporter-stats timeout
n1000v(config-flow-exporter)#
```

## Related Commands

| Command | Description |
|---|---|
| **version 9** | Designates NetFlow export version 9 in the NetFlow exporter. |
| **option exporter-stats timeout** | Specifies a timeout period for resending NetFlow flow exporter data. |

| Command | Description |
|---|---|
| **template data timeout** | Specifies a timeout period for resending NetFlow flow exporter template data. |
| **flow exporter** | Creates a Flexible NetFlow flow exporter. |
| **flow record** | Creates a Flexible NetFlow flow record. |
| **flow monitor** | Creates a Flexible NetFlow flow monitor. |
| **show flow exporter** | Displays information about the NetFlow flow exporter. |
| **show flow record** | Displays information about NetFlow flow records. |
| **show flow monitor** | Displays information about the NetFlow flow monitor. |

# P Commands

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

## packet vlan

To identify a packet VLAN, use the **packet vlan** command. To remove the packet vlan, use the **no** form of this command.

**packet vlan** {*vlan-number*}

**no packet vlan** {*vlan-number*}

**Syntax Description**

| | |
|---|---|
| *vlan-number* | Specifies the packet VLAN ID. The range of values is 1 to 3967 and 4048 to 4093. |

**Defaults**

None

**Command Modes**

SVS domain (config-svs-domain)

**SupportedUserRoles**

network-admin

**Command History**

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

**Examples**

This example shows how to create packet VLAN 261:

```
n1000v# configure terminal
n1000v(config)# svs-domain
n1000v(config-svs-domain)# packet vlan 261
n1000v(config-svs-domain)#
```

This example shows how to remove the packet VLAN 261:

```
n1000v# configure terminal
n1000v(config)# svs-domain
n1000v(config-svs-domain)# no packet vlan 261
n1000v(config-svs-domain)#
```

**Related Commands**

| Command | Description |
|---|---|
| **show running-config** | Displays information about the running configuration on the n1000v. |

# password strength-check

To enable password-strength checking, use the **password strength-check** command. To disable the checking of password strength, use the **no** form of this command.

**password strength-check**

**no password strength-check**

## Syntax Description

This command has no arguments or keywords.

## Defaults

This feature is enabled by default.

## 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 enable the checking of password strength:

```
n1000v# config t
n1000v(config)# password strength-check
n1000v(config)#
```

This example shows how to disable the checking of password strength:

```
n1000v# config t
n1000v(config)# no password strength-check
n1000v(config)#
```

## Related Commands

| Command | Description |
|---|---|
| **show password strength-check** | Displays the configuration for checking password strength. |
| **username** | Creates a user account. |
| **role name** | Names a user role and places you in role configuration mode for that role. |

# permit (IPv4)

To create an IPv4 access control list (ACL) rule that permits traffic matching its conditions, use the **permit** command. To remove a rule, use the **no** form of this command.

### General Syntax

[*sequence-number*] **permit** *protocol source destination* [**dscp** *dscp* | **precedence** *precedence*]

**no permit** *protocol source destination* [**dscp** *dscp* | **precedence** *precedence*]

**no** *sequence-number*

### Internet Control Message Protocol

[*sequence-number*] **permit icmp** *source destination* [*icmp-message*] [**dscp** *dscp* | **precedence** *precedence*]

### Internet Group Management Protocol

[*sequence-number*] **permit igmp** *source destination* [*igmp-message*] [**dscp** *dscp* | **precedence** *precedence*]

### Internet Protocol v4

[*sequence-number*] **permit ip** *source destination* [**dscp** *dscp* | **precedence** *precedence*]

### Transmission Control Protocol

[*sequence-number*] **permit tcp** *source* [*operator port* [*port*] | **portgroup** *portgroup*] *destination* [*operator port* [*port*] | **portgroup** *portgroup*] [**dscp** *dscp* | **precedence** *precedence*]

### User Datagram Protocol

[*sequence-number*] **permit udp** *source* [*operator port* [*port*] | **portgroup** *portgroup*] *destination* [*operator port* [*port*] | **portgroup** *portgroup*] [**dscp** *dscp* | **precedence** *precedence*]

## Syntax Description

| | |
|---|---|
| *sequence-number* | (Optional) Sequence number of the **permit** 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.<br><br>A sequence number can be any integer between 1 and 4294967295.<br><br>By default, the first rule in an ACL has a sequence number of 10.<br><br>If you do not specify a sequence number, the device adds the rule to the end of the ACL and assigns a sequence number that is 10 greater than the sequence number of the preceding rule.<br><br>Use the **resequence** command to reassign sequence numbers to rules. |
| *protocol* | Name or number of the protocol of packets that the rule matches. Valid numbers are from 0 to 255. Valid protocol names are the following keywords:<br><br>• **icmp**—Specifies that the rule applies to ICMP traffic only. When you use this keyword, the *icmp-message* argument is available, in addition to the keywords that are available for all valid values of the *protocol* argument.<br><br>• **igmp**—Specifies that the rule applies to IGMP traffic only. When you use this keyword, the *igmp-type* argument is available, in addition to the keywords that are available for all valid values of the *protocol* argument.<br><br>• **ip**—Specifies that the rule applies to all IPv4 traffic. When you use this keyword, only the other keywords and arguments that apply to all IPv4 protocols are available. They include the following:<br><br>– **dscp**<br><br>– **precedence**<br><br>• **tcp**—Specifies that the rule applies to TCP traffic only. When you use this keyword, the *flags* and *operator* arguments and the **portgroup** and **established** keywords are available, in addition to the keywords that are available for all valid values of the *protocol* argument.<br><br>• **udp**—Specifies that the rule applies to UDP traffic only. When you use this keyword, the *operator* argument and the **portgroup** keyword are available, in addition to the keywords that are available for all valid values of the *protocol* argument. |
| *source* | Source IPv4 addresses that the rule matches. For details about the methods that you can use to specify this argument, see “Source and Destination” in the “Usage Guidelines” section. |
| *destination* | Destination IPv4 addresses that the rule matches. For details about the methods that you can use to specify this argument, see “Source and Destination” in the “Usage Guidelines” section. |

| | |
|---|---|
| **dscp** *dscp* | (Optional) Specifies that the rule matches only those packets with the specified 6-bit differentiated services value in the DSCP field of the IP header. The *dscp* argument can be one of the following numbers or keywords:<br>• 0–63—The decimal equivalent of the 6 bits of the DSCP field. For example, if you specify 10, the rule matches only those packets that have the following bits in the DSCP field: 001010.<br>• **af11**—Assured Forwarding (AF) class 1, low drop probability (001010)<br>• **af12**—AF class 1, medium drop probability (001100)<br>• **af13**—AF class 1, high drop probability (001110)<br>• **af21**—AF class 2, low drop probability (010010)<br>• **af22**—AF class 2, medium drop probability (010100)<br>• **af23**—AF class 2, high drop probability (010110)<br>• **af31**—AF class 3, low drop probability (011010)<br>• **af32**—AF class 3, medium drop probability (011100)<br>• **af33**—AF class 3, high drop probability (011110)<br>• **af41**—AF class 4, low drop probability (100010)<br>• **af42**—AF class 4, medium drop probability (100100)<br>• **af43**—AF class 4, high drop probability (100110)<br>• **cs1**—Class-selector (CS) 1, precedence 1 (001000)<br>• **cs2**—CS2, precedence 2 (010000)<br>• **cs3**—CS3, precedence 3 (011000)<br>• **cs4**—CS4, precedence 4 (100000)<br>• **cs5**—CS5, precedence 5 (101000)<br>• **cs6**—CS6, precedence 6 (110000)<br>• **cs7**—CS7, precedence 7 (111000)<br>• **default**—Default DSCP value (000000)<br>• **if**—Expedited Forwarding (101110) |

| | |
|---|---|
| **precedence** *precedence* | (Optional) Specifies that the rule matches only packets that have an IP Precedence field with the value specified by the *precedence* argument. The *precedence* argument can be a number or a keyword, as follows:<br>• 0–7—Decimal equivalent of the 3 bits of the IP Precedence field. For example, if you specify 3, the rule matches only packets that have the following bits in the DSCP field: 011.<br>• **critical**—Precedence 5 (101)<br>• **flash**—Precedence 3 (011)<br>• **flash-override**—Precedence 4 (100)<br>• **immediate**—Precedence 2 (010)<br>• **internet**—Precedence 6 (110)<br>• **network**—Precedence 7 (111)<br>• **priority**—Precedence 1 (001)<br>• **routine**—Precedence 0 (000) |
| *icmp-message* | (ICMP only: Optional) ICMP message type that the rule matches. This argument can be an integer from 0 to 255 or one of the keywords listed under “ICMP Message Types” in the “Usage Guidelines” section. |
| *igmp-message* | (IGMP only: Optional) IGMP message type that the rule matches. The *igmp-message* argument can be the IGMP message number, which is an integer from 0 to 15. It can also be one of the following keywords:<br>• **dvmrp**—Distance Vector Multicast Routing Protocol<br>• **host-query**—Host query<br>• **host-report**—Host report<br>• **pim**—Protocol Independent Multicast<br>• **trace**—Multicast trace |

| | |
|---|---|
| *operator port* [*port*] | (Optional; TCP and UDP only) Rule matches only packets that are from a source port or sent to a destination port that satisfies the conditions of the *operator* and *port* arguments. Whether these arguments apply to a source port or a destination port depends upon whether you specify them after the *source* argument or after the *destination* argument.<br><br>The *port* argument can be the name or the number of a TCP or UDP port. Valid numbers are integers from 0 to 65535. For listings of valid port names, see "TCP Port Names" and "UDP Port Names" in the "Usage Guidelines" section.<br><br>A second *port* argument is required only when the *operator* argument is a range.<br><br>The *operator* argument must be one of the following keywords:<br>• **eq**—Matches only if the port in the packet is equal to the *port* argument.<br>• **gt**—Matches only if the port in the packet is greater than and not equal to the *port* argument.<br>• **lt**—Matches only if the port in the packet is less than and not equal to the *port* argument.<br>• **neq**—Matches only if the port in the packet is not equal to the *port* argument.<br>• **range**—Requires two *port* arguments and matches only if the port in the packet is equal to or greater than the first *port* argument and equal to or less than the second *port* argument. |
| *flags* | (TCP only; Optional) TCP control bit flags that the rule matches. The value of the *flags* argument must be one or more of the following keywords:<br>• **ack**<br>• **fin**<br>• **psh**<br>• **rst**<br>• **syn**<br>• **urg** |

## Defaults

A newly created IPv4 ACL contains no rules.

If you do not specify a sequence number, the device assigns to the rule a sequence number that is 10 greater than the last rule in the ACL.

## Command Modes

IPv4 ACL configuration (config-acl)

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

When the device applies an IPv4 ACL to a packet, it evaluates the packet with every rule in the ACL. The device enforces the first rule that has conditions that are satisfied by the packet. When the conditions of more than one rule are satisfied, the device enforces the rule with the lowest sequence number.

### Source and Destination

You can specify the *source* and *destination* arguments in one of several ways. In each rule, the method you use to specify one of these arguments does not affect how you specify the other. When you configure a rule, use the following methods to specify the *source* and *destination* arguments:

- Address and network wildcard—You can use an IPv4 address followed by a network wildcard to specify a host or a network as a source or destination. The syntax is as follows:

  *IPv4-address network-wildcard*

  The following example shows how to specify the *source* argument with the IPv4 address and network wildcard for the 192.168.67.0 subnet:

  ```
  n1000v(config-acl)# permit tcp 192.168.67.0 0.0.0.255 any
  ```

- Address and variable-length subnet mask—You can use an IPv4 address followed by a variable-length subnet mask (VLSM) to specify a host or a network as a source or destination. The syntax is as follows:

  *IPv4-address/prefix-len*

  The following example shows how to specify the *source* argument with the IPv4 address and VLSM for the 192.168.67.0 subnet:

  ```
  n1000v(config-acl)# permit udp 192.168.67.0/24 any
  ```

- Host address—You can use the **host** keyword and an IPv4 address to specify a host as a source or destination. The syntax is as follows:

  **host** *IPv4-address*

  This syntax is equivalent to *IPv4-address*/32 and *IPv4-address* 0.0.0.0.

  The following example shows how to specify the *source* argument with the **host** keyword and the 192.168.67.132 IPv4 address:

  ```
  n1000v(config-acl)# permit icmp host 192.168.67.132 any
  ```

- Any address—You can use the **any** keyword to specify that a source or destination is any IPv4 address. For examples of the use of the **any** keyword, see the examples in this section. Each example shows how to specify a source or destination by using the **any** keyword.

### ICMP Message Types

The *icmp-message* argument can be the ICMP message number, which is an integer from 0 to 255. It can also be one of the following keywords:

- **administratively-prohibited**—Administratively prohibited
- **alternate-address**—Alternate address
- **conversion-error**—Datagram conversion
- **dod-host-prohibited**—Host prohibited
- **dod-net-prohibited**—Net prohibited
- **echo**—Echo (ping)
- **echo-reply**—Echo reply

- **general-parameter-problem**—Parameter problem
- **host-isolated**—Host isolated
- **host-precedence-unreachable**—Host unreachable for precedence
- **host-redirect**—Host redirect
- **host-tos-redirect**—Host redirect for ToS
- **host-tos-unreachable**—Host unreachable for ToS
- **host-unknown**—Host unknown
- **host-unreachable**—Host unreachable
- **information-reply**—Information replies
- **information-request**—Information requests
- **mask-reply**—Mask replies
- **mask-request**—Mask requests
- **mobile-redirect**—Mobile host redirect
- **net-redirect**—Network redirect
- **net-tos-redirect**—Net redirect for ToS
- **net-tos-unreachable**—Network unreachable for ToS
- **net-unreachable**—Net unreachable
- **network-unknown**—Network unknown
- **no-room-for-option**—Parameter required but no room
- **option-missing**—Parameter required but not present
- **packet-too-big**—Fragmentation needed and DF set
- **parameter-problem**—All parameter problems
- **port-unreachable**—Port unreachable
- **precedence-unreachable**—Precedence cutoff
- **protocol-unreachable**—Protocol unreachable
- **reassembly-timeout**—Reassembly timeout
- **redirect**—All redirects
- **router-advertisement**—Router discovery advertisements
- **router-solicitation**—Router discovery solicitations
- **source-quench**—Source quenches
- **source-route-failed**—Source route failed
- **time-exceeded**—All time exceeded messages
- **timestamp-reply**—Timestamp replies
- **timestamp-request**—Timestamp requests
- **traceroute**—Traceroute
- **ttl-exceeded**—TTL exceeded
- **unreachable**—All unreachables

### TCP Port Names

When you specify the *protocol* argument as **tcp**, the *port* argument can be a TCP port number, which is an integer from 0 to 65535. It can also be one of the following keywords:

**bgp**—Border Gateway Protocol (179)

**chargen**—Character generator (19)

**cmd**—Remote commands (rcmd, 514)

**daytime**—Daytime (13)

**discard**—Discard (9)

**domain**—Domain Name Service (53)

**drip**—Dynamic Routing Information Protocol (3949)

**echo**—Echo (7)

**exec**—Exec (rsh, 512)

**finger**—Finger (79)

**ftp**—File Transfer Protocol (21)

**ftp-data**—FTP data connections (2)

**gopher**—Gopher (7)

**hostname**—NIC hostname server (11)

**ident**—Ident Protocol (113)

**irc**—Internet Relay Chat (194)

**klogin**—Kerberos login (543)

**kshell**—Kerberos shell (544)

**login**—Login (rlogin, 513)

**lpd**—Printer service (515)

**nntp**—Network News Transport Protocol (119)

**pim-auto-rp**—PIM Auto-RP (496)

**pop2**—Post Office Protocol v2 (19)

**pop3**—Post Office Protocol v3 (11)

**smtp**—Simple Mail Transport Protocol (25)

**sunrpc**—Sun Remote Procedure Call (111)

**tacacs**—TAC Access Control System (49)

**talk**—Talk (517)

**telnet**—Telnet (23)

**time**—Time (37)

**uucp**—UNIX-to-UNIX Copy Program (54)

**whois**—WHOIS/NICNAME (43)

**www**—World Wide Web (HTTP, 8)

### UDP Port Names

When you specify the *protocol* argument as **udp**, the *port* argument can be a UDP port number, which is an integer from 0 to 65535. It can also be one of the following keywords:

**biff**—Biff (mail notification, comsat, 512)

**bootpc**—Bootstrap Protocol (BOOTP) client (68)

**bootps**—Bootstrap Protocol (BOOTP) server (67)

**discard**—Discard (9)

**dnsix**—DNSIX security protocol auditing (195)

**domain**—Domain Name Service (DNS, 53)

**echo**—Echo (7)

**isakmp**—Internet Security Association and Key Management Protocol (5)

**mobile-ip**—Mobile IP registration (434)

**nameserver**—IEN116 name service (obsolete, 42)

**netbios-dgm**—NetBIOS datagram service (138)

**netbios-ns**—NetBIOS name service (137)

**netbios-ss**—NetBIOS session service (139)

**non500-isakmp**—Internet Security Association and Key Management Protocol (45)

**ntp**—Network Time Protocol (123)

**pim-auto-rp**—PIM Auto-RP (496)

**rip**—Routing Information Protocol (router, in.routed, 52)

**snmp**—Simple Network Management Protocol (161)

**snmptrap**—SNMP Traps (162)

**sunrpc**—Sun Remote Procedure Call (111)

**syslog**—System Logger (514)

**tacacs**—TAC Access Control System (49)

**talk**—Talk (517)

**tftp**—Trivial File Transfer Protocol (69)

**time**—Time (37)

**who**—Who service (rwho, 513)

**xdmcp**—X Display Manager Control Protocol (177)

## Examples

This example shows how to configure an IPv4 ACL named acl-lab-01 with rules permitting all TCP and UDP traffic from the 10.23.0.0 and 192.168.37.0 networks to the 10.176.0.0 network:

```
n1000v# config t
n1000v(config)# ip access-list acl-lab-01
n1000v(config-acl)# permit tcp 10.23.0.0/16 10.176.0.0/16
n1000v(config-acl)# permit udp 10.23.0.0/16 10.176.0.0/16
n1000v(config-acl)# permit tcp 192.168.37.0/16 10.176.0.0/16
n1000v(config-acl)# permit udp 192.168.37.0/16 10.176.0.0/16
```

This example shows how to configure an IPv4 ACL named acl-eng-to-marketing with a rule that permits all IP traffic from an IP-address object group named eng_workstations to an IP-address object group named marketing_group:

```
n1000v# config t
n1000v(config)# ip access-list acl-eng-to-marketing
n1000v(config-acl)# permit ip addrgroup eng_workstations addrgroup marketing_group
```

## Related Commands

| Command | Description |
|---|---|
| **deny (IPv4)** | Configures a deny rule in an IPv4 ACL. |
| **ip access-list** | Configures an IPv4 ACL. |
| **remark** | Configures a remark in an ACL. |
| **show ip access-list** | Displays all IPv4 ACLs or one IPv4 ACL. |
| **statistics per-entry** | Enables collection of statistics for each entry in an ACL. |

# permit (MAC)

To create a MAC ACL rule that permits traffic matching its conditions, use the **permit** command. To remove a rule, use the **no** form of this command.

[*sequence-number*] **permit** *source destination* [*protocol*] [**cos** *cos-value*] [**vlan** *VLAN-ID*]

**no permit** *source destination* [*protocol*] [**cos** *cos-value*] [**vlan** *VLAN-ID*]

**no** *sequence-number*

## Syntax Description

| | |
|---|---|
| *sequence-number* | (Optional) Sequence number of the **permit** 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.<br>A sequence number can be any integer between 1 and 4294967295.<br>By default, the first rule in an ACL has a sequence number of 10.<br>If you do not specify a sequence number, the device adds the rule to the end of the ACL and assigns a sequence number that is 10 greater than the sequence number of the preceding rule.<br>Use the **resequence** command to reassign sequence numbers to rules. |
| *source* | Source MAC addresses that the rule matches. For details about the methods that you can use to specify this argument, see “Source and Destination” in the “Usage Guidelines” section. |
| *destination* | Destination MAC addresses that the rule matches. For details about the methods that you can use to specify this argument, see “Source and Destination” in the “Usage Guidelines” section. |
| *protocol* | (Optional) Protocol number that the rule matches. Valid protocol numbers are 0x0 to 0xffff. For listings of valid protocol names, see “MAC Protocols” in the “Usage Guidelines” section. |
| **cos** *cos-value* | (Optional) Specifies that the rule matches only packets with an IEEE 802.1Q header that contains the Class of Service (CoS) value given in the *cos-value* argument. The *cos-value* argument can be an integer from 0 to 7. |
| **vlan** *VLAN-ID* | (Optional) Specifies that the rule matches only packets with an IEEE 802.1Q header that contains the VLAN ID given. The *VLAN-ID* argument can be an integer from 1 to 4094. |

## Defaults

None

## Command Modes

MAC ACL configuration (config-acl)

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

A newly created MAC ACL contains no rules.

If you do not specify a sequence number, the device assigns a sequence number that is 10 greater than the last rule in the ACL.

When the device applies a MAC ACL to a packet, it evaluates the packet with every rule in the ACL. The device enforces the first rule that has conditions that are satisfied by the packet. When the conditions of more than one rule are satisfied, the device enforces the rule with the lowest sequence number.

### Source and Destination

You can specify the *source* and *destination* arguments in one of two ways. In each rule, the method you use to specify one of these arguments does not affect how you specify the other. When you configure a rule, use the following methods to specify the *source* and *destination* arguments:

- Address and mask—You can use a MAC address followed by a mask to specify a single address or a group of addresses. The syntax is as follows:

  *MAC-address MAC-mask*

  The following example specifies the *source* argument with the MAC address 00c0.4f03.0a72:

  ```
  n1000v(config-acl)# permit 00c0.4f03.0a72 0000.0000.0000 any
  ```

  The following example specifies the *destination* argument with a MAC address for all hosts with a MAC vendor code of 00603e:

  ```
  n1000v(config-acl)# permit any 0060.3e00.0000 0000.0000.0000
  ```

- Any address—You can use the **any** keyword to specify that a source or destination is any MAC address. For examples of the use of the **any** keyword, see the examples in this section. Each of the examples shows how to specify a source or destination by using the **any** keyword.

### MAC Protocols

The *protocol* argument can be the MAC protocol number or a keyword. The protocol number is a four-byte hexadecimal number prefixed with 0x. Valid protocol numbers are from 0x0 to 0xffff. Valid keywords are the following:

- **aarp**—Appletalk ARP (0x80f3)
- **appletalk**—Appletalk (0x809b)
- **decnet-iv**—DECnet Phase IV (0x6003)
- **diagnostic**—DEC Diagnostic Protocol (0x6005)
- **etype-6000**—Ethertype 0x6000 (0x6000)
- **etype-8042**—Ethertype 0x8042 (0x8042)
- **ip**—Internet Protocol v4 (0x0800)
- **lat**—DEC LAT (0x6004)
- **lavc-sca**—DEC LAVC, SCA (0x6007)
- **mop-console**—DEC MOP Remote console (0x6002)
- **mop-dump**—DEC MOP dump (0x6001)

- **vines-echo**—VINES Echo (0x0baf)

## Examples

This example shows how to configure a MAC ACL named mac-ip-filter with a rule that permits all IPv4 traffic between two groups of MAC addresses:

```
n1000v# config t
n1000v(config)# mac access-list mac-ip-filter
n1000v(config-mac-acl)# permit 00c0.4f00.0000 0000.00ff.ffff 0060.3e00.0000 0000.00ff.ffff
ip
```

## Related Commands

| Command | Description |
|---|---|
| **deny (MAC)** | Configures a deny rule in a MAC ACL. |
| **mac access-list** | Configures a MAC ACL. |
| **remark** | Configures a remark in an ACL. |
| **statistics per-entry** | Enables collection of statistics for each entry in an ACL. |
| **show mac access-list** | Displays all MAC ACLs or one MAC ACL. |

# permit interface

To specify the interfaces that users assigned to this role can access, use the **permit interface** command.

To remove the policy restrictions, use the **no** form of this command.

**permit interface** *interface-list*

**no permit interface** *interface-list*

## Syntax Description

| | |
|---|---|
| *interface-list* | List of one or more interfaces that can be accessed by users with a specified role. |

## Defaults

None

## Command Modes

Interface configuration (config-role-interface)

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

Repeat this command to specify all interface lists that users assigned to this role are permitted to access.

## Examples

This example shows how to specify ethernet 2/1-4 as interfaces that users assigned to this role can access:

```
n1000v# config t
n1000v(config)# role name network-observer
n1000v(config-role)# interface policy deny
n1000v(config-role-interface)# permit interface ethernet 2/1-4
n1000v(config-role-interface)#
```

This example shows how to remove the policy restrictions for ethernet 2/1-4:

```
n1000v# config t
n1000v(config)# role name network-observer
n1000v(config-role)# interface policy deny
n1000v(config-role-interface)# no permit interface ethernet 2/1-4
n1000v(config-role-interface)#
```

## Related Commands

| Command | Description |
|---|---|
| **role name** | Specifies a user role and enters role configuration mode for the named role. |
| **interface policy deny** | Enters the interface configuration mode and denies all interface access for the role. |
| **show role** | Displays the role configuration. |

# ping

To determine the network connectivity to another device using IPv4 addressing, use the **ping** command.

**ping** [*dest-ipv4-address* | *hostname* | **mulitcast** *multicast-group-address* **interface [ethernet** *slot/port* | **loopback** *number* | **mgmt0** | **port-channel** *channel-number* | **vethernet** *number*]] [**count** {*number* | **unlimited**}] [**df-bit**] [**interval** *seconds*] [**packet-size** *bytes*] [**source** *src-ipv4-address*] [**timeout** *seconds*] [**vrf** *vrf-name*]

## Syntax Description

| | |
|---|---|
| *dest-ipv4-address* | IPv4 address of destination device. The format is *A.B.C.D*. |
| *hostname* | Hostname of destination device. The hostname is case sensitive. |
| **multicast** | Multicast ping. |
| *multicast-group-address* | Multicast group address. The format is *A.B.C.D*. |
| **interface** | Specifies the interface to send the multicast packet. |
| **ethernet** *slot/port* | Specifies the slot and port number for the Ethernet interface. |
| **loopback** *number* | Specifies a virtual interface number from 0 to 1023. |
| **mgmt0** | Specifies the management interface. |
| **port-channel** *channel-number* | Specifies a port-channel interface in the range 1 to 4096. |
| **vethernet** *number* | Specifies a virtual Ethernet interface in the range 1 to 1048575. |
| **count** | (Optional) Specifies the number of transmissions to send. |
| *number* | Number of pings. The range is from 1 to 655350. The default is 5. |
| **unlimited** | Allows an unlimited number of pings. |
| **df-bit** | (Optional) Enables the do-not-fragment bit in the IPv4 header. The default is disabled. |
| **interval** *seconds* | (Optional) Specifies the interval in seconds between transmissions. The range is from 0 to 60. The default is 1 second. |
| **packet-size** *bytes* | (Optional) Specifies the packet size in bytes to transmit. The range is from 1 to 65468. The default is 56 bytes. |
| **source** *scr-ipv4-address* | (Optional) Specifies the source IPv4 address to use. The format is *A.B.C.D*. The default is the IPv4 address for the management interface of the device. |
| **timeout** *seconds* | (Optional) Specifies the nonresponse timeout interval in seconds. The range is from 1 to 60. The default is 2 seconds. |
| **vrf** *vrf-name* | (Optional) Specifies the virtual routing and forwarding (VRF) name. The default is the default VRF. |

## Defaults

For the default values, see the “Syntax Description” section for this command.

## Command Modes

Any

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

To determine the network connectivity to another device using IPv6 addressing, use the **ping6** command.

## Examples

This example shows how to determine connectivity to another device using IPv4 addressing:

```
n1000v# ping 172.28.231.246 vrf management
PING 172.28.231.246 (172.28.231.246): 56 data bytes
Request 0 timed out
64 bytes from 172.28.231.246: icmp_seq=1 ttl=63 time=0.799 ms
64 bytes from 172.28.231.246: icmp_seq=2 ttl=63 time=0.597 ms
64 bytes from 172.28.231.246: icmp_seq=3 ttl=63 time=0.711 ms
64 bytes from 172.28.231.246: icmp_seq=4 ttl=63 time=0.67 ms

--- 172.28.231.246 ping statistics ---
5 packets transmitted, 4 packets received, 20.00% packet loss
round-trip min/avg/max = 0.597/0.694/0.799 ms
```

## Related Commands

| Command | Description |
|---|---|
| **ping6** | Determines connectivity to another device using IPv6 addressing. |

# pinned-sgid

To pin control or packet VLAN traffic to a specific sub group, use the **pinning** command. To remove the configuration, use the **no** form of this command.

**pinned-sgid** {**control-vlan-pinned-sgid** | **packet-vlan-pinned-sgid**} *sub-group_id*

**no pinned-sgid** {**control-vlan-pinned-sgid** | **packet-vlan-pinned-sgid**} *sub-group_id*

## Syntax Description

| | |
|---|---|
| **control-vlan-pinned-sgid** | Specifies to pin control VLAN traffic to a specific sub group. |
| **packet-vlan-pinned-sgid** | Specifies to pin packet VLAN traffic to a specific sub group. |
| *sub-group-id* | ID number of the sub group. Range is from 0 to 31. |

## Defaults

None

## Command Modes

Port profile configuration (config-port-prof)

## SupportedUserRoles

network-admin

## Command History

| Release | Modification |
|---|---|
| 4.0(4)SV1(2) | This command was introduced. |

## Examples

This example shows how to pin traffic on the control VLAN to a sub group 0:

```
n1000v# config t
n1000v(config)# port-profile SystemProfile1
n1000v(config-port-prof)# pinned-sgid control-vlan-pinned-sgid 3
n1000v(config-port-prof)# show port-profile SystemProfile1
port-profile SystemProfile1
  description:
  type: ethernet
  status: disabled
  capability l3control: no
  pinning control-vlan: 3
  pinning packet-vlan: -
  system vlans: 1
  port-group: SystemProfile1
  max ports: -
  inherit:
  config attributes:
    switchport mode trunk
    switchport trunk allowed vlan 1-5
    no shutdown
  evaluated config attributes:
    switchport mode trunk
```

```
    switchport trunk allowed vlan 1-5
    no shutdown
  assigned interfaces:
n1000v(config-port-prof)# copy running-config startup-config
```

This example shows how to pin traffic on the packet VLAN to sub group 0:

```
n1000v# config t
n1000v(config)# port-profile SystemProfile1
n1000v(config-port-prof)# pinned-sgid packet-vlan-pinned-sgid 0
n1000v(config-port-prof)# show port-profile name SystemProfile1
port-profile SystemProfile1
  description:
  type: ethernet
  status: disabled
  capability l3control: no
  pinning control-vlan: -
  pinning packet-vlan: 0
  system vlans: 1
  port-group:
  max ports: -
  inherit:
  config attributes:
    switchport mode access
    switchport access vlan 1
    switchport trunk native vlan 1
    no shutdown
  evaluated config attributes:
    switchport mode access
    switchport access vlan 1
    switchport trunk native vlan 1
    no shutdown
  assigned interfaces:
n1000v(config-port-prof)# copy running-config startup-config
```

## Related Commands

| Command | Description |
|---|---|
| **show port-profile** [**brief** \| **expand-interface** \| **usage**] [**name** *profile-name*] | Displays port profile information. |
| **show running-config port-profile** *profile-name* | Displays the running configuration of the specified port profile, including the pinning configuration. |

# pinning id

To pin vEthernet traffic to a specific sub-group, use the **pinning id** command. To remove the configuration, use the no form of this command.

**pinning id** *sub-group-id*

**no pinning id**

## Syntax Description

| | |
|---|---|
| *sub-group-id* | ID number of the sub group. Range is from 0 to 31. |

## Defaults

None

## Command Modes

Interface configuration mode (config-if)
Port profile configuration (config-port-prof)

## SupportedUserRoles

network-admin

## Command History

| Release | Modification |
|---|---|
| 4.0(4)SV1(2) | This command was introduced. |

## Examples

This example shows how to pin vEthernet interfaces to sub-group 3:

```
n1000v(config)# config t
n1000v(config)# interface vethernet 1
n1000v(config-if)# pinning id 0
n1000v(config-if)# show running-config interface vethernet 1
version 4.0(4)SV1(2)

interface Vethernet3
  service-policy type qos input policy1
  pinning id 0

n1000v(config-if)# exit
n1000v(config)# exit
n1000v# module vem 3 execute vemcmd show pinning
  LTL    IfIndex  PC_LTL  VSM_SGID  VEM_SGID  Eff_SGID
   48   1b040000     304         0         0         0

n1000v(config-if)# copy running-config startup-config
```

## Related Commands

| Command | Description |
|---|---|
| **module vem** *module_number* **execute vemcmd show pinning** | Displays the pinning configuration on the specified VEM. |
| **show port-profile** [**brief** \| **expand-interface** \| **usage**] [**name** *profile-name*] | Displays port profile information. |
| **show running-config interface vethernet** *interface-number* | Displays the running configuration of the specified vEthernet interface, including the pinning configuration. |
| **show running-config port-profile** *profile-name* | Displays the running configuration of the specified port profile, including the pinning configuration. |

# police

To control traffic rates, use the **police** command. To remove control, use the **no** form of this command.

**police** {{[**cir**] {*cir* [**bps**|**kbps**|**mbps**|**gbps**] | **percent** *cir-percent*} [[**bc**] {*committed-burst* [**bytes**|**kbytes**|**mbytes**|**ms**|**us**]}] [**pir** {*pir-* [**bps2**|**kbps2**|**mbps2**|**gbps2**] | **percent** *pir-percent*} [[**be**] {*extended-burst* [**bytes2**|**kbytes2**|**mbytes2**|**ms2**|**us2**]}]] [**conform** {**transmit** | **set-prec-transmit** {*precedence-number*} | **set-dscp-transmit** {*dscp-value* | *dscp-number*} | **set-cos-transmit** *cos-value* | **set-discard-class-transmit** *discard-class-value* | **set-qos-transmit** *qos-group-value*} [**exceed** {**drop1** | **set** *exc-from-field exc-to-field* **table cir-markdown-map**}] [**violate** {**drop2** | **set** *vio-from-field vio-to-field* **table2 pir-markdown-map**}]]}}

**no police** {{[**cir**] {*cir* [**bps**|**kbps**|**mbps**|**gbps**] | **percent** *cir-percent*} [[**bc**] {*committed-burst* [**bytes**|**kbytes**|**mbytes**|**ms**|**us**]}] [**pir** {*pir* [**bps2**|**kbps2**|**mbps2**|**gbps2**] | **percent** *pir-percent*} [[**be**] {*extended-burst* [**bytes2**|**kbytes2**|**mbytes2**|**ms2**|**us2**]}]] [**conform** {**transmit** | **set-prec-transmit** {*precedence-number*} | **set-dscp-transmit** {*dscp-value* | *dscp-number*} | **set-cos-transmit** *cos-value* | **set-discard-class-transmit** *discard-class-value* | **set-qos-transmit** *qos-group-value*} [**exceed** {**drop1** | **set** *exc-from-field exc-to-field* **table cir-markdown-map**}] [**violate** {**drop2** | **set** *vio-from-field vio-to-field* **table2 pir-markdown-map**}]]}}

## Syntax Description

| | |
|---|---|
| **cir** | (Optional) Specifies CIR (Committed Information Rate). |
| *cir* | Committed Information Rate in **bps** or **kbps** or **mbps** or **gbps**. |
| **bps** | (Optional) Specifies bits per second. |
| **kbps** | (Optional) Specifies kilobits per second. |
| **mbps** | (Optional) Specifies megabits per second. |
| **gbps** | (Optional) Specifies gigabits per second. |
| **percent** | Specifies CIR (Committed Information Rate) percentage. |
| *cir-percent* | CIR percentage. |
| **bc** | (Optional) Specifies BC (Burst Commit). |
| *committed-burst* | Packet burst. |
| **bytes** | (Optional) Specifies burst size in bytes. |
| **kbytes** | (Optional) Specifies burst size in kilobytes. |
| **mbytes** | (Optional) Specifies burst size in megabytes. |
| **ms** | (Optional) Specifies burst interval in milliseconds. |
| **us** | (Optional) Specifies burst interval in microseconds. |
| **pir** | (Optional) Specifies PIR (Peak Information Rate). |
| *pir* | Peak Information Rate in **bps** or **kbps** or **mbps** or **gbps**. |
| **bps2** | (Optional) Specifies bits per second. |
| **kbps2** | (Optional) Specifies kilobits per second. |
| **mbps2** | (Optional) Specifies megabits per second. |
| **gbps2** | (Optional) Specifies gigabits per second. |
| **be** | (Optional) Specifies extended burst. |
| *extended-burst* | Extended packet burst. |

| | |
|---|---|
| **ms2** | (Optional) Specifies burst interval in milliseconds. |
| **us2** | (Optional) Specifies burst interval in microseconds. |
| **conform** | (Optional) Specifies a conform action. |
| **transmit** | Specifies packet transmission. |
| **set-prec-transmit** | Specifies a precedence and transmits it. |
| *precedence-number* | Precedence number. The following are valid numbers:<br>• 0—Routine precedence<br>• 1—Priority precedence<br>• i2—Immediate precedence<br>• 3—Flash precedence<br>• 4—Flash override precedence<br>• 5—Critical precedence<br>• 6—Internetwork control precedence<br>• 7— Network control precedence |
| **set-dscp-transmit** | Specifies a DSCP (Differentiated Services Code Point) and transmits it. |
| *dscp-number* | DSCP number or code. The range of valid values is 1 to 63. You can also set DSCP to one of the following codes:<br>• af11—AF11 dscp (001010)<br>• af12—AF12 dscp (001100)<br>• af13—AF13 dscp (001110)<br>• af21—AF21 dscp (010010)<br>• af22—AF22 dscp (010100)<br>• af23—AF23 dscp (010110)<br>• af31—AF31 dscp (011010)<br>• af32—AF32 dscp (011100)<br>• af33—AF33 dscp (011110)<br>• af41—AF41 dscp (100010)<br>• af42—AF42 dscp (100100)<br>• af43—AF43 dscp (100110)<br>• cs1—CS1(precedence 1) dscp (001000)<br>• cs2—CS2(precedence 2) dscp (010000)<br>• cs3—CS3(precedence 3) dscp (011000)<br>• cs4—CS4(precedence 4) dscp (100000)<br>• cs5—CS5(precedence 5) dscp (101000)<br>• cs6—CS6(precedence 6) dscp (110000)<br>• cs7—CS7(precedence 7) dscp (111000)<br>• default—default dscp (000000)<br>• ef—EF dscp (101110) |

| | |
|---|---|
| **set-cos-transmit** | Specifies a CoS number and transmits it. |
| *cos-value* | CoS group number. The range of valid values is 0 to 7. |
| **set-discard-class-transmit** | Specifies a discard class number and transmits it. |
| *discard-class-value* | The discard class number. The range of valid values is 0 to 63. |
| **set-qos-transmit** | Specifies a QoS group number and transmits it. |
| *qos-group-value* | QoS group number. The range of valid values is 0 to 126. |
| **exceed** | (Optional) Specifies an exceed action. |
| **drop1** | Specifies that packets are to be dropped. |
| **set** | Specifies a particular value in a table or markdown map. |
| *exc-from-field* | . |
| *exc-to-field* | . |
| **table** | . |
| **cir-markdown-map** | . |
| **violate** | (Optional) Specifies a violate action. |
| **drop2** | .Specifies that packets are to be dropped. |
| *vio-from-field* | . |
| *vio-to-field* | . |
| **table2** | . |
| **pir-markdown-map** | . |

## Defaults

None

## Command Modes

Policy map configuration (config-pmap-c-qos)

## SupportedUserRoles

network-admin

## Command History

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

## Examples

This example shows how to control traffic rates:

```
n1000v# configure terminal
n1000v(config)# policy-map pm10
n1000v(config-pmap-qos)# class class-default
n1000v(config-pmap-c-qos)# police 100000 bps 10000 bytes
n1000v(config-pmap-c-qos)#
```

**Related Commands**

| Command | Description |
|---|---|
| **show policy-map** | Displays the policy map configuration for all policy maps or for a specified policy map. |

# policy-map

To create and configure policy maps, use the **policy-map** command. To remove policy maps, use the **no** form of this command.

**policy-map** {*name* | **type qos** *name*}

**no policy-map** {*name* | **type qos** *name*}

## Syntax Description

| | |
|---|---|
| *name* | Policy map name. The range of valid values is 1 to 40. |
| **type qos** | Specifies the policy map type as QoS. |

## Defaults

The policy map does not exist.

## Command Modes

Global configuration (config)

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

When you create or configure a policy map, you automatically enter configure policy map mode.

## Examples

This example shows how to create policy maps:

```
n1000v# configure terminal
n1000v(config)# policy-map pm20
n1000v(config-pmap-qos)#
```

This example shows how to remove policy maps:

```
n1000v# configure terminal
n1000v(config)# no policy-map pm20
n1000v(config)#
```

## Related Commands

| Command | Description |
|---|---|
| **show policy-map** | Displays policy map information. |

# port-channel load-balance ethernet

To set the load-balancing method among the interfaces in the channel-group bundle, use the **port-channel load-balance ethernet** command. To return the system priority to the default value, use the **no** form of this command.

**port-channel load-balance ethernet** *method* [**module** *slot*]

**no port-channel load-balance ethernet** [*method* [**module** *slot*]]

## Syntax Description

| | |
|---|---|
| *method* | Load-balancing method. See the "Usage Guidelines" section for a list of valid values. |
| **module** | (Optional) Specifies a module number. The range is 1 to 66. |

## Defaults

Layer 2 packets—**source-mac**

Layer 3 packets—**source-mac**

## Command Modes

Global configuration (config)

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

When you do not specify a module, you are configuring load balancing for the entire device. When you use the **module** parameter, you are configuring load balancing for the specified modules

Valid *method* values are as follows:

- **dest-ip-port**—Loads distribution on the destination IP address and L4 port.
- **dest-ip-port-vlan**—Loads distribution on the destination IP address, L4 port, and VLAN.
- **destination-ip-vlan**—Loads distribution on the destination IP address and VLAN
- **destination-mac**—Loads distribution on the destination MAC address.
- **destination-port**—Loads distribution on the destination L4 port.
- **source-dest-ip-port**—Loads distribution on the source and destination IP address and L4 port.
- **source-dest-ip-port-vlan**—Loads distribution on the source and destination IP address, L4 port, and VLAN.
- **source-dest-ip-vlan**—Loads distribution on the source and destination IP address and VLAN.
- **source-dest-mac**—Loads distribution on the source and destination MAC address.
- **source-dest-port**—Loads distribution on the source and destination L4 port.

- **source-ip-port**—Loads distribution on the source IP address.
- **source-ip-port-vlan**—Loads distribution on the source IP address, L4, and VLAN
- **source-ip-vlan**—Loads distribution on the source IP address and VLAN.
- **source-mac**—Loads distribution on the source MAC address.
- **source-port**—Loads distribution on the source port.
- **source-virtual-port-id**—Loads distribution on the source virtual port ID.
- **vlan-only**—Loads distribution on the VLAN only.

Use the **module** argument to configure the module independently for port-channeling and load-balancing mode. When you do this, the remaining module use the current load-balancing method configured for the entire device, or the default method if you have not configured a method for the entire device. When you enter the **no** argument in conjunction with a **module** argument, the load-balancing method for the specified module takes the current load-balancing method that is in use for the entire device. If you configured a load-balancing method for the entire device, the specified module uses that configured method, rather than the default **source-mac**. The per module configuration takes precedence over the load-balancing method configured for the entire device.

Use the option that provides the balance criteria with the greatest variety in your configuration. For example, if the traffic on a port channel is going only to a single MAC address and you use the destination MAC address as the basis of port channel load balancing, the port channel always chooses the same link in that port channel; using source addresses or IP addresses might result in better load balancing.

## Examples

This example shows how to set the load-balancing method for the entire device to use the source port:

```
n1000v(config)# port-channel load-balance ethernet src-port
n1000v(config)#
```

## Related Commands

| Command | Description |
|---|---|
| **show port-channel load-balance** | Displays information on port-channel load balancing. |

# port-profile

To create a port profile and enter port-profile configuration mode, use the **port-profile** command. To remove the port profile configuration, use the **no** form of this command.

**port-profile [type {ethernet | vethernet}]** *profilename*

**no port-profile [type {ethernet | vethernet}]** *profilename*

## Syntax Description

| | |
|---|---|
| type | (Optional) Specify interface of type ethernet or vethernet. The default is vethernet. |
| *profilename* | Specifies the port profile name. The name can be up to 80 characters in length. |

## Defaults

Default type is vethernet.

## Command Modes

Global configuration (config)

## SupportedUserRoles

network-admin

## Command History

| Release | Modification |
|---|---|
| 4.0(4)SV1(2) | Port profiles are not classified as uplink, but are, instead, configured as type Ethernet or type vEthernet. |
| 4.0(4)SV1(1) | This command was introduced. |

## Usage Guidelines

The port profile name must be unique for each port profile on the Cisco Nexus 1000V.

The port profile type can be Ethernet or vEthernet. Once configured, the type cannot be changed.

Defining a port profile type as Ethernet allows the port profile to be used for physical (Ethernet) ports. In the vCenter Server, the corresponding port group can be selected and assigned to physical ports (PNICs).

If a port profile is configured as an Ethernet type, then it cannot be used to configure VMware virtual ports.

## Examples

This example shows how to create an Ethernet type port profile with the name AccessProf:

```
n1000v# configure terminal
n1000v(config)# port-profile type ethernet AccessProf
n1000v(config-port-prof)
```

This example shows how to remove the port profile with the name AccessProf:

```
n1000v# configure terminal
n1000v(config)# no port-profile AccessProf
n1000v(config)
```

**Related Commands**

| Command | Description |
|---|---|
| **show port-profile name** | Displays information about the port profiles. |

# port-security stop learning

To set the Drop on Source Miss (DSM) bit on the port so that it prevents the port from learning new MAC addresses, use the **port-security stop learning** command. To clear the DSM bit, use the **no** form of this command.

**port-security stop learning**

**no port-security stop learning**

## Syntax Description

This command has no arguments or keywords.

## Defaults

None

## Command Modes

Any

## SupportedUserRoles

network-admin
network-operatorr

## Command History

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

## Examples

This example shows how to set the DSM bit on the port:

```
n1000v# port-security stop learning
n1000v#
```

This example shows how to clear the DSM bit on the port:

```
n1000v# no port-security stop learning
n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **show port-security** | Displays the secured MAC addresses in the system. |
| **module vem execute** | Remotely executes commands on the Virtual Ethernet Module (VEM) from the Cisco Nexus 1000V. |
| **show cdp neighbors** | Displays the configuration and capabilities of upstream devices. |

# private-vlan association

To configure an association between a primary and secondary private VLAN, use the **private-vlan association** command. To remove the association, use the **no** form of this command.

**private-vlan association** [{**add** | **remove**}] *secondary-vlan-ids*

**no private-vlan association** [*secondary-vlan-ids*]

## Syntax Description

| | |
|---|---|
| **add** | Adds a secondary VLAN to a private VLAN list. |
| **remove** | Removes a secondary VLAN from a private VLAN list. |
| *secondary-vlan-ids* | IDs of the secondary VLANs to be added or removed. |

## Defaults

None

## Command Modes

VLAN (config-vlan)

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

You must enable the private VLAN feature (**feature private-vlan** command) before the private VLAN commands are visible in the CLI for configuration.

## Examples

This example shows how to associate primary VLAN 202 with secondary VLAN 303:

```
n1000v#configure t
n1000v(config)# vlan 202
n1000v(config-vlan)# private-vlan association add 303
n1000v(config-vlan)#
```

## Related Commands

| Command | Description |
|---|---|
| **private-vlan primary** | Designates the private VLAN as primary. |
| **private-vlan** {**community** \| **isolated**} | Designates the private VLAN as community or isolated. |
| **show vlan private-vlan** | Displays the private VLAN configuration. |

# private-vlan { community | isolated}

To designate a VLAN as either a community or isolated private VLAN, use the **private-vlan** {**community** | **isolated**} command. To remove the configuration, use the **no** form of this command.

**private-vlan** {**community** | **isolated**}

**no private-vlan** {**community** | **isolated**}

## Syntax Description

| | |
|---|---|
| **community** | Designates the VLAN as a community private VLAN. |
| **isolated** | Designates the VLAN as an isolated private VLAN. |

## Defaults

None

## Command Modes

VLAN (config-vlan)

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

You must enable the private VLAN feature (**feature private-vlan** command) before the private VLAN commands are visible in the CLI for configuration.

## Examples

This example shows how to configure VLAN 303 as a community private VLAN:

```
n1000v#configure t
n1000v(config)# vlan 303
n1000v(config-vlan)# private-vlan community
n1000v(config-vlan)#
```

## Related Commands

| Command | Description |
|---|---|
| **private-vlan primary** | Designates the private VLAN as primary. |
| **private-vlan association** | Configures an association between a primary VLAN and a secondary VLAN |
| **show vlan private-vlan** | Displays the private VLAN configuration. |

# private-vlan primary

To designate a private VLAN as a primary VLAN, use the **private-vlan primary** command. To remove the configuration, use the **no** form of this command.

**private-vlan primary**

**no private-vlan primary**

## Syntax Description

This command has no arguments or keywords.

## Defaults

None

## Command Modes

VLAN (config-vlan)

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

You must enable the private VLAN feature (**feature private-vlan** command) before the private VLAN commands are visible in the CLI for configuration.

## Examples

This example shows how to configure VLAN 202 as the primary VLAN in a private VLAN:

```
n1000v#configure t
n1000v(config)# vlan 202
n1000v(config-vlan)# private-vlan primary
n1000v(config-vlan)# show vlan private-vlan
Primary Secondary Type Ports
------- --------- --------------- ----------------------------------------------
202 primary
n1000v(config-vlan)#
```

## Related Commands

| Command | Description |
|---|---|
| **private-vlan** {**community** \| **isolated**} | Designates the private VLAN as community or isolated. |
| **show vlan private-vlan** | Displays the private VLAN configuration. |
| **private-vlan association** | Associates a primary and secondary private VLAN. |

# protocol vmware-vim

To enable the VMware VI SDK, use the **protocol vmware-vim** command. To disable the VMware VI SDK, use the **no** form of this command.

**protocol vmware-vim**

**no protocol vmware-vim**

## Syntax Description

This command has no arguments or keywords.

## Defaults

The VMware VI SDK is disabled.

## Command Modes

SVS connection configuration (config-svs-conn)

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

The VMware VI SDK is published by VMware and it allows clients to talk to VMware vCenter.

You must first create an SVS connection before you you enable the VMware VI SDK.

## Examples

This example shows how to enable the VMware VI SDK.:

```
n1000v# configure terminal
n1000v(config)# svs connection svs1
n1000v(config-svs-conn)# protocol vmware-vim
n1000v(config-svs-conn)#
```

## Related Commands

| Command | Description |
|---|---|
| **show svs connection** | Displays SVS connection information. |

# pwd

To view the current directory, use the **pwd** command.

**pwd**

## 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 view the current directory:

```
n1000v# pwd
bootflash:
n1000v#
```

# Q Commands

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

## qos statistics

To enable the recording of QoS statistics, use the **qos statistics** command. To disable the recording of QoS statistics,, use the **no** form of this command.

**qos statistics**

**no qos statistics**

**Syntax Description** This command has no arguments or keywords.

**Defaults** QoS statistics are not recorded.

**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 enable the recording of QoS statistics:

```
n1000v# configure terminal
n1000v(config)# qos statistics
n1000v(config)#
```

**Related Commands**

| Command | Description |
|---|---|
| **show policy-map** | Displays the policy map configuration for all policy maps or for a specified policy map. |

# R Commands

This chapter describes the Cisco Nexus 1000V commands that begin with the letter 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. |
| **test aaa** | Tests for AAA on a TACACS+ or RADIUS server or server group. |

# 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 virutal 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. |
| **test aaa** | Tests for AAA on a TACACS+ or RADIUS server or server group. |

# 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. |
| **test aaa** | Tests for AAA on a TACACS+ or RADIUS server or server group. |

# 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. |
| **test aaa** | Tests for AAA on a TACACS+ or RADIUS server or server group. |

# 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. |
| **test aaa** | Tests for AAA on a TACACS+ or RADIUS server or server group. |

# 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. |
| **test aaa** | Tests for AAA on a TACACS+ or RADIUS server or server group. |

# 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 1-1 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 1-1 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 1-1 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 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** | **protocol-port**} | **netflow-original**}

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

## Syntax Description

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

## Defaults

None

## Command Modes

Flow monitor configuration (config-flow-monitor)

## SupportedUserRoles

network-admin

## Command History

| Release | Modification |
|---|---|
| 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 module

To reload a module in the device, use the **reload module** command.

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

## Syntax Description

| | |
|---|---|
| *slot* | Chassis slot number. |
| **force-dnld** | (Optional) Forces the download of software to the module. |

## Defaults

None

## Command Modes

Any

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

Use the **show hardware** command to display information about the hardware on your device.

## Examples

This example shows how to reload a module:

```
n1000v# reload module 2
```

## Related Commands

| Command | Description |
|---|---|
| **show version** | Displays information about the software version. |

# 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. |

# 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. |

# 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. |

# 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). |

# S Commands

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

## send

To send a message to an open session, use the **send** command.

**send** {*message* | **session** *device message*}

**Syntax Description**

| | |
|---|---|
| *message* | Message. |
| **session** | Specifies a specific session. |
| *device* | Device type. |

**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 send a message to an open session:

```
n1000v# send session sessionOne testing
n1000v#
```

**Related Commands**

| Command | Description |
|---|---|
| **show banner** | Displays a banner. |

# server

To configure the RADIUS server as a member of the RADIUS server group, use the **server** command. To remove a server, use the **no** form of this command.

**server** {*ipv4-address* | *server-name*}

**no server** {*ipv4-address* | *server-name*}

## Syntax Description

| | |
|---|---|
| *ipv4-address* | IPV4 address of the RADIUS server. |
| *server-name* | Name that identifies the RADIUS server. |

## Defaults

None

## Command Modes

Radius configuration (config-radius)

## SupportedUserRoles

network-admin

## Command History

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

## Examples

This example shows how to configure the RADIUS server as a member of the RADIUS server group:

```
n1000v# config t
n1000v(config)# aaa group server radius RadServer
n1000v(config-radius)# server 10.10.1.1
n1000v(config-radius)#
```

This example shows how to remove the server configuration:

```
n1000v# config t
n1000v(config)# aaa group server radius RadServer
n1000v(config)# no server 10.10.1.1
```

## Related Commands

| Command | Description |
|---|---|
| **aaa group server radius** | Creates a RADIUS server group and enters the RADIUS server group configuration submode for that group. |
| **deadtime** | Configures the monitoring dead time. |
| **use-vrf** | Specifies the Virtual Routing and Forwarding (VRF) to use to contact the servers in the server group. |
| **show radius-server groups** | Displays the RADIUS server group configuration. |

# service-policy

To configure a service policy for an interface, use the **service-policy** command. To remove the service policy configuration, use the **no** form of this command.

**service-policy** {**input** *name* [**no-stats**] | **output** *name* [**no-stats**] | **type qos** {**input** *name* [**no-stats**] | **output** *name* [**no-stats**]}}

**no service-policy** {**input** *name* [**no-stats**] | **output** *name* [**no-stats**] | **type qos** {**input** *name* [**no-stats**] | **output** *name* [**no-stats**]}}

## Syntax Description

| | |
|---|---|
| **input** | Specifies an input service policy. |
| *name* | Policy name. The range of valid values is 1 to 40. |
| **no-stats** | (Optional) Specifies no statistics. |
| **output** | Specifies an output service policy. |
| **type qos** | Specifies a QoS service policy. |

## Defaults

No service policy exists.

## Command Modes

Interface configuration (config-if)

## SupportedUserRoles

network-admin

## Command History

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

## Examples

This example shows how to configure a service policy for an interface:

```
n1000v# configure terminal
n1000v(config)# interface vethernet 10
n1000v(config-if)# service-policy type qos input sp10 no-stats
n1000v(config-if)#
```

This example shows how to remove a service policy configuration for an interface:

```
n1000v# configure terminal
n1000v(config)# interface vethernet 10
n1000v(config-if)# no service-policy type qos input sp10 no-stats
n1000v(config-if)#
```

## Related Commands

| Command | Description |
|---|---|
| **show running interface** | Displays interface configuration information. |

# service-port

To configure an inside or outside interface in a virtual service domain (VSD) port profile, use the **service-port** command. To remove the configuration, use the **no** form of this command.

**service-port** {**inside** | **outside**} **default-action** {**drop** | **forward**}

**no service-port**

## Syntax Description

| | |
|---|---|
| **inside** | Inside Network |
| **outside** | Outside Network |
| **default-action** | Action to be taken if service port is down.<br>• **drop**: drops packets<br>• **forward**: forwards packets |

## Defaults

None

## Command Modes

Port profile configuration (config-port-prof)

## SupportedUserRoles

network-admin

## Command History

| Release | Modification |
|---|---|
| 4.0(4)SV1(2) | This command was introduced. |

## Usage Guidelines

If a port profile without a service port is configured on an SVM, it will flood the network with packets.

When configuring a port profile on an SVM, first bring the SVM down, This prevents a port-profile that is mistakenly configured without a service port from flooding the network with packets. The SVM can be returned to service after the configuration is complete and verified.

The **service-port** command is configurable only after the port-profile is configured for trunk mode and the virtual-service-domain has been configured.

**Caution** You should not add packet and control VLANs to the allowed VLAN list of a port-profile that has the service port configured. This causes a loop.

## Examples

This example shows how to configure an inside interface on a VSD port profile that drops packets if the service port is down:

```
n1000v# config t
n1000v(config)# port-profile svm_vsd1_in
```

```
n1000v(config-port-prof)# switchport mode trunk
n1000v(config-port-prof)# virtual-service-domain test
n1000v(config-port-prof)# service-port inside default-action drop
n1000v(config-port-prof)#
```

This example shows how to remove a service port configuration:

```
n1000v# config t
n1000v(config)# port-profile svm_vsd1_in
n1000v(config-port-prof)# no service-port
n1000v(config-port-prof)#
```

**Related Commands**

| Command | Description |
|---|---|
| **show virtual-service-domain brief** | Displays a list of the VSDs currently configured in a VSM, including VSD names and port profiles. |
| **show virtual-service-domain interface** | Displays a list of currently assigned interfaces to the VSDs in a VSM. |
| **show virtual-service-domain name** | Displays a specific VSD currently configured in a VSM. |

# session-limit

To limit the number of VSH sessions, use the **session-limit** command. To remove the limit, use the **no** form of this command.

**session-limit** *number*

**no session-limit** *number*

## Syntax Description

| | |
|---|---|
| *number* | Number of VSH sessions. The range of valid values is 1 to 64 |

## Defaults

No limit is set.

## Command Modes

Line configuration (config-line)

## SupportedUserRoles

network-admin

## Command History

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

## Examples

This example shows how to limit the number of VSH sessions:

```
n1000v# configure terminal
n1000v(config)# line vty
n1000v(config-line)# session-limit 10
n1000v(config-line)#
```

This example shows how to remove the limit:

```
n1000v# configure terminal
n1000v(config)# line vty
n1000v(config-line)# no session-limit 10
n1000v(config-line)#
```

# set

To set QoS class attributes, use the **set** command. To remove class attributes, use the **no** form of this command.

**set** {{**cos** *cos-val*} | {**dscp** [**tunnel**] {*dscp-val* | *dscp-enum*}} | {**precedence** [**tunnel**] {*prec-val* | *prec-enum*}} | {**discard-class** *dis-class-val*} | {**qos-group** *qos-grp-val*} | {{{**cos cos**} | {**dscp dscp**} | {**precedence precedence**} | {**discard-class discard-class**}} **table** *table-map-name*} | {**cos1** {{**dscp table cos-dscp-map**} | {**precedence table cos-precedence-map**} | {**discard-class table cos-discard-class-map**}}} | {**dscp1** {{**cos table dscp-cos-map**} | {**prec3 table dscp-precedence-map**} | {**dis-class3 table dscp-discard-class-map**}}} | {**prec1** {{**cos3 table precedence-cos-map**} | {**dscp3 table precedence-dscp-map**} | {**dis-class3 table precedence-discard-class-map**}}} | {**dis-class1** {{**cos3 table discard-class-cos-map**} | {**dscp3 table discard-class-dscp-map**} | {**prec3 table discard-class-precedence-map**}}}}

**no set** {{**cos** *cos-val*} | {**dscp** [**tunnel**] {*dscp-val* | *dscp-enum*}} | {**precedence** [**tunnel**] {*prec-val* | *prec-enum*}} | {**discard-class** *dis-class-val*} | {**qos-group** *qos-grp-val*} | {{{**cos cos**} | {**dscp dscp**} | {**precedence precedence**} | {**discard-class discard-class**}} **table** *table-map-name*} | {**cos1** {{**dscp table cos-dscp-map**} | {**precedence table cos-precedence-map**} | {**discard-class table cos-discard-class-map**}}} | {**dscp1** {{**cos table dscp-cos-map**} | {**prec3 table dscp-precedence-map**} | {**dis-class3 table dscp-discard-class-map**}}} | {**prec1** {{**cos3 table precedence-cos-map**} | {**dscp3 table precedence-dscp-map**} | {**dis-class3 table precedence-discard-class-map**}}} | {**dis-class1** {{**cos3 table discard-class-cos-map**} | {**dscp3 table discard-class-dscp-map**} | {**prec3 table discard-class-precedence-map**}}}}

## Syntax Description

| | |
|---|---|
| **cos** | Specifies IEEE 802.1Q CoS (Class of Service). |
| *cos-value* | CoS value. The range of valid values is 0 to 7. |
| **dscp** | Specifies DSCP (Differentiated Services Code Point) in IPv4 and IPv6 packets. |
| **tunnel** | (Optional) Specifies DSCP in tunnel encapsulation. |
| *dscp-value* | DSCP value. |
| *dscp-enum* | |
| **precedence** | Precedence in IP(v4) and IPv6 packets. |
| *prec-val* | IP Precedence value. |
| *prec-enum* | . |
| **discard-class** *dis-class-val* | Discard class + Discard class value. |
| **qos-group** *qos-grp-val* | Qos-group + Qos-group value. |
| **table** *table-map-name* | Table defining mapping from input to output + Table-map name. |
| **cos1** | IEEE 802.1Q class of service. |
| **cos-dscp-map** | Cos to DSCP Mutation map. |
| **cos-precedence-map** | Cos to Precedence Mutation map. |
| **cos-discard-class-map** | Cos to Discard Class Mutation map. |

| | |
|---|---|
| **dscp1** | DSCP in IP(v4) and IPv6 packets. |
| **dscp-cos-map** | DSCP to COS Mutation map. |
| **prec3** | Precedence in IP(v4) and IPv6 packets. |
| **dscp-precedence-map** | DSCP to Precedence Mutation map. |
| **dis-class3** | Discard class. |
| **dscp-discard-class-map** | DSCP to Discard Class Mutation map. |
| **prec1** | Precedence in IP(v4) and IPv6 packets. |
| **cos3** | IEEE 802.1Q class of service. |
| **precedence-cos-map** | Precedence to COS Mutation map. |
| **dscp3** | DSCP in IP(v4) and IPv6 packets. |
| **precedence-dscp-map** | Precedence to DSCP Mutation map. |
| **precedence-discard-class-map** | Precedence to Discard Class Mutation map. |
| **dis-class1** | Discard class. |
| **discard-class-cos-map** | Discard Class to COS Mutation map. |
| **discard-class-dscp-map** | Discard Class to DSCP Mutation map. |
| **discard-class-precedence-map** | Discard Class to Precedence Mutation map. |

## Defaults

None

## Command Modes

Policy map class configuration (config-pmap-c-qos)

## SupportedUserRoles

network-admin

## Command History

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

## Examples

This example shows how to set class attributes:

```
n1000v# configure terminal
n1000v(config)# policy-map pm1
n1000v(config-pmap-qos)# class class-default
n1000v(config-pmap-c-qos)# set qos-group 1
```

```
n1000v(config-pmap-c-qos)#
```

This example shows how to remove class attributes:

```
n1000v# configure terminal
n1000v(config)# policy-map pm1
n1000v(config-pmap-qos)# class class-default
n1000v(config-pmap-c-qos)# no set qos-group 1
n1000v(config-pmap-c-qos)#
```

**Related Commands**

| Command | Description |
|---|---|
| **show policy-map** | Displays policy maps. |

# setup

To use the Basic System Configuration Dialog for creating or modifying a configuration file, use the **setup** command.

**setup**

## Syntax Description

This command has no arguments or keywords, but the Basic System Configuration Dialog prompts you for complete setup information (see the example below).

## Defaults

None

## Command Modes

Any

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

The Basic System Configuration Dialog assumes the factory defaults. Keep this in mind when using it to modify an existing configuration.

All changes made to your configuration are summarized for you at the completion of the setup sequence with an option to save the changes or not.

You can exit the setup sequence at any point by pressing Ctrl-C.

## Examples

This example shows how to use the setup command to create or modify a basic system configuration:

```
n1000v# setup


  Enter the domain id<1-4095>: 400

  Enter HA role[standalone/primary/secondary]: standalone

[########################################] 100%


          ---- Basic System Configuration Dialog ----

This setup utility will guide you through the basic configuration of
the system. Setup configures only enough connectivity for management
of the system.

*Note: setup is mainly used for configuring the system initially,
```

```
when no configuration is present. So setup always assumes system
defaults and not the current system configuration values.

Press Enter at anytime to skip a dialog. Use ctrl-c at anytime
to skip the remaining dialogs.

Would you like to enter the basic configuration dialog (yes/no): y

  Create another login account (yes/no) [n]: n

  Configure read-only SNMP community string (yes/no) [n]: n

  Configure read-write SNMP community string (yes/no) [n]: n

  Enter the switch name : n1000v

  Continue with Out-of-band (mgmt0) management configuration? (yes/no) [y]:

    Mgmt0 IPv4 address :

  Configure the default gateway? (yes/no) [y]: n

  Configure advanced IP options? (yes/no) [n]:

  Enable the telnet service? (yes/no) [y]:

  Enable the ssh service? (yes/no) [n]:

  Configure the ntp server? (yes/no) [n]:

  Configure vem feature level? (yes/no) [n]:

  Configure svs domain parameters? (yes/no) [y]:

    Enter SVS Control mode (L2 / L3) : l2
    Invalid SVS Control Mode
    Enter SVS Control mode (L2 / L3) : L2
    Enter control vlan <1-3967, 4048-4093> : 400

    Enter packet vlan <1-3967, 4048-4093> : 405

The following configuration will be applied:
  switchname n1000v
  telnet server enable
  no ssh server enable
  svs-domain
    svs mode L2
    control vlan 400
    packet vlan 405
    domain id 400
vlan 400
vlan 405

Would you like to edit the configuration? (yes/no) [n]:

Use this configuration and save it? (yes/no) [y]: n

n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **show running-config** | Displays the running configuration. |

# shutdown

To shutdown VLAN switching, use the **shutdown** command. To turn on VLAN switching, use the **no** form of this command.

**shutdown**

**no shutdown**

## Syntax Description

This command has no arguments or keywords.

## Defaults

None

## Command Modes

VLAN configuration (config-vlan)

## SupportedUserRoles

network-admin

## Command History

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

## Examples

This example shows how to shutdown VLAN switching:

```
n1000v# configure terminal
n1000v(config)# vlan 10
n1000v(config-vlan)# shutdown
n1000v(config-vlan)#
```

This example shows how to turn on VLAN switching:

```
n1000v# configure terminal
n1000v(config)# vlan 10
n1000v(config-vlan)# no shutdown
n1000v(config-vlan)#
```

## Related Commands

| Command | Description |
|---|---|
| **show vlan** | Displays VLAN information. |

# sleep

To set a sleep time, use the **sleep** command.

**sleep** *time*

## Syntax Description

| | |
|---|---|
| *time* | Sleep time, in seconds. The range of valid values is 0 to 2147483647. |

## Defaults

Sleep time is not set.

## Command Modes

Any

## SupportedUserRoles

network-admin
network-operator

## Command History

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

## Usage Guidelines

When you set *time* to 0, sleep is disabled.

## Examples

This example shows how to set a sleep time:

```
n1000v# sleep 100
n1000v#
```

This example shows how to disable sleep:

```
n1000v# sleep 0
n1000v#
```

# snmp-server aaa-user cache-timeout

To configure how long the AAA-synchronized user configuration stays in the local cache, use the **snmp-server aaa-user cache-timeout** command. To revert back to the default value of 3600 seconds, use the **no** form of this command.

**snmp-server user aaa-user cache-timeout** *seconds*

**no snmp-server user aaa-user cache-timeout** *seconds*

## Syntax Description

| | |
|---|---|
| *seconds* | Length of the time for the user configuration to remain in the local cache. The range is 1 to 86400 seconds. |

## Defaults

The default timeout is 3600 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 AAA-synchronized user configuration to stay in the local cache for 1200 seconds:

```
n1000v# config t
n1000v(config)# snmp-server aaa-user cache-timeout 1200
```

This example shows how to revert back to the default value of 3600 seconds:

```
n1000v# config t
n1000v(config)# no snmp-server aaa-user cache-timeout 1200
```

## Related Commands

| Command | Description |
|---|---|
| **show snmp** | Displays SNMP information. |
| **snmp-server contact** | Configures sysContact, (the SNMP contact). |
| **snmp-server protocol enable** | Enables the SNMP protocol. |
| **snmp-server globalEnforcePriv** | Enforces SNMP message encryption for all users. |
| **snmp-server host** | Configures a host receiver for SNMP traps or informs. |
| **snmp-server location** | Configures sysLocation (the SNMP location). |

| Command | Description |
|---|---|
| **snmp-server tcp-session** | Enables a one-time authentication for SNMP over a TCP session. |
| **snmp-server user** | Configures an SNMP user with authentication and privacy parameters. |

# snmp-server community

To create an SNMP community string and assign access privileges for the community, use the **snmp-server community** command.

To remove the community or its access privileges, use the **no** form of this command.

**snmp-server community** *string* [**group** *group-name*] [**ro** | **rw**]

**no snmp-server community** *string* [**group** *group-name*] [**ro** | **rw**]

## Syntax Description

| | |
|---|---|
| *string* | SNMP community string, which identifies the community. |
| **group** | (Optional) Specifies a group to which this community belongs. |
| *group-name* | Name that identifies an existing group. |
| **ro** | (Optional) Specifies read-only access for this community. |
| **rw** | (Optional) Specifies read-write access for this community. |

## Defaults

None

## 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 create SNMP communities for SNMPv1 or SNMPv2c.

## Examples

This example shows how to configure read-only access for the SNMP community called public:

```
n1000v# config t
n1000v(config)# snmp-server community public ro
```

This example shows how to remove the SNMP community called public:

```
n1000v# config t
n1000v(config)# no snmp-server community public
```

## Related Commands

| Command | Description |
|---|---|
| **show snmp** | Displays SNMP information. |
| **snmp-server aaa-user cache-timeout** | Configures how long the AAA-synchronized user configuration stays in the local cache. |
| **snmp-server contact** | Configures sysContact, (the SNMP contact). |
| **snmp-server protocol enable** | Enables SNMP. |
| **snmp-server globalEnforcePriv** | Enforces SNMP message encryption for all users. |
| **snmp-server host** | Configures a host receiver for SNMP traps or informs. |
| **snmp-server location** | Configures sysLocation (the SNMP location). |
| **snmp-server tcp-session** | Enables a one-time authentication for SNMP over a TCP session. |
| **snmp-server user** | Configures an SNMP user with authentication and privacy parameters. |
| **snmp-server community** | Creates an SNMP community string and assigns access privileges for the community. |

# snmp-server contact

To configure the sysContact, which is the SNMP contact name, use the **snmp-server contact** command.

To remove or modify the sysContact, use the **no** form of this command.

**snmp-server contact** [*name*]

**no snmp-server contact** [*name*]

## Syntax Description

| | |
|---|---|
| *name* | (Optional) SNMP contact name (sysContact), which can contain a maximum of 32 characters. |

## Defaults

None

## 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 create SNMP communities for SNMPv1 or SNMPv2c.

## Examples

This example shows how to configure the sysContact to be Admin:

```
n1000v# config t
n1000v(config)# snmp-server contact Admin
```

This example shows how to remove the sysContact:

```
n1000v# config t
n1000v(config)# no snmp-server contact
```

## Related Commands

| Command | Description |
|---|---|
| **show snmp** | Displays SNMP information. |
| **snmp-server aaa-user cache-timeout** | Configures how long the AAA-synchronized user configuration stays in the local cache. |
| **snmp-server protocol enable** | Enables SNMP. |

| Command | Description |
|---|---|
| **snmp-server globalEnforcePriv** | Enforces SNMP message encryption for all users. |
| **snmp-server host** | Configures a host receiver for SNMP traps or informs. |
| **snmp-server location** | Configures sysLocation (the SNMP location). |
| **snmp-server tcp-session** | Enables a one-time authentication for SNMP over a TCP session. |
| **snmp-server user** | Configures an SNMP user with authentication and privacy parameters. |

# snmp-server globalEnforcePriv

To enforce SNMP message encryption for all users, use the **snmp-server globalEnforcePriv** command.

**snmp-server globalEnforcePriv**

## Syntax Description

This command has no arguments or keywords.

## 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 enforce SNMP message encryption for all users:

```
n1000v# config t
n1000v(config)# snmp-server mib globalEnforcePriv
```

## Related Commands

| Command | Description |
|---|---|
| **show snmp** | Displays SNMP information. |
| **snmp-server aaa-user cache-timeout** | Configures how long the AAA-synchronized user configuration stays in the local cache. |
| **snmp-server contact** | Configures sysContact, (the SNMP contact). |
| **snmp-server protocol enable** | Enables SNMP. |
| **snmp-server host** | Configures a host receiver for SNMP traps or informs. |
| **snmp-server location** | Configures sysLocation (the SNMP location). |
| **snmp-server tcp-session** | Enables a one-time authentication for SNMP over a TCP session. |
| **snmp-server user** | Configures an SNMP user with authentication and privacy parameters. |

# snmp-server host

To configure a host receiver for SNMPv1 or SNMPv2c traps, use the **snmp-server host** command. To remove the host, use the **no** form of this command.

**snmp-server host** *ip-address* {**traps** | **informs**}{**version** {**1** | **2c** | **3**}} [**auth** | **noauth** | **priv**] *community* [**udp_port** *number*]

**no snmp-server host** *ip-address* {**traps** | **informs**} {**version** {**1** | **2c** | **3**}} [**auth** | **noauth** | **priv**] *community* [**udp_port** *number*]

## Syntax Description

| | |
|---|---|
| *ip-address* | IPv4 address, IPv6 address, or DNS name of the SNMP notification host. |
| **informs** | Specifies Inform messages to this host. |
| **traps** | Specifies Traps messages to this host. |
| **version** | Specifies the SNMP version to use for notification messages. |
| **1** | Specifies SNMPv1 as the version. |
| **2c** | Specifies SNMPv2c as the version. |
| **3** | Specifies SNMPv3 as the version. |
| **auth** | (Optional) Specifies (for SNMPv3) the authNoPriv Security Level. |
| **noauth** | (Optional) Specifies (for SNMPv3) the noAuthNoPriv Security Level. |
| **priv** | (Optional) Specifies (for SNMPv3) the authPriv Security Level. |
| *community* | SNMPv1/v2c community string or SNMPv3 user name. The community string can be any alphanumeric string up to 255 characters. |
| **udp-port** | (Optional) Specifies an existing UDP port. |
| *number* | Number that identifies the UDP port of the notification host. The range is 0 to 65535. |

## Defaults

None

## Command Modes

Global configuration (config)

## SupportedUserRoles

network-admin

## Command History

| Release | Modification |
|---|---|
| 4.0(1) | This command was introduced. |

## Examples

This example shows how to configure the host receiver, 192.0.2.1, for SNMPv1 traps:

```
n1000v# config t
n1000v(config)# snmp-server host 192.0.2.1 traps version 1 public
```

This example shows how to remove the configuration:

```
n1000v# config t
n1000v(config)# no snmp-server host 192.0.2.1 traps version 1 public
```

## Related Commands

| Command | Description |
|---|---|
| **show snmp** | Displays SNMP information. |
| **snmp-server aaa-user cache-timeout** | Configures how long the AAA-synchronized user configuration stays in the local cache. |
| **snmp-server contact** | Configures sysContact, (the SNMP contact). |
| **snmp-server protocol enable** | Enables SNMP. |
| **snmp-server globalEnforcePriv** | Enforces SNMP message encryption for all users. |
| **snmp-server location** | Configures sysLocation (the SNMP location). |
| **snmp-server tcp-session** | Enables a one-time authentication for SNMP over a TCP session. |
| **snmp-server user** | Configures an SNMP user with authentication and privacy parameters. |

# snmp-server location

To configure the sysLocation, which is the SNMP location name, use the **snmp-server location** command.

To remove the sysLocation, use the **no** form of this command.

**snmp-server location** [*name*]

**no snmp-server location** [*name*]

## Syntax Description

| | |
|---|---|
| *name* | (Optional) SNMP location name (sysLocation), which can contain a maximum of 32 characters. |

## 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 configure the sysLocation to be Lab-7:

```
n1000v# config t
n1000v(config)# snmp-server location Lab-7
```

This example shows how to remove the sysLocation:

```
n1000v# config t
n1000v(config)# no snmp-server location
```

## Related Commands

| Command | Description |
|---|---|
| **show snmp** | Displays SNMP information. |
| **snmp-server aaa-user cache-timeout** | Configures how long the AAA-synchronized user configuration stays in the local cache. |
| **snmp-server contact** | Configures sysContact (the SNMP contact). |
| **snmp-server protocol enable** | Enables SNMP. |
| **snmp-server globalEnforcePriv** | Enforces SNMP message encryption for all users. |

| Command | Description |
|---|---|
| **snmp-server host** | Configures a host receiver for SNMP traps or informs. |
| **snmp-server tcp-session** | Enables a one-time authentication for SNMP over a TCP session. |
| **snmp-server user** | Configures an SNMP user with authentication and privacy parameters. |

# snmp-server protocol enable

To enable SNMP protocol operations, use the **snmp-server protocol enable** command. To disable SNMP protocol operations, use the **no** form of this command.

**snmp-server protocol enable**

**no snmp-server protocol enable**

## Syntax Description

This command has no arguments or keywords.

## Defaults

This command is enabled by default.

## 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 enable SNMP protocol operations:

```
n1000v# config t
n1000v(config)# snmp-server protocol enable
```

This example shows how to disable SNMP protocol operations:

```
n1000v# config t
n1000v(config)# no snmp-server protocol enable
```

## Related Commands

| Command | Description |
|---|---|
| **show snmp** | Displays SNMP information. |
| **snmp-server aaa-user cache-timeout** | Configures how long the AAA-synchronized user configuration stays in the local cache. |
| **snmp-server contact** | Configures sysContact (the SNMP contact). |
| **snmp-server globalEnforcePriv** | Enforces SNMP message encryption for all users. |
| **snmp-server host** | Configures a host receiver for SNMP traps or informs. |
| **snmp-server location** | Configures sysLocation (the SNMP location). |

| Command | Description |
|---|---|
| **snmp-server tcp-session** | Enables a one-time authentication for SNMP over a TCP session. |
| **snmp-server user** | Configures an SNMP user with authentication and privacy parameters. |

# snmp-server tcp-session

To enable authentication for SNMP over TCP, use the **snmp-server tcp-session** command. To disable authentication for SNMP over TCP, use the **no** form of this command.

**snmp-server tcp-session** [**auth**]

**no snmp-server tcp-session**

## Syntax Description

| | |
|---|---|
| **auth** | (Optional) Enables one-time authentication for SNMP over the entire TCP session (rather than on a per-command basis). |

## Defaults

This command is disabled by default.

## 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 enable one-time authentication for SNMP over TCP:

```
n1000v# config t
n1000v(config)# snmp-server tcp-session auth
```

This example shows how to disable one-time authentication for SNMP over TCP:

```
n1000v# config t
n1000v(config)# no snmp-server tcp-session
```

## Related Commands

| Command | Description |
|---|---|
| **show snmp** | Displays SNMP information. |
| **snmp-server aaa-user cache-timeout** | Configures how long the AAA-synchronized user configuration stays in the local cache. |
| **snmp-server contact** | Configures sysContact, (the SNMP contact). |
| **snmp-server protocol enable** | Enables SNMP. |
| **snmp-server globalEnforcePriv** | Enforces SNMP message encryption for all users. |
| **snmp-server host** | Configures a host receiver for SNMP traps or informs. |
| **snmp-server location** | Configures sysLocation (the SNMP location). |
| **snmp-server user** | Configures an SNMP user with authentication and privacy parameters. |

# snmp-server user

To define a user who can access the SNMP engine, use the **snmp-server user** command. To deny a user access to the SNMP engine, use the **no** form of this command.

**snmp-server user** *name* [**auth** {**md5** | **sha**} *passphrase-1* [**priv** [**aes-128**] *passphrase-2*] [**engineID** *id*] [**localizedkey**]]

**no snmp-server user** *name*

## Syntax Description

| | |
|---|---|
| *name* | Name of a user who can access the SNMP engine. |
| **auth** | (Optional) Enables one-time authentication for SNMP over a TCP session |
| **md5** | (Optional) Specifies HMAC MD5 algorithm for authentication. |
| **sha** | (Optional) Specifies HMAC SHA algorithm for authentication. |
| *passphrase-1* | Authentication passphrase for this user. The passphrase can be any case-sensitive alphanumeric string up to 64 characters. |
| **priv** | (Optional) Specifies encryption parameters for the user. |
| **aes-128** | (Optional) Specifies a 128-byte AES algorithm for privacy. |
| *passphrase-2* | Encryption passphrase for this user. The passphrase can be any case-sensitive alphanumeric string up to 64 characters. |
| **engineID** | (Optional) Specifies the engineID for configuring the notification target user (for V3 informs). |
| *id* | Number that identifies the engineID, in a 12-digit, colon-separated decimal format. |
| **localizedkey** | (Optional) Specifies the passphrase as any case-sensitive alphanumeric string up to 130 characters. |

## 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 provide one-time SNMP authorization for the user, Admin, using the HMAC SHA algorithm for authentication:

```
n1000v# config t
n1000v(config)# snmp-server user Admin auth sha abcd1234 priv abcdefgh
```

This example shows how to deny a user access to the SNMP engine:

```
n1000v# config t
n1000v(config)# no snmp-server user Admin
```

## Related Commands

| Command | Description |
|---|---|
| **show snmp** | Displays SNMP information. |
| **snmp-server aaa-user cache-timeout** | Configures how long the AAA-synchronized user configuration stays in the local cache. |
| **snmp-server contact** | Configures sysContact (the SNMP contact). |
| **snmp-server protocol enable** | Enables SNMP. |
| **snmp-server globalEnforcePriv** | Enforces SNMP message encryption for all users. |
| **snmp-server host** | Configures a host receiver for SNMP traps or informs. |
| **snmp-server location** | Configures sysLocation (the SNMP location). |
| **snmp-server tcp-session** | Enables a one-time authentication for SNMP over a TCP session. |

# snmp trap link-status

To enable SNMP link-state traps for the interface, use the **snmp trap link-status** command. To disable SNMP link-state traps for the interface, use the **no** form of this command.

**snmp trap link-status**

**no snmp trap link-status**

## Syntax Description

This command has no arguments or keywords.

## Defaults

None

## Command Modes

CLI interface configuration (config-if)

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

This command is enabled by default.

## Examples

This example shows how to enable SNMP link-state traps for the interface:

```
n1000v# config t
n1000v(config)# interface veth 2
n1000v(config-if)# snmp trap link-status
n1000v(config-if)#
```

This example shows how to disable SNMP link-state traps for the interface:

```
n1000v# config t
n1000v(config)# interface veth 2
n1000v(config-if)# no snmp trap link-status
n1000v(config-if)#
```

## Related Commands

| Command | Description |
|---|---|
| **interface vethernet** | Creates a virtual Ethernet interface and enters interface configuration mode. |
| **snmp-server enable traps** | Enables all SNMP notifications. |
| **snmp-server tcp-session** | Enables a one-time authentication for SNMP over a TCP session. |

# source mgmt (NetFlow)

To add an interface to a flow exporter designating it as the source for NetFlow flow records, use the **source** command. To remove the source interface from the flow exporter, use the **no** form of this command.

**source mgmt** *0*

**no source**

## Syntax Description

| | |
|---|---|
| **mgmt 0** | Adds the mgmt 0 interface to the flow exporter. |

## Defaults

None

## Command Modes

NetFlow flow exporter configuration (config-flow-exporter)

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

The mgmt0 interface is the only interface that can be added to the flow exporter.

## Examples

This example shows how to add source management interface 0 to the ExportTest flow exporter:

```
n1000v(config)# config t
n1000v(config)# flow exporter ExportTest
n1000v(config-flow-exporter)# source mgmt 0
```

This example shows how to remove source management interface 0 from the ExportTest flow exporter:

```
n1000v(config)# config t
n1000v(config)# flow exporter ExportTest
n1000v(config-flow-exporter)# no source mgmt 0
```

## Related Commands

| Command | Description |
|---|---|
| **flow exporter** | Creates a Flexible NetFlow flow exporter. |
| **flow record** | Creates a Flexible NetFlow flow record. |
| **flow monitor** | Creates a Flexible NetFlow flow monitor. |
| **show flow exporter** | Displays information about the NetFlow flow exporter. |

| Command | Description |
|---|---|
| **show flow record** | Displays information about NetFlow flow records. |
| **show flow monitor** | Displays information about the NetFlow flow monitor. |

# speed

To set the speed for an interface, use the **speed** command. To automatically set both the speed and duplex parameters to auto, use the **no** form of this command.

**speed** {*speed_val* | **auto** [**10 100** [**1000**]]}

**no speed** [{*speed_val* | **auto** [**10 100** [**1000**]]}]

## Syntax Description

| | |
|---|---|
| *speed_val* | Port speed on the interface, in Mbps. |
| **auto** | Sets the interface to autonegotiate the speed with the connecting port. |
| **10** | (Optional) Specifies a speed of 10 Mbps. |
| **100** | (Optional) Specifies a speed of 100 Mbps. |
| **1000** | (Optional) Specifies a speed of 1000 Mbps. |

## Defaults

None

## Command Modes

Interface configuration (config-if)

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

If you configure an Ethernet port speed to a value other than auto (for example, 10, 100, or 1000 Mbps), you must configure the connecting port to match. Do not configure the connecting port to negotiate the speed.

## Examples

This example shows how to set the speed of Ethernet port 1 on the module in slot 3 to 1000 Mbps:

```
n1000v config t
n1000v(config)# interface ethernet 2/1
n1000v(config-if)# speed 1000
```

This example shows how to automatically set the speed to auto:

```
n1000v config t
n1000v(config)# interface ethernet 2/1
n1000v(config-if)# no speed 1000
```

## Related Commands

| Command | Description |
|---|---|
| **interface** | Specifies the interface that you are configuring. |
| **duplex** | Specifies the duplex mode as full, half, or autonegotiate. |
| **show interface** | Displays the interface status, which includes the speed and duplex mode parameters. |

# ssh

To create a Secure Shell (SSH) session, use the **ssh** command.

**ssh** [*username*@]{*ipv4-address* | *hostname*} [**vrf** *vrf-name*]

## Syntax Description

| | |
|---|---|
| *username* | (Optional) Username for the SSH session. The user name is not case sensitive. |
| *ipv4-address* | IPv4 address of the remote device. |
| *hostname* | Hostname of the remote device. The hostname is case sensitive. |
| **vrf** *vrf-name* | (Optional) Specifies the virtual routing and forwarding (VRF) name to use for the SSH session. The VRF name is case sensitive. |

## Defaults

Default VRF

## Command Modes

Any

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

The NX-OS software supports SSH version 2.

## Examples

This example shows how to start an SSH session:

```
n1000v# ssh 10.10.1.1 vrf management
The authenticity of host '10.10.1.1 (10.10.1.1)' can't be established.
RSA key fingerprint is 9b:d9:09:97:f6:40:76:89:05:15:42:6b:12:48:0f:d6.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.10.1.1' (RSA) to the list of known hosts.
User Access Verification
Password:
```

## Related Commands

| Command | Description |
|---|---|
| **clear ssh session** | Clears SSH sessions. |
| **ssh server enable** | Enables the SSH server. |

# ssh key

To generate the key pair for the switch, which is used if SSH server is enabled, use the **ssh key** command. To remove the SSH server key, use the **no** form of this command.

**ssh key** {**dsa** [**force**] | **rsa** [*length* [**force**]]}

**no ssh key** [**dsa** | **rsa**]

## Syntax Description

| | |
|---|---|
| **dsa** | Specifies the Digital System Algrorithm (DSA) SSH server key. |
| **force** | (Optional) Forces the replacement of an SSH key. |
| **rsa** | Specifies the Rivest, Shamir, and Adelman (RSA) public-key cryptography SSH server key. |
| *length* | (Optional) Number of bits to use when creating the SSH server key. The range is from 768 to 2048. |

## Defaults

1024-bit length

## Command Modes

Global configuration (config)

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

The NX-OS software supports SSH version 2.

If you want to remove or replace an SSH server key, you must first disable the SSH server using the **no ssh server enable** command.

## Examples

This example shows how to create an SSH server key using DSA:

```
n1000v# config t
n1000v(config)# ssh key dsa
generating dsa key(1024 bits).....
..
generated dsa key
```

This example shows how to create an SSH server key using RSA with the default key length:

```
n1000v# config t
n1000v(config)# ssh key rsa
generating rsa key(1024 bits).....
.
```

```
generated rsa key
```

This example shows how to create an SSH server key using RSA with a specified key length:

```
n1000v# config t
n1000v(config)# ssh key rsa 768
generating rsa key(768 bits).....
.
generated rsa key
```

This example shows how to replace an SSH server key using DSA with the force option:

```
n1000v# config t
n1000v(config)# no ssh server enable
n1000v(config)# ssh key dsa force
deleting old dsa key.....
generating dsa key(1024 bits).....
.
generated dsa key
n1000v(config)# ssh server enable
```

This example shows how to remove the DSA SSH server key:

```
n1000v# config t
n1000v(config)# no ssh server enable
XML interface to system may become unavailable since ssh is disabled
n1000v(config)# no ssh key dsa
n1000v(config)# ssh server enable
```

This example shows how to remove all SSH server keys:

```
n1000v# config t
n1000v(config)# no ssh server enable
XML interface to system may become unavailable since ssh is disabled
n1000v(config)# no ssh key
n1000v(config)# ssh server enable
```

## Related Commands

| Command | Description |
|---|---|
| **show ssh key** | Displays the SSH server key information. |
| **ssh server enable** | Enables the SSH server. |

# ssh server enable

To enable the Secure Shell (SSH) server, use the **ssh server enable** command. To disable the SSH server, use the **no** form of this command.

**ssh server enable**

**no ssh server enable**

## 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

The NX-OS software supports SSH version 2.

## Examples

This example shows how to enable the SSH server:

```
n1000v# config t
n1000v(config)# ssh server enable
```

This example shows how to disable the SSH server:

```
n1000v# config t
n1000v(config)# no ssh server enable
XML interface to system may become unavailable since ssh is disabled
```

## Related Commands

| Command | Description |
|---|---|
| **show ssh server** | Displays the SSH server key information. |

# state (VLAN)

To set the operational state of a VLAN, use the **state** command. To disable state configuration, use the **no** form of this command.

**state** {**active** | **suspend**}

**no state**

## Syntax Description

| | |
|---|---|
| **active** | Specifies the active state. |
| **suspend** | Specifies the suspended state. |

## Defaults

None

## Command Modes

VLAN configuration (config-vlan)

## SupportedUserRoles

network-admin

## Command History

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

## Examples

This example shows how to set the operational state of a VLAN:

```
n1000v# configure terminal
n1000v(config)# vlan 10
n1000v(config-vlan)# state active
n1000v(config-vlan)#
```

This example shows how to disable state configuration:

```
n1000v# configure terminal
n1000v(config)# vlan 10
n1000v(config-vlan)# no state
n1000v(config-vlan)#
```

## Related Commands

| Command | Description |
|---|---|
| **show vlan** | Displays VLAN information. |

# state (Port Profile)

To set the operational state of a port profile, use the **state** command.

**state enabled**

## Syntax Description

| | |
|---|---|
| **enabled** | Enables or disables the port profile. |

## Defaults

Disabled

## Command Modes

Port profile configuration (config-port-prof)

## SupportedUserRoles

network-admin

## Command History

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

## Examples

This example shows how to enable or disable the operational state of a port profile:

```
n1000v# configure terminal
n1000v(config)# port-profile testprofile
n1000v(config-port-prof)# state enabled
n1000v(config-port-prof)#
```

## Related Commands

| Command | Description |
|---|---|
| **show port-profile** | Displays port profile information. |

# statistics per-entry

To collect statistics for each ACL entry, use the **statistics per-entry** command. To remove statistics, use the **no** form of this command.

**statistics per-entry**

**no statistics per-entry**

## Syntax Description

This command has no arguments or keywords.

## Defaults

No statistics are collected.

## Command Modes

ACL configuration (config-acl)

## SupportedUserRoles

network-admin

## Command History

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

## Examples

This example shows how to collect statistics for each ACL entry:

```
n1000v# configure terminal
n1000v(config)# ip access-list 1
n1000v(config-acl)# statistics per-entry
n1000v(config-acl)#
```

This example shows how to remove statistics:

```
n1000v# configure terminal
n1000v(config)# ip access-list 1
n1000v(config-acl)# no statistics per-entry
n1000v(config-acl)#
```

## Related Commands

| Command | Description |
|---|---|
| **show statistics** | Displays statistics. |

# sub-group

To configure interface port channel subgroup assignment, use the **sub-group** command. To remove this configuration, use the **no** form of this command.

**sub-group** {**cdp** | **manual**}

**no sub-group**

## Syntax Description

| | |
|---|---|
| **cdp** | Specifies that Cisco Discovery Protocol (CDP) information is used to automatically create subgroups for managing the traffic flow. |
| **manual** | Specifies that subgroups are configured manually. This option is used if CDP is not configured on the upstream switches. |

## Defaults

None

## Command Modes

Interface configuration (config-if)

## SupportedUserRoles

network-admin

## Command History

| Release | Modification |
|---|---|
| 4.0 | This command was introduced. |
| 4.0(4)SV1(2) | The **manual** keyword was added. |

## Usage Guidelines

Use this command to identify the port channel as being in vPC-HM, which requires traffic to be managed separately for each upstream switch connected to the member ports. If the upstream switches have CDP enabled, the Cisco Nexus 1000V can use this information to automatically assign subgroups. If the upstream swiches do not have CDP enabled, then you must configure subgroups manually.

This command overrides any subgroup configuration specified in the port-profile inherited by the port channel interface.

## Examples

This example shows how to configure a subgroup type for a port channel interface:

```
h1000v# config t
n1000v(config)# interface port-channel 1
n1000v(config-if)# sub-group cdp
```

This example shows how to remove the configuration:

```
h1000v# config t
n1000v(config)# interface port-channel 1
n1000v(config-if)# no sub-group
```

**Related Commands**

| Command | Description |
|---|---|
| **show interface port channel** *channel-number* | Displays port-channel information. |

# sub-group-id

To configure subgroup IDs for Ethernet member ports of vPC-HM, use the **sub-group-id** command. To remove the subgroup IDs, use the **no** form of this command.

**sub-group-id** *group_id*

**no sub-group-id**

## Syntax Description

| | |
|---|---|
| *group_id* | Subgroup ID number. Range is from 0 to 31. |

## Defaults

None

## Command Modes

Interface configuration (config-if)

## SupportedUserRoles

network-admin

## Command History

| Release | Modification |
|---|---|
| 4.0 | This command was introduced. |
| 4.0(4)SV1(2) | The number of subgroups was increased to 32. |

## Examples

This example shows how to configure an Ethernet member port on subgroup 5:

```
n1000v# config t
n1000v(config)# interface Ethernet 3/2
n1000v(config-if)# sub-group-id 1
```

This example shows how to remove the configuration:

```
n1000v# config t
n1000v(config)# interface Ethernet 3/2
n1000v(config-if)# no sub-group-id
```

## Related Commands

| Command | Description |
|---|---|
| **show interface ethernet** *slot/port* | Displays information about Ethernet interfaces. |

# svs connection

To enable an SVS connection, use the **svs connection** command. To disable an SVS connection, use the **no** form of this command.

**svs connection** *name*

**no svs connection** *name*

## Syntax Description

| | |
|---|---|
| *name* | Connection name. |

## Defaults

None

## Command Modes

Global configuration (config)

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

Only one SVS connection can be enabled per session.

## Examples

This example shows how to enable an SVS connection:

```
n1000v# configure terminal
n1000v(config)# svs connection conn1
n1000v(config-svs-conn)#
```

This example shows how to disable an SVS connection:

```
n1000v# configure terminal
n1000v(config)# no svs connection conn1
n1000v(config)#
```

## Related Commands

| Command | Description |
|---|---|
| **show svs** | Displays SVS information. |

# svs-domain

To configure an SVS domain and enter SVS domain configuration mode, use the **svs-domain** command.

**svs-domain**

## Syntax Description

This command has no arguments or keywords.

## 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 enter SVS domain configuration mode to configure an SVS domain:

```
n1000v# configure terminal
n1000v(config)# svs-domain
n1000v(config-svs-domain)#
```

## Related Commands

| Command | Description |
|---|---|
| **show svs** | Displays SVS information. |

# svs license transfer src-vem

To transfer licenses from a specified source VEM to another VEM, or to transfer an unused license to the VSM license pool, use the **svs license transfer src-vem** command.

**svs license transfer src-vem** *module number* [ **dst-vem** *module number* | **license_pool** ]

## Syntax Description

| | |
|---|---|
| **dst-vem** *module-number* | Specifies the VEM to receive the transferred license. |
| **license_pool** | Transfers a license back to the VSM license pool. |

## Defaults

None

## Command Modes

Global configuration (config)

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

- Licenses cannot be transferred to a VEM unless there are sufficient licenses in the pool for all CPUs on that VEM.
- When licenses are successfully transferred from one VEM to another, then the following happens:
  - The virtual Ethernet interfaces on the source VEM are removed from service.
  - The virtual Ethernet interfaces on the destination VEM are brought into service.
- When licenses are successfully transferred from a VEM to the VSM license pool, then the following happens:
  - The virtual Ethernet interfaces on the source VEM are removed from service.

## Examples

This example shows how to transfer a license from VEM 3 to VEM 5, and then display the license configuration:

```
n1000v# config t
n1000v(config)# svs license transfer src-vem 3 dst-vem 5
n1000v(config)# show license usage NEXUS1000V_LAN_SERVICES_PKG
Application
-----------
VEM 5 - Socket 1
VEM 5 - Socket 2
VEM 4 - Socket 1
VEM 4 - Socket 2
```

```
-----------

n1000v#
```

This example shows how to transfer a license from VEM 3 to the VSM license pool, and then display the license configuration:

```
n1000v# config t
n1000v(config)# svs license transfer src-vem 3 license_pool
n1000v(config)# show license usage NEXUS1000V_LAN_SERVICES_PKG
Application
-----------
VEM 4 - Socket 1
VEM 4 - Socket 2
-----------

n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **show license usage** | Displays the number and location of CPU licenses in use on your VEMs. |
| **logging level license** | Designates the level of severity at which license messages should be logged. |
| **install license** | Installs a license file(s) on a VSM. |
| **svs license transfer src-vem** | Transfers licenses from a source VEM to another VEM, or to the VSM pool of available licenses. |

# svs license volatile

To enable volatile licenses so that, whenever a VEM is taken out of service, its licenses are returned to the VSM pool of available licenses, use the **svs license volatile** command. To disable volatile licenses, use the **no** form of this command.

**svs license volatile**

**no svs license volatile**

## 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

**Caution** **Service Disruption**
Volatile licenses are removed from a VEM during a loss in connectivity and are not returned to the VEM when connectivity resumes. Cisco recommends that the volatile license feature remain disabled and that you, instead, transfer unused licenses using the **svs license transfer src-vem** command.

## Examples

This example shows how to enable the volatile license feature for a VSM:

```
n1000v(config)# svs license volatile
n1000v(config)#
```

This example shows how to disable the volatile license feature for a VSM:

```
n1000v(config)# no svs license volatile
```

## Related Commands

| Command | Description |
|---|---|
| **show license** | Displays the license configuration for the VSM. |
| **logging level license** | Designates the level of severity at which license messages should be logged. |
| **install license** | Installs a license file(s) on a VSM. |
| **svs license transfer src-vem** | Transfers licenses from a source VEM to another VEM, or to the VSM pool of available licenses. |

# svs mode

To configure a transport mode for control and packet traffic in the virtual supervisor module (VSM) domain, use the **svs mode** command.

**svs mode** {**L2** | **L3 interface** {**mgmt0** | **control0**}}

## Syntax Description

| | |
|---|---|
| **L2** | Specifies Layer 2 as the transport mode for the VSM domain. |
| **L3 interface** | Specifies Layer 3 as the transport mode for the VSM domain and configures the Layer 3 transport interface. |
| **mgmt0** | Specifies mgmt0 as the Layer 3 transport interface. |
| **control0** | Specifies control0 as the Layer 3 transport interface. |

## Defaults

Layer 2 mode

## Command Modes

SVS domain configuration (config-svs-domain)

## SupportedUserRoles

network-admin

## Command History

| Release | Modification |
|---|---|
| 4.0(4)SV1(2) | This command was introduced. |

## Usage Guidelines

If you use mgmt0 as the Layer 3 control interface, then in the VSM VM, Ethernet adapters 1 and 3 are not used.

If you use control0 as the Layer 3 control interface, then in the VSM VM, Ethernet adapter 3 is not used.

## Examples

This example shows how to configure mgmt0 as the Layer 3 transport interface for the VSM domain:

```
n1000v# config t
n1000v(config)# svs-domain
n1000v(config-svs-domain)# svs mode l3 interface mgmt0
n1000v(config-svs-domain)#
```

## Related Commands

| Command | Description |
|---|---|
| **show svs-domain** | Displays the VSM domain configuration. |
| **svs-domain** | Creates and configures the VSM domain. |

# switchname

To configure the hostname for the device, use the **switchname** command. To revert to the default, use the **no** form of this command.

**switchname** *name*

**no switchname**

## Syntax Description

| | |
|---|---|
| *name* | Name for the device. The name is alphanumeric, case sensitive, can contain special characters, and can have a maximum of 32 characters. |

## Defaults

switch

## Command Modes

Global configuration (config)

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

The Cisco NX-OS software uses the hostname in command-line interface (CLI) prompts and in default configuration filenames.

The **switchname** command performs the same function as the **hostname** command.

## Examples

This example shows how to configure the device hostname:

```
n1000v# configure terminal
n1000v(config)# switchname Engineering2
Engineering2(config)#
```

This example shows how to revert to the default device hostname:

```
Engineering2# configure terminal
Engineering2(config)# no switchname
n1000v(config)#
```

## Related Commands

| Command | Description |
|---|---|
| **hostname** | Configures the device hostname. |
| **show switchname** | Displays the device hostname. |

# switchport access vlan

To set the access mode of an interface, use the **switchport access vlan** command. To remove access mode configuration, use the **no** form of this command.

**switchport access vlan** *id*

**no switchport access vlan**

## Syntax Description

| | |
|---|---|
| *id* | VLAN identification number. The range of valid values is 1 to 3967. |

## Defaults

Access mode is not set.

## Command Modes

Interface configuration (config-if)
Port profile configuration (config-port-prof)

## SupportedUserRoles

network-admin

## Command History

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

## Examples

This example shows how to set the access mode of an interface:

```
n1000v# configure terminal
n1000v(config)# interface vethernet 1
n1000v(config-if)# switchport access vlan 10
n1000v(config-if)#
```

This example shows how to remove access mode configuration:

```
n1000v# configure terminal
n1000v(config)# interface vethernet 1
n1000v(config-if)# no switchport access vlan
n1000v(config-if)#
```

## Related Commands

| Command | Description |
|---|---|
| **show interface** | Displays interface information. |

# switchport mode

To set the port mode of an interface, use the **switchport mode** command. To remove the port mode configuration, use the **no** form of this command.

**switchport mode {access | private-vlan {host | promiscuous} | trunk}**

**no switchport mode {access | private-vlan {host | promiscuous} | trunk}**

## Syntax Description

| | |
|---|---|
| **access** | Sets port mode access. |
| **private-vlan** | Sets the port mode to private VLAN. |
| **host** | Sets the port mode private VLAN to host. |
| **promiscuous** | Sets the port mode private VLAN to promiscuous. |
| **trunk** | Sets the port mode to trunk. |

## Defaults

Switchport mode is not set.

## Command Modes

Interface configuration (config-if)
Port profile configuration (config-port-prof)

## SupportedUserRoles

network-admin

## Command History

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

## Examples

This example shows how to set the port mode of an interface:

```
n1000v# configure terminal
n1000v(config)# interface vethernet 1
n1000v(config-if)# switchport mode private-vlan host
n1000v(config-if)#
```

This example shows how to remove mode configuration:

```
n1000v# configure terminal
n1000v(config)# interface vethernet 1
n1000v(config-if)# no switchport mode private-vlan host
n1000v(config-if)#
```

## Related Commands

| Command | Description |
|---|---|
| **show interface** | Displays interface information. |

# switchport port-security

To set the port security characteristics of an interface, use the **switchport port-security** command. To remove the port security configuration, use the **no** form of this command.

**switchport port-security [aging {time** *time* **| type {absolute | inactivity}} | mac-address {***address* **[vlan** *id***] |sticky} | maximum** *number* **[vlan** *id***] | violation {protect | shutdown}]**

**no switchport port-security [aging {time** *time* **| type {absolute | inactivity}} | mac-address {***address* **[vlan** *id***] |sticky} | maximum** *number* **[vlan** *id***] | violation {protect | shutdown}]}**

## Syntax Description

| | |
|---|---|
| **aging** | Configures port security aging characteristics. |
| **time** | Specifies the port security aging time. |
| *time* | Aging time in minutes, in the range of 0 to 1440. |
| **type** | Specifies the type of timers. |
| **absolute** | Specifies an absolute timer. |
| **inactivity** | Specifies an inactivity timer. |
| **mac-address** *address* | Specifies a 48-bit MAC address in the format *HHHH.HHHH.HHHH*. |
| **vlan** | Specifies the VLAN where the MAC address should be secured. |
| *id* | VLAN identification number. The range of valid values is 1 to 4094. |
| **sticky** | Specifies a sticky MAC address. |
| **maximum** *number* | Specifies the maximum number of addresses, in the range of 1 to 1025. |
| **violation** | Specifies the security violation mode. |
| **protect** | Specifies the security violation protect mode. |
| **shutdown** | Specifies the security violation shutdown mode. |

## Defaults

None

## Command Modes

Interface configuration (config-if)
Port profile configuration (config-port-prof)

## SupportedUserRoles

network-admin

## Command History

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

## Examples

This example shows how to set the port security aging inactivity timer:

```
n1000v# configure terminal
n1000v(config)# interface vethernet 1
n1000v(config-if)# switchport port-security aging type inactivity
n1000v(config-if)#
```

This example shows how to remove the port security aging inactivity timer:

```
n1000v# configure terminal
n1000v(config)# interface vethernet 1
n1000v(config-if)# no switchport port-security aging type inactivity
n1000v(config-if)#
```

## Related Commands

| Command | Description |
|---|---|
| **show interface** | Displays interface information. |
| **show port-security** | Displays port security information. |

# switchport private-vlan host-association

To define a private VLAN association for an isolated or community port, use the **switchport private-vlan host-association** command. To remove the private VLAN association from the port, use the **no** form of this command.

**switchport private-vlan host-association** {*primary-vlan-id*} {*secondary-vlan-id*}

**no switchport private-vlan host-association**

## Syntax Description

| | |
|---|---|
| *primary-vlan-id* | Number of the primary VLAN of the private VLAN relationship. |
| *secondary-vlan-id* | Number of the secondary VLAN of the private VLAN relationship. |

## Defaults

None

## Command Modes

Interface configuration (config-if)
Port profile configuration (config-port-prof)

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

There is no run-time effect on the port unless it is in private VLAN-host mode. If the port is in private VLAN-host mode but neither of the VLANs exist, the command is allowed but the port is made inactive. The port also may be inactive when the association between the private VLANs is suspended.

The secondary VLAN may be an isolated or community VLAN.

## Examples

This example shows how to configure a host private VLAN port with a primary VLAN (VLAN 18) and a secondary VLAN (VLAN 20):

```
n1000v(config-if)# switchport private-vlan host-association 18 20
n1000v(config-if)#
```

This example shows how to remove the private VLAN association from the port:

```
n1000v(config-if)# no switchport private-vlan host-association
n1000v(config-if)#
```

**Related Commands**

| Command | Description |
|---|---|
| **show vlan private-vlan [type]** | Displays information on private VLANs. |

# switchport private-vlan mapping

To define the private VLAN association for a promiscuous port, use the **switchport private-vlan mapping** command. To clear all mapping from the primary VLAN, use the **no** form of this command.

**switchport private-vlan mapping** {*primary-vlan-id*} {[**add**] *secondary-vlan-list* | **remove** *secondary-vlan-list*}

**no switchport private-vlan mapping**

## Syntax Description

| | |
|---|---|
| *primary-vlan-id* | Number of the primary VLAN of the private VLAN relationship. |
| **add** | Associates the secondary VLANs to the primary VLAN. |
| *secondary-vlan-list* | Number of the secondary VLAN of the private VLAN relationship. |
| **remove** | Clears the association between the secondary VLANs and the primary VLAN. |

## Defaults

None

## Command Modes

Interface configuration (config-if)
Port profile configuration (config-port-prof)

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

There is no run-time effect on the port unless it is in private VLAN-promiscuous mode. If the port is in private VLAN-promiscuous mode but the primary VLAN does not exist, the command is allowed but the port is made inactive.

The secondary VLAN may be an isolated or community VLAN.

## Examples

This example shows how to configure the associate primary VLAN 18 to secondary isolated VLAN 20 on a private VLAN promiscuous port:

```
n1000v(config-if)# switchport private-vlan mapping 18 20
n1000v(config-if)#
```

This example shows how to add a VLAN to the association on the promiscuous port:

```
n1000v(config-if)# switchport private-vlan mapping 18 add 21
n1000v(config-if)#
```

This example shows how to remove the all private VLAN association from the port:

```
n1000v(config-if)# no switchport private-vlan mapping
n1000v(config-if)#
```

## Related Commands

| Command | Description |
|---|---|
| **show interface switchport** | Displays information on all interfaces configured as switchports. |
| **show interface private-vlan mapping** | Displays the information about the private VLAN mapping for VLAN interfaces, or SVIs. |

# switchport private-vlan mapping trunk

To designate the primary private VLAN, use the **switchport private-vlan trunk mapping trunk** command. To remove the primary private VLAN, use the **no** form of this command.

**switchport private-vlan mapping trunk** *primary-vlan* [{**add** | **remove**}] *secondary_vlans*

**no switchport private-vlan mapping trunk** [*primary-vlan* [*secondary_vlans*]]

## Syntax Description

| | |
|---|---|
| *primary-vlan* | Primary private VLAN. |
| **add** | Add a VLAN to private VLAN list. |
| **remove** | Remove a VLAN from private VLAN list. |
| *secondary_vlans* | Secondary VLAN IDs. |

## Defaults

None

## Command Modes

Interface configuration (config-if)
Port profile configuration (config-port-prof)

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

When you use this command, you must either add a secondary VLAN, or remove a VLAN.

## Examples

This example shows how to designate the primary private VLAN:

```
n1000v# configure terminal
n1000v(config)# interface vethernet 1
n1000v(config-if)# switchport private-vlan mapping trunk 10 add 11
n1000v(config-if)#
```

This example shows how to remove the primary private VLAN:

```
n1000v# configure terminal
n1000v(config)# interface vethernet 1
n1000v(config-if)# n1000v(config-if)# no switchport private-vlan mapping trunk 10
n1000v(config-if)#
```

## Related Commands

| Command | Description |
|---|---|
| **show vlan** | Displays VLAN information. |

# switchport trunk allowed vlan

To set the list of allowed VLANs on the trunking interface, use the **switchport trunk allowed vlan** command. To allow *all* VLANs on the trunking interface, use the **no** form of this command.

**switchport trunk allowed vlan** {*vlan-list* | **all** | **none** | [**add** | **except** | **remove** {*vlan-list*}]}

**no switchport trunk allowed vlan**

## Syntax Description

| | |
|---|---|
| *vlan-list* | Allowed VLANs that transmit through this interface in tagged format when in trunking mode; the range of valid values is from 1 to 4094. |
| **all** | Allows all appropriate VLANs to transmit through this interface in tagged format when in trunking mode. |
| **none** | Blocks all VLANs transmitting through this interface in tagged format when in trunking mode. |
| **add** | (Optional) Adds the defined list of VLANs to those currently set instead of replacing the list. |
| **except** | (Optional) Allows all VLANs to transmit through this interface in tagged format when in trunking mode except the specified values. |
| **remove** | (Optional) Removes the defined list of VLANs from those currently set instead of replacing the list. |

## Defaults

All VLANs

## Command Modes

Interface configuration (config-if)
Port profile configuration (config-port-prof)

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

You must enter the **switchport** command without any keywords to configure the LAN interface as a Layer 2 interface before you can enter the **switchport trunk allowed vlan** command. This action is required only if you have not entered the **switchport** command for the interface.

If you remove VLAN 1 from a trunk, the trunk interface continues to send and receive management traffic in VLAN 1.

## Examples

This example shows how to add a series of consecutive VLANs to the list of allowed VLANs on a trunking port:

```
n1000v(config-if)# switchport trunk allowed vlan add 40-50
n1000v(config-if)#
```

## Related Commands

| Command | Description |
|---|---|
| **show interface switchport** | Displays the administrative and operational status of a switching (nonrouting) port. |

# switchport trunk native vlan

To configure trunking parameters on an interface, use the **switchport trunk native vlan** command. To remove the configuration, use the **no** form of this command.

**switchport trunk native vlan** *id*

**no switchport trunk native vlan**

## Syntax Description

| | |
|---|---|
| *id* | VLAN identification number. The range of valid values is 1 to 3967. |

## Defaults

None

## Command Modes

Interface configuration (config-if)
Port profile configuration (config-port-prof)

## SupportedUserRoles

network-admin

## Command History

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

## Examples

This example shows how to configure trunking parameters on an interface:

```
n1000v# configure terminal
n1000v(config)# interface vethernet 10
n1000v(config-if)# switchport trunk native vlan 20
n1000v(config-if)#
```

## Related Commands

| Command | Description |
|---|---|
| **show vlan** | Displays VLAN information. |

# system jumbomtu

To configure a system-wide jumbo frame size, specifying the maximum frame size that Ethernet ports can process, use the **system jumbomtu** command.

**system jumbomtu** *size*

## Syntax Description

| | |
|---|---|
| *size* | Size, in bytes, of the Layer 2 Ethernet interface jumbo maximum transmission unit (MTU). Frames larger than this are dropped. The setting must be an even number between 1500 and 9000 bytes. |

## Defaults

9000 bytes

## Command Modes

Global configuration (config)

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

- For transmissions to occur between two ports, you must configure the same MTU size for both ports.
- A port drops any frames that exceed its MTU size.
- If you do not configure a system jumbo MTU size, it defaults to 1500 bytes.
- For a Layer 2 port, you can configure an MTU size as the system default of 1500 bytes or the system default jumbo MTU size of 9000 bytes.
- If you change the system jumbo MTU size, Layer 2 ports automatically use the system default MTU size of 1500 bytes unless you specifically configure the MTU size differently per port.

## Examples

This example shows how to configure a system-wide maximum frame size of 8000 bytes:

```
n1000v# config t
n1000v(config)# system jumbomtu 8000
n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **show interface ethernet** | Displays information about Ethernet interfaces, including the configured MTU size. |
| **show running-config** | Displays the current operating configuration, which includes the system jumbo MTU size. |

| Command | Description |
|---|---|
| **interface ethernet** | Specifies an interface to configure and enters interface configuration mode. |
| **mtu** | Specifies the system jumbo MTU size. |

# system mtu

To override any maximum transmission unit (MTU) setting that has already been set on the uplink using the **mtu** command on the interface, use the **system mtu** command. To reset the switch to the default of 1500 for all the ports inheriting this system profile, use the no form of this command.

**system mtu** *size*

**no system mtu**

## Syntax Description

| | |
|---|---|
| *size* | Size, in bytes, of the Layer 2 Ethernet interface maximum transmission unit (MTU). The range is 1500 to 9000, even numbers only. |

## Defaults

1500 bytes

## Command Modes

Global configuration (config)

## SupportedUserRoles

network-admin

## Command History

| Release | Modification |
|---|---|
| 4.0(4)SV1(3) | This command was introduced. |

## Usage Guidelines

The **system mtu** command is only applicable, and the configuration is only effective, for system uplink profiles. The value that is configured for **system mtu** command must be less then value configured in the **system jumbomtu** command.

Configuring the system MTU value on the system port-profile causes the interface inheriting this port-profile to flap. If the system port-profile includes the control VLAN, then the module, itself, will flap.

## Examples

This en1000vxample shows how to configure the system MTU value as 3000 bytes for the system uplink profile called PP1:

```
n1000v# config t
n1000v(config-port-prof)# port-profile PP1
n1000v# system mtu 3000
n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **show interface ethernet** | Displays information about Ethernet interfaces, including the configured MTU size. |
| **show running-config** | Displays the current operating configuration, which includes the system jumbo MTU size. |
| **port-profile** | Creates a port profile and enters port-profile configuration mode. |
| **mtu** | Specifies the system jumbo MTU size. |

# system redundancy role

To configure a redundancy role for the VSM, use the **system redundancy role** command. To revert to the default setting, use the **no** form of the command.

**system redundancy role {primary | secondary | standalone}**

**no system redundancy role {primary | secondary | standalone}**

## Syntax Description

| | |
|---|---|
| **primary** | Specifies the primary redundant VSM. |
| **secondary** | Specifies the secondary redundant VSM. |
| **standalone** | Specifies no redundant VSM. |

## Command Default

None

## Command Modes

EXEC

## SupportedUserRoles

network-admin

## Command History

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

## Examples

This example shows how to configure no redundant VSM:

```
n1000v# system redundancy role standalone
n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **show system redundancy** | Displays the system redundancy status. |

# system switchover

To switch over to the standby supervisor, use the **system switchover** command.

**system switchover**

## Syntax Description

This command has no arguments or keywords.

## Command Default

None

## Command Modes

EXEC

## SupportedUserRoles

network-admin

## Command History

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

## Examples

This example shows how to switch over to the standby supervisor:

```
n1000v# system switchover
n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **show system redundancy** | Displays the system redundancy status. |

# system update vem feature level

To change the software version supported on VEMs, use the **system update vem feature level** command.

**system update vem feature level** [*version_number*]

## Syntax Description

| | |
|---|---|
| *version_number* | (Optional) version number index from the list above. |

## Defaults

None

## Command Modes

Any

## SupportedUserRoles

network-admin

## Command History

| Release | Modification |
|---|---|
| 4.0(4)SV1(2) | This command was introduced. |

## Examples

This example shows how to change the software version supported:

```
n1000v# system update vem feature level
Error : the feature level is set to the highest value possible
n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **show system vem feature level** | Displays the current software release supported. |

# system vlan

To add the system VLAN to a port profile, use the **system vlan** command. To remove the system VLAN from a port profile, use the **no** form of this command.

**system vlan** *vlan-ID-list*

**no system vlan**

## Syntax Description

| | |
|---|---|
| *vlan-ID-list* | List of VLAN IDs, separated by commas. The allowable range is 1–3967 and 4048–4093. |

## Defaults

None

## Command Modes

Port profile configuration (config-port-prof)

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

A system VLAN is used to configure and bring up physical or vEthernet ports before the Virtual Supervisor Module (VSM) has established communication with the Virtual Ethernet Module (VEM).

## Examples

This example shows how to add system VLANs 260 and 261 to the port profile:

```
n1000v# config t
n1000v (config)# port-profile system-uplink
n1000v(config-port-prof)# system vlan 260, 261
n1000v(config-port-prof)#
```

This example shows how to remove all system VLANs from the port profile:

```
n1000v# config t
n1000v (config)# port-profile system-uplink
n1000v(config-port-prof)# no system vlan
n1000v(config-port-prof)#
```

## Related Commands

| Command | Description |
|---|---|
| **vlan** | Creates a VLAN and enters the VLAN configuration mode. |
| **show vlan all-ports** | Displays the status of all VLANs and the ports that are configured on them. |
| **show vlan private-vlan** | Displays private VLAN information. |
| **show vlan summary** | Displays VLAN summary information. |

# Show Commands

This chapter describes the Cisco Nexus 1000V show commands.

## show aaa accounting

To display the AAA accounting configuration, use the **show aaa accounting** command.

**show aaa accounting**

**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 display the accounting configuration:

```
n1000v# show aaa accounting
         default: local
n1000v#
```

**Related Commands**

| Command | Description |
|---|---|
| **aaa accounting login** | Configures the console or default login accounting method. |
| **show running-config aaa [all]** | Displays the AAA configuration as it currently exists in the running configuration. |

# show aaa authentication

To display the configuration for AAA authentication, use the **show aaa authentication** command.

**show aaa authentication** [**login error-enable** | **login mschap**]

## Syntax Description

| | |
|---|---|
| **login error-enable** | (Optional) Displays the authentication login error message enable configuration. |
| **login mschap** | (Optional) Displays the authentication login MS-CHAP enable configuration. |

## 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 display the configured authentication parameters:

```
n1000v# show aaa authentication
         default: local
         console: local
```

This example shows how to display the authentication-login error-enable configuration:

```
n1000v# show aaa authentication login error-enable
disabled
```

This example shows how to display the authentication-login MSCHAP configuration:

```
n1000v# show aaa authentication login mschap
disabled
```

## Related Commands

| Command | Description |
|---|---|
| **aaa authentication login** | Configures the console or default login authentication method. |
| **show running-config aaa [all]** | Displays the AAA configuration as it currently exists in the running configuration. |

# show aaa groups

To display the configured AAA server groups, use the **show aaa groups** command.

**show aaa groups**

## 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 display AAA group information:

```
n1000v# show aaa groups
radius
TacServer
```

## Related Commands

| Command | Description |
|---|---|
| **aaa group** | Configures an AAA server group. |
| **show running-config aaa [all]** | Displays the AAA configuration as it currently exists in the running configuration. |

# show access-list summary

To display configured access control lists (ACLs), use the **show access-list summary** command.

**show access-list summary**

## 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. |

## Examples

This example shows how to display configured ACLs:

```
n1000v# show access-lists summary

IP access list acl1
        Total ACEs Configured:1

n1000v#n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **ip access-list** | Creates the IP ACL and enters IP ACL configuration mode. |
| **show ip access-lists** | Displays the IP ACL configuration. |

# show accounting log

To display the accounting log contents, use the **show accounting log** command.

**show accounting log** [*size*] [**start-time** *year month day HH*:*MM*:*SS*]

## Syntax Description

| | |
|---|---|
| *size* | (Optional) Size of the log to display in bytes. The range is from 0 to 250000. |
| **start-time** *year month day HH*:*MM*:*SS* | (Optional) Specifies a start time as follows.<br>• The year is shown in the *yyyy* format, such as 2009.<br>• The month is shown in the three-letter English abbreviation, such as Feb.<br>• The day of the month is shown as a number from 1 to 31.<br>• Hours, minutes, and seconds are shown in the standard 24-hour format, such as 16:00:00. |

## 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 display the entire accounting log:

```
n1000v# show accounting log
Wed Jul 22 02:09:44 2009:update:vsh.3286:root:configure terminal ; port-profile Unused_O
r_Quarantine_Uplink ; capability uplink (SUCCESS)
Wed Jul 22 07:57:50 2009:update:171.71.55.185@pts/2:admin:configure terminal ; flow reco
rd newflowrecord (SUCCESS)
Wed Jul 22 08:48:57 2009:start:swordfish-build1.cisco.com@pts:admin:
Wed Jul 22 08:49:03 2009:stop:swordfish-build1.cisco.com@pts:admin:shell terminated grac
efully
Wed Jul 22 08:50:36 2009:update:171.71.55.185@pts/2:admin:configure terminal ; no flow r
ecord newflowrecord (SUCCESS)
Thu Jul 23 07:21:50 2009:update:vsh.29016:root:configure terminal ; port-profile Unused_
Or_Quarantine_Veth ; state enabled (SUCCESS)
Thu Jul 23 10:25:19 2009:start:171.71.55.185@pts/5:admin:
Thu Jul 23 11:07:37 2009:update:171.71.55.185@pts/5:admin:enabled aaa user default role
enabled/disabled
doc-n1000v(config)#
```

This example shows how to display 400 bytes of the accounting log:

```
n1000v# show accounting log 400

Sat Feb 16 21:15:24 2008:update:/dev/pts/1_172.28.254.254:admin:show accounting log
start-time 2008 Feb 16 18:31:21
Sat Feb 16 21:15:25 2008:update:/dev/pts/1_172.28.254.254:admin:show system uptime
Sat Feb 16 21:15:26 2008:update:/dev/pts/1_172.28.254.254:admin:show clock
```

This example shows how to display the accounting log starting at 16:00:00 on February 16, 2008:

```
n1000v(config)# show accounting log start-time 2008 Feb 16 16:00:00

Sat Feb 16 16:00:18 2008:update:/dev/pts/1_172.28.254.254:admin:show logging log file
start-time 2008 Feb 16 15:59:16
Sat Feb 16 16:00:26 2008:update:/dev/pts/1_172.28.254.254:admin:show accounting log
start-time 2008 Feb 16 12:05:16
Sat Feb 16 16:00:27 2008:update:/dev/pts/1_172.28.254.254:admin:show system uptime
Sat Feb 16 16:00:28 2008:update:/dev/pts/1_172.28.254.254:admin:show clock
Sat Feb 16 16:01:18 2008:update:/dev/pts/1_172.28.254.254:admin:show logging log file
start-time 2008 Feb 16 16:00:16
Sat Feb 16 16:01:26 2008:update:/dev/pts/1_172.28.254.254:admin:show accounting log
start-time 2008 Feb 16 12:05:16
Sat Feb 16 16:01:27 2008:update:/dev/pts/1_172.28.254.254:admin:show system uptime
Sat Feb 16 16:01:29 2008:update:/dev/pts/1_172.28.254.254:admin:show clock
Sat Feb 16 16:02:18 2008:update:/dev/pts/1_172.28.254.254:admin:show logging log file
start-time 2008 Feb 16 16:01:16
Sat Feb 16 16:02:26 2008:update:/dev/pts/1_172.28.254.254:admin:show accounting log
start-time 2008 Feb 16 12:05:16
Sat Feb 16 16:02:28 2008:update:/dev/pts/1_172.28.254.254:admin:show system uptime
```

## Related Commands

| Command | Description |
|---|---|
| **clear accounting log** | Clears the accounting log. |

# show banner motd

To display the configured banner message, use the **show banner motd** command.

**show banner motd**

## 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 display the configured banner message:

```
n1000v(config)# show banner motd
April 16, 2008 Welcome to the Switch
```

## Related Commands

| Command | Description |
|---|---|
| **banner motd** | Configures the banner message of the day. |
| **switchname** | Changes the switch prompt. |

# show boot

To display the system and kickstart boot variables for verification, use the **show boot** command.

**show boot** [**auto-copy** [**list**] | **sup-1** | **sup-2** | **variables**]

## Syntax Description

| | |
|---|---|
| **auto-copy** | (Optional) Determines whether auto-copy is enabled. |
| **list** | (Optional) Displays the list of files to be auto-copied. |
| **sup-1** | (Optional) Displays the sup-1 supervisor module configuration. |
| **sup-2** | (Optional) Displays the sup-2 supervisor module configuration. |
| **variables** | (Optional) Displays a list of boot variables. |

## 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 display the system and kickstart boot variables for verification:

```
n1000v# config t
n1000v(config)# show boot

sup-1
kickstart variable =
bootflash:/nexus-1000v-kickstart-mzg.4.0.4
.SV1.2.bin
system variable =
bootflash:/nexus-1000v-mzg.4.0.4.SV1.2.bin
sup-2
kickstart variable =
bootflash:/nexus-1000v-kickstart-mzg.4.0.4
.SV1.2.bin
system variable =
bootflash:/nexus-1000v-mzg.4.0.4.SV1.2.bin
No module boot variable set
n1000v(config)#
```

## Related Commands

| Command | Description |
|---|---|
| **boot system bootflash:** | Adds the new system boot variable. |
| **boot kickstart bootflash:** | Adds the new kickstart boot variable. |
| **reload** | Reloads the Virtual Supervisor Module (VSM). |
| **show version** | Displays the software version is present on the VSM. |

# show cdp

To display your Cisco Discovery Protocol (CDP) configuration, use the **show cdp** command.

**show cdp** {**all** | **entry** {**all** | **name** *s0*} | **global** | **interface** *if0* | **traffic interface** *if2*}

## Syntax Description

| | |
|---|---|
| **all** | Display all interfaces in CDP database. |
| **entry** | Display CDP entries in database. |
| **name** *name* | Display a specific CDP entry matching a name. |
| **global** | Display CDP parameters for all interfaces. |
| **interface** *interface* | Display CDP parameters for a specified interface. |
| **traffic interface** *interface* | Display CDP traffic statistics. |

## 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 display the global CDP configuration:

```
n1000v(config)# show cdp global
Global CDP information:
    CDP enabled globally
    Sending CDP packets every 5 seconds
    Sending a holdtime value of 10 seconds
    Sending CDPv2 advertisements is disabled
    Sending DeviceID TLV in Mac Address Format
```

This example shows how to display the CDP configuration for a specified interface:

```
n1000v(config)# show cdp interface ethernet 2/3
Ethernet2/3 is up
    CDP enabled on interface
    Sending CDP packets every 60 seconds
    Holdtime is 180 seconds
```

This example shows how to display the CDP traffic statistics for a specified interface:

```
n1000v(config)# show cdp traffic interface ethernet 2/3
----------------------------------------
Traffic statistics for Ethernet2/3
```

```
Input Statistics:
    Total Packets: 98
    Valid CDP Packets: 49
        CDP v1 Packets: 49
        CDP v2 Packets: 0
    Invalid CDP Packets: 49
        Unsupported Version: 49
        Checksum Errors: 0
        Malformed Packets: 0

Output Statistics:
    Total Packets: 47
        CDP v1 Packets: 47
        CDP v2 Packets: 0
    Send Errors: 0
```

This example shows how to display CDP parameters for all interfaces:

```
n1000v# show cdp all
Ethernet2/2 is up
    CDP enabled on interface
    Sending CDP packets every 60 seconds
    Holdtime is 180 seconds
Ethernet2/3 is up
    CDP enabled on interface
    Sending CDP packets every 60 seconds
    Holdtime is 180 seconds
Ethernet2/4 is up
    CDP enabled on interface
    Sending CDP packets every 60 seconds
    Holdtime is 180 seconds
Ethernet2/5 is up
    CDP enabled on interface
    Sending CDP packets every 60 seconds
    Holdtime is 180 seconds
Ethernet2/6 is up
    CDP enabled on interface
    Sending CDP packets every 60 seconds
    Holdtime is 180 seconds
mgmt0 is up
    CDP enabled on interface
    Sending CDP packets every 60 seconds
    Holdtime is 180 seconds
```

## Related Commands

| Command | Description |
|---|---|
| **show cdp neighbors** | Displays the configuration and capabilities of upstream devices. |
| **cdp enable** | In interface mode, enables CDP on an interface.<br>In EXEC mode, enables CDP for your device. |
| **cdp advertise** | Assigns the CDP version to advertise. |

# show cdp neighbors

To display the configuration and capabilities of upstream devices, use the **show cdp neighbors** command.

**show cdp neighbors** [**interface** *if*] **detail**

## Syntax Description

| | |
|---|---|
| **interface** *if* | (Optional) Show CDP neighbors for a specified interface. |
| **detail** | Show the detailed configuration of all CDP neighbors. |

## 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 display the configuration and capabilities of upstream devices:

```
n1000v(config)# show cdp neighbors
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute

Device ID              Local Intrfce   Hldtme  Capability  Platform      Port ID

swordfish-6k-2         Eth2/2          169     R S I    WS-C6503-E    Gig1/14
swordfish-6k-2         Eth2/3          139     R S I    WS-C6503-E    Gig1/15
swordfish-6k-2         Eth2/4          135     R S I    WS-C6503-E    Gig1/16
swordfish-6k-2         Eth2/5          177     R S I    WS-C6503-E    Gig1/17
swordfish-6k-2         Eth2/6          141     R S I    WS-C6503-E    Gig1/18
```

This example shows how to display configuration and capabilities of upstream devices for a specific interface:

```
n1000v(config)# show cdp neighbors interface ethernet 2/3
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute


Device ID              Local Intrfce   Hldtme  Capability  Platform      Port ID
```

```
swordfish-6k-2          Eth2/3          173     R S I    WS-C6503-E    Gig1/15
```

## Related Commands

| Command | Description |
|---|---|
| **show cdp** | Displays the CDP configuration and capabilities for your device. |
| **cdp enable** | In interface mode, enables CDP on an interface.<br>In EXEC mode, enables CDP for your device. |
| **cdp advertise** | Assigns the CDP version to advertise. |

# show class-map

To display the class map configuration for all class maps or for a specified class map, use the **show class-map** command.

**show class-map** [[**type qos**] [*cmap-name*]]

## SyntaxDescription

| | |
|---|---|
| **type** | (Optional) Specifies the type of the class map. |
| **qos** | (Optional) Specifies the type QoS. |
| *cmap-name* | (Optional) Name of an existing class map. |

## 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 display the class map configuration for all class maps with the type qos:

```
n1000v# show class-map type qos


  Type qos class-maps
  ===================

    class-map type qos match-all class1

    class-map type qos match-all class2

n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **class-map** | Puts you in Class Map QoS configuration mode for the specified class map, and configures and saves the map name in the running configuration. |
| **match access-group name** | Configures and saves the access group to match for this class in the running configuration. |
| **show ip access-lists** | Displays all IPv4 access control lists (ACLs) or a specific IPv4 ACL. |

# show cli variables

To display user-defined CLI persistent variables, use the **show cli variables** command.

To remove user-defined CLI persistent variables, use the **cli no var name** command in configuration mode.

**show cli variables**

**cli no var name** *name*

## Syntax Description

| | |
|---|---|
| *name* | Name of an existing variable. |

## 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 display user-defined CLI persistent variables:

```
n1000v# show cli variables
VSH Variable List
-----------------
TIMESTAMP="2008-07-02-13.45.15"
testinterface="ethernet 3/1"
```

This example shows how to remove the user-defined CLI persistent variable, *mgmtport*.

```
n1000v# cli no var name mgmtport
n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **cli var name** | Defines a command-line interface (CLI) variable for a terminal session. |
| **run-script** | Runs a command script that is saved in a file. |

# show cores

To view recent core images, use the **show cores** command.

**show cores**

## 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

System core image files are generated when a service fails.

## Examples

This example shows how to display recent core images:

```
n1000v# show cores
Module-num       Instance-num      Process-name     PID      Core-create-time
----------       ------------      ------------     ---      ----------------
n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **show processes** | Displays information regarding process logs. |

# show file

To display a full filename by entering a partial filename and pressing the Tab key, use the **show file** command.

**show file** {**bootflash:** | **volatile:** | **debug:**} *partial_filename* [**cksum** | **md5sum**]

## Syntax Description

| | |
|---|---|
| **bootflash** | Specifies a directory or filename. |
| **volatile:** | Specifies a directory or filename on volatile flash. |
| **debug:** | Specifies a directory or filename on expansion flash. |
| *partial_filename* | Portion of the filename to be displayed. Pressing Tab lists any existing files that match the partial name. |
| **cksum** | Displays CRC checksum for a file. |
| **md5sum** | Displays MD5 checksum for a file. |

## 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

When you type a partial filename and then press Tab, the CLI completes the filename if the characters that you typed are unique to a single file.

If not, the CLI lists a selection of filenames that match the characters that you typed.

You can then retype enough characters to make the filename unique; and CLI completes the filename for you.

## Examples

This example shows how to display a full filename by entering a partial filename and pressing the Tab key:

```
n1000v# show file bootflash:nexus-1000v <Tab>
bootflash:nexus-1000v-dplug-mzg.4.0.4.SV1.0.42.bin
bootflash:nexus-1000v-mzg.4.0.4.SV1.0.42.bin
bootflash:nexus-1000v-kickstart-mzg.4.0.4.SV1.0.42.bin
```

**Related Commands**

| Command | Description |
|---|---|
| **dir** | Displays the contents of a directory or file. |
| **copy** | Copies a file from the specified source location to the specified destination location. |
| **mkdir** | Creates a directory at the current directory level. |
| **rmdir** | Removes a directory. |

# show flow exporter

To display information about the flow exporter, use the **show flow exporter** command.

**show flow exporter** [*name*]

## Syntax Description

| | |
|---|---|
| *name* | (Optional) Name of an existing flow exporter. |

## Defaults

None

## Command Modes

CLI flow exporter configuration (config-flow-exporter)

## SupportedUserRoles

network-admin
network-operator

## Command History

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

## Examples

This example shows how to display information about the flow exporter:

```
n1000v(config-flow-exporter)# show flow exporter
```

## Related Commands

| Command | Description |
|---|---|
| **flow exporter** | Creates a flow exporter, saves it in the running configuration, and then places you in CLI flow exporter configuration mode. |
| **show flow interface** | Displays flow interface information. |
| **show flow monitor** | Displays the monitor configuration. |
| **show flow record** | Displays the record configuration. |

# show flow interface

To display the NetFlow configuration for the specified interface, use the **show flow interface** command.

**show flow interface** {**ethernet** *slot_number/port_number* | **vethernet** *interface_number*}

## Syntax Description

| | |
|---|---|
| **ethernet** | Indicates Ethernet IEEE 802.3z. |
| *slot_number* | Number identifying the slot. The range is 1-66. |
| *port_number* | Number identifying the port. The range is 1-256. |
| **vethernet** | Indicates virtual Ethernet interface. |
| *interface_number* | Number that identifies this interface. The range is 1–1048575. |

## 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 display NetFlow configuration information for Ethernet slot 2:

```
n1000v(config-if)# show flow interface eth 2
Interface eth 2:
Monitor: MonitorTest
Direction: Output
```

## Related Commands

| Command | Description |
|---|---|
| **flow monitor** | Creates a flow monitor, by name, saves it in the running configuration, and then places you in the CLI flow monitor configuration mode. |
| **flow exporter** | Creates a flow exporter, saves it in the running configuration, and puts you in CLI flow exporter configuration mode. |
| **show flow exporter** | Displays information about the flow exporter. |
| **show flow monitor** | Displays the monitor configuration. |
| **show flow record** | Displays the record configuration. |

# show flow monitor

To display information about existing flow monitors, use the **show flow monitor** command.

**show flow monitor** [*name*]

## Syntax Description

| | |
|---|---|
| *name* | (Optional) Name of an existing flow monitor. |

## 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 display information about the flow monitor called MonitorTest:

```
n1000v(config-flow-monitor)# show flow monitor MonitorTest
Flow Monitor monitortest:
Use count: 0
Inactive timeout: 600
Active timeout: 1800
Cache Size: 15000
n1000v(config-flow-monitor)#
```

## Related Commands

| Command | Description |
|---|---|
| **flow monitor** | Creates a flow monitor, by name, saves it in the running configuration, and then places you in the CLI flow monitor configuration mode. |
| **flow exporter** | Creates a flow exporter, saves it in the running configuration, and then places you in CLI flow exporter configuration mode. |
| **show flow exporter** | Displays information about the flow exporter. |
| **show flow record** | Displays the record configuration. |

# show flow record

To display information about NetFlow flow records, use the **show flow record** command.

**show flow record** [*recordname* | **netflow-original** | **netflow** {**ipv4** {**original-input** | **original-output** | **protocol-port**}}]

## Syntax Description

| | |
|---|---|
| *recordname* | (Optional) Name of an existing NetFlow flow record. |
| **netflow-original** | (Optional) Specifies traditional IPv4 input NetFlow with an AS origin. |
| **netflow** | (Optional) Specifies traditional NetFlow collection schemes. |
| **ipv4** | Specifies IPv4 collection schemes. |
| **original-input** | Indicates the input NetFlow. |
| **original-output** | Indicates the output NetFlow. |
| **protocol-port** | Specifies the protocol and ports aggregation scheme. |

## Defaults

None

## Command Modes

CLI flow exporter configuration (config-flow-exporter)

## SupportedUserRoles

network-admin
network-operator

## Command History

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

## Examples

This example shows how to display information about the NetFlow flow record called RecordTest:

```
n1000v# config t
n1000v(config)# flow record RecordTest
n1000v(config-flow-record)# show flow record RecordTest
Flow record RecordTest:
    Description: Ipv4flow
    No. of users: 0
    Template ID: 0
    Fields:
        match ipv4 destination address
        match interface input
        match interface output
        match flow direction
        collect counter packets
n1000v(config-flow-record)#
```

## Related Commands

| 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. |
| **flow exporter** | Creates a flow exporter, saves it in the running configuration, and then puts you in CLI flow exporter configuration mode. |
| **show flow exporter** | Displays information about the flow exporter. |

# show interface brief

To display a short version of the interface configuration, use the **show interface brief** command.

**show interface brief**

## 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 to display a short version of the interface configuration:

```
n1000v# show int brief
--------------------------------------------------------------------------------
Port VRF Status IP Address Speed MTU
--------------------------------------------------------------------------------
mgmt0 -- up 172.23.232.141 1000 1500
--------------------------------------------------------------------------------
Ethernet VLAN Type Mode Status Reason Speed Port
Interface Ch #
--------------------------------------------------------------------------------
Eth3/2 1 eth trunk up none 1000(D) --
Eth3/3 1 eth access up none 1000(D) --
n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **interface** | Adds, removes or configures interfaces. |
| **show interface ethernet** | Displays information about Ethernet interfaces. |
| **show interface port-channel** | Displays descriptive information about port channels. |
| **show interface switchport** | Displays information about switchport interfaces. |

| Command | Description |
|---|---|
| **show interface trunk** | Displays information about all the trunk interfaces. |
| **show interface vethernet** | Displays statistical information about vEthernet interfaces. |

# show interface capabilities

To display information about the capabilities of the interfaces, use the **show interface capabilities** command.

**show interface capabilities**

## Syntax Description

This command has no arguments or keywords.

## Defaults

None

## Command Modes

Any configuration mode

## SupportedUserRoles

network-admin

## Command History

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

## Examples

This example shows how to display information about the capabilities of the interfaces:

```
n1000v# show interface capabilities
mgmt0
  Model:                 --
  Type:                  --
  Speed:                 10,100,1000,auto
  Duplex:                half/full/auto
  Trunk encap. type:     802.1Q
  Channel:               no
  Broadcast suppression: none
  Flowcontrol:           rx-(none),tx-(none)
  Rate mode:             none
  QOS scheduling:        rx-(none),tx-(none)
  CoS rewrite:           yes
  ToS rewrite:           yes
  SPAN:                  yes
  UDLD:                  yes
  Link Debounce:         no
  Link Debounce Time:    no
  MDIX:                  no
  Port Group Members:    none

port-channel1
  Model:                 unavailable
  Type:                  unknown
  Speed:                 10,100,1000,10000,auto
  Duplex:                half/full/auto
  Trunk encap. type:     802.1Q
  Channel:               yes
```

```
  Broadcast suppression: percentage(0-100)
  Flowcontrol:           rx-(off/on/desired),tx-(off/on/desired)
  Rate mode:             none
  QOS scheduling:        rx-(none),tx-(none)
  CoS rewrite:           yes
  ToS rewrite:           yes
  SPAN:                  yes
  UDLD:                  no
  Link Debounce:         no
  Link Debounce Time:    no
  MDIX:                  no
  Port Group Members:    none

port-channel2
  Model:                 unavailable
  Type:                  unknown
  Speed:                 10,100,1000,10000,auto
  Duplex:                half/full/auto
  Trunk encap. type:     802.1Q
  Channel:               yes
  Broadcast suppression: percentage(0-100)
  Flowcontrol:           rx-(off/on/desired),tx-(off/on/desired)
  Rate mode:             none
  QOS scheduling:        rx-(none),tx-(none)
  CoS rewrite:           yes
  ToS rewrite:           yes
  SPAN:                  yes
  UDLD:                  no
  Link Debounce:         no
  Link Debounce Time:    no
  MDIX:                  no
  Port Group Members:    none

port-channel12
  Model:                 unavailable
  Type:                  unknown
  Speed:                 10,100,1000,10000,auto
  Duplex:                half/full/auto
  Trunk encap. type:     802.1Q
  Channel:               yes
  Broadcast suppression: percentage(0-100)
  Flowcontrol:           rx-(off/on/desired),tx-(off/on/desired)
  Rate mode:             none
  QOS scheduling:        rx-(none),tx-(none)
  CoS rewrite:           yes
  ToS rewrite:           yes
  SPAN:                  yes
  UDLD:                  no
  Link Debounce:         no
  Link Debounce Time:    no
  MDIX:                  no
  Port Group Members:    none

control0
  Model:                 --
  Type:                  --
  Speed:                 10,100,1000,auto
  Duplex:                half/full/auto
  Trunk encap. type:     802.1Q
  Channel:               no
  Broadcast suppression: none
  Flowcontrol:           rx-(none),tx-(none)
  Rate mode:             none
  QOS scheduling:        rx-(none),tx-(none)
```

```
  CoS rewrite:            yes
  ToS rewrite:            yes
  SPAN:                   yes
  UDLD:                   yes
  Link Debounce:          no
  Link Debounce Time:     no
  MDIX:                   no
  Port Group Members:     none

n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **show interface ethernet status** | Displays the status for a specified Ethernet interface. |
| **show interface switchport** | Displays interface configuration information, including the mode. |
| **show interface trunk** | Displays information, including access and trunk interface, for all Layer 2 interfaces. |
| **show interface counters** | Displays the counters for a specified Ethernet interface. |
| **show interface brief** | Displays a short version of the interface configuration. |

# show interface counters trunk

To display the counters for Layer 2 switch port trunk interfaces, use the **show interface counters trunk** command.

**show interface** {**ethernet** *slot/port*} **counters trunk**

## Syntax Description

| | |
|---|---|
| **ethernet** *slot/port* | Specifies the module number and port number for the trunk interface that you want to display. |

## Defaults

None

## Command Modes

Any

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

The device supports only IEEE 802.1Q encapsulation. This command also displays the counters for trunk port channels.

## Examples

This example shows how to display the counters for a trunk interface. This display shows the frames transmitted and received through the trunk interface, as well as the number of frames with the wrong trunk encapsulation:

```
n1000v# show interface ethernet 2/9 counters trunk

--------------------------------------------------------------------------
Port            TrunkFramesTx   TrunkFramesRx      WrongEncap
--------------------------------------------------------------------------
Ethernet2/9                 0               0               0
n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **clear counters interface** | Clears the counters for the specified interfaces. |

# show interface ethernet

To display information about Ethernet interfaces, use the **show interface ethernet** command.

**show interface ethernet** *slot/port* [**brief** | **capabilities** | **debounce** | **description** | **flowcontrol** | **mac-address** | **switchport** | **trunk**]

## Syntax Description

| | |
|---|---|
| *slot/port* | Slot number of the interface that you want to display. The slot number range is from 1 to 66, and the port number range is from 1 to 256. |
| **brief** | (Optional) Specifies to display only a brief summary of the information for the specified interface. |
| **capabilities** | (Optional) Specifies to display capability information for the specified interface. |
| **debounce** | (Optional) Specifies to display interface debounce time information. |
| **description** | (Optional) Specifies to display the description of the specified interface. |
| **flowcontrol** | (Optional) Specifies to display information about the flow-control status and statistics on received and transmitted flow-control pause packets for the specified interface. |
| **mac-address** | (Optional) Specifies to display MAC address information for the specified interface. |
| **switchport** | (Optional) Specifies to display information for the specified interface including access and trunk modes. |
| **trunk** | (Optional) Specifies to display trunk mode information for the specified interface. |

## Defaults

None

## Command Modes

Any

## SupportedUserRoles

network-admin

## Command History

| Release | Modification |
|---|---|
| 4.0(4)SV1(1) | This command was introduced. |
| 4.0(4)SV1(2) | Displays 5-minute input and output packet/bit rate statistics for the specified Ethernet interface. |

## Examples

This example shows how to display statistical information for Ethernet interface 3/2:

```
n1000v# show interface ethernet 3/2
Ethernet3/2 is up
  Hardware: Ethernet, address: 0050.5652.a9ba (bia 0050.5652.a9ba)
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 0/255, txload 0/255, rxload 0/255
```

```
Encapsulation ARPA
Port mode is trunk
full-duplex, 1000 Mb/s
Beacon is turned off
Auto-Negotiation is turned off
Input flow-control is off, output flow-control is off
Auto-mdix is turned on
Switchport monitor is off
  5 minute input rate 570 bytes/second, 6 packets/second
  5 minute output rate 220 bytes/second, 0 packets/second
  Rx
  7570522 Input Packets 1120178 Unicast Packets
  5340163 Multicast Packets 1110181 Broadcast Packets
  647893616 Bytes
  Tx
  1177170 Output Packets 1168661 Unicast Packets
  7269 Multicast Packets 1240 Broadcast Packets 0 Flood Packets
  252026472 Bytes
  4276048 Input Packet Drops 0 Output Packet Drops
1 interface resets
```

## Related Commands

| Command | Description |
|---|---|
| **clear interface** | Clears the interface statistics. |

# show interface ethernet counters

To display the counters for an Ethernet interface, use the **show interface ethernet counters** command.

**show interface ethernet** *slot/port* **counters** [**brief** | **detailed** | **errors** | **snmp** | **storm-control** | **trunk**]

## Syntax Description

| | |
|---|---|
| *slot/port* | Slot number of the interface that you want to display. The slot number range is from 1 to 66, and the port number range is from 1 to 256. |
| **brief** | (Optional) Specifies to display only a brief summary of the counter information for the specified interface. |
| **detailed** | (Optional) Specifies to display the nonzero counters for the specified interface. |
| **errors** | (Optional) Specifies to display the interface error counters for the specified interface. |
| **snmp** | (Optional) Specifies to display the SNMP MIB values for the specified interface. |
| **storm-control** | (Optional) Specifies to display the storm-control counters for the specified interface. |
| **trunk** | (Optional) Specifies to display the trunk counters for the specified interface. |

## Defaults

None

## 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 display counters for Ethernet interface 3/2:

```
n1000v# show interface ethernet 3/2 counters

--------------------------------------------------------------------------------
Port                InOctets       InUcastPkts      InMcastPkts      InBcastPkts
--------------------------------------------------------------------------------
Eth3/2              684023652           1182824          5637863          1171780
--------------------------------------------------------------------------------
Port                OutOctets      OutUcastPkts     OutMcastPkts     OutBcastPkts
--------------------------------------------------------------------------------
n1000v#             265927107           1233866             7269             1240
```

**Related Commands**

| Command | Description |
|---|---|
| **clear interface** | Clears the interface statistics. |

# show interface ethernet status

To display the status for an Ethernet interface, use the **show interface ethernet status** command.

**show interface ethernet** *slot/port* **status** [**err-disable**]

## Syntax Description

| | |
|---|---|
| *slot/port* | Slot number of the interface that you want to display. The slot number range is from 1 to 66, and the port number range is from 1 to 256. |
| **err-disabled** | (Optional) Specifies to display the err-disabled state for the specified interface. |

## Defaults

None

## 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 display the err-disabled status for Ethernet interface 3/2:

```
n1000v# show interface ethernet 3/2 status err-disabled

--------------------------------------------------------------------------------
Port       Name               Status    Reason
--------------------------------------------------------------------------------
Eth3/2     --                 up        none
```

## Related Commands

| Command | Description |
|---|---|
| **clear interface** | Clears the interface statistics. |

# show interface ethernet transceiver

To display the transceiver information for an Ethernet interface, use the **show interface ethernet transceiver** command.

**show interface ethernet** *slot/port* **transceiver** [**calibrations** | **details**]

## Syntax Description

| | |
|---|---|
| *slot/port* | Slot number of the interface that you want to display. The slot number range is from 1 to 66, and the port number range is from 1 to 256. |
| **calibrations** | (Optional) Specifies to display the calibration information for the specified interface. |
| **details** | (Optional) Specifies to display detailed information for the specified interface. |

## Defaults

None

## 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 display transceiver information for Ethernet interface 3/2:

```
n1000v# show interface ethernet 3/2 transceiver calibrations
Ethernet3/2
    sfp is not applicable
```

## Related Commands

| Command | Description |
|---|---|
| **clear interface** | Clears the interface statistics. |

# show interface port-channel

To display descriptive information about port channels, use the **show interface port-channel** command.

**show interface port-channel** *channel-number* [**brief** | **description** | **flowcontrol** | **status** | **switchport** | **trunk**]

## Syntax Description

| | |
|---|---|
| *channel-number* | Number of the port-channel group. Valid values are from 1 to 4096. |
| **brief** | (Optional) Specifies the summary information for specified port channels. |
| **description** | (Optional) Specifies the description of specified port channels. |
| **flowcontrol** | (Optional) Specifies information about the flow-control status control for specified port channels and the statistics on received and transmitted flow-control pause packets. |
| **status** | (Optional) Specifies information about the status for specified port channels. |
| **switchport** | (Optional) Specifies information for specified Layer 2 port channels including access and trunk modes. |
| **trunk** | (Optional) Specifies information for specified Layer 2 port channels on the trunk mode. |

## Defaults

None

## Command Modes

Any

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

To display more statistics for the specified port channels, use the **show interface port-channel counters** command.

## Examples

This example shows how to display information for a specific port channel. This command displays statistical information gathered on the port channel at 1-minute intervals:

```
n1000v(config)# show interface port-channel 50
port-channel50 is down (No operational members)
  Hardware is Port-Channel, address is 0000.0000.0000 (bia 0000.0000.0000)
  MTU 1500 bytes, BW 100000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA
  Port mode is access
```

```
  auto-duplex, auto-speed
  Beacon is turned off
  Input flow-control is off, output flow-control is off
  Switchport monitor is off
  Members in this channel: Eth2/10
  Last clearing of "show interface" counters 2d71.2uh
  5 minute input rate 0 bytes/sec, 0 packets/sec
  5 minute output rate 0 bytes/sec, 0 packets/sec
  Rx
    0 input packets 0 unicast packets 0 multicast packets
    0 broadcast packets 0 jumbo packets 0 storm suppression packets
    0 bytes
  Tx
    0 output packets 0 multicast packets
    0 broadcast packets 0 jumbo packets
    0 bytes
    0 input error 0 short frame 0 watchdog
    0 no buffer 0 runt 0 CRC 0 ecc
    0 overrun  0 underrun 0 ignored 0 bad etype drop
    0 bad proto drop 0 if down drop 0 input with dribble
    0 input discard
    0 output error 0 collision 0 deferred
    0 late collision 0 lost carrier 0 no carrier
    0 babble
    0 Rx pause 0 Tx pause 0 reset
```

This example shows how to display a brief description for a specific port channel, including the mode for the port channel, the status, speed, and protocol:

```
n1000v# show interface port-channel 5 brief

--------------------------------------------------------------------------------
Port-channel VLAN  Type Mode   Status  Reason                    Speed  Protocol
Interface
--------------------------------------------------------------------------------
                   eth  access down    No operational members      auto(D)  lacp
```

This example shows how to display the description for a specific port channel:

```
n1000v# show interface port-channel 5 description

--------------------------------------------------------------------------------
Interface                Description
--------------------------------------------------------------------------------
port-channel5            test
```

This example shows how to display the flow-control information for a specific port channel:

```
n1000v# show interface port-channel 50 flowcontrol

--------------------------------------------------------------------------------
Port       Send FlowControl  Receive FlowControl  RxPause TxPause
           admin    oper     admin    oper
--------------------------------------------------------------------------------
Po50       off      off      off      off         0       0
```

This example shows how to display the status of a specific port channel:

```
n1000v# show interface port-channel 5 status

--------------------------------------------------------------------------------
Port           Name               Status    Vlan      Duplex  Speed   Type
--------------------------------------------------------------------------------
               test               down      1         auto    auto    --
```

This example shows how to display information for a specific Layer 2 port channel:

```
n1000v# show interface port-channel 50 switchport
Name: port-channel50
  Switchport: Enabled
  Switchport Monitor: Not enabled
  Operational Mode: trunk
  Access Mode VLAN: 1 (default)
  Trunking Native Mode VLAN: 1 (default)
  Trunking VLANs Enabled: 1-3967,4048-4093
  Administrative private-vlan primary host-association: none
  Administrative private-vlan secondary host-association: none
  Administrative private-vlan primary mapping: none
  Administrative private-vlan secondary mapping: none
  Administrative private-vlan trunk native VLAN: none
  Administrative private-vlan trunk encapsulation: dot1q
  Administrative private-vlan trunk normal VLANs: none
  Administrative private-vlan trunk private VLANs: none
  Operational private-vlan: none
```

This command displays information for Layer 2 port channels in both the access and trunk modes.

When you use this command for a routed port channel, the device returns the following message:

```
Name: port-channel20
  Switchport: Disabled
```

This example shows how to display information for a specific Layer 2 port channel that is in trunk mode:

```
n1000v# show interface port-channel 5 trunk

n1000v# show interface port-channel 50 trunk
port-channel50 is down (No operational members)
    Hardware is Ethernet, address is 0000.0000.0000
    MTU 1500 bytes, BW 100000 Kbit, DLY 10 usec
    Port mode is access
    Speed is auto-speed
    Duplex mode is auto
    Beacon is turned off
    Receive flow-control is off, Send flow-control is off
    Rate mode is dedicated
  Members in this channel: Eth2/10
    Native Vlan: 1
    Allowed Vlans: 1-3967,4048-4093
```

This command displays information for only Layer 2 port channels in the trunk modes; you cannot display information about Layer 2 port channels in the access mode with this command.

## Related Commands

| Command | Description |
|---|---|
| **show interface port-channel counters** | Displays the statistics for channel groups. |
| **show port-channel summary** | Displays summary information for all channel groups. |

# show interface port-channel counters

To display information about port-channel statistics, use the **show interface port-channel counters** command.

**show interface port-channel** *channel-number* **counters** [**brief** | **detailed** [**all** | **snmp**] | **errors** [**snmp**] | **trunk**]

## Syntax Description

| | |
|---|---|
| *channel-number* | Number of the port-channel group. Valid values are from 1 to 4096. |
| **brief** | (Optional) Specifies the rate MB/s and total frames for specified port channels. |
| **detailed** | (Optional) Specifies the nonzero counters for specified port channels. |
| **all** | (Optional) Specifies the counters for specified port channels. |
| **snmp** | (Optional) Specifies the SNMP MIB values for specified port channels. |
| **errors** | (Optional) Specifies the interface error counters for specified port channels. |
| **trunk** | (Optional) Specifies the interface trunk counters for specified port channels. |

## Defaults

None

## Command Modes

Any

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

This command displays statistics for all port channels including LACP-enabled port channels and those port channels that are not associated with an aggregation protocol.

## Examples

This example shows how to display the counters for a specific port channel. This display shows the transmitted and received unicast and multicast packets:

```
n1000v# show interface port-channel 2 counters

Port            InOctets    InUcastPkts    InMcastPkts    InBcastPkts
Po2                 6007              1             31              1

Port           OutOctets   OutUcastPkts   OutMcastPkts   OutBcastPkts
```

```
Po2                 4428            1           25            1
n1000v#
```

This example shows how to display the brief counters for a specific port channel. This display shows the transmitted and received rate and total frames:

```
n1000v# show interface port-channel 20 counters brief

--------------------------------------------------------------------------------
Interface              Input (rate is 1 min avg)  Output (rate is 1 min avg)
                       -------------------------  --------------------------
                       Rate     Total             Rate     Total
                       MB/s     Frames            MB/s     Frames
--------------------------------------------------------------------------------
port-channel20         0        0                 0        0
```

This example shows how to display all the detailed counters for a specific port channel:

```
n1000v# show interface port-channel 20 counters detailed all
port-channel20
  64 bit counters:
   0.                      rxHCTotalPkts = 0
   1.                       txHCTotalPks = 0
   2.                    rxHCUnicastPkts = 0
   3.                    txHCUnicastPkts = 0
   4.                  rxHCMulticastPkts = 0
   5.                  txHCMulticastPkts = 0
   6.                  rxHCBroadcastPkts = 0
   7.                  txHCBroadcastPkts = 0
   8.                         rxHCOctets = 0
   9.                         txHCOctets = 0
  10.                 rxTxHCPkts64Octets = 0
  11.           rxTxHCpkts65to127Octets = 0
  12.          rxTxHCpkts128to255Octets = 0
  13.          rxTxHCpkts256to511Octets = 0
  14.         rxTxHCpkts512to1023Octets = 0
  15.        rxTxHCpkts1024to1518Octets = 0
  16.        rxTxHCpkts1519to1548Octets = 0
  17.                   rxHCTrunkFrames = 0
  18.                   txHCTrunkFrames = 0
  19.                    rxHCDropEvents = 0

  All Port Counters:
   0.                           InPackets = 0
   1.                            InOctets = 0
   2.                         InUcastPkts = 0
   3.                         InMcastPkts = 0
   4.                         InBcastPkts = 0
   5.                         InJumboPkts = 0
   6.                  StormSuppressPkts = 0
   7.                         OutPackets = 0
   8.                          OutOctets = 0
   9.                       OutUcastPkts = 0
  10.                       OutMcastPkts = 0
  11.                       OutBcastPkts = 0
  12.                       OutJumboPkts = 0
  13.                   rxHCPkts64Octets = 0
  14.             rxHCPkts65to127Octets = 0
  15.            rxHCPkts128to255Octets = 0
  16.            rxHCPkts256to511Octets = 0
  17.           rxHCpkts512to1023Octets = 0
  18.          rxHCpkts1024to1518Octets = 0
  19.          rxHCpkts1519to1548Octets = 0
  20.                   txHCPkts64Octets = 0
```

```
            txHCPkts65to127Octets = 0
           txHCPkts128to255Octets = 0
           txHCPkts256to511Octets = 0
          txHCpkts512to1023Octets = 0
         txHCpkts1024to1518Octets = 0
         txHCpkts1519to1548Octets = 0
                     ShortFrames = 0
                      Collisions = 0
                       SingleCol = 0
                        MultiCol = 0
                         LateCol = 0
                    ExcessiveCol = 0
                     LostCarrier = 0
                       NoCarrier = 0
                           Runts = 0
                          Giants = 0
                        InErrors = 0
                       OutErrors = 0
                    InputDiscards = 0
                    BadEtypeDrops = 0
                      IfDownDrops = 0
                  InUnknownProtos = 0
                            txCRC = 0
                            rxCRC = 0
                           Symbol = 0
                        txDropped = 0
                      TrunkFramesTx = 0
                      TrunkFramesRx = 0
                       WrongEncap = 0
                          Babbles = 0
                        Watchdogs = 0
                              ECC = 0
                         Overruns = 0
                        Underruns = 0
                         Dribbles = 0
                         Deferred = 0
                          Jabbers = 0
                         NoBuffer = 0
                          Ignored = 0
                       bpduOutLost = 0
                       cos0OutLost = 0
                       cos1OutLost = 0
                       cos2OutLost = 0
                       cos3OutLost = 0
                       cos4OutLost = 0
                       cos5OutLost = 0
                       cos6OutLost = 0
                       cos7OutLost = 0
                           RxPause = 0
                           TxPause = 0
                            Resets = 0
                           SQETest = 0
                    InLayer3Routed = 0
                InLayer3RoutedOctets = 0
                     OutLayer3Routed = 0
               OutLayer3RoutedOctets = 0
                    OutLayer3Unicast = 0
              OutLayer3UnicastOctets = 0
                  OutLayer3Multicast = 0
            OutLayer3MulticastOctets = 0
                     InLayer3Unicast = 0
                InLayer3UnicastOctets = 0
                    InLayer3Multicast = 0
             InLayer3MulticastOctets = 0
```

```
  85.              InLayer3AverageOctets = 0
  86.             InLayer3AveragePackets = 0
  87.             OutLayer3AverageOctets = 0
  88.            OutLayer3AveragePackets = 0
```

This example shows how to display the error counters for a specific port channel:

```
n1000v# show interface port-channel 5 counters errors

--------------------------------------------------------------------------------
Port       Align-Err     FCS-Err    Xmit-Err     Rcv-Err   UnderSize OutDiscards
--------------------------------------------------------------------------------
Po5                0           0           0           0           0           0
--------------------------------------------------------------------------------
Port      Single-Col   Multi-Col    Late-Col   Exces-Col   Carri-Sen       Runts
--------------------------------------------------------------------------------
Po5                0           0           0           0          0           0

--------------------------------------------------------------------------------
Port          Giants SQETest-Err Deferred-Tx IntMacTx-Er IntMacRx-Er  Symbol-Err
--------------------------------------------------------------------------------
                   0          --           0           0           0           0
```

This example shows how to display information about the trunk interfaces for a specific port channel:

```
n1000v# show interface port-channel 5 counters trunk

--------------------------------------------------------------------------------
Port             TrunkFramesTx   TrunkFramesRx      WrongEncap
--------------------------------------------------------------------------------
port-channel5               0               0               0
```

## Related Commands

| Command | Description |
|---|---|
| **clear counters interface port-channel** | Clears the statistics for all interfaces that belong to a specific channel group. |

# show interface status

To display the interface line status, use the **show interface status** command.

**show interface status** [**down** | **err-disabled** | **inactive** | **module** *module-number* | **up**]

## Syntax Description

| | |
|---|---|
| **down** | (Optional) Specifies interfaces that are in the down state. |
| **err-disabled** | (Optional) Specifies interfaces that are in the errdisabled state. |
| **inactive** | (Optional) Specifies interfaces that are in the inactive state. |
| **module** | (Optional) Limits the display to interfaces on a particular module. |
| *module-number* | Number that identifies an existing module. The range is 1–66. |
| **up** | (Optional) Specifies interfaces that are in the up state. |

## Defaults

None

## 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 display line status for interfaces in the up state:

```
n1000v# show interface status up

--------------------------------------------------------------------------------
Port           Name               Status    Vlan      Duplex  Speed   Type
--------------------------------------------------------------------------------
mgmt0          --                 up        routed    full    1000    --
ctrl0          --                 up        routed    full    1000    --
n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **show interface brief** | Displays a short version of the interface configuration. |
| **show interface** | Displays interface status and information. |

| Command | Description |
|---|---|
| **show interface capabilities** | Displays information about interface capabilities. |
| **interface** | Adds, removes, or configures interfaces. |

# show interface switchport

To display information about switchport interfaces, use the **show interface switchport** command.

**show interface** [**ethernet** *slot number*\ **port-channel** *channel number*] **switchport**

## Syntax Description

| | |
|---|---|
| **ethernet** *slot number* | (Optional) Specify the slot number for the display of an ethernet switchport interface. |
| **port- channel** *channel-number* | (Optional) Specify the channel number for the display of a port channel switchport interface. |

## Defaults

None

## Command Modes

Any

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

If you do not specify an interface, this command displays information about all Layer 2 interfaces, including access, trunk, and port channel interfaces and all private VLAN ports.

## Examples

This example shows how to display information for all Layer 2 interfaces:

```
n1000v# show interface switchport
Name: Ethernet2/5
  Switchport: Enabled
  Switchport Monitor: Not enabled
  Operational Mode: access
  Access Mode VLAN: 1 (default)
  Trunking Native Mode VLAN: 1 (default)
  Trunking VLANs Enabled: 1-3967,4048-4093
  Administrative private-vlan primary host-association: none
  Administrative private-vlan secondary host-association: none
  Administrative private-vlan primary mapping: none
  Administrative private-vlan secondary mapping: none
  Administrative private-vlan trunk native VLAN: none
  Administrative private-vlan trunk encapsulation: dot1q
  Administrative private-vlan trunk normal VLANs: none
  Administrative private-vlan trunk private VLANs: none
  Operational private-vlan: none

Name: Ethernet2/9
  Switchport: Enabled
```

```
  Switchport Monitor: Not enabled
  Operational Mode: trunk
  Access Mode VLAN: 1 (default)
  Trunking Native Mode VLAN: 1 (default)
  Trunking VLANs Enabled: 1-3967,4048-4093
  Administrative private-vlan primary host-association: none
  Administrative private-vlan secondary host-association: none
  Administrative private-vlan primary mapping: none
  Administrative private-vlan secondary mapping: none
  Administrative private-vlan trunk native VLAN: none
  Administrative private-vlan trunk encapsulation: dot1q
  Administrative private-vlan trunk normal VLANs: none
  Administrative private-vlan trunk private VLANs: none
  Operational private-vlan: none

Name: port-channel5
  Switchport: Enabled
  Switchport Monitor: Not enabled
  Operational Mode: access
  Access Mode VLAN: 1 (default)
  Trunking Native Mode VLAN: 1 (default)
  Trunking VLANs Enabled: 1-3967,4048-4093
  Administrative private-vlan primary host-association: none
  Administrative private-vlan secondary host-association: none
  Administrative private-vlan primary mapping: none
  Administrative private-vlan secondary mapping: none
  Administrative private-vlan trunk native VLAN: none
  Administrative private-vlan trunk encapsulation: dot1q
  Administrative private-vlan trunk normal VLANs: none
  Administrative private-vlan trunk private VLANs: none
  Operational private-vlan: none

n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **switchport mode** | Sets the specified interfaces as either Layer 2 access or trunk interfaces. |
| **show interface counters** | Displays statistics for a specified Layer 2 interface. |

# show interface trunk

To display information about all the trunk interfaces, use the **show interface trunk** command.

**show interface** [**ethernet** *type/slot* | **port-channel** *channel-number*] **trunk** [**module** *number* | **vlan** *vlan-id*]

## Syntax Description

| | |
|---|---|
| **ethernet** *type/slot* \| **port-channel** *channel-number* | (Optional) Type and number of the interface you want to display. |
| **module** *number* | (Optional) Specifies the module number. |
| **vlan** *vlan-id* | (Optional) Specifies the VLAN number. |

## Defaults

None

## Command Modes

Any

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

If you do not specify an interface, a module number or a VLAN number, the system displays information for all trunk interfaces.

This command displays information about all Layer 2 trunk interfaces and trunk port-channel interfaces.

Use the **show interface counters** command to display statistics for the specified Layer 2 interface.

## Examples

This example shows how to display information for all Layer 2 trunk interfaces:

```
n1000v(config)# show interface trunk

--------------------------------------------------------------------------------
Port       Native  Status        Port
           Vlan                  Channel
--------------------------------------------------------------------------------
Eth2/9     1       trunking      --
Eth2/10    1       trnk-bndl     Po50
Po50       1       not-trunking  --

--------------------------------------------------------------------------------
Port       Vlans Allowed on Trunk
--------------------------------------------------------------------------------
```

```
Eth2/9      1-3967,4048-4093
Eth2/10     1-3967,4048-4093
Po50        1-3967,4048-4093

--------------------------------------------------------------------------------
Port        STP Forwarding
--------------------------------------------------------------------------------
Eth2/9      none
Eth2/10     none
Po50        none

n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **switchport mode trunk** | Sets the specified interfaces as Layer 2 trunk interfaces. |

# show interface vethernet

To display statistical information about vEthernet interfaces, use the **show interface vethernet** command.

**show interface vethernet** *interface-number* [**brief** | **description** | **mac-address** | **switchport** | **trunk**]

## Syntax Description

| | |
|---|---|
| *interface-number* | (Optional) Number of the interface that you want to display. The range is from 1 to 1048575. |
| **brief** | (Optional) Specifies to display only a brief summary of information for the specified interface. |
| **description** | (Optional) Specifies to display the description of the specified interface. |
| **mac-address** | (Optional) Specifies to display MAC address information for the specified interface. |
| **switchport** | (Optional) Specifies to display switchport information for the specified interface, including access and trunk modes. |
| **trunk** | (Optional) Specifies to display trunk mode information for the specified interface. |

## Defaults

None

## Command Modes

Any

## SupportedUserRoles

network-admin

## Command History

| Release | Modification |
|---|---|
| 4.0(4)SV1(2) | This command was introduced. |
| 4.0(4)SV1(2) | Displays 5-minute input and output packet/bit rate statistics for the specified vEthernet interface. |

## Examples

This example shows how to display statistical information for vEthernet interface 1:

```
n1000v# show interface vethernet 1
Vethernet1 is up
    Port description is gentoo, Network Adapter 1
    Hardware is Virtual, address is 0050.5687.3bac
    Owner is VM "gentoo", adapter is Network Adapter 1
    Active on module 4
    VMware DVS port 1
    Port-Profile is vm
    Port mode is access
    5 minute input rate 1 bytes/second, 0 packets/second
    5 minute output rate 94 bytes/second, 1 packets/second
```

```
Rx
655 Input Packets 594 Unicast Packets
0 Multicast Packets 61 Broadcast Packets
114988 Bytes
Tx
98875 Output Packets 1759 Unicast Packets
80410 Multicast Packets 16706 Broadcast Packets 0 Flood Packets
6368452 Bytes
0 Input Packet Drops 0 Output Packet Drops
```

## Related Commands

| Command | Description |
|---|---|
| **clear interface** | Clears the interface statistics. |

# show interface vethernet counters

To display the counters for a vEthernet interface, use the **show interface vethernet counters** command.

**show interface vethernet** *interface-number* **counters** [**brief** | **detailed** | **errors** | **trunk**]

## Syntax Description

| | |
|---|---|
| *interface-number* | Number of the interface that you want to display. The range is from 1 to 1048575. |
| **brief** | (Optional) Specifies to display only a brief summary of counter information for the specified interface. |
| **detailed** | (Optional) Specifies to display the nonzero counters for the specified interface. |
| **errors** | (Optional) Specifies to display the interface error counters for the specified interface. |
| **trunk** | (Optional) Specifies to display the trunk counters for the specified interface. |

## Defaults

None

## 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 display counters for vEthernet interface 1:

```
n1000v# show interface vethernet 1 counters

--------------------------------------------------------------------------------
Port                InOctets       InUcastPkts      InMcastPkts      InBcastPkts
--------------------------------------------------------------------------------
Veth1                2434320              5024               12            32363

--------------------------------------------------------------------------------
Port               OutOctets      OutUcastPkts     OutMcastPkts     OutBcastPkts
--------------------------------------------------------------------------------
Veth1                4357946              4910              127            64494
```

## Related Commands

| Command | Description |
|---|---|
| **clear interface** | Clears the interface statistics. |

# show interface vethernet status

To display the status for a vEthernet interface, use the **show interface vethernet status** command.

**show interface vethernet** *interface-number* **status** [**err-disable**]

## Syntax Description

| | |
|---|---|
| *interface-number* | Number of the interface that you want to display. The range is from 1 to 1048575. |
| **err-disabled** | (Optional) Specifies to display the err-disabled state for the specified interface. |

## Defaults

None

## 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 display the err-disabled status for vEthernet interface 1:

```
n1000v# show interface vethernet 1 status err-disabled

--------------------------------------------------------------------------------
Port       Name               Status    Reason
--------------------------------------------------------------------------------
Veth1      VM1-48, Network Ad up        none
n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **clear interface** | Clears the interface statistics. |

# show interface virtual

To display information about virtual interfaces, use the **show interface virtual** command.

**show interface virtual** [**vm** [*vm_name*] | **vmk** | **vswif**] [**module** *module_number*]

## Syntax Description

| | |
|---|---|
| **vm** | (Optional) Specifies interfaces owned by a virtual machine. |
| *vm_name* | (Optional) Name that identifies an existing virtual machine. |
| **vmk** | (Optional) Specifies interfaces owned by the Virtual Machine Kernel. |
| **vswif** | (Optional) Specifies interfaces owned by the Virtual Service Console. |
| **module** | (Optional) Specifies interfaces on a particular module. |
| *module_number* | Number that identifies an existing module. |

## Defaults

None

## 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 display information for virtual interfaces:

```
n1000v# show interface virtual
--------------------------------------------------------------------------------
Port        Adapter        Owner                       Mod Host
--------------------------------------------------------------------------------
Veth1                      Vm1-kl61                     2
Veth2                      VM1-kl65                     5
Veth3                      VM2-kl61                     2
Veth1       Net Adapter 1  austen-gentoo1              33 austen-strider.austen.
Veth2       Net Adapter 2  austen-gentoo1              33 austen-strider.austen.
n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **show interface virtual port-mapping** | Displays the virtual port mapping for all vEthernet interfaces. |
| **show interface ethernet** | Displays information about Ethernet interfaces. |

| Command | Description |
|---|---|
| **show interface port-channel** | Displays descriptive information about port channels. |
| **show interface trunk** | Displays information about all the trunk interfaces. |
| **show interface vethernet** | Displays statistical information about vEthernet interfaces. |

# show interface virtual port-mapping

To display the virtual port mapping for all vEthernet interfaces, use the **show interface virtual port-mapping** command.

**show interface virtual port-mapping** [**vm** [*vm_name*] | **vmk** | **vswif**] [**module** *module_number*]

## Syntax Description

| | |
|---|---|
| **vm** | (Optional) Specifies interfaces owned by a virtual machine. |
| *vm_name* | (Optional) Name that identifies an existing virtual machine. |
| **vmk** | (Optional) Specifies interfaces owned by the Virtual Machine Kernel. |
| **vswif** | (Optional) Specifies interfaces owned by the Virtual Service Console. |
| **module** | (Optional) Specifies interfaces on a particular module. |
| *module_number* | Number that identifies an existing module. |

## Defaults

None

## 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 display the virtual port mapping for all vEthernet interfaces:

```
n1000v# show interface virtual port-mapping
--------------------------------------------------------------------------------
Port        Hypervisor Port   Status    Reason
--------------------------------------------------------------------------------
Veth1       DVPort100         up        none
Veth2       DVPort160         up        none
n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **show interface virtual** | Displays information about virtual interfaces. |
| **show interface ethernet** | Displays information about Ethernet interfaces. |
| **show interface port-channel** | Displays descriptive information about port channels. |

| Command | Description |
|---|---|
| **show interface trunk** | Displays information about all the trunk interfaces. |
| **show interface vethernet** | Displays statistical information about vEthernet interfaces. |

# show ip access-list

To display all IPv4 access control lists (ACLs) or a specific IPv4 AC, use the **show ip access-list** command.

**show ip access-list** [*name*]

## Syntax Description

| | |
|---|---|
| *name* | (Optional) Name of an existing IPv4 access control list. |

## 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 display the IPv4 access control list called protoacl:

```
n1000v(config)# show ip access-lists protoacl

IP access list protoacl
        statistics per-entry
        10 permit icmp 7.120.1.10/32 7.120.1.20/32
        20 permit tcp 7.120.1.10/32 7.120.1.20/32 dscp af11
        30 permit udp 7.120.1.10/32 7.120.1.20/32 precedence critical
        50 permit ip 7.120.1.20/32 7.120.1.10/32
        60 permit ip 7.120.1.20/32 7.120.1.10/32 dscp af11
        70 permit ip 7.120.1.20/32 7.120.1.10/32 precedence critical
n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **ip access-list** | Creates the IP ACL and enters IP ACL configuration mode. |
| **statistics per-entry** | Specifies that the device maintains global statistics for packets that match the rules in the ACL. |
| **show ip access-list summary** | Displays the IP ACL configuration. If the ACL remains applied to an interface, the command lists the interfaces. |

# show ip access-list summary

To display the IP ACL configuration, use the **show ip access-list** command.

**show ip access-list** [*name*] **summary**

## Syntax Description

| | |
|---|---|
| *name* | (Optional) Name of an existing IPv4 access control list. |

## 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

If the ACL remains applied to an interface, this command lists the interfaces.

## Examples

This example shows how to display the IPv4 access control list called ACL1:

```
n1000v# show ip access-lists summary IPV4 ACL1
        Total ACEs Configured: 1
        Configured on interfaces:
                Vethernet1 - ingress (Port ACL)
        Active on interfaces:
                Vethernet1 - ingress (Port ACL)
n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **ip access-list** | Creates the IP ACL and enters IP ACL configuration mode. |
| **statistics per-entry** | Specifies that the device maintains global statistics for packets that match the rules in the ACL. |
| **show ip access-list** | Displays all IPv4 access control lists (ACLs) or a specific IPv4 ACL. |

# show ip arp client

To display the ARP client table, use the **show ip arp client** command.

**show ip arp client**

## 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 display the ARP client table:

```
n1000v# show ip arp client
Number of ARP Clients: 1

Protocol uuid: 442,    Client type: L2
 Flags: 8,    Recv fn: dhcp_snoop_verify_mac2ip_binding
n1000v#
```

## Related Commands.

| Command | Description |
|---|---|
| **ip arp inspection vlan** | Configures the specified VLAN or list of VLANs for Dynamic ARP Inspection (DAI). |
| **show ip arp inspection vlan** | Displays the DAI status for the specified list of VLANs. |
| **show ip arp inspection statistics** | Displays the DAI statistics. |
| **show ip arp inspection interface** | Displays the trust state and the ARP packet rate for a specified interface. |
| **show ip arp statistics** | Displays ARP statistics. |

# show ip arp inspection interface

To display the trust state for the specified interface, use the **show ip arp inspection interface** command.

**show ip arp inspection interface vethernet** *interface-number*

## Syntax Description

| | |
|---|---|
| **vethernet** *number* | Specifies that the output is for a vEthernet interface. |

## Defaults

None

## Command Modes

Any

## SupportedUserRoles

network-admin
network-operator

## Command History

| Release | Modification |
|---|---|
| 4.0(4)SV1(2) | This command was introduced. |

## Examples

This example shows how to display the trust state for a trusted interface:

```
n1000v# show ip arp inspection interface vethernet 6

 Interface        Trust State
 -------------    -----------
 vEthernet 6        Trusted
n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **ip arp inspection vlan** | Enables Dynamic ARP Inspection (DAI) for a specified list of VLANs. |
| **show ip arp inspection statistics** | Displays the DAI statistics. |

# show ip arp inspection statistics

Use the **show ip arp inspection statistics** command to display the Dynamic ARP Inspection (DAI) statistics. You can specify a VLAN or range of VLANs.

**show ip arp inspection statistics** [**vlan** *vlan-list*]

## Syntax Description

| | |
|---|---|
| **vlan** *vlan-list* | (Optional) Specifies the list of VLANs for which to display DAI statistics. Valid VLAN IDs are from 1 to 4096. |

## Defaults

None

## Command Modes

Any

## SupportedUserRoles

network-admin
network-operator

## Command History

| Release | Modification |
|---|---|
| 4.0(4)SV1(2) | This command was introduced. |

## Examples

This example shows how to display the DAI statistics for VLAN 1:

```
n1000v# show ip arp inspection statistics vlan 1

Vlan : 1
-----------
ARP Req Forwarded  = 0
ARP Res Forwarded  = 0
ARP Req Dropped    = 0
ARP Res Dropped    = 0
DHCP Drops         = 0
DHCP Permits       = 0
SMAC Fails-ARP Req = 0
SMAC Fails-ARP Res = 0
DMAC Fails-ARP Res = 0
IP Fails-ARP Req   = 0
IP Fails-ARP Res   = 0
n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **clear ip arp inspection statistics vlan** | Clears the DAI statistics for a specified VLAN. |
| **show ip arp inspection interface** | Displays the trust state and the ARP packet rate for a specified interface. |

# show ip arp inspection vlan

To display the Dynamic ARP Inspection (DAI) status for the specified list of VLANs, use the **show ip arp inspection vlan** command.

**show ip arp inspection vlan** *list*

## Syntax Description

| | |
|---|---|
| *list* | Number identifying an existing VLAN, or range of VLANs, from 1–3967 and 4048–4093. You can specify groups of VLANs or individual VLANs; for example, 1–5, 10 or 2–5, 7–19. |

## 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 display the DAI status for VLAN 13:

```
n1000v# show ip arp inspection vlan 13

Source Mac Validation      : Disabled
Destination Mac Validation : Enabled
IP Address Validation      : Enabled

n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **ip arp inspection vlan** | Configures the specified VLAN or list of VLANs for DAI. |
| **show ip arp client** | Displays the ARP client table. |
| **show ip arp inspection statistics** | Displays the DAI statistics. |
| **show ip arp inspection interface** | Displays the trust state and the ARP packet rate for a specified interface. |
| **show ip arp statistics** | Displays ARP statistics. |

# show ip arp statistics

To display the ARP statistics, use the **show ip arp statistics** command.

**show ip arp statistics** [**interface-all**] [**vrf** {*name* | **all** | **default** | **management**}]

## Syntax Description

| | |
|---|---|
| **interface-all** | (Optional) Specifies ARP statistics for all interfaces. |
| **vrf** | (Optional) Specifies information about a specific Virtual Routing and Forwarding (VRF). |
| *name* | Name of an existing VRF. |
| **all** | Displays ARP statistics for all VRFs. |
| **default** | Specifies the default VRF currently in the system configuration. |
| **management** | Specifies the existing VRF currently used for management connections. |

## 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 display ARP statistics for all VRFs:

```
n1000v# show ip arp statistics vrf all

ARP packet statistics for all contexts
 Sent:
 Total 101994, Requests 3920, Replies 98074, Requests on L2 0, Replies on L2 0,
 Gratuitous 2, Dropped 0
 Received:
 Total 8070240, Requests 98074, Replies 4034, Requests on L2 0, Replies on L2 0
 Proxy arp 0, Local-Proxy arp 0, Dropped 7968132
 Received packet drops details:
    Appeared on a wrong interface       : 0
    Incorrect length                    : 0
    Invalid protocol packet             : 228
    Invalid context                     : 0
    Context not yet created             : 0
    Invalid layer 2 address length      : 0
    Invalid layer 3 address length      : 0
    Invalid source IP address           : 221153
    Source IP address is our own        : 0
```

```
    No mem to create per intf structure : 0
    Source address mismatch with subnet : 0
    Directed broadcast source           : 0
    Invalid destination IP address      : 0
   Non-local destination IP address    : 7746751
    Invalid source MAC address          : 0
    Source MAC address is our own       : 0
    Received before arp initialization  : 0
    Received packet on unknown iod      : 0
    L2 packet on proxy-arp-enabled interface
                                        : 0
    L2 packet on untrusted L2 port      : 0

ARP adjacency statistics

Adds 13, Deletes 11, Timeouts 11
```

## Related Commands

| Command | Description |
|---|---|
| **ip arp inspection vlan** | Configures the specified VLAN or list of VLANs for Dynamic ARP Inspection (DAI). |
| **show ip arp client** | Displays the ARP client table. |
| **show ip arp inspection statistics** | Displays the DAI statistics. |
| **show ip arp inspection interface** | Displays the trust state and the ARP packet rate for a specified interface. |
| **show ip arp inspection vlan** | Displays the DAI status for the specified list of VLANs. |

# show ip dhcp snooping

To display general status information for DHCP snooping, use the **show ip dhcp snooping** command.

**show ip dhcp snooping**

## 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(2) | This command was introduced. |

## Examples

This example shows how to display general status information about DHCP snooping:

```
n1000v# show ip dhcp snooping
DHCP snooping service is enabled
Switch DHCP snooping is enabled
DHCP snooping is configured on the following VLANs:
1,13
DHCP snooping is operational on the following VLANs:
1
Insertion of Option 82 is disabled
Verification of MAC address is enabled
DHCP snooping trust is configured on the following interfaces:
Interface             Trusted
------------          -------
vEthernet 3           Yes

n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **ip dhcp snooping** | Globally enables DHCP snooping on the device. |
| **show ip dhcp snooping binding** | Displays IP-MAC address bindings, including the static IP source entries. |

| Command | Description |
|---|---|
| **show ip dhcp snooping statistics** | Displays DHCP snooping statistics. |
| **show running-config dhcp** | Displays DHCP snooping configuration. |

# show ip dhcp snooping binding

To display IP-to-MAC address bindings for all interfaces or a specific interface, use the **show ip dhcp snooping binding** command.

**show ip dhcp snooping binding** [*IP-address*] [*MAC-address*] [**interface vethernet** *interface-number*] [**vlan** *vlan-id*]

**show ip dhcp snooping binding** [**dynamic**]

**show ip dhcp snooping binding** [**static**]

## Syntax Description

| | |
|---|---|
| *IP-address* | (Optional) IPv4 address that the bindings shown must include. Valid entries are in dotted-decimal format. |
| *MAC-address* | (Optional) MAC address that the bindings shown must include. Valid entries are in dotted-hexadecimal format. |
| **interface vethernet** *interface-number* | (Optional) Specifies the vEthernet interface that the bindings shown must be associated with. |
| **vlan** *vlan-id* | (Optional) Specifies a VLAN ID that the bindings shown must be associated with. Valid VLAN IDs are from 1 to 4096. |
| **dynamic** | (Optional) Limits the output to all dynamic IP-MAC address bindings. |
| **static** | (Optional) Limits the output to all static IP-MAC address bindings. |

## Defaults

None

## Command Modes

Any

## SupportedUserRoles

network-admin
network-operator

## Command History

| Release | Modification |
|---|---|
| 4.0(4)SV1(2) | This command was introduced. |

## Usage Guidelines

The command output includes static IP source entries. Static entries appear with the term “static” in the Type column.

## Examples

This example shows how to show all bindings:

```
n1000v# show ip dhcp snooping binding
MacAddress          IpAddress        LeaseSec  Type        VLAN  Interface
------------------  ---------------  --------  ----------  ----  -------------
0f:00:60:b3:23:33   10.3.2.2         infinite  static      13    vEthernet 6
0f:00:60:b3:23:35   10.2.2.2         infinite  static      100   vEthernet 10
n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **ip dhcp snooping** | Globally enables DHCP snooping on the device. |
| **show ip dhcp snooping** | Displays general information about DHCP snooping. |

# show ip dhcp snooping statistics

To display statistics related to the Dynamic Host Configuration Protocol (DHCP), use the **show ip dhcp snooping statistics** command.

**show ip dhcp snooping statistics**

## 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

Before you can configure DHCP, you must enable the feature using the **feature dhcp** command.

## Examples

This example shows how to display statistics related to DHCP:

```
n1000v# show ip dhcp snooping statistics
Packets processed 0
Packets received through cfsoe 0
Packets forwarded 0
Total packets dropped 0
Packets dropped from untrusted ports 0
Packets dropped due to MAC address check failure 0
Packets dropped due to Option 82 insertion failure 0
Packets dropped due to o/p intf unknown 0
Packets dropped which were unknown 0
Packets dropped due to dhcp relay not enabled 0
Packets dropped due to no binding entry 0
Packets dropped due to interface error/no interface 0
Packets dropped due to max hops exceeded 0
n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **ip dhcp snooping** | Globally enables DHCP snooping on the device. |
| **show ip dhcp snooping** | Displays general information about DHCP snooping. |

| Command | Description |
|---|---|
| **show ip dhcp snooping binding** | Displays IP-MAC address bindings, including the static IP source entries. |
| **feature dhcp** | Enables the DHCP snooping feature on the device. |

# show ip igmp snooping

To ensure that IGMP snooping is enabled on the VLAN, use the **show ip igmp snooping** command.

**show ip igmp snooping**

## 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. |

## Examples

This example shows how to ensure that IGMP snooping is enabled on the VLAN:

```
n1000v# show ip igmp snooping
Global IGMP Snooping Information:
  IGMP Snooping enabled
  IGMPv1/v2 Report Suppression enabled
  IGMPv3 Report Suppression disabled

IGMP Snooping information for vlan 1
  IGMP snooping enabled
  IGMP querier none
  Switch-querier disabled
  IGMPv3 Explicit tracking enabled
  IGMPv2 Fast leave disabled
  IGMPv1/v2 Report suppression enabled
  IGMPv3 Report suppression disabled
  Router port detection using PIM Hellos, IGMP Queries
  Number of router-ports: 0
  Number of groups: 0
IGMP Snooping information for vlan 2
  IGMP snooping enabled
  IGMP querier none
  Switch-querier disabled
  IGMPv3 Explicit tracking enabled
  IGMPv2 Fast leave disabled
  IGMPv1/v2 Report suppression enabled
  IGMPv3 Report suppression disabled
  Router port detection using PIM Hellos, IGMP Queries
  Number of router-ports: 0
  Number of groups: 0
IGMP Snooping information for vlan 100
  IGMP snooping enabled
```

```
  IGMP querier none
  Switch-querier disabled
  IGMPv3 Explicit tracking enabled
  IGMPv2 Fast leave disabled
  IGMPv1/v2 Report suppression enabled
  IGMPv3 Report suppression disabled
  Router port detection using PIM Hellos, IGMP Queries
  Number of router-ports: 0
  Number of groups: 0
IGMP Snooping information for vlan 101
  IGMP snooping enabled
  IGMP querier none
  Switch-querier disabled
  IGMPv3 Explicit tracking enabled
  IGMPv2 Fast leave disabled
  IGMPv2 Fast leave disabled
  IGMPv1/v2 Report suppression enabled
  IGMPv3 Report suppression disabled
  Router port detection using PIM Hellos, IGMP Queries
  Number of router-ports: 0
  Number of groups: 0
IGMP Snooping information for vlan 102
  IGMP snooping enabled
  IGMP querier none
  Switch-querier disabled
  IGMPv3 Explicit tracking enabled
  IGMPv2 Fast leave disabled
  IGMPv1/v2 Report suppression enabled
  IGMPv3 Report suppression disabled
  Router port detection using PIM Hellos, IGMP Queries
  Number of router-ports: 0
  Number of groups: 0
IGMP Snooping information for vlan 103
  IGMP snooping enabled
  IGMP querier none
  Switch-querier disabled
  IGMPv3 Explicit tracking enabled
  IGMPv2 Fast leave disabled
  IGMPv2 Fast leave disabled
  IGMPv1/v2 Report suppression enabled
  IGMPv3 Report suppression disabled
  Router port detection using PIM Hellos, IGMP Queries
  Number of router-ports: 0
  Number of groups: 0
IGMP Snooping information for vlan 104
  IGMP snooping enabled
  IGMP querier none
  Switch-querier disabled
  IGMPv3 Explicit tracking enabled
  IGMPv2 Fast leave disabled
  IGMPv1/v2 Report suppression enabled
  IGMPv3 Report suppression disabled
  Router port detection using PIM Hellos, IGMP Queries
  Number of router-ports: 0
  Number of groups: 0
IGMP Snooping information for vlan 105
  IGMP snooping enabled
  IGMP querier none
  Switch-querier disabled
  IGMPv3 Explicit tracking enabled
  IGMPv2 Fast leave disabled
  IGMPv2 Fast leave disabled
  IGMPv1/v2 Report suppression enabled
  IGMPv3 Report suppression disabled
```

```
  Router port detection using PIM Hellos, IGMP Queries
  Number of router-ports: 0
  Number of groups: 0
IGMP Snooping information for vlan 106
  IGMP snooping enabled
  IGMP querier none
  Switch-querier disabled
  IGMPv3 Explicit tracking enabled
  IGMPv2 Fast leave disabled
  IGMPv1/v2 Report suppression enabled
  IGMPv3 Report suppression disabled
  Router port detection using PIM Hellos, IGMP Queries
  Number of router-ports: 0
  Number of groups: 0
IGMP Snooping information for vlan 107
  IGMP snooping enabled
  IGMP querier none
  Switch-querier disabled
  IGMPv3 Explicit tracking enabled
  IGMPv2 Fast leave disabled
  IGMPv2 Fast leave disabled
  IGMPv1/v2 Report suppression enabled
  IGMPv3 Report suppression disabled
  Router port detection using PIM Hellos, IGMP Queries
  Number of router-ports: 0
  Number of groups: 0
IGMP Snooping information for vlan 108
  IGMP snooping enabled
  IGMP querier none
  Switch-querier disabled
  IGMPv3 Explicit tracking enabled
  IGMPv2 Fast leave disabled
  IGMPv1/v2 Report suppression enabled
  IGMPv3 Report suppression disabled
  Router port detection using PIM Hellos, IGMP Queries
  Number of router-ports: 0
  Number of groups: 0
IGMP Snooping information for vlan 109
  IGMP snooping enabled
  IGMP querier none
  Switch-querier disabled
  IGMPv3 Explicit tracking enabled
  IGMPv2 Fast leave disabled
  IGMPv2 Fast leave disabled
  IGMPv1/v2 Report suppression enabled
  IGMPv3 Report suppression disabled
  Router port detection using PIM Hellos, IGMP Queries
  Number of router-ports: 0
  Number of groups: 0
IGMP Snooping information for vlan 115
  IGMP snooping enabled
  IGMP querier none
  Switch-querier disabled
  IGMPv3 Explicit tracking enabled
  IGMPv2 Fast leave disabled
  IGMPv1/v2 Report suppression enabled
  IGMPv3 Report suppression disabled
  Router port detection using PIM Hellos, IGMP Queries
  Number of router-ports: 0
  Number of groups: 0
IGMP Snooping information for vlan 260
  IGMP snooping enabled
  IGMP querier none
  Switch-querier disabled
```

```
  IGMPv3 Explicit tracking enabled
  IGMPv2 Fast leave disabled
  IGMPv1/v2 Report suppression enabled
  IGMPv3 Report suppression disabled
  Router port detection using PIM Hellos, IGMP Queries
  Number of router-ports: 0
  Number of groups: 0
IGMP Snooping information for vlan 261
  IGMP snooping enabled
  IGMP querier none
  Switch-querier disabled
  IGMPv3 Explicit tracking enabled
  IGMPv2 Fast leave disabled
  IGMPv1/v2 Report suppression enabled
  IGMPv3 Report suppression disabled
  Router port detection using PIM Hellos, IGMP Queries
  Number of router-ports: 0
  Number of groups: 0

n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **show cores** | Displays a list of cores. |
| **show cdp neighbor** | Displays the configuration and capabilities of upstream devices. |
| **module vem execute** | Remotely executes commands on the Virtual Ethernet Module (VEM) from the Cisco Nexus 1000V. |
| **show ip igmp snooping groups** | Verifies if the Cisco Nexus 1000V is configured correctly and is ready to forward multicast traffic. |

# show ip igmp snooping explicit-tracking vlan

To display IGMPv3 snooping explicit tracking information for a VLAN, use the **show ip igmp snooping explicit-tracking vlan** command.

**show ip igmp snooping explicit-tracking vlan** *vlan-id*

## Syntax Description

| | |
|---|---|
| *vlan-id* | Specifies a VLAN ID. |

## 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

## Examples

## Related Commands

| Command | Description |
|---|---|
| **show ip igmp snooping** | Ensures that IGMP snooping is enabled on the VLAN. |
| **show ip igmp snooping groups** | Verifies if the Cisco Nexus 1000V is configured correctly and is ready to forward multicast traffic. |
| **show ip igmp snooping mrouter** | Displays multicast router ports on the VLAN. |
| **show ip igmp snooping querier** | Displays IGMP snooping queriers enabled on the VLAN |

# show ip igmp snooping groups

To verify if the Cisco Nexus 1000V is configured correctly and is ready to forward multicast traffic, use the **show ip igmp snooping groups** command.

**show ip igmp snooping groups**

## 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

When troubleshooting multicast IGMP issues, execute this command and look for the letter R under the port heading. The R indicates that the Virtual Supervisor Module (VSM) has learned the uplink router port from the IGMP query that was sent by the upstream switch, which means that the Cisco Nexus 1000V is ready to forward multicast traffic.

## Examples

This example shows how to ensure that IGMP snooping is enabled on the VLAN:

```
n1000v# show ip igmp snooping groups
Type: S - Static, D - Dynamic, R - Router port

Vlan  Group Address      Ver  Type  Port list
59    */*                v3   R     Po1
n1000v#n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **show cdp neighbor** | Displays the configuration and capabilities of upstream devices. |
| **module vem execute** | Remotely executes commands on the Virtual Ethernet Module (VEM) from the Cisco Nexus 1000V. |
| **show ip igmp snooping** | Ensures that IGMP snooping is enabled on the VLAN. |

# show ip igmp snooping mrouter

To display VLAN multicast router ports , use the **show ip igmp snooping mrouter** command.

**show ip igmp snooping mrouter** [**vlan** *vlan-id*]

## Syntax Description

| | |
|---|---|
| **vlan** *vlan-id* | Specifies a VLAN and its ID. |

## 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

## Examples

## Related Commands

| Command | Description |
|---|---|
| **show ip igmp snooping** | Ensures that IGMP snooping is enabled on the VLAN. |
| **show ip igmp snooping groups** | Verifies if the Cisco Nexus 1000V is configured correctly and is ready to forward multicast traffic. |
| **show ip igmp snooping explicit-tracking vlan** | Display IGMP snooping information for a VLAN. |
| **show ip igmp snooping querier** | Displays IGMP snooping queriers enabled on the VLAN |

# show ip igmp snooping querier

To display IGMP snooping querier information, use the **show ip igmp snooping querier** command.

**show ip igmp snooping querier** [**vlan** *vlan-id*]

## Syntax Description

| | |
|---|---|
| **vlan** *vlan-id* | Specifies a VLAN and its ID. |

## 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

## Examples

## Related Commands

| Command | Description |
|---|---|
| **show ip igmp snooping** | Ensures that IGMP snooping is enabled on the VLAN. |
| **show ip igmp snooping groups** | Verifies if the Cisco Nexus 1000V is configured correctly and is ready to forward multicast traffic. |
| **show ip igmp snooping explicit-tracking vlan** | Display IGMP snooping information for a VLAN. |
| **show ip igmp snooping mrouter** | Displays multicast router ports on the VLAN. |

# show ip verify source

To display the IP-to-MAC address bindings, use the **show ip verify source** command.

**show ip verify source** [ **interface** {**vethernet** *interface-number* }]

## Syntax Description

| | |
|---|---|
| **interface** | (Optional) Specifies that the output is limited to IP-to-MAC address bindings for an interface. |
| **vethernet** *interface-number* | Specifies the vEthernet interface. Range is from 1 to 1048575. |

## Defaults

None

## Command Modes

Any

## SupportedUserRoles

network-admin
network-operator

## Command History

| Release | Modification |
|---|---|
| 4.0(4)SV1(2) | This command was introduced. |

## Examples

This example shows how to display the IP-to-MAC address bindings:

```
n1000v# show ip verify source
n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **ip source binding** | Creates a static IP source entry for the specified Ethernet interface. |
| **ip verify source dhcp-snooping-vlan** | Enables IP Source Guard on an interface. |

# show lacp counters

To display information about Link Aggregation Control Protocol (LACP) statistics, use the **show lacp counters** command.

**show lacp counters** [**interface port-channel** *channel-number*]

## Syntax Description

| | |
|---|---|
| *channel-number* | (Optional) Number of the LACP channel group. Valid values are from 1 to 4096. |

## Defaults

None

## Command Modes

Any

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

If you do not specify the *channel-number*, all channel groups are displayed.

## Examples

This example shows how to display the LACP statistics for a specific channel group:

```
n1000v# show lacp counters interface port-channel 1

LACPDUs          Marker      Marker Response    LACPDUs
Port               Sent   Recv     Sent   Recv      Sent   Recv      Pkts Err
--------------------------------------------------------------------------------
port-channel1
Ethernet1/1         554    536       0      0         0      0         0
Ethernet1/2         527    514       0      0         0      0         0
Ethernet1/3         535    520       0      0         0      0         0
Ethernet1/4         515    502       0      0         0      0         0
Ethernet1/5         518    505       0      0         0      0         0
Ethernet1/6         540    529       0      0         0      0         0
Ethernet1/7         541    530       0      0         0      0         0
Ethernet1/8         547    532       0      0         0      0         0
Ethernet1/9         544    532       0      0         0      0         0
Ethernet1/10        513    501       0      0         0      0         0
Ethernet1/11        497    485       0      0         0      0         0
Ethernet1/12        493    486       0      0         0      0         0
Ethernet1/13        492    485       0      0         0      0         0
Ethernet1/14        482    481       0      0         0      0         0
Ethernet1/15        481    476       0      0         0      0         0
Ethernet1/16        482    477       0      0         0      0         0
```

**Related Commands**

| Command | Description |
|---|---|
| **clear lacp counters** | Clears the statistics for all LACP interfaces or those interfaces that belong to a specific LACP channel group. |

# show lacp interface

To display information about specific Link Aggregation Control Protocol (LACP) interfaces, use the **show lacp interface** command.

**show lacp interface ethernet** *slot/port*

## Syntax Description

| | |
|---|---|
| *slot/port* | Slot number and port number for the interface you want to display. |

## Defaults

None

## Command Modes

Any

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

The LACP_Activity field displays whether the link is configured in the active or passive port-channel mode.

The Port Identifier field displays the port priority as part of the information. The part of the information in this field is the port number. The following example shows how to identify the port priority and the port number:

```
Port Identifier=0x8000,0x101
```

The port priority value is `0x8000`, and the port number value is `0x101` in this example.

## Examples

This example shows how to display the LACP statistics for a specific channel group:

```
n1000v# show lacp interface ethernet 1/1

n1000v(config-if-range)# show lacp interface eth1/1
Interface Ethernet1/1 is up
  Channel group is 1 port channel is Po1
  PDUs sent: 556
  PDUs rcvd: 538
  Markers sent: 0
  Markers rcvd: 0
  Marker response sent: 0
  Marker response rcvd: 0
  Unknown packets rcvd: 0
  Illegal packets rcvd: 0
Lag Id: [ [(8000, 0-11-11-22-22-74, 0, 8000, 101), (8000, 0-11-11-22-22-75, 0, 8
000, 401)] ]
```

```
Operational as aggregated link since Wed Jun 11 20:37:59 2008

Local Port: Eth1/1   MAC Address= 0-11-11-22-22-74
  System Identifier=0x8000,0-11-11-22-22-74
  Port Identifier=0x8000,0x101
  Operational key=0
  LACP_Activity=active
  LACP_Timeout=Long Timeout (30s)
  Synchronization=IN_SYNC
  Collecting=true
  Distributing=true
  Partner information refresh timeout=Long Timeout (90s)
Actor Admin State=
Actor Oper State=
Neighbor: 4/1
  MAC Address= 0-11-11-22-22-75
  System Identifier=0x8000,0-11-11-22-22-75
  Port Identifier=0x8000,0x401
  Operational key=0
  LACP_Activity=active
  LACP_Timeout=Long Timeout (30s)
  Synchronization=IN_SYNC
  Collecting=true
  Distributing=true
Partner Admin State=
Partner Oper State=
```

## Related Commands

| Command | Description |
|---|---|
| **show port-channel summary** | Displays information about all port-channel groups. |

# show lacp neighbor

To display information about Link Aggregation Control Protocol (LACP) neighbors, use the **show lacp neighbor** command.

**show lacp neighbor [interface port-channel** *channel-number*]

## Syntax Description

| | |
|---|---|
| *channel-number* | Port-channel number for the LACP neighbor that you want to display. The range of values is from 1 to 4096. |

## Defaults

None

## Command Modes

Any

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

If you do not specify the *channel-number*, all channel groups are displayed.

## Examples

This example shows how to display the information about the LACP neighbors for a specific port channel:

```
n1000v# show lacp neighbor interface port-channel 1
Flags:  S - Device is sending Slow LACPDUs F - Device is sending Fast LACPDUs
        A - Device is in Active mode       P - Device is in Passive mode
port-channel1 neighbors
Partner's information
          Partner               Partner                   Partner
Port      System ID             Port Number     Age       Flags
Eth1/1    32768,0-11-11-22-22-750x401           44817     SA

          LACP Partner          Partner                   Partner
          Port Priority         Oper Key                  Port State
          32768                 0x0                       0x3d

Partner's information
          Partner               Partner                   Partner
Port      System ID             Port Number     Age       Flags
Eth1/2    32768,0-11-11-22-22-750x402           44817     SA

          LACP Partner          Partner                   Partner
          Port Priority         Oper Key                  Port State
          32768                 0x0                       0x3d
```

**Related Commands**

| Command | Description |
|---|---|
| **show port-channel summary** | Displays information about all port-channel groups. |

# show lacp port-channel

To display information about Link Aggregation Control Protocol (LACP) port channels, use the **show lacp port-channel** command.

**show lacp port-channel [interface port-channel** *channel-number*]

## Syntax Description

| | |
|---|---|
| **interface port-channel** | (Optional) Specifies an existing LACP port channel. |
| *channel-number* | Port-channel number for the LACP channel group that you want to display. The range of values is from 1 to 4096. |

## Defaults

None

## Command Modes

Any

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

If you do not specify the *channel-number*, all channel groups are displayed.

## Examples

This example shows how to display the information about LACP port channels:

```
n1000v# show lacp port-channel

port-channel1
  Local System Identifier=0x8000,0-11-11-22-22-74
  Admin key=0x0
  Operational key=0x0
  Partner System Identifier=0x8000,0-11-11-22-22-75
  Operational key=0x0
  Max delay=0
  Aggregate or individual=1
port-channel2
  Local System Identifier=0x8000,0-11-11-22-22-74
  Admin key=0x1
  Operational key=0x1
  Partner System Identifier=0x8000,0-11-11-22-22-75
  Operational key=0x1
  Max delay=0
  Aggregate or individual=1
```

**Related Commands**

| Command | Description |
|---|---|
| **show port-channel summary** | Displays information about all port-channel groups. |

# show lacp system-identifier

To display the Link Aggregation Control Protocol (LACP) system identifier for the device, use the **show lacp system-identifier** command.

**show lacp system-identifier**

## 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

The LACP system ID is the combination of the configurable LACP system priority value and the MAC address.

Each system that runs LACP has an LACP system priority value. You can accept the default value of 32768 for this parameter, or you can configure a value between 1 and 65535. LACP uses the system priority with the MAC address to form the system ID and also uses the system priority during negotiation with other devices. A higher system priority value means a lower priority.

## Examples

This example shows how to display the information about the LACP port channel for a specific port channel:

```
n1000v> show lacp system-identifier
8000,AC-12-34-56-78-90
```

## Related Commands

| Command | Description |
|---|---|
| **lacp system-priority** | Sets the system priority for LACP. |

# show license

To display the content of all the license files that are installed on the virtual supervisor module (VSM), use the **show license** command.

**show license**

## Syntax Description

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 display the content of all the license files that are installed on the VSM:

```
n1000v# show license
license_file.lic:
SERVER this_host ANY
VENDOR cisco
INCREMENT NEXUS1000V_LAN_SERVICES_PKG cisco 1.0 permanent 16 \
        HOSTID=VDH=8449368321243879080 \
        NOTICE="<LicFileID>kathleen.lic</LicFileID><LicLineID>0</LicLineID> \
        <PAK>dummyPak</PAK>" SIGN=34FCB2B24AE8

n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **show license brief** | Displays a list of license files that are installed on the VSM. |
| **show license usage** [*package-name*] | Displays the license packages that are supported on the VSM. Optionally, you can display a specific license package. |

# show license brief

To display a list of license files that are installed on the virtual supervisor module (VSM), use the **show license brief** command.

**show license brief**

## Syntax Description

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 display the content of all the license files that are installed on the VSM:

```
n1000v# show license brief
license_file.lic
n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **show license** | Displays the content of all the license files that are installed on the VSM. |
| **show license usage** [*package-name*] | Displays the license packages that are supported on the VSM. Optionally, you can display a specific license package. |

# show license file

To verify the license installation by displaying the license configured for the Virtual Supervisor Module (VSM), use the **show license file** command.

**show license file** *filename*

## Syntax Description

| | |
|---|---|
| *filename* | Name of the existing license file (.lic). |

## Defaults

None

## Command Modes

Any

## SupportedUserRoles

network-admin
network-operator

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

## Usage Guidelines

To find the name of the existing file, enter the following command at the prompt:

```
n1000v# show license file ?
```

## Examples

This example shows how to display the license file, *sample.lic*, configured for the VSM:

```
n1000v# show license file sample.lic
sample.lic:
SERVER this_host ANY
VENDOR cisco
INCREMENT NEXUS1000V_LAN_SERVICES_PKG cisco 1.0 permanent 16 \
        HOSTID=VDH=8449368321243879080 \
        NOTICE="<LicFileID>sample.lic</LicFileID><LicLineID>0</LicLineID> \
        <PAK>dummyPak</PAK>" SIGN=34FCB2B24AE8

n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **show license** | Displays the content of all the license files that are installed on the VSM. |
| **show license brief** | Displays a list of license files that are installed on the VSM. |
| **show license host-id** | Displays the serial number (host ID) for your VSM |
| **show license usage** | Displays the license packages that are supported on the VSM. |

# show license host-id

To obtain the serial number, also called the *host ID*, for your Virtual Supervisor Module (VSM), use the **show license host-id** command.

**show license host-id**

## Syntax Description

This command has no arguments or keywords.

## Defaults

None

## Command Modes

Any

## SupportedUserRoles

network-admin
network-operator

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

## Usage Guidelines

The host ID includes everything that appears after the equal sign (=).

The host ID is required to obtain a license key file and register your VSM license.

## Examples

This example shows how to obtain the host ID for your VSM:

```
n1000v# show license host-id
License hostid: VDH=8449368321243879080
n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **show license** | Displays the content of all the license files that are installed on the VSM. |
| **show license brief** | Displays a list of license files that are installed on the VSM. |
| **show license file** | Displays the license configured for the VSM |
| **show license usage** | Displays the license packages that are supported on the VSM. |

# show license usage

To display the various license packages that are supported on the virtual supervisor module (VSM), use the **show license usage** command.

**show license usage** [*package-name*]

## Syntax Description

| | |
|---|---|
| *package-name* | (Optional) Name of a license file. In the Cisco Nexus 1000V, the VSM supports only one package (NEXUS1000V_LAN_SERVICES_PKG). |

## 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 display a brief summary of the various license packages that are supported on the VSM:

```
n1000v# show license usage
Feature                      Ins  Lic   Status Expiry Date Comments
                                 Count
--------------------------------------------------------------------------------
NEXUS1000V_LAN_SERVICES_PKG   No   16   In use Never       -
n1000v# --------------------------------------------------------------------------
```

This example shows how to display the license usage information for a specific license package:

```
Example:
n1000v# show license usage NEXUS1000V_LAN_SERVICES_PKG
--------------------------------------
Feature Usage Info
--------------------------------------
       Installed Licenses :    10
            Eval Licenses :   0
   Max Overdraft Licenses :    16
Installed Licenses in Use :    4
Overdraft Licenses in Use :    0
     Eval Licenses in Use :    0
       Licenses Available :   22
--------------------------------------
Application
--------------------------------------
VEM 3 - Socket 1
VEM 3 - Socket 2
VEM 4 - Socket 1
VEM 4 - Socket 2
```

```
--------------------------------------
n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **show license** | Displays the content of all the license files that are installed on the VSM. |
| **show license brief** | Displays a list of license files that are installed on the VSM. |
| **show license** *package-name* | Displays the content of a specific license file that is installed on the VSM. In the Cisco Nexus 1000V, the VSM supports only one package (NEXUS1000V_LAN_SERVICES_PKG). |

# show logging logfile

To display the contents of the log file, use the **show logging logfile** command.

**show logging logfile [start-time** *time* | **end-time** *time*]

## Syntax Description

| | | |
|---|---|---|
| **start-time** | (Optional)Specify the starting time for which you want the logfile displayed. | |
| **end-time** | (Optional) Specify the ending time for which you want the logfile displayed. | |
| *time* | Specify the time as follows: | |
| | **Time** | **Description** |
| | *yyyy* | Specify the year. |
| | *mmm* | Specify the month, for example, *jan, feb, mar.* |
| | *dd* | Specify the day of month, for example *01*. |
| | *hh:mm:ss* | Specify the hour, minutes, seconds, for example, *04:00:00*. |

## 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 display the contents of the logfile:

```
n1000v# show logging logfile start-time 2009 Aug 23 22:00:00 end-time 2009 Aug 24 24:00:00
2009 Aug 23 22:58:00 doc-n1000v %PORTPROFILE-5-SYNC_COMPLETE: Sync completed.
2009 Aug 24 23:53:15 doc-n1000v %MODULE-5-MOD_OK: Module 3 is online (serial: )
2009 Aug 24 23:53:15 doc-n1000v %PLATFORM-5-MOD_STATUS: Module 3 current-status is MOD_S
TATUS_ONLINE/OK
n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **logging logfile** | Configures the log file used to store system messages. |

# show logging module

To display the current configuration for logging module messages to the log file, use the **show logging module** command.

**show logging module**

## 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 display the configuration for logging of messages to the log file:

```
n1000v# show logging module
Logging linecard:                disabled
n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **logging module** | Starts logging of module messages to the log file. |

# show logging server

To display the current server configuration for logging system messages, use the **show logging server** command.

**show logging server**

## 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 display the :

```
n1000v## show logging server
Logging server:                 enabled
{172.28.254.253}
        server severity:        notifications
        server facility:        local7
        server VRF:             management
n1000v##
```

## Related Commands

| Command | Description |
|---|---|
| **logging server** | Designates a remote server for system message logging, and configures it. |

# show logging timestamp

To display the unit of measure used in the system messages timestamp, use the **show logging timestamp** command.

**show logging timestamp**

## 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 display the unit of measure used in the system messages timestamp:

```
n1000v## show logging timestamp
Logging timestamp:              Seconds
n1000v##
```

## Related Commands

| Command | Description |
|---|---|
| **logging timestamp** | Sets the unit of measure for the system messages timestamp. |

# show mac access-lists

To display the MAC access control list (ACL) configuration, use the **show mac access lists** command.

**show mac access-lists** *name*

## Syntax Description

| | |
|---|---|
| *name* | Enter the name of the MAC access list. |

## Defaults

None

## Command Modes

ACL configuration (config-mac-acl)

## SupportedUserRoles

network-admin
network-operator

## Command History

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

## Examples

This example shows how to display the MAC ACL configuration for the MAC access list called acl-mac-01:

```
n1000v# config t
n1000v(config)# mac access-list acl-mac-01
n1000v(config-mac-acl)# show mac access-lists acl-mac-01
n1000v(config-mac-acl)#
```

## Related Commands

| Command | Description |
|---|---|
| **mac access-list** | Creates the MAC ACL and enters ACL configuration mode. |
| **show mac address-list** | Displays the MAC address table. |

# show mac address-table

To display the MAC address table, use the **show mac address-table** command.

**show mac address-table** [**module** *number*] [**static** | **dynamic** | **secure**] [**address** *mac-addr*] [**interface** {**ethernet** *slot/port* | **port-channel** *port-channel-number* | **vethernet** *interface -number*}] [**vlan** *id*]

## Syntax Description

| | |
|---|---|
| **module** | (Optional) Specifies a module number. |
| *number* | Identifier for the specified module. |
| **static** | (Optional) Specifies static entries in the MAC address table. |
| **dynamic** | (Optional) Specifies dynamic entries in the MAC address table. |
| **secure** | (Optional) Specifies secure entries in the MAC address table. |
| **address** | (Optional) Specifies a MAC address to display. |
| *mac-addr* | MAC address, in one of the following formats:<br>• A.B.C<br>• AA-BB-CC-DD-EE-FF<br>• AA:BB:CC:DD:EE:FF<br>• AAAA.BBBB.CCCC |
| **interface** | (Optional) Specifies an interface associated with this MAC address table. |
| **ethernet** | Specifes an Ethernet type of interface. |
| *slot/port* | Slot number (the range is 1–66) and port number (the range is 1–256), separated by a slash (/). |
| **port-channel** | Specifes an port channel type of interface. |
| *port-channel-number* | Number identifying this interface. The range is 1–4096. |
| **vethernet** | Specifes an Virtual Ethernet type of interface. |
| *interface-number* | Number identifying this interface. The range is 1–1048575 |
| **vlan** | (Optional) Specifies the VLAN associated with this MAC address table. |
| *id* | Identifier for the VLAN. The range is 1–4094. |

## 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 display static MAC addresses:

```
n1000v# show mac address-table static

Legend:
         * - primary entry, G - Gateway MAC, (R) - Routed MAC
         age - seconds since last seen
   VLAN      MAC Address      Type      age     Secure  NTFY       Ports
---------+-----------------+--------+---------+------+------+----------------
G     -   12ab.47dd.ff89     static      -     False   False      eth2/1

n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **mac address-table static** | Adds a static MAC address in the Layer 2 MAC address table and saves it in the running configuration. |
| **show mac address-table aging-time** | Displays the aging time in the MAC address table. |
| **show mac access-lists** | Displays the MAC ACL configuration. |

# show mac address-table aging-time

To display the aging time in the MAC address table, use the **show mac address-table aging-time** command.

**show mac address-table aging-time** [**vlan** *id*]

## Syntax Description

| | |
|---|---|
| **vlan** | (Optional) Specifies the VLAN associated with this MAC address table. |
| *id* | Identifier for the VLAN. The range is 1–4094. |

## 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 display the aging time in the MAC address table:

```
n1000v# show mac address-table aging-time
Vlan    Aging Time
----    ----------
1       300
2       300
100     300
101     300
102     300
103     300
104     300
105     300
106     300
107     300
108     300
109     300
115     300
260     300
261     300
n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **mac address-table aging-time** | Specifies and saves in the running configuration the amount of time that will elapse before an entry in the Layer 2 MAC address table is discarded. |
| **show mac address-table** | Displays the MAC address table. |
| **show mac access-lists** | Displays the MAC ACL configuration. |

# show module

To display module information, use the **show module** command.

**show module** [*module-number* | **internal** | **ipv6-info** | **uptime** | **vem**]

## Syntax Description

| | |
|---|---|
| *module-number* | (Optional) Number identifying an existing module. The range is 1–22. |
| **internal** | (Optional) Displays information about the module. |
| **ipv6-info** | (Optional) Displays information related to the server IPv6 address. |
| **uptime** | (Optional) Displays how long the module has been up and running. |
| **vem** | (Optional) Displays information about the Virtual Ethernet Module. |

## 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 display module information:

```
n1000v# show module
Mod  Ports  Module-Type                      Model              Status
---  -----  -------------------------------- ------------------ ------------
1    0      Virtual Supervisor Module        Nexus1000V         active *

Mod  Sw               Hw
---  ---------------  ------
1    4.0(4)SV1(2)     0.0

Mod  MAC-Address(es)                         Serial-Num
---  --------------------------------------  ----------
1    00-19-07-6c-5a-a8 to 00-19-07-6c-62-a8  NA

Mod  Server-IP        Server-UUID                           Server-Name
---  ---------------  ------------------------------------  --------------------

1    172.23.232.152   NA                                    NA


* this terminal session
n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **show module uptime** | Displays how long the module has been up and running. |
| **show module vem** | Displays VEM module information. |
| **show module ipv6-info** | Displays IPv6-related information. |
| **show module internal** | Displays module manager-related information. |

# show module vem mapping

To display information about the Virtual Ethernet Module (VEM) module mapping, use the **show module vem mapping** command.

**show module vem** [*module-number*] **mapping**

## Syntax Description

| | |
|---|---|
| *module-number* | (Optional) Number identifying an existing module. The range is 1–22. |

## 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 display information about the host/module mapping:

```
n1000v# show module vem mapping
Mod     Status          UUID                                    License Status
---     -----------     ------------------------------------    --------------
  3          absent     c43cfa32-08b4-4a12-b899-90f54fb05db0    licensed
n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **show module** | Displays module information. |
| **module vem** | Allows remote entry of commands on the VEM from the Cisco Nexus 1000V. |

# show monitor

To display the status of the Switched Port Analyzer (SPAN) sessions, use the **show monitor** command.

**show monitor**

## 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 display the status of the SPAN sessions:

```
n1000v# show monitor
Session  State        Reason                 Description
-------  -----------  ---------------------  --------------------------------
17       down         Session admin shut     folio
```

## Related Commands

| Command | Description |
|---|---|
| **monitor session** | Starts the specified SPAN monitor session from either global configuration mode or monitor-configuration mode. |
| **show monitor session** | Displays the ERSPAN session configuration as it exists in the running configuration. |

# show monitor session

To display the Switched Port Analyzer (SPAN) session configuration, use the **show monitor session** command.

**show monitor session** {*session_number* | **all** | **range** {*session_range*}} [**brief**]

## SyntaxDescription

| | |
|---|---|
| *session_number* | Number identifying the SPAN session number. The range is 1–64. |
| **all** | Specifies all sessions. |
| **range** | Indicates a session range. |
| *session_range* | Range of SPAN sessions from 1–64. |
| **brief** | (Optional) Specifies a shortened version. |

## 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 display the SPAN session configuration for session 1:

```
n1000v(config)# show monitor session 1
session 1
---------------
type : erspan-source
state : up
source intf :
    rx : Eth3/3
    tx : Eth3/3
    both : Eth3/3
source VLANs :
    rx :
    tx :
    both :
filter VLANs : filter not specified
destination IP : 10.54.54.1
ERSPAN ID : 999
ERSPAN TTL : 64
ERSPAN IP Prec. : 0
ERSPAN DSCP : 0
ERSPAN MTU : 1000
```

## Related Commands

| Command | Description |
|---|---|
| **show monitor** | Displays the status of the SPAN sessions. |
| **monitor session** | Starts the specified SPAN monitor session from either global configuration mode or monitor-configuration mode. |

# show ntp peer-status

To display the status for all Network Time Protocol (NTP) servers and peers, use the **show ntp peer-status** command.

**show ntp peer-status**

## 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

A domain name is resolved only when you have a DNS server configured.

## Examples

This example shows how to display the configured server and peers:

```
n1000v# show ntp peer-status
Total peers : 2
* - selected for sync, + -  peer mode(active),
- - peer mode(passive), = - polled in client mode
    remote          local        st  poll  reach   delay      vrf
-------------------------------------------------------------------------------
=192.0.2.10      0.0.0.0         16   16      0   0.00000 default
+72.229.253.127  0.0.0.0         16   16      0   0.00000 default
n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **show ntp peers** | Displays all NTP peers. |
| **show ntp statistics** | Displays NTP statistics. |
| **ntp server** | Forms an association with a server. |
| **ntp peer** | Forms an association with a peer. |

# show ntp peers

To display all Network Time Protocol (NTP) peers, use the **show ntp peers** command.

**show ntp peers**

## 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

A domain name is resolved only when you have a DNS server configured.

## Examples

This example shows how to display the configured server and peers:

```
n1000v# show ntp peers
-------------------------------------------------
  Peer IP Address               Serv/Peer
-------------------------------------------------
  192.0.2.10                    Server (configured)
  72.229.253.127                Peer (configured)
n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **show ntp peer-status** | Displays the status for all NTP servers and peers. |
| **show ntp statistics** | Displays NTP statistics. |
| **ntp server** | Forms an association with a server. |
| **ntp peer** | Forms an association with a peer. |

# show ntp statistics

To display Network Time Protocol (NTP) statistics, use the **show ntp statistics** command.

**show ntp statistics** {**io** | **local** | **memory** | **peer** {*ip-address* | *dns-name*}}

## Syntax Description

| | |
|---|---|
| **io** | Specifies the input-output statistics. |
| **local** | Specifies the counters maintained by the local NTP. |
| **memory** | Specifies the statistics counters related to the memory code. |
| **peer** | Specifies the per-peer statistics counter of a peer. |
| *ip-address* | IP address of this peer. |
| *dns-name* | DNS name of this peer. |

## 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

A domain name is resolved only when you have a DNS server configured.

## Examples

This example shows how to display the configured server and peers:

```
n1000v# show ntp statistics local
system uptime:          6742265
time since reset:       6742265
old version packets:    0
old version packets:    0
unknown version number: 0
bad packet format:      0
packets processed:      0
bad authentication:     0
packets rejected:       0
n1000v#
```

**Related Commands**

| Command | Description |
|---|---|
| **ntp server** | Forms an association with a server. |
| **ntp peer** | Forms an association with a peer. |

# show password strength-check

To display whether password strength is being checked, use the **show password strength-check** command.

**show password strength-check**

## 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 display whether password strength is being checked:

```
n1000v# show password strength-check
Password strength check enabled
n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **password strength-check** | Enables password-strength checking. |
| **username** | Creates a user account. |
| **role name** | Names a user role and puts you in role configuration mode for that role. |

# show policy-map

To display the policy map configuration for all policy maps or for a specified policy map, use the **show policy-map** command.

**show policy-map** [**type qos**] [*policy_map_name*]

## Syntax Description

| | |
|---|---|
| **type** | (Optional) Specifies the type of the policy map. |
| **qos** | (Optional) Specifies type QoS. |
| *policy_map_name* | (Optional) Name of an existing policy map. |

## 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 display the policy map configuration for all policy maps:

```
n1000v# show policy-map


Type qos policy-maps
  ====================

  policy-map type qos class1
    class  class-default
  policy-map type qos policy1
    class  class1
      set dscp 26
    class  class2
      set dscp 14
    class  class-default
      set dscp 20
      police cir 256000 bps bc 300 ms pir 256000 bps be 300 ms conform transmit

exceed set dscp dscp table cir-markdown-map violate drop
  policy-map type qos policy2
  policy-map type qos policy3
    class  class-default
      police cir 256000 bps bc 300 ms pir 256000 bps be 300 ms conform transmit
```

```
exceed set dscp dscp table cir-markdown-map violate drop
n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **show policy-map** | Displays the policy map configuration for all policy maps or for a specified policy map. |
| **class** | Creates a reference to class-map-name and enters policy-map class QoS configuration mode for the specified class map. |
| **set dscp** | Defines the DSCP value that should be used in all IP headers for the specified class and saves it in the running configuration. |

# show policy-map interface

To display the status of the global statistics and the configured policy maps on all interfaces, use the **show policy-map interface** command.

**show policy-map interface** [**brief**] [**ethernet** *slot/port* | **port-channel** *port_channel_number* | **vethernet** *interface_number*] [[**input** | **output**] [**type qos**]]

## Syntax Description

| | |
|---|---|
| **brief** | (Optional) Specifies the shortened output. |
| **ethernet** | (Optional) Specifies an Ethernet interface. |
| *slot/port* | Valid slot and port of the interface, separated by a slash (/). The slot range 1–66; the port range is 1–256. |
| **port-channel** | (Optional) Specifies a port channel interface. |
| *port_channel_number* | Identifier for a valid port channel. The range is 1–4096. |
| **vethernet** | (Optional) Specifies a Virtual Ethernet interface. |
| *interface_number* | Identifier for a valid Virtual Ethernet interface. The range is 1–1048575. |
| **input** | (Optional) Specifies the input policy |
| **output** | (Optional) Specifies the output policy. |
| **type** | (Optional) Specifies the type of the class-map. |
| **qos** | (Optional) Specifies type QoS. |

## 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 display statistics for policy maps that are configured on interfaces:

```
n1000v(config)# show policy-map interface

Global statistics status : enabled

Vethernet3
  Service-policy (qos) input: new-policy
```

```
    policy statistics status: enabled

    Class-map (qos): class-default (match-any)
      59610700 packets
      set prec 5

Vethernet5

  Service-policy (qos) output: new-policer
    policy statistics status: enabled

    Class-map (qos): new-class (match-all)
      344661013 packets
      Match: precedence 5
      police cir 900 mbps bc 200 ms
        conformed 505953339796 bytes, 899924196 bps action: transmit
        violated 12285218014 bytes, 22283000 bps action: dropn1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **policy-map** | Defines a policy map that represents a set of policies to be applied to a set of class maps. |
| **qos statistics** | Enables QoS statistics on all interfaces. |
| **clear qos statistics** | Clears the specified QoS statistics. |

# show port-channel compatibility-parameters

To display the parameters that must be the same among the member ports in order to join a port channel, use the **show port-channel compatibility parameters** command.

**show port-channel compatibility-parameters**

## 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

When you add an interface to a channel group, the software checks certain interface attributes to ensure that the interface is compatible with the channel group. For example, you cannot add a Layer 3 interface to a Layer 2 channel group. The software also checks a number of operational attributes for an interface before allowing that interface to participate in the port-channel aggregation.

This command displays the list of compatibility checks that the system uses.

Using the **channel-group** command, you can force ports with incompatible parameters to join the port channel as long as the following parameters are the same:

- (Link) speed capability
- Speed configuration
- Duplex capability
- Duplex configuration
- Flow-control capability
- Flow-control configuration

**Note** See the **channel-group** command for information about forcing ports to join a port channel.

## Examples

This example shows how to display the list of compatibility checks that the system makes before an interface to a channel group:

```
n1000v# show port-channel compatibility-parameters
```

```
* port mode

Members must have the same port mode configured, either E or AUTO. If they
are configured in AUTO port mode, they have to negotiate E mode when they
come up. If a member negotiates a different mode, it will be suspended.

* speed

Members must have the same speed configured. If they are configured in AUTO
speed, they have to negotiate the same speed when they come up. If a member
negotiates a different speed, it will be suspended.

* MTU

Members have to have the same MTU configured. This only applies to ethernet
port-channel.

* MEDIUM

Members have to have the same medium type configured. This only applies to
ethernet port-channel.

* Span mode

Members must have the same span mode.

* sub interfaces

Members must not have sub-interfaces.

* Duplex Mode

Members must have same Duplex Mode configured.

* Ethernet Layer

Members must have same Ethernet Layer (switchport/no-switchport) configured.

* Span Port

Members cannot be SPAN ports.

* Storm Control

Members must have same storm-control configured.

* Flow Control

Members must have same flowctrl configured.

* Capabilities

Members must have common capabilities.

* port

Members port VLAN info.

* port

Members port does not exist.

* switching port
```

```
Members must be switching port, Layer 2.

* port access VLAN

Members must have the same port access VLAN.

* port native VLAN

Members must have the same port native VLAN.

* port allowed VLAN list

Members must have the same port allowed VLAN list.
```

## Related Commands

| Command | Description |
|---|---|
| **channel-group** | Adds or removes interfaces to port-channel groups and assigns the port-channel mode to the interface. |

# show port-channel database

To display information about the current running of the port channels, use the **show port-channel database** command.

**show port-channel database** [**interface port-channel** *channel-number*]

## Syntax Description

| | |
|---|---|
| *channel-number* | Port-channel number for the information that you want to display. The range of values is from 1 to 4096. |

## Defaults

None

## Command Modes

Any

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

If you do not specify the *channel-number*, all channel groups are displayed. This command displays Link Aggregation Control Protocol (LACP)-enabled ports channels and port channels without an associated aggregation protocol.

## Examples

This example shows how to display information on the current running of all port channels:

```
n1000v# show port-channel database
port-channel5
    Administrative channel mode is active
    Operational channel mode is active
    Last membership update is successful
    1 ports in total, 0 ports up
    Age of the port-channel is 1d:16h:18m:50s
    Time since last bundle is 1d:16h:18m:56s
    Last bundled member is
    Ports:   Ethernet2/5            [down]

port-channel20
    Administrative channel mode is active
    Operational channel mode is active
    Last membership update is successful
    1 ports in total, 0 ports up
    Age of the port-channel is 1d:16h:18m:50s
    Time since last bundle is 1d:16h:18m:56s
    Last bundled member is
    Ports:   Ethernet2/20           [down]
```

This example shows how to display information on the current running of a specific port channel:

```
n1000v# show port-channel database interface port-channel 20
port-channel20
    Administrative channel mode is active
    Operational channel mode is active
    Last membership update is successful
    1 ports in total, 0 ports up
    Age of the port-channel is 1d:16h:23m:14s
    Time since last bundle is 1d:16h:23m:20s
    Last bundled member is
    Ports:   Ethernet2/20           [down]
```

## Related Commands

| Command | Description |
|---|---|
| **show port-channel summary** | Displays a summary of information about all port channels. |

# show port-channel load-balance

To display information about load-balancing using port channels, use the **show port-channel load-balance** command.

**show port-channel load-balance** [**forwarding-path interface port-channel** *channel-number*]

## Syntax Description

| | |
|---|---|
| **forwarding-path interface port-channel** | (Optional) Identifies the port in the port channel that forwards the packet. |
| *channel-number* | Port-channel number for the load-balancing forwarding path that you want to display. The range of values is from 1 to 4096. |

## Defaults

None

## 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 display information about the current port-channel load balancing for the system:

```
n1000v# show port-channel load-balance

Port Channel Load-Balancing Configuration:
System: source-dest-ip-vlan

Port Channel Load-Balancing Addresses Used Per-Protocol:
Non-IP: source-dest-mac
IP: source-dest-ip-vlan
```

## Related Commands

| Command | Description |
|---|---|
| **port-channel load-balance ethernet** | Configures load balancing using port channels. |

# show port-channel rbh-distribution

To display information about the Result Bundle Hash (RBH) for port channels, use the **show port-channel rbh-distribution** command.

**show port-channel rbh-distribution** [**interface port-channel** *channel-number*]

## Syntax Description

| | |
|---|---|
| *channel-number* | Port-channel number for the information the you want to display. The range of values is from 1 to 4096. |

## Defaults

None

## Command Modes

Any

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

The RBH value ranges from 0 to 7 and is shared among port members in a port channel.

## Examples

This example shows how to display RBH distribution for a specific port channel:

```
n1000v# show port-channel rbh-distribution interface port-channel 4

ChanId    Member port    RBH values         Num of buckets
--------  -------------  -----------------  ----------------
 4         Eth3/13        4,5,6,7            4
 4         Eth3/14        0,1,2,3            4
```

## Related Commands

| Command | Description |
|---|---|
| **port-channel summary** | Displays summary information on port channels. |

# show port-channel summary

To display summary information about the port channels, use the **show port-channel summary** command.

**show port-channel summary**

## 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

If the Link Aggregation Control Protocol (LACP) is not enabled, the output shows **NONE** in the Protocol column of the display.

A channel-group interface can be in the following operational states:

- Down—The interface is down because it is administratively shut down or some other reason not related to port channels.
- Individual—The interface is part of a port channel but unable to aggregate into a port channel because of protocol exchange problems.
  - This interface continues to forward traffic as an individual link.
  - STP is aware of this interface.
- Suspended—The operational parameters of the interface are not compatible with the port channel. This interface is not forwarding traffic, although the physical MAC link state is still up.
- Switched—The interface is switched.
- Up (port channel)—The port channel is up.
- Up in port channel (members)—The port member of the port channel is up.
- Hot standby (LACP only)—The interface is eligible to join the port group if one of the interfaces currently participating in the LACP channel goes down.
  - This interface does not forward data traffic, only protocol data units (PDUs).
  - This interface does not run STP.
- Module-removed—The module has been removed.

- Routed—The interface is routed.

## Examples

This example shows how to display summary information for the port channels:

```
n1000v# show port-channel summary
Flags:  D - Down        P - Up in port-channel (members)
        I - Individual  H - Hot-standby (LACP only)
        s - Suspended   r - Module-removed
        S - Switched    R - Routed
        U - Up (port-channel)
--------------------------------------------------------------------------
Group Port-       Type     Protocol  Member Ports
      Channel
--------------------------------------------------------------------------
5     Po5(SD)     Eth      LACP      Eth2/5(D)
20    Po20(RD)    Eth      LACP      Eth2/20(D)
```

## Related Commands

| Command | Description |
|---|---|
| **show port-channel usage** | Displays the port-channel numbers used and available. |
| **show port-channel traffic** | Displays transmitted and received unicast, multicast, and broadcast percentages for the port channels. |

# show port-channel traffic

To display traffic statistics for port channels, use the **show port-channel traffic** command.

**show port-channel traffic** [**interface port-channel** *channel-number*]

## Syntax Description

| | |
|---|---|
| *channel-number* | Port-channel number for the traffic statistics that you want to display. The range of values is from 1 to 4096. |

## Defaults

None

## Command Modes

Any

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

This command displays the percentage of transmitted and received unicast, multicast, and broadcast traffic on the port channel.

If you do not specify the *channel-number*, information for all port channels is displayed.

## Examples

This example shows how to display the traffic statistics for all port channels:

```
n1000v(config)# show port-channel traffic
ChanId      Port Rx-Ucst Tx-Ucst Rx-Mcst Tx-Mcst Rx-Bcst Tx-Bcst
------ --------- ------- ------- ------- ------- ------- -------
     5    Eth2/5    0.0%    0.0%    0.0%    0.0%    0.0%    0.0%
------ --------- ------- ------- ------- ------- ------- -------
    20   Eth2/20    0.0%    0.0%    0.0%    0.0%    0.0%    0.0%
```

This example shows how to display the traffic statistics for a specific port channel:

```
n1000v(config)# show port-channel traffic interface port-channel 5
ChanId      Port Rx-Ucst Tx-Ucst Rx-Mcst Tx-Mcst Rx-Bcst Tx-Bcst
------ --------- ------- ------- ------- ------- ------- -------
     5    Eth2/5    0.0%    0.0%    0.0%    0.0%    0.0%    0.0%
```

## Related Commands

| Command | Description |
|---|---|
| **port-channel summary** | Displays summary information about port channels. |

# show port-channel usage

To display the port-channel numbers used and available, use the **show port-channel usage** command.

**show port-channel usage**

## 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. |

## Examples

This example shows how to display the usage for all port channels:

```
n1000v# show port-channel usage
Totally 2 port-channel numbers used
====================================
Used  :   5 , 20
Unused:   1 - 4 , 6 - 19 , 21 - 4096
n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **port-channel summary** | Displays summary information about port channels. |

# show port-profile

To display configurations for port profiles, use the **show port-profile** command.

**show port-profile** [**name** *prof_name*]

## Syntax Description

| | |
|---|---|
| **name** | (Optional) Specifies to display information about a specific port profile. |
| *prof_name* | Name of the port profile to display. |

## Defaults

None

## Command Modes

Any

## SupportedUserRoles

network-admin
network-operator

## Command History

| Release | Modification |
|---|---|
| 4.0(4)SV1(1) | This command was introduced. |
| 4.0(4)SV1(2) | This command shows the port profile type and does not show the capability uplink. This command also shows pinning and channel-group configuration. |

## Examples

The following example shows how to display the configuration of port profile UplinkProfile1:

```
n1000v(config-port-prof)# show port-profile name UplinkProfile1
port-profile UplinkProfile1
  description: "Profile for critical system ports"
  type: ethernet
  status: disabled
  capability l3control: no
  pinning control-vlan: -
  pinning packet-vlan: -
  system vlans: none
  port-group: UplinkProfile1
  max ports: -
  inherit:
  config attributes:
    switchport mode access
    switchport access vlan 113
    switchport trunk native vlan 113
    channel-group auto mode on
    no shutdown
  evaluated config attributes:
    switchport mode access
    switchport access vlan 113
    switchport trunk native vlan 113
    channel-group auto mode on
```

```
    no shutdown
  assigned interfaces:
n1000v(config-port-prof)#
```

## Related Commands

| Command | Description |
|---|---|
| **virtual-service-domain** | Classifies and separates traffic for network services. |

# show port-profile expand-interface

To verify that the interface level configuration did not overwrite the port profile configuration, use the **show port-profile expand-interface** command.

**show port-profile expand-interface** [**name** *port-profile-name*]

## Syntax Description

| | |
|---|---|
| **name** | (Optional) Limits the display to a particular port profile name. |
| *module-number* | Name that identifies an existing port profile. |

## Defaults

None

## 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 verify that the interface level configuration did not overwrite the port profile configuration:

```
n1000v# show port-profile expand-interface

port-profile 1

port-profile 2

port-profile AccessProf

port-profile AccessProfile

port-profile AccessProfile1

port-profile AllAccess

port-profile AllAccess1

port-profile AllAccess2

port-profile PortProfile1

port-profile Profile1

port-profile SystemProfile

n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **show port-profile** | Displays configurations for port profiles. |
| **port-profile** | Creates a port profile and enters port-profile configuration mode. |
| **inherit port-profile** | Adds the inherited configuration to the new port profile as a default configuration. |

# show port-security

To display the secured MAC addresses in the system, use the **show port-security** command.

**show port-security**

## 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. |

## Examples

This example shows how to display the secured MAC addresses in the system:

```
n1000V# show port-security
Total Secured Mac Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 8192

-------------------------------------------------------------------------------
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                (Count)       (Count)          (Count)

-------------------------------------------------------------------------------
Vethernet1            1             0                0             Shutdown
===============================================================================
```

## Related Commands

| Command | Description |
|---|---|
| **port-security stop learning** | Sets the Drop on Source Miss (DSM) bit on the port. |
| **module vem execute** | Remotely executes commands on the Virtual Ethernet Module (VEM) from the Cisco Nexus 1000V. |
| **show cdp neighbors** | Displays the configuration and capabilities of upstream devices. |

# show port-security address

To display information about all secure MAC-addresses in the system, use the **show port-security address** command.

**show port-security address** *interface-id*

## Syntax Description

| | |
|---|---|
| **interface vethernet** | (Optional) Limits the secure MAC address information to a specific vEthernet interface. |
| **interface ethernet** | (Optional) Limits the secure MAC address information to a specific Ethernet interface. |

## 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

## Examples

This example shows how to use the **show port-security address** command to view information about all MAC addresses in the system:

```
n1000v# show port-security address
Total Secured Mac Addresses in System (excluding one mac per port) : 0
Max Addresses limit in System (excluding one mac per port) : 8192
------------------------------------------------------------------------
Secure Mac Address Table
------------------------------------------------------------------------
Vlan Mac Address Type Ports Remaining Age
(mins)
---- ----------- ------ ----- -------------
1 0054.AAB3.770F STATIC port-channel1 0
1 00EE.378A.ABCE STATIC Ethernet1/4 0
========================================================================
n1000v#
```

This example shows how to use the **show port-security address** command to view the MAC addresses secured by the port security feature on the Ethernet 1/4 interface:

```
n1000v# show port-security address interface ethernet 1/4
Secure Mac Address Table
------------------------------------------------------------------------
Vlan Mac Address Type Ports Remaining Age
(mins)
---- ----------- ------ ----- -------------
1 00EE.378A.ABCE STATIC Ethernet1/4 0
------------------------------------------------------------------------
n1000v#
```

This example shows how to use the **show port-security address** command to view the MAC addresses secured by the port security feature on the vethernet1 interface:

```
n1000v# show port-security address interface vethernet 1
Total Secured Mac Addresses in System (excluding one mac per port) : 0
Max Addresses limit in System (excluding one mac per port) : 8192
------------------------------------------------------------------------
Secure Mac Address Table
------------------------------------------------------------------------
Vlan Mac Address Type Ports Remaining age
(mins)
---- ----------- ------ ----- ---------------
65 0050.56B7.7DE2 DYNAMIC Vethernet1 0
========================================================================
n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **clear port-security** | Clears dynamically learned, secure MAC addresses. |
| **switchport port-security** | Enables port security on a Layer 2 interface. |
| **show port-security** | Shows information about port security. |
| **show port-security interface** | Displays information about secure interfaces. |
| **show running-config port-security** | Displays port-security configuration. |

# show port-security interface

To display information about the secure interfaces on the system, use the **show port-security interface** command.

**show port-security interface** *interface-id*

## Syntax Description

| | |
|---|---|
| *interface-id* | Interface ID. |

## 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

## Examples

This example shows how to use the **show port-security interface** command to view the status of the port security feature on the Ethernet 1/4 interface:

```
n1000v# show port-security interface ethernet 1/4
Port Security : Enabled
Port Status : Secure Down
Violation Mode : Shutdown
Aging Time : 0 mins
Aging Type : Absolute
Maximum MAC Addresses : 5
Total MAC Addresses : 1
Configured MAC Addresses : 1
Sticky MAC Addresses : 0
Security violation count : 0
n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **clear port-security** | Clears dynamically learned, secure MAC addresses. |
| **switchport port-security** | Enables port security on a Layer 2 interface. |

| Command | Description |
|---|---|
| **show port-security** | Shows information about port security. |
| **show port-security address** | Displays secure MAC addresses of the interfaces. |
| **show running-config port-security** | Displays port-security configuration. |

# show processes

To display the state and the start count of all processes, use the **show processes** command.

**show processes** [**cpu** | **log** | **memory**]

## Syntax Description

| | |
|---|---|
| **cpu** | (Optional) Specifies processes related to the CPU. |
| **log** | (Optional) Specifies information regarding process logs. |
| **memory** | (Optional) Specifies processes related to memory. |

## 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 display the state and the start count of all processe:

```
n1000v# show processes

PID    State  PC        Start_cnt    TTY   Type  Process
-----  -----  --------  -----------  ----  ----  -------------
    1      S  77f8a468            1     -     O  init
    2      S         0            1     -     O  ksoftirqd/0
    3      S         0            1     -     O  desched/0
    4      S         0            1     -     O  events/0
    5      S         0            1     -     O  khelper
   10      S         0            1     -     O  kthread
   18      S         0            1     -     O  kblockd/0
   35      S         0            1     -     O  khubd
  121      S         0            1     -     O  pdflush
  122      S         0            1     -     O  pdflush
  124      S         0            1     -     O  aio/0
  123      S         0            1     -     O  kswapd0
  709      S         0            1     -     O  kseriod
  756      S         0            1     -     O  kide/0
  766      S         0            1     -     O  ata/0
  770      S         0            1     -     O  scsi_eh_0
 1096      S         0            1     -     O  kjournald
 1101      S         0            1     -     O  kjournald
 1620      S         0            1     -     O  kjournald
 1627      S         0            1     -     O  kjournald
 1952      S  77f6c18e            1     -     O  portmap
```

```
1965      S         0            1      -     O  nfsd
1966      S         0            1      -     O  nfsd
1967      S         0            1      -     O  nfsd
1968      S         0            1      -     O  nfsd
1969      S         0            1      -     O  nfsd
1970      S         0            1      -     O  nfsd
1971      S         0            1      -     O  nfsd
1972      S         0            1      -     O  nfsd
1973      S         0            1      -     O  lockd
1974      S         0            1      -     O  rpciod
1979      S  77f6e468            1      -     O  rpc.mountd
1989      S  77f6e468            1      -     O  rpc.statd
2016      S  77e0e468            1      -    VG  sysmgr
2298      S         0            1      -     O  mping-thread
2299      S         0            1      -     O  mping-thread
2315      S         0            1      -     O  stun_kthread
2316      S         0            1      -     O  stun_arp_mts_kt
2339      S         0            1      -     O  redun_kthread
2340      S         0            1      -     O  redun_timer_kth
2866      S         0            1      -     O  sf_rdn_kthread
2866      S         0            1      -     O  sf_rdn_kthread
2867      S  77f37468            1      -    VU  xinetd
2868      S  77f6e468            1      -    VU  tftpd
2869      S  7788c1b6            1      -    VL  syslogd
2870      S  77ecf468            1      -    VU  sdwrapd
2872      S  77d94468            1      -    VU  platform
2877      S         0            1      -     O  ls-notify-mts-t
2889      S  77eb2be4            1      -    VU  pfm_dummy
2896      S  77f836be            1      -     O  klogd
2903      S  77d9ebe4            1      -    VL  vshd
2904      S  77e41468            1      -    VU  stun
2905      S  77a74f43            1      -    VL  smm
2906      S  77e5a468            1      -    VL  session-mgr
2907      S  77c4e468            1      -    VL  psshelper
2908      S  77f75468            1      -    VU  lmgrd
2909      S  77e36be4            1      -    VG  licmgr
2910      S  77ebe468            1      -    VG  fs-daemon
2911      S  77ec5468            1      -    VL  feature-mgr
2912      S  77e7a468            1      -    VU  confcheck
2913      S  77eb3468            1      -    VU  capability
2915      S  77c4e468            1      -    VU  psshelper_gsvc
2922      S  77f75468            1      -     O  cisco
2937      S  77895f43            1      -    VL  clis
2937      S  77895f43            1      -    VL  clis
2952      S  77cba468            1      -    VL  xmlma
2953      S  77e8b468            1      -    VL  vmm
2955      S  77e80468            1      -    VU  ttyd
2957      S  77ecb6be            1      -    VL  sysinfo
2958      S  77b57468            1      -    VL  sksd
2959      S  77ea7468            1      -    VG  res_mgr
2960      S  77e53468            1      -    VG  plugin
2961      S  77ccf468            1      -    VL  mvsh
2962      S  77e05468            1      -    VU  module
2963      S  77cce468            1      -    VL  evms
2964      S  77ccf468            1      -    VL  evmc
2965      S  77ecc468            1      -    VU  core-dmon
2966      S  7765b40d            1      -    VL  ascii-cfg
2967      S  77cebbe4            1      -    VL  securityd
2968      S  77cb5468            1      -    VU  cert_enroll
2969      S  77b17be4            1      -    VL  aaa
2973      S  77e19468            1      -    VU  ExceptionLog
2975      S  77dfb468            1      -    VU  bootvar
2976      S  77df9468            1      -    VG  ifmgr
2977      S  77ead468            1      -    VU  tcap
```

```
 2978      S  77a6bf43           1      -    VL  l3vm
 2978      S  77a6bf43           1      -    VL  l3vm
 2979      S  77a62f43           1      -    VL  u6rib
 2980      S  77a62f43           1      -    VL  urib
 2981      S  77f30be4           1      -    VU  core-client
 2983      S  77b95468           1      -    VL  aclmgr
 3008      S  77d51468           1      -    VU  aclcomp
 3011      S  7774440d           1      -    VL  tacacs
 3012      S  77a72f43           1      -    VL  adjmgr
 3016      S  77a74f43           1      -    VL  arp
 3021      S  778a1896           1      -    VL  icmpv6
 3022      S  7791ef43           1      -    VL  netstack
 3050      S  7770240d           1      -    VL  radius
 3051      S  77f59be4           1      -    VL  ip_dummy
 3052      S  77f59be4           1      -    VL  ipv6_dummy
 3053      S  7783c40d           1      -    VU  ntp
 3054      S  77f59be4           1      -    VL  pktmgr_dummy
 3055      S  778ae40d           1      -    VL  snmpd
 3056      S  77f59be4           1      -    VL  tcpudp_dummy
 3063      S  7782d40d           1      -    VL  cdp
 3064      S  77b1540d           1      -    VL  dcos-xinetd
 3154      S  77b4040d           1      -     O  ntpd
 3195      S  77e0d468           1      -    VL  vsim
 3196      S  778ee40d           1      -    VL  ufdm
 3196      S  778ee40d           1      -    VL  ufdm
 3197      S  77d42468           1      -    VU  sf_nf_srv
 3198      S  778e240d           1      -    VL  sal
 3199      S  77a14f43           1      -    VL  rpm
 3200      S  778cd40d           1      -    VG  pltfm_config
 3201      S  77efc468           1      -    VU  pixmc
 3202      S  77e0f468           1      -    VG  pixm
 3203      S  77c43468           1      -    VU  pdl_srv_tst
 3204      S  7789e40d           1      -    VL  nfm
 3205      S  77ddc468           1      -    VU  msp
 3206      S  77dbc468           1      -    VL  monitor
 3207      S  7789c40d           1      -    VL  mfdm
 3208      S  7787340d           1      -    VL  l2fm
 3209      S  77dc0468           1      -    VL  ipqosmgr
 3210      S  77e81468           1      -    VU  ethanalyzer
 3211      S  777b740d           1      -    VL  dhcp_snoop
 3212      S  77b3940d           1      -    VL  dcos-thttpd
 3213      S  77c26468           1      -    VU  copp
 3214      S  77b2b468           1      -    VL  eth_port_channel
 3215      S  77d15468           1      -    VL  vlan_mgr
 3219      S  758bc40d           1      -    VU  vms
 3220      S  77b8a468           1      -    VL  eth-port-sec
 3221      S  77abb468           1      -    VL  stp
 3221      S  77abb468           1      -    VL  stp
 3226      S  77de5468           1      -    VL  lacp
 3228      S  777ba40d           1      -    VL  ethpm
 3232      S  77a0127b           1      -    VL  igmp
 3235      S  77dba468           1      -    VL  private-vlan
 3241      S  77d70468           1      -    VU  vim
 3246      S  77d4b468           1      -    VU  portprofile
 3285      S  77f836be           1      1     O  getty
 3286      S  77f806be           1     S0     O  getty
 3290      S  77f1deee           1      -     O  gettylogin1
 3308      S  77f836be           1     S1     O  getty
 3360      S  77ae140d           1      -     O  dcos_sshd
 3361      S  77aaa468           1      8     O  vsh
 4213      Z           0         1      -     O  vmw_maintenance
25188      Z           0         1      -     O  vmw_maintenance
31228      Z           0         1      -     O  vmw_maintenance
  427      Z           0         1      -     O  vmw_maintenance
```

```
 1035      Z         0           1      -     O  vmw_maintenance
 2439      Z         0           1      -     O  vmw_maintenance
 7167      Z         0           1      -     O  vmw_maintenance
 8246      Z         0           1      -     O  vmw_maintenance
 8856      Z         0           1      -     O  vmw_maintenance
10539      Z         0           1      -     O  vmw_maintenance
10539      Z         0           1      -     O  vmw_maintenance
16083      Z         0           1      -     O  vmw_maintenance
19353      S  77ae140d           1      -     O  dcos_sshd
19354      S  7752340d           1      -     O  xmlsa
13167      S  77ae140d           1      -     O  dcos_sshd
13169      S  77aaa468           1     17     O  vsh
14253      S  7798140d           1      -     O  in.dcos-telnetd
14254      S  77aaa468           1     18     O  vsh
14757      S  7798140d           1      -     O  in.dcos-telnetd
14758      S  77a82eee           1     19     O  vsh
14933      S  77f426be           1     19     O  more
14934      S  77aa9be4           1     19     O  vsh
14935      R  77f716be           1      -     O  ps
    -     NR        -           0      -    VL  eigrp
    -     NR        -           0      -    VL  isis
    -     NR        -           0      -    VL  ospf
    -     NR        -           0      -    VL  ospfv3
    -     NR        -           0      -    VL  rip
    -     NR        -           0      -    VL  eigrp
    -     NR        -           0      -    VL  isis
    -     NR        -           0      -    VL  ospf
    -     NR        -           0      -    VL  ospfv3
    -     NR        -           0      -    VL  rip
    -     NR        -           0      -    VL  rip
    -     NR        -           0      -    VL  eigrp
    -     NR        -           0      -    VL  isis
    -     NR        -           0      -    VL  ospf
    -     NR        -           0      -    VL  ospfv3
    -     NR        -           0      -    VL  rip
    -     NR        -           0      -    VL  eigrp
    -     NR        -           0      -    VL  isis
    -     NR        -           0      -    VL  ospf
    -     NR        -           0      -    VL  ospfv3
    -     NR        -           0      -    VL  rip
    -     NR        -           0      -    VL  amt
    -     NR        -           0      -    VL  bgp
    -     NR        -           0      -    VL  eou
    -     NR        -           0      -    VL  glbp
    -     NR        -           0      -    VL  hsrp_engine
    -     NR        -           0      -    VU  installer
    -     NR        -           0      -    VL  interface-vlan
    -     NR        -           0      -    VU  lisp
    -     NR        -           0      -    VL  msdp
    -     NR        -           0      -    VL  pim
    -     NR        -           0      -    VL  pim6
    -     NR        -           0      -    VL  scheduler
    -     NR        -           0      -    VL  isis
    -     NR        -           0      -    VL  ospf
    -     NR        -           0      -    VL  ospfv3
    -     NR        -           0      -    VL  rip
    -     NR        -           0      -    VL  amt
    -     NR        -           0      -    VL  bgp
    -     NR        -           0      -    VL  eou
    -     NR        -           0      -    VL  glbp
    -     NR        -           0      -    VL  hsrp_engine
    -     NR        -           0      -    VU  installer
    -     NR        -           0      -    VL  interface-vlan
    -     NR        -           0      -    VU  lisp
```

```
    -     NR          -            0     -    VL  msdp
    -     NR          -            0     -    VL  pim
    -     NR          -            0     -    VL  pim6
    -     NR          -            0     -    VL  scheduler
    -     NR          -            0     -    VU  vbuilder

State: R(runnable), S(sleeping), Z(defunct)

Type:  U(unknown), O(non sysmgr)
       NR(not running), ER(terminated etc)
n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **show system redundancy status** | Displays the HA status of the system. |
| **show module** | Displays information about all available VSMs and VEMs in the system. |
| **module vem** | Allows you to enter commands on the VEM remotely from the Cisco Nexus 1000V. |

# show radius-server

To display the RADIUS server configuration, use the **show radius-server** command.

**show radius-server** [*host*]

## Syntax Description

| | |
|---|---|
| *host* | (Optional) DNS name or IP address for the RADIUS server. |

## 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 display the RADIUS server configuration:

```
n1000v# show radius-server ads
        ads:
                available for authentication on port:1812
                available for accounting on port:1813
                idle time:0
                test user:test
                test password:********
n1000v(config)#
```

## Related Commands

| Command | Description |
|---|---|
| **radius-server host** | Defines the IP address or hostname for the RADIUS server. |
| **radius-server directed-request** | Enables directed requests. |
| **show radius-server groups** | Displays information about the RADIUS server group configuration. |
| **show radius-server sorted** | Displays RADIUS servers sorted by name. |
| **show radius-server statistics** | Displays RADIUS statistics. |
| **show radius-server directed-request** | Displays the directed request configuration. |

# show radius-server directed-request

To display the directed request configuration, use the **show radius-server directed-request** command.

**show radius-server directed-request**

## 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 display the directed request configuration:

```
n1000v(config)# show radius-server directed-request
disabled
n1000v(config)#
```

## Related Commands

| Command | Description |
|---|---|
| **radius-server directed-request** | Enables directed requests. |
| **show radius-server groups** | Displays information about the RADIUS server group configuration. |
| **show radius-server sorted** | Displays RADIUS servers sorted by name. |
| **show radius-server statistics** | Displays RADIUS statistics. |

# show radius-server groups

To display information about the RADIUS server group configuration, use the **show radius-server groups** command.

**show radius-server groups** [*group-name*]

## Syntax Description

| | |
|---|---|
| *group-name* | (Optional) Name of the RADIUS server group. |

## 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 display information about the RADIUS server group configuration:

```
n1000v# show radius-server groups
n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **aaa group server radius** | Creates a RADIUS server group and enters the RADIUS server group configuration submode for that group. |
| **radius-server host** | Defines the IP address or hostname for the RADIUS server. |
| **radius-server directed-request** | Enables directed requests. |
| **show radius-server sorted** | Displays RADIUS servers sorted by name. |
| **show radius-server statistics** | Displays RADIUS statistics. |
| **show radius-server directed-request** | Displays the directed request configuration. |

# show radius-server sorted

To display the RADIUS server configuration in a sorted format, use the **show radius-server sorted** command.

**show radius-server sorted**

## 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 display the RADIUS server configuration in a sorted format:

```
n1000v(config)# show radius-server sorted
```

## Related Commands

| Command | Description |
|---|---|
| **radius-server host** | Defines the IP address or hostname for the RADIUS server. |
| **radius-server directed-request** | Enables directed requests. |
| **show radius-server groups** | Displays information about the RADIUS server group configuration. |
| **show radius-server statistics** | Displays RADIUS statistics. |
| **show radius-server directed-request** | Displays the directed request configuration. |

# show radius-server statistics

To displays the RADIUS statistics, use the **show radius-server statistics** command.

**show radius-server statistics** {*hostname* | *ipv4-address*}

## Syntax Description

| | |
|---|---|
| *hostname* | DNS name for the RADIUS server host. |
| *ipv4-address* | IP address of the RADIUS server host. |

## 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 display the RADIUS statistics:

```
n1000v# show radius-server statistics 10.10.1.1
Server is not monitored

Authentication Statistics
        failed transactions: 0
        sucessfull transactions: 0
        requests sent: 0
        requests timed out: 0
        responses with no matching requests: 0
        responses not processed: 0
        responses containing errors: 0

Accounting Statistics
        failed transactions: 0
        sucessfull transactions: 0
        requests sent: 0
        requests timed out: 0
        responses with no matching requests: 0
        responses not processed: 0
        responses containing errors: 0
```

## Related Commands

| Command | Description |
|---|---|
| **radius-server host** | Defines the IP address or hostname for the RADIUS server. |
| **radius-server directed-request** | Enables directed requests. |
| **show radius-server groups** | Displays information about the RADIUS server group configuration. |
| **show radius-server sorted** | Displays RADIUS servers sorted by name. |
| **show radius-server statistics** | Displays RADIUS statistics. |
| **show radius-server directed-request** | Displays the directed request configuration. |

# show running-config diff

To verify the difference between the running and startup configurations, use the **show running-config diff** command.

**show running-config diff**

## 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

When you switch over from one VSM to another, any unsaved running configuration that was available in an active VSM is still unsaved in the new active VSM. You can verify this unsaved running configuration with this command. Then, save that configuration in the startup. if needed.

## Examples

This example shows how to verify the difference between the running and startup configurations:

```
n1000v# show running-config diff
*** Startup-config
--- Running-config
***************
*** 1,38 ****
version 4.0(4)SV1(1)
role feature-group name new
role name testrole
username admin password 5 $1$S7HvKc5G$aguYqHl0dPttBJAhEPwsy1 role network-admin
telnet server enable
ip domain-lookup
```

## Related Commands

| Command | Description |
|---|---|
| **system switchover** | Initiates, on the active VSM, a manual switchover to the standby VSM. |
| **copy running-config startup-config** | Copies the running configuration to the startup configuration. |

# show running-config interface ethernet

To display the running configuration for a specific Ethernet interface, use the **show running-config interface ethernet** command.

**show running-config interface ethernet** *slot/port*

## Syntax Description

| | |
|---|---|
| *slot/port* | Slot number and port number for an existing Ethernet interface. |

## Defaults

None

## 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 display the running configuration for a Ethernet interface 2/1:

```
n1000v# show running-config interface ethernet 2/1
version 4.0(4)SV1(3)

interface Ethernet3/2
  inherit port-profile uplink_all
```

## Related Commands

| Command | Description |
|---|---|
| **show running-config interface port-channel** | Displays information about the running configuration of the port channel. |
| **show running-config interface vethernet** | Displays information about the running configuration of the vEthernet interface. |

# show running-config interface port-channel

To display the running configuration for a specific port channel, use the **show running-config interface port-channel** command.

**show running-config interface port-channel** {*channel-number*}

## Syntax Description

| | |
|---|---|
| *channel-number* | Number of the port-channel group. The range of values is from 1 to 4096. |

## Defaults

None

## Command Modes

Any

## SupportedUserRoles

network-admin

## Command History

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

## Examples

The following example shows how to display the running configuration for port channel 10:

```
n1000v(config)# show running-config interface port-channel 10
version 4.0(4)SV1(1)

interface port-channel10
  switchport
  switchport mode trunk
```

## Related Commands

| Command | Description |
|---|---|
| **show port-channel summary** | Displays a summary of port-channel information. |

# show running-config interface vethernet

To display the running configuration for a specific vEthernet interface, use the **show running-config interface vethernet** command.

**show running-config interface vethernet** *interface-number*

## Syntax Description

| | |
|---|---|
| *interface-number* | Number that identifies an existing vEthernet interface. |

## Defaults

None

## 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 display the running configuration for a vEthernet interface 2/1:

```
n1000v# show running-config interface vethernet 1
version 4.0(4)SV1(2)

interface Vethernet1
  description isp_pvlan1
  pinning id 3
  switchport mode private-vlan host
  no shutdown

n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **show running-config interface port-channel** | Displays information about the running configuration of the port channel. |
| **show running-config interface ethernet** | Displays information about the running configuration of the Ethernet interface. |

# show running-config vlan

To display the running configuration for a specified VLAN, use the **show running-config vlan** command.

**show running-config vlan** *vlan-id*

## Syntax Description

| | |
|---|---|
| *vlan-id* | VLAN ID number or range of VLANs. Valid VLAN IDs are1-4094 or ranges are 1-5, 10 or 2-5, 7-19. |

## 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

## Examples

This example shows how display the running configuration for VLAN100:

```
n1000v(config)# show running-config vlan 100
version 4.2(1)SV1(4)
vlan 100
n1000v(config)#
```

## Related Commands

| Command | Description |
|---|---|
| **show vlan** | Displays VLAN information. |
| **vlan** | Creates a VLAN. |

# show radius-server directed-request

To display the directed request configuration, use the **show radius-server directed-request** command.

**show radius-server directed-request**

## 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 display the directed request configuration:

```
n1000v(config)# show radius-server directed-request
disabled
n1000v(config)#
```

## Related Commands

| Command | Description |
|---|---|
| **radius-server directed-request** | Enables directed requests. |
| **show radius-server groups** | Displays information about the RADIUS server group configuration. |
| **show radius-server sorted** | Displays RADIUS servers sorted by name. |
| **show radius-server statistics** | Displays RADIUS statistics. |

# show snmp

To display information about one or more destination profiles, use the **show snmp** command.

**show snmp** [**community** | **context** | **engineID** | **group** | **host** | **sessions** | **trap** | **user**]

## Syntax Description

| | |
|---|---|
| **community** | (Optional) Specifies SNMP community strings. |
| **context** | (Optional) Specifies SNMP context mapping entries. |
| **engineID** | (Optional) Specifies the SNMP engineID. |
| **group** | (Optional) Specifies the SNMP group. |
| **host** | (Optional) Specifies SNMP hosts. |
| **sessions** | (Optional) Specifies SNMP sessions. |
| **trap** | (Optional) Specifies SNMP traps. |
| **user** | (Optional) Specifies SNMPv3 users. |

## 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 display information about the SNMP engineID:

```
n1000v# show snmp engineID
Local SNMP engineID: [Hex] 8000000903020000C000000
                     [Dec] 128:000:000:009:003:002:000:012:000:000:000:000
n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **snmp-server contact** | Configures sysContact, which is the SNMP contact name. |
| **snmp-server location** | Configures sysLocation, which is the SNMP location. |

# show ssh key

To display the Secure Shell (SSH) server keys, use the **show ssh key** command.

**show ssh key** [**dsa** | **rsa**]

## Syntax Description

| | |
|---|---|
| **dsa** | (Optional) Specifies the display of DSA SSH keys. |
| **rsa** | (Optional) Specifies the display of RSA SSH keys. |

## 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 display SSH server keys:

```
n1000v# show ssh key
n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **ssh key** | Generates the SSH server key. |
| **show ssh server** | Displays whether the SSH server is enabled. |

# show ssh server

To display the Secure Shell (SSH) server configuration, use the **show ssh server** command.

**show ssh server**

## 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 display the SSH server configuration:

```
n1000v# show ssh server
ssh is enabled
version 2 enabled
n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **ssh** | Creates an SSH IP session to a remote device using IP. |
| **ssh key** | Generates the SSH server key. |
| **show ssh server** | Displays whether the SSH server is enabled. |
| **show ssh key** | Displays the SSH server keys. |

# show startup-config aaa

To display the Authentication, Authorization and Accounting protocol (AAA) configuration in the startup configuration, use the **show startup-config aaa** command.

**show startup-config aaa**

## 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 display the AAA configuration in the startup configuration:

```
n1000v# show startup-config aaa
version 4.0(4)SV1(2)

n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **show startup-config aclmanager** | Displays startup configuration for the access control list (ACL) manager. |
| **show startup-config am** | Displays information about the Arthur–Merlin protocol (AM). |
| **show startup-config arp** | Displays information about ARP. |
| **show startup-config dhcp** | Displays information about DHCP. |
| **show startup-config icmpv6** | Displays information about ICMPv6. |
| **show startup-config igmp** | Displays information about IGMP. |
| **show startup-config interface** | Displays the interface configuration. |

| Command | Description |
|---|---|
| **show startup-config ip** | Displays information about IP. |
| **show startup-config ipqos** | Displays the startup configuration for IP QoS Manager. |
| **show startup-config ipv6** | Displays information about IPv6. |
| **show startup-config l3vm** | Displays information about l3vm. |
| **show startup-config license** | Displays information about licensing. |
| **show startup-config log** | Displays the execution log of the last-used ASCII startup configuration. |
| **show startup-config monitor** | Displays configured Ethernet SPAN sessions. |
| **show startup-config netflow** | Displays the NetFlow configuration. |
| **show startup-config port-profile** | Displays the port-profile configuration. |
| **show startup-config port-security** | Displays the port-security configuration. |
| **show startup-config radius** | Displays the RADIUS configuration. |
| **show startup-config tacacs+** | Displays the TACACS configuration. |

# show startup-config radius

To display the RADIUS configuration in the startup configuration, use the **show startup-config radius** command.

**show startup-config radius**

## 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 display the RADIUS configuration in the startup configuration:

```
n1000v# show startup-config radius
version 4.0(4)SV1(2)

n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **show startup-config aaa** | Displays the Authentication, Authorization and Accounting protocol (AAA) configuration in the startup configuration. |
| **show startup-config aclmanager** | Displays startup configuration for the access control list (ACL) manager. |
| **show startup-config am** | Displays information about Arthur-Merlin protocol (AM). |
| **show startup-config arp** | Displays information about ARP. |
| **show startup-config dhcp** | Displays information about DHCP. |
| **show startup-config icmpv6** | Displays information about ICMPv6. |
| **show startup-config igmp** | Displays information about IGMP. |

| Command | Description |
|---|---|
| **show startup-config interface** | Displays the interface configuration. |
| **show startup-config ip** | Displays information about IP. |
| **show startup-config ipqos** | Displays the startup configuration for the IP QoS Manager. |
| **show startup-config ipv6** | Displays information about IPv6. |
| **show startup-config l3vm** | Displays information about l3vm. |
| **show startup-config license** | Displays information about licensing. |
| **show startup-config log** | Displays the execution log of the last-used ASCII startup configuration. |
| **show startup-config monitor** | Displays configured Ethernet SPAN sessions. |
| **show startup-config netflow** | Displays the NetFlow configuration. |
| **show startup-config port-profile** | Displays the port-profile configuration. |
| **show startup-config port-security** | Displays the port-security configuration. |
| **show startup-config radius** | Displays the RADIUS configuration. |
| **show startup-config tacacs+** | Displays the TACACS configuration. |

# show startup-config security

To dsplay the user account configuration in the startup configuration, use the **show startup-config security** command.

**show startup-config security**

## 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 display the user account configuration in the startup configuration:

```
n1000v# show startup-config security
version 4.0(4)SV1(2)
username admin password 5 $1$3/cH7rWm$W3QUjfQOyfySds5p3/PtX.  role network-admin

username kathleen password 5 $1$7vewiaFA$iLCfmalyKeSBySqrAgvNZ/  role network-op

erator
username kathleen role network-admin
telnet server enable

n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **show startup-config aaa** | Displays the Authentication, Authorization and Accounting protocol (AAA) configuration. |
| **show startup-config aclmanager** | Displays the startup configuration for Access Control List (ACL) manager. |
| **show startup-config am** | Displays information about the Arthur–Merlin protocol (AM). |
| **show startup-config arp** | Displays information about ARP. |
| **show startup-config dhcp** | Displays information about DHCP. |

| Command | Description |
|---|---|
| **show startup-config icmpv6** | Displays information about ICMPv6. |
| **show startup-config igmp** | Displays information about IGMP. |
| **show startup-config interface** | Displays the interface configuration. |
| **show startup-config ip** | Displays information about IP. |
| **show startup-config ipqos** | Displays the startup configuration for the IP QoS Manager. |
| **show startup-config ipv6** | Displays information about IPv6. |
| **show startup-config l3vm** | Displays information about l3vm. |
| **show startup-config license** | Displays information about licensing. |
| **show startup-config log** | Displays the execution log of last used ASCII startup configuration. |
| **show startup-config monitor** | Displays configured Ethernet SPAN sessions. |
| **show startup-config netflow** | Displays the NetFlow configuration. |
| **show startup-config port-profile** | Displays the port profile configuration. |
| **show startup-config port-security** | Displays the port-security configuration. |
| **show startup-config radius** | Displays the RADIUS configuration. |
| **show startup-config tacacs+** | Displays the TACACS configuration. |

# show svs connections

To display the current connections to the Cisco Nexus 1000V for verification, use the **show svs connections** command.

**show svs connections** [*conn_name*]

## Syntax Description

| | |
|---|---|
| *conn_name* | (Optional) Name of an existing connection. |

## 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 display information about the SVS connection:

```
n1000v# show svs connections

connection vc:
    hostname: 172.23.232.139
    remote port: 80
    protocol: vmware-vim https
    certificate: default
    datacenter name: Documentation-DC
    DVS uuid: 9b dd 36 50 2e 27 27 8b-07 ed 81 89 ef 43 31 17
    config status: Enabled
    operational status: Disconnected
    sync status: -
    version: -
n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **svs connection** | Places you into connection configuration mode for adding this connection between Cisco Nexus 1000V and the vCenter Server. |
| **show svs domain** | Displays the domain configuration. |
| **show svs neighbors** | Displays information about SVS neighbors. |

# show svs domain

To display the VSM domain configuration, use the **show svs domain** command.

**show svs domain**

## 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. |
| 4.0(4)SV1(2) | The output of this command was modified to include the Layer 2 and Layer 3 transport mode configuration. |

## Examples

This example shows how to display the VSM domain configuration:

```
n1000v# config t
n1000v(config)# svs-domain
n1000v(config-svs-domain)# show svs domain
SVS domain config:
  Domain id:    100
  Control vlan: 100
  Packet vlan:  101
  Management vlan:  0
  L2/L3 Control mode: L3
  L2/L3 Control interface: mgmt0
  Status: Config push to VC successful.
n1000v(config-svs-domain)#
```

## Related Commands

| Command | Description |
|---|---|
| **svs-domain** | Creates and configures a domain for the Cisco Nexus 1000V that identifies the VSM and VEMs and the control and packet VLANs for communication and management. |

# show svs neighbors

To display all SVS neighbors, use the **show svs neighbors** command.

**show svs neighbors**

## 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. |

## Examples

This example shows how to display all SVS neighbors:

```
n1000v# show svs neighbors

Active Domain ID: 113

AIPC Interface MAC: 0050-56b6-2bd3
Inband Interface MAC: 0050-56b6-4f2d

Src MAC           Type   Domain-id    Node-id     Last learnt (Sec. ago)
------------------------------------------------------------------------

0002-3d40-7102     VEM       113         0302     71441.12
0002-3d40-7103     VEM       113         0402       390.77

n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **show svs domain** | Displays the Virtual Supervisor Module (VSM) domain configuration. |
| **svs-domain** | Creates and configures a domain for the Cisco Nexus 1000V that identifies the VSM and Virtual Ethernet Modules (VEMs) and the control and packet VLANs for communication and management. |

# show system error-id

To display detailed information on system error codes, use the **show system error-id** command.

**show system error-id** {**list** | *error-code*}

## Syntax Description

| | |
|---|---|
| **list** | Displays brief information for all the system error messages. |
| *error-code* | Displays description about a specific error code. |

## 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

## Examples

This example shows how to display detailed information about error code 0x401e0008:

```
n1000v# show system error-id 0x401e0008
Error Facility: sysmgr
Error Description: request was aborted, standby disk may be full
n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **show system vem feature level** | Displays the current software release supported. |
| **show system redundancy status** | Displays the system redundancy status. |
| **system vlan** | Adds the system VLAN to this port profile. |
| **show system resources** | Displays the system resources. |

# show system redundancy status

To display the current redundancy status for the Virtual Supervisor Module (VSM), use the **show system redundancy status** command.

**show system redundancy status**

## 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 display the current redundancy status for the VSM:

```
n1000v# show system redundancy status
Redundancy role
---------------
      administrative:   standalone
         operational:   standalone

Redundancy mode
---------------
      administrative:   HA
         operational:   None

This supervisor (sup-1)
-----------------------
    Redundancy state:   Active
    Supervisor state:   Active
      Internal state:   Active with no standby

Other supervisor (sup-2)
------------------------
    Redundancy state:   Not present
n1000v#
```

**Related Commands**

| Command | Description |
|---|---|
| **system redundancy role** | Designates the HA role of the VSM. |
| **show system resources** | Displays the system resources. |

# show system resources

To display system-related CPU and memory statistics, use the **show system resources** command.

**show system resources**

## 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. |

## Examples

This example shows how to display system-related CPU and memory statistics:

```
n1000v# show system resources
Load average:   1 minute: 0.00   5 minutes: 0.00   15 minutes: 0.00
Processes   :   261 total, 1 running
CPU states  :   0.0% user,   0.0% kernel,   100.0% idle
Memory usage:   2075012K total,    946780K used,   1128232K free
                  66764K buffers,  475404K cache

n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **show system vem feature level** | Displays the current software release supported. |
| **show system redundancy** | Displays the system redundancy status. |
| **system vlan** | Adds the system VLAN to this port profile. |

# show system vem feature level

To display the current software release supported, use the **show system vem feature level** command.

**show system vem feature level**

## 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(2) | This command was introduced. |

## Examples

This example shows how to display the current VEM feature level:

```
n1000v# show system vem feature level
current feature level: 4.0(4)SV1(2)
n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **system update vem feature level** | Changes the software version supported on VEMs. |

# show tacacs-server

To display the TACACS+ server configuration, use the **show tacacs-server** command.

**show tacacs-server**

## 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

The global shared key is saved in encrypted form in the running configuration. To display the key, use the **show running-config** command.

## Examples

This example shows how to displays the TACACS+ server configuration:

```
n1000v# show tacacs-server
Global TACACS+ shared secret:********
timeout value:5
deadtime value:0
total number of servers:1
following TACACS+ servers are configured:
10.10.2.2:
available on port:49
```

## Related Commands

| Command | Description |
|---|---|
| **tacacs+ enable** | Enables TACACS+. |
| **tacacs-server key** | Designates the global key shared between the Cisco Nexus 1000V and the TACACS+ server hosts. |
| **show tacacs-server directed-request** | Displays the directed server enable configuration. |
| **show tacacs-server groups** | Displays information about the TACACS+ server group configuration. |

| Command | Description |
|---|---|
| **show tacacs-server sorted** | Displays TACACS+ servers, sorted by server name. |
| **show tacacs-server statistics** | Displays TACACS statistics. |

# show tcp client

To display information about the TCP client, use the **show tcp client** command.

**show tcp client** [**pid** *pid*] [**detail**]

## Syntax Description

| | |
|---|---|
| **pid** | (Optional) Specifies information about the client process. |
| *pid* | ID for the specified client process. |
| **detail** | (Optional) Specifies socket details. |

## 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 display information about the TCP client:

```
n1000v# show tcp client
Total number of clients: 12
Total number of cancels: 255372
client: syslogd, pid: 2962, sockets: 2
client: ntp, pid: 3148, sockets: 2
client: dcos-xinetd, pid: 3156, sockets: 2
client: snmpd, pid: 3150, sockets: 4
client: ntpd, pid: 3243, sockets: 3
client: dcos-thttpd, pid: 3305, sockets: 2
client: radiusd, pid: 3143, sockets: 2
client: vms, pid: 3318, sockets: 0
client: dcos_sshd, pid: 3491, sockets: 3
client: vsh, pid: 3494, sockets: 0
client: in.dcos-telnetd, pid: 25028, sockets: 3
client: vsh, pid: 25029, sockets: 0
```

## Related Commands

| Command | Description |
|---|---|
| **show tcp connection** | Displays information about the TCP connection. |
| **show tcp statistics** | Displays TCP protocol statistics. |

# show tcp connection

To display information about the connection, use the **show tcp connection** command.

**show tcp connection** [**pid** *pid* | **tcp** | **udp** | **raw**] [**local** {*srcIP* | *srcIP6*}] [**foreign** {*dstIP* | *dstIP6*}] [**detail**]

## Syntax Description

| | |
|---|---|
| **pid** | (Optional) Specifies the client process connection status. |
| *pid* | ID for the client process connection status. |
| **tcp** | (Optional) Specifies all TCP connections. |
| **udp** | (Optional) Specifies all UDP connections. |
| **raw** | (Optional) Specifies all RAW connections. |
| **local** | (Optional) Specifies all TCP connections with a specified local address. |
| *srcIP* | Local IP address in the format A.B.C.D. |
| *srcIP6* | Local IP address in the format A:B::C:.D. |
| **foreign** | (Optional) Specifies all TCP connections with a specified foreign address. |
| *dstIP* | Destination IP address in the format A.B.C.D. |
| *dstIP6* | Destination IP address in the format A:B::C:.D. |
| **detail** | (Optional) Specifies detailed connection infomation. |

## 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 display detailed information about the connection:

```
n1000v# show tcp connection detail
Total number of tcp sockets: 8
Active connections (including servers)
Local host: * (22), Foreign host: * (0)
  Protocol: tcp6, type: stream, ttl: 64, tos: 0, Id: 6
  Options: none, state:
  Receive buffer:
    cc: 0, hiwat: 25300, lowat: 1, flags: none
  Send buffer:
    cc: 0, hiwat: 25300, lowat: 2048, flags:
```

```
  Sequence number state:
    iss: 0, snduna: 0, sndnxt: 0, sndwnd: 0
    irs: 0, rcvnxt: 0, rcvwnd: 0, sndcwnd: 1012
  Timing parameters:
    srtt: 0 ms, rtt: 0 ms, rttv: 12000 ms, krtt: 3000 ms
    rttmin: 1000 ms, mss: 1012, duration: 1390144100 ms
  State: LISTEN
  Flags: none
  Context: management

Local host: * (23), Foreign host: * (0)
  Protocol: tcp6, type: stream, ttl: 64, tos: 0, Id: 17
  Options: none, state:
  Receive buffer:
    cc: 0, hiwat: 17204, lowat: 1, flags: none
  Send buffer:
    cc: 0, hiwat: 17204, lowat: 2048, flags:
  Sequence number state:
    iss: 0, snduna: 0, sndnxt: 0, sndwnd: 0
    irs: 0, rcvnxt: 0, rcvwnd: 0, sndcwnd: 1012
  Timing parameters:
    srtt: 0 ms, rtt: 0 ms, rttv: 12000 ms, krtt: 3000 ms
    rttmin: 1000 ms, mss: 1012, duration: 1390144100 ms
  State: LISTEN
  Flags: none
  Context: management

Local host: * (80), Foreign host: * (0)
  Protocol: tcp6, type: stream, ttl: 64, tos: 0, Id: 13
  Options: none, state: none
  Receive buffer:
    cc: 0, hiwat: 16384, lowat: 1, flags: none
  Send buffer:
    cc: 0, hiwat: 16384, lowat: 2048, flags:
  Sequence number state:
    iss: 0, snduna: 0, sndnxt: 0, sndwnd: 0
    irs: 0, rcvnxt: 0, rcvwnd: 0, sndcwnd: 1073725440
  Timing parameters:
    srtt: 0 ms, rtt: 0 ms, rttv: 12000 ms, krtt: 3000 ms
    rttmin: 1000 ms, mss: 1024, duration: 1390144100 ms
  State: LISTEN
  Flags: none
  Context: management

Local host: * (80), Foreign host: * (0)
  Protocol: tcp, type: stream, ttl: 64, tos: 0, Id: 14
  Options: none, state: none
  Receive buffer:
    cc: 0, hiwat: 16500, lowat: 1, flags: none
  Send buffer:
    cc: 0, hiwat: 16500, lowat: 2048, flags:
  Sequence number state:
    iss: 0, snduna: 0, sndnxt: 0, sndwnd: 0
    irs: 0, rcvnxt: 0, rcvwnd: 0, sndcwnd: 500
  Timing parameters:
    srtt: 0 ms, rtt: 0 ms, rttv: 12000 ms, krtt: 3000 ms
    rttmin: 1000 ms, mss: 500, duration: 1390144100 ms
  State: LISTEN
  Flags: none
  Context: management

Local host: * (161), Foreign host: * (0)
  Protocol: tcp, type: stream, ttl: 64, tos: 0, Id: 3
  Options: none, state: none
```

```
  Receive buffer:
    cc: 0, hiwat: 16384, lowat: 1, flags: none
  Send buffer:
    cc: 0, hiwat: 16384, lowat: 2048, flags:
  Sequence number state:
    iss: 0, snduna: 0, sndnxt: 0, sndwnd: 0
    irs: 0, rcvnxt: 0, rcvwnd: 0, sndcwnd: 512
  Timing parameters:
    srtt: 0 ms, rtt: 0 ms, rttv: 12000 ms, krtt: 3000 ms
    rttmin: 1000 ms, mss: 512, duration: 1390144100 ms
  State: LISTEN
  Flags: none
  Context: management

Local host: * (161), Foreign host: * (0)
  Protocol: tcp6, type: stream, ttl: 64, tos: 0, Id: 5
  Options: none, state: none
  Receive buffer:
    cc: 0, hiwat: 16384, lowat: 1, flags: none
  Send buffer:
    cc: 0, hiwat: 16384, lowat: 2048, flags:
  Sequence number state:
    iss: 0, snduna: 0, sndnxt: 0, sndwnd: 0
    irs: 0, rcvnxt: 0, rcvwnd: 0, sndcwnd: 1073725440
  Timing parameters:
    srtt: 0 ms, rtt: 0 ms, rttv: 12000 ms, krtt: 3000 ms
    rttmin: 1000 ms, mss: 1024, duration: 1390144100 ms
  State: LISTEN
  Flags: none
  Context: management

Local host: 10.10.233.74 (22), Foreign host: 10.10.185.189 (48131)
  Protocol: tcp, type: stream, ttl: 64, tos: 0, Id: 20
  Options: none, state: none
  Receive buffer:
    cc: 0, hiwat: 17500, lowat: 1, flags: none
  Send buffer:
    cc: 0, hiwat: 17500, lowat: 2048, flags:
  Sequence number state:
    iss: 3575780911, snduna: 3576001996, sndnxt: 3576001996, sndwnd: 32767
    irs: 905490047, rcvnxt: 905574926, rcvwnd: 17500, sndcwnd: 1953
  Timing parameters:
    srtt: 700 ms, rtt: 0 ms, rttv: 0 ms, krtt: 1000 ms
    rttmin: 1000 ms, mss: 500, duration: 1390101600 ms
  State: ESTABLISHED
  Flags: none
  Context: management

Local host: 10.10.233.74 (23), Foreign host: 10.10.22.107 (35030)
  Protocol: tcp, type: stream, ttl: 64, tos: 0, Id: 18
  Options: none, state: none
  Receive buffer:
    cc: 0, hiwat: 17500, lowat: 1, flags: none
  Send buffer:
    cc: 0, hiwat: 17500, lowat: 2048, flags:
  Sequence number state:
    iss: 3273730667, snduna: 3273793065, sndnxt: 3273793065, sndwnd: 32767
    irs: 3760023047, rcvnxt: 3760024636, rcvwnd: 17500, sndcwnd: 25095
  Timing parameters:
    srtt: 700 ms, rtt: 0 ms, rttv: 0 ms, krtt: 1000 ms
    rttmin: 1000 ms, mss: 500, duration: 467168700 ms
  State: ESTABLISHED
  Flags: none
  Context: management
```

```
Total number of udp sockets: 11
Active connections (including servers)
Local host: * (123), Foreign host: * (0)
  Protocol: udp6, type: dgram, ttl: 64, tos: 0, Id: 11
  Options: none, state: none
  Receive buffer:
    cc: 0, hiwat: 42240, lowat: 1, flags: none
  Send buffer:
    cc: 0, hiwat: 9216, lowat: 2048, flags:
  Context: management

Local host: * (123), Foreign host: * (0)
  Protocol: udp, type: dgram, ttl: 64, tos: 0x10, Id: 10
  Options: none, state: none
  Receive buffer:
    cc: 0, hiwat: 42240, lowat: 1, flags: none
  Send buffer:
    cc: 0, hiwat: 9216, lowat: 2048, flags:
  Context: management

Local host: * (161), Foreign host: * (0)
  Protocol: udp, type: dgram, ttl: 64, tos: 0, Id: 1
  Options: none, state:
  Receive buffer:
    cc: 0, hiwat: 131072, lowat: 1, flags: none
  Send buffer:
    cc: 0, hiwat: 131072, lowat: 2048, flags:
  Context: management

Local host: * (161), Foreign host: * (0)
  Protocol: udp6, type: dgram, ttl: 64, tos: 0, Id: 2
  Options: none, state:
  Receive buffer:
    cc: 0, hiwat: 131072, lowat: 1, flags: none
  Send buffer:
    cc: 0, hiwat: 131072, lowat: 2048, flags:
  Context: management

Local host: 127.0.0.1 (123), Foreign host: * (0)
  Protocol: udp, type: dgram, ttl: 64, tos: 0x10, Id: 12
  Options: none, state: none
  Receive buffer:
    cc: 0, hiwat: 42240, lowat: 1, flags: none
  Send buffer:
    cc: 0, hiwat: 9216, lowat: 2048, flags:
  Context: management

Local host: 127.0.0.1 (130), Foreign host: * (0)
  Protocol: udp, type: dgram, ttl: 64, tos: 0, Id: 9
  Options: none, state:
  Receive buffer:
    cc: 0, hiwat: 42240, lowat: 1, flags: none
  Send buffer:
    cc: 0, hiwat: 9216, lowat: 2048, flags:
  Context: management

Local host: 127.0.0.1 (27613), Foreign host: 127.0.0.1 (123)
  Protocol: udp, type: dgram, ttl: 64, tos: 0, Id: 8
  Options: , state: none
  Receive buffer:
    cc: 0, hiwat: 42240, lowat: 1, flags:
  Send buffer:
    cc: 0, hiwat: 9216, lowat: 2048, flags:
```

```
  Context: management


Total number of raw sockets: 0
```

## Related Commands

| Command | Description |
|---|---|
| **show telnet server** | Displays the Telnet server configuration. |
| **show running-config security** | Displays the user account configuration in the running configuration. |
| **show tcp client** | Displays information about the TCP client. |
| **show tcp statistics** | Displays TCP protocol statistics. |

# show tcp statistics

To display TCP protocol statistics, use the **show tcp statistics** command.

**show tcp statistics** [**all** | **tcp4** | **tcp6** | **tcpsum** | **udp4** | **udp6** | **udpsum** | **raw4** | **raw6** | **rawsum**]

## Syntax Description

| | |
|---|---|
| **all** | (Optional) Specifies all TCPv4, TCPv6, UDPv4, UDPv6, RAWv4, and RAWv6 protocol statistics. |
| **tcp4** | (Optional) Specifies TCPv4 protocol statistics. |
| **tcp6** | (Optional) Specifies TCPv6 protocol statistics. |
| **tcpsum** | (Optional) Specifies the sum of TCPv4 and TCPv6 protocols statistics. |
| **udp4** | (Optional) Specifies UDPv4 protocol statistics. |
| **udp6** | (Optional) Specifies UDPv6 protocol statistics. |
| **udpsum** | (Optional) Specifies the sum of UDPv4 and UDPv6 protocols statistics. |
| **raw4** | (Optional) Specifies RAWv4 protocol statistics. |
| **raw6** | (Optional) Specifies RAWv6 protocol statistics. |
| **rawsum** | (Optional) Specifies the sum of RAWv4 and RAWv6 protocols statistics. |

## 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 display TCP protocol statistics:

```
n1000v# show tcp statistics
TCP Received:
        479908 packets total
        0 checksum error, 0 bad offset, 0 too short, 0 MD5 error
        232451 packets (72213943 bytes) in sequence
        195 duplicate packets (192 bytes)
        0 partially dup packets (0 bytes)
        8652 out-of-order packets (0 bytes)
        0 packets (0 bytes) with data after window
        2 packets after close
        0 window probe packets, 0 window update packets
        44339 duplicate ack packets, 0 ack packets with unsent data
        252581 ack packets (103465405 bytes)
```

```
TCP Sent:
        533421 total, 0 urgent packets
        94694 control packets
        326430 data packets (105082025 bytes)
        90 data packets (22114 bytes) retransmitted
        105144 ack only packets
        34 window probe packets, 7029 window update packets
TCP:
44330 connections initiated, 6715 connections accepted, 50669 connections established
51045 connections closed (including 165 dropped, 376 embryonic dropped)
3067 total rxmt timeout, 0 connections dropped in rxmt timeout
463 keepalive timeout, 92 keepalive probe, 371 connections dropped in keepalive
```

## Related Commands

| Command | Description |
|---|---|
| **show tcp connection** | Displays information about the TCP connection. |
| **show tcp statistics** | Displays TCP protocol statistics. |

# show tech-support

To collect switch information for Cisco TAC to assist you in diagnosing issues, use the **show tech-support** command.

**show tech-support** {**aclmgr** | **dhcp** | **ipqos** | **ipv6** | **netflow** | **svs** | **vsd**}

## Syntax Description

| | |
|---|---|
| **aclmgr** | Gathers information regarding access control list (ACL) commands. |
| **dhcp** | Gathers information related to DHCP, such as snooping statistics and VLAN configuration. |
| **ipqos** | Displays IP QoS Manager information, such as event details and policy configuration. |
| **ipv6** | Displays IPv6 information, such as IPv6 static routes and traffic statistics. |
| **netflow** | Displays information regarding NetFlow, such as event details and statistics. |
| **svs** | Displays SVS information, such as interface and software configurations. |
| **vsd** | Displays virtual service domain (VSD) events and statistical information. |

## Defaults

None

## 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 collect switch information for Cisco TAC regarding IPv6 issues:

```
n1000v# show tech-support ipv6
`show ipv6 interface vrf all`
`show ipv6 static-route`
IPv6 Configured Static Routes

`show ipv6 statistic`
FTM related Statistics
ftm_stats_get : 0.00 0
ftm_stats_get_init : 0.00 0
ftm_stats_get_tx : 0.00 0
ftm_stats_get_rx : 0.00 0
ftm_stats_get_flush : 0.00 0
ftm_stats_get_radix : 0.00 0
ftm_stats_csm_fp : 0.00 0
`show ipv6 client`
IPv6 Registered Client Status
```

```
Client: icmpv6, status: up, pid: 3021, extended pid: 3021
  Protocol: 58, pib-index: 4, routing context id: 255
  Control mts SAP: 1280
  Data mts SAP: 1281
  IPC messages to control mq: 0
  IPC messages to data mq: 0

Client: tcpudp, status: up, pid: 3022, extended pid: 3022
  Protocol: 17, pib-index: 3, routing context id: 255
  Control mts SAP: 1219
  Data mts SAP: 1220
  IPC messages to control mq: 1
  IPC messages to data mq: 0
  Recv fn: tcp_process_ipv6_data_msg (0x81fd22a)

Client: tcpudp, status: up, pid: 3022, extended pid: 3022
  Protocol: 6, pib-index: 2, routing context id: 255
  Control mts SAP: 1219
  Data mts SAP: 1220
  IPC messages to control mq: 1
  IPC messages to data mq: 0
  Recv fn: tcp_process_ipv6_data_msg (0x81fd22a)
`show ipv6 traffic`
IPv6 Software Processed Traffic and Error Statistics, last reset: never

RP-Traffic Statistics:
  Counter                  Unicast  Multicast
  -------                  -------  ---------
  Packets forwarded:             0  0
  Bytes forwarded:               0  0
  Packets originated:            0  0
  Bytes originated:              0  0
  Packets consumed:              0  0
  Bytes consumed:                0  0
  Fragments originated:          0  0
  Fragments consumed:            0  0

Error Statistics:
  Bad version: 0, route lookup failed: 0, hop limit exceeded: 0
  Option header errors: 0, payload length too small: 0
  PM errors: 0, MBUF errors: 0, encapsulation errors: 0
Syntax error while parsing 'show ipv6 route'

`show ipv6 internal mem-stats all`

Mem stats for IPV6

Private Mem stats for UUID : Malloc track Library(103) Max types: 5
--------------------------------------------------------------------------------

Curr alloc: 1591 Curr alloc bytes: 76678(74k)
  IPC messages to control mq: 0

Curr alloc: 1522 Curr alloc bytes: 164596(160k)


Private Mem stats for UUID : Routing IPC Library(528) Max types: 10
--------------------------------------------------------------------------------

Curr alloc: 0 Curr alloc bytes: 0(0k)


Private Mem stats for UUID : Routing Library for managing mbufs(522) Max types:
```

```
6
-------------------------------------------------------------------------------

Curr alloc: 120 Curr alloc bytes: 485008(473k)


Private Mem stats for UUID : Patricia Trie Library(523) Max types: 3
-------------------------------------------------------------------------------

Curr alloc: 29 Curr alloc bytes: 916(0k)

  IPC messages to control mq: 0

Curr alloc: 1522 Curr alloc bytes: 164596(160k)


Private Mem stats for UUID : Routing IPC Library(528) Max types: 10
-------------------------------------------------------------------------------

Curr alloc: 0 Curr alloc bytes: 0(0k)


Private Mem stats for UUID : Routing Library for managing mbufs(522) Max types:

6
-------------------------------------------------------------------------------

Curr alloc: 120 Curr alloc bytes: 485008(473k)


Private Mem stats for UUID : Patricia Trie Library(523) Max types: 3
-------------------------------------------------------------------------------

Curr alloc: 29 Curr alloc bytes: 916(0k)

  IPC messages to control mq: 0

Curr alloc: 1522 Curr alloc bytes: 164596(160k)


Private Mem stats for UUID : Routing IPC Library(528) Max types: 10
-------------------------------------------------------------------------------

Curr alloc: 0 Curr alloc bytes: 0(0k)


Private Mem stats for UUID : Routing Library for managing mbufs(522) Max types:

6
-------------------------------------------------------------------------------

Curr alloc: 120 Curr alloc bytes: 485008(473k)


Private Mem stats for UUID : Patricia Trie Library(523) Max types: 3
-------------------------------------------------------------------------------

Curr alloc: 29 Curr alloc bytes: 916(0k)

  IPC messages to control mq: 0

Curr alloc: 1522 Curr alloc bytes: 164596(160k)
```

```
Private Mem stats for UUID : Routing IPC Library(528) Max types: 10
-------------------------------------------------------------------------------

Curr alloc: 0 Curr alloc bytes: 0(0k)


Private Mem stats for UUID : Routing Library for managing mbufs(522) Max types:

6
-------------------------------------------------------------------------------

Curr alloc: 120 Curr alloc bytes: 485008(473k)


Private Mem stats for UUID : Patricia Trie Library(523) Max types: 3
-------------------------------------------------------------------------------

Curr alloc: 29 Curr alloc bytes: 916(0k)


Curr alloc: 0 Curr alloc bytes: 0(0k)


Private Mem stats for UUID : libfsrv(404) Max types: 11
-------------------------------------------------------------------------------

Curr alloc: 65 Curr alloc bytes: 1888(1k)


Private Mem stats for UUID : FSM Utils(53) Max types: 68
-------------------------------------------------------------------------------

Curr alloc: 10 Curr alloc bytes: 376(0k)


Private Mem stats for UUID : IM LIB(319) Max types: 33
-------------------------------------------------------------------------------

Curr alloc: 0 Curr alloc bytes: 0(0k)


Private Mem stats for UUID : Packet Manager(263) Max types: 16
-------------------------------------------------------------------------------

Curr alloc: 22 Curr alloc bytes: 236504(230k)


Private Mem stats for UUID : Internet Protocol version 6 (IPv6)(269) Max types:

16
-------------------------------------------------------------------------------

Curr alloc: 6 Curr alloc bytes: 1088(1k)


Private Mem stats for UUID : Transmission Control Protocol (TCP)(271) Max types:

 18
-------------------------------------------------------------------------------

Curr alloc: 70 Curr alloc bytes: 272444(266k)


Private Mem stats for UUID : Lcache(544) Max types: 3
```

```
Private Mem stats for UUID : Adjacency Manager(264) Max types: 16
--------------------------------------------------------------------------------

Curr alloc: 0 Curr alloc bytes: 0(0k)


Private Mem stats for UUID : Internet Control Message Protocol version 6 (ICMPv6

)(270) Max types: 27
--------------------------------------------------------------------------------

Curr alloc: 0 Curr alloc bytes: 0(0k)


Private Mem stats for UUID : NF DDB Utils(515) Max types: 15
--------------------------------------------------------------------------------

Curr alloc: 0 Curr alloc bytes: 0(0k)

Curr alloc: 3838 Curr alloc bytes: 15194210 (14838k)

Shared Mem stats for UUID : Non mtrack users(0) Max types: 155

Shared Mem stats for UUID : Patricia Trie Library(523) Max types: 2
--------------------------------------------------------------------------------

Curr alloc: 2 Curr alloc bytes: 64(0k)


Shared Mem stats for UUID : Slab Library(529) Max types: 3
--------------------------------------------------------------------------------

Curr alloc: 4 Curr alloc bytes: 288(0k)


Shared Mem stats for UUID : Bitlogic Library(517) Max types: 6
--------------------------------------------------------------------------------

Curr alloc: 0 Curr alloc bytes: 0(0k)


Shared Mem stats for UUID : Cisco Regex Package(525) Max types: 2
--------------------------------------------------------------------------------

Curr alloc: 0 Curr alloc bytes: 0(0k)
--------------------------------------------------------------------------------

Curr alloc: 0 Curr alloc bytes: 0(0k)


Shared Mem stats for UUID : Routing Queue Library(526) Max types: 2
--------------------------------------------------------------------------------

Curr alloc: 0 Curr alloc bytes: 0(0k)


Shared Mem stats for UUID : Internet Protocol (IP)(267) Max types: 12
--------------------------------------------------------------------------------

Curr alloc: 10 Curr alloc bytes: 65888(64k)


Shared Mem stats for UUID : SMM Library(561) Max types: 2
```

```
------------------------------------------------------------------------------

Curr alloc: 0 Curr alloc bytes: 0(0k)


Shared Mem stats for UUID : Internet Protocol version 6 (IPv6)(269) Max types: 1

4
------------------------------------------------------------------------------

Curr alloc: 7 Curr alloc bytes: 536(0k)


Shared Mem stats for UUID : Adjacency Manager(264) Max types: 5
------------------------------------------------------------------------------

Curr alloc: 0 Curr alloc bytes: 0(0k)

Curr alloc: 23 Curr alloc bytes: 66776 (65k)
n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **show logging logfile** | Displays the contents of the log file. |
| **logging logfile** | Configures the log file used to store system messages. |

# show telnet server

To display the Telnet server configuration, use the **show telnet server** command.

**show telnet server**

## 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 display the Telnet server configuration:

```
n1000v# show telnet server
telnet service enabled
n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **show tcp connection** | Displays information about the connection. |
| **telnet** | Uses Telnet to connect to another system. |
| **telnet6** | Uses Telnet6 to connect to another system. |

# show terminal

To display the terminal settings for the current session, use the **show terminal** command.

**show terminal**

## 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 display the terminal settings for the current session:

```
n1000v# show terminal
TTY: /dev/pts/8 type: "vt100"
Length: 24 lines, Width: 88 columns
Session Timeout: None
n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **terminal width** | Configures the number of characters to display on each line for the current console session. |
| **terminal terminal-type** | Sets the terminal type. |
| **terminal length** | Sets the number of lines on the screen. |
| **terminal width** | Sets the width of the display terminal. |
| **line console** | Puts you in console configuration mode. |
| **line vty** | Puts you in line configuration mode. |

# show user-account

To display user account configuration, use the **show user-account** command.

**show user-account** [*username*]

## Syntax Description

| | |
|---|---|
| *username* | (Optional) Name of a user with an existing account. |

## 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 display user account configuration for the user called NewUser:

```
n1000v(config)# show user-account NewUser
user:NewUser
this user account has no expiry date
roles:network-operator network-admin
n1000v(config)#
```

## Related Commands

| Command | Description |
|---|---|
| **show role** | Displays the available roles that can be assigned to users. |
| **role name** | Names a user role and places you in role configuration mode for that role. |
| **username password** | Creates a user account. |
| **show users** | Displays the current users logged in the system. |

# show users

To display information about the user session, use the **show users** command.

**show users**

## 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 display information about the user session:

```
n1000v# show users
NAME     LINE         TIME         IDLE          PID COMMENT
admin    pts/17       Dec 16 06:37   .         30406 (172.28.254.254) session=ss

h
admin    pts/18       Jan  3 19:01   .          3847 (sjc-vpn5-786.cisco.com) *
n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **show user-account** | Displays the new user account configuration. |
| **show role** | Displays the available roles that can be assigned to users. |
| **username password** | Creates a user account. |
| **role name** | Names a user role and places you in role configuration mode for that role. |

# show version

To display the versions of system software and hardware that are currently running on the switch, use the **show version** command.

**show version** [**module**]

## Syntax Description

| | |
|---|---|
| **module** | (Optional) Specifies the software version of a module. |

## 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 display the versions of system software and hardware that are currently running on the switch:

```
n1000v# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2009, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php

Software
  loader:    version 1.2(2) [last: image booted through mgmt0]
  kickstart: version 4.0(4)SV1(2)
  system:    version 4.0(4)SV1(2)
  kickstart image file is:
  kickstart compile time:  9/22/2009 2:00:00
  system image file is:    bootflash:/nexus-1000v-mz.4.0.4.SV1.2.bin
  system compile time:     9/22/2009 2:00:00 [10/07/2009 10:11:01]

Software
  loader:    version 1.2(2) [last: image booted through mgmt0]
  kickstart: version 4.0(4)SV1(2)
  system:    version 4.0(4)SV1(2)
```

```
  kickstart image file is:
  kickstart compile time:  9/22/2009 2:00:00
  system image file is:    bootflash:/nexus-1000v-mz.4.0.4.SV1.2.bin
  system compile time:     9/22/2009 2:00:00 [10/07/2009 10:11:01]

Hardware
  Cisco Nexus 1000V Chassis ("Virtual Supervisor Module")
  Intel(R) Xeon(R) CPU         with 2075012 kB of memory.
  Processor Board ID T5056B645A8

  Device name: n1000v
  bootflash:    2332296 kB

Kernel uptime is 79 day(s), 0 hour(s), 24 minute(s), 55 second(s)

plugin
  Core Plugin, Ethernet Plugin
n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **show version image** | Displays the versions of system software and hardware that are currently running on the switch. |
| **show running-config** | Displays information about the configuration currently running on the system. |
| **show running-config diff** | Displays the difference between the startup configuration and the running configuration currently on the switch. |
| **show interface** | Displays details about the specified interface configuration. |

# show version image

To display the software version of a given image, use the **show version** command.

**show version image** {**bootflash:** *URI* | **volatile:** *URI*}

## Syntax Description

| | |
|---|---|
| **bootflash:** | Specifies bootflash as the directory name. |
| *URI* | URI of the system where the image resides. |
| **volatile:** | Specifies volatile as the directory name. |

## 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 display the versions of system software and hardware that are currently running on the switch:

```
n1000v# show version image bootflash:isan.bin
   image name: nexus-1000v-mz.4.0.4.SV1.1.bin
   bios: version unavailable
   system: version 4.0(4)SV1(1)
   compiled: 4/2/2009 23:00:00 [04/23/2009 09:55:29]
n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **show version** | Displays the software version of a given image. |
| **show running-config** | Displays information about the configuration currently running on the system. |
| **show running-config diff** | Displays the difference between the startup configuration and the running configuration currently on the switch. |
| **show interface** | Displays details about the specified interface configuration. |

# show virtual-service-domain brief

To display a list of the VSDs currently configured in a VSM, including VSD names and port profiles, use the **show virtual-service-domain brief** command.

**show virtual-service-domain brief**

## Syntax Description

This command has no arguments or keywords.

## Defaults

None

## Command Modes

Any

## SupportedUserRoles

network-admin
network-operatorr

## Command History

| Release | Modification |
|---|---|
| 4.0(4)SV1(2) | This command was introduced. |

## Examples

This example shows how to display a list of the VSDs currently configured in a VSM:

```
n1000v# show virtual-service-domain brief
Name             default action    in-ports    out-ports   mem-ports
vsd1             drop              1           1           4
vsd2             forward           1           1           0
vsim-cp# sho virtual-service-domain interface
_ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _
Name             Interface             Type      Status
_ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _
vsd1             Vethernet1            Member    Active
vsd1             Vethernet2            Member    Active
vsd1             Vethernet3            Member    Active
vsd1             Vethernet6            Member    Active
vsd1             Vethernet7            Inside    Active
vsd1             Vethernet8            Outside   Active
vsd2             Vethernet9            Inside    Active
vsd2             Vethernet10           Outside   Active
vsim-cp# show virtual-service-domain name vsd1
Default Action: drop
_____________________________
Interface        Type
_____________________________
Vethernet1       Member
Vethernet2       Member
Vethernet3       Member
Vethernet6       Member
Vethernet7       Inside
Vethernet8       Outside
```

```
n1000v#
```

**Related Commands**

| Command | Description |
|---|---|
| **virtual-service-domain** | Creates a virtual service domain that classifies and separates traffic for network services. |

# show virtual-service-domain interface

To do the interfaces currently assigned to the VSDs in a VSM, use the **show virtual-service-domain interface** command.

**show virtual-service-domain interface**

## 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(2) | This command was introduced. |

## Examples

This example shows how to display the interfaces currently assigned to the VSDs in a VSM:

```
n1000v# show virtual-service-domain interface
_ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _
Name             Interface             Type      Status
_ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _
vsd1             Vethernet1            Member    Active
vsd1             Vethernet2            Member    Active
vsd1             Vethernet3            Member    Active
vsd1             Vethernet6            Member    Active
vsd1             Vethernet7            Inside    Active
vsd1             Vethernet8            Outside   Active
vsd2             Vethernet9            Inside    Active
vsd2             Vethernet10           Outside   Active
```

## Related Commands

| Command | Description |
|---|---|
| **virtual-service-domain** | Creates a virtual service domain that classifies and separate traffic for network services. |

# show virtual-service-domain name

To display a specific VSD currently configured in a VSM, including associated port profiles, use the **show virtual-service-domain name** command.

**show virtual-service-domain name** *virtual-service-domain_name*

## Syntax Description

| | |
|---|---|
| *virtual-service-domain_name* | Name of the VSD. |

## Defaults

None

## Command Modes

Any

## SupportedUserRoles

network-admin
network-operator

## Command History

| Release | Modification |
|---|---|
| 4.0(4)SV1(2) | This command was introduced. |

## Examples

This example shows how to display a specific VSD configuration:

```
n1000v# show virtual-service-domain name vsd1
Default Action: drop

_____________________________
Interface        Type
_____________________________
Vethernet1       Member
Vethernet2       Member
Vethernet3       Member
Vethernet6       Member
Vethernet7       Inside
Vethernet8       Outside

n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **virtual-service-domain** | Creates a virtual service domain that classifies and separate traffic for network services. |

# show vlan

To display the status and information for VLANs. use the **show vlan** command.

**show vlan**

## 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 display the status and information for VLANs:

```
n1000v# show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Po1, Po12, Veth1, Veth2, Veth3
                                                Veth10, Veth100
2    VLAN0002                         active
100  VLAN0100                         active
101  VLAN0101                         active
102  VLAN0102                         active
103  VLAN0103                         active
104  VLAN0104                         active
105  VLAN0105                         active
106  VLAN0106                         active
107  VLAN0107                         active
108  VLAN0108                         active
109  VLAN0109                         active
115  VLAN0115                         active
260  cp_control                       active
261  cp_packet                        active

VLAN Type
---- -----
1    enet
2    enet
100  enet
101  enet
102  enet
```

```
103  enet
104  enet
105  enet
106  enet
107  enet
108  enet
109  enet
115  enet
260  enet
261  enet

Remote SPAN VLANs
------------------------------------------------------------------------------

Primary  Secondary  Type             Ports
-------  ---------  ---------------  ------------------------------------------


n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **interface** | Specifies the interface that you are configuring and places you in interface configuration mode. |
| **switchport trunk native vlan** | Designates the native VLAN for the 802.1Q trunk in the running configuration. |
| **switchport trunk allowed vlan** | Sets the allowed VLANs for the trunk interface in the running configuration. |
| **vlan dot1q tag native** | Modifies the behavior of a 802.1Q trunked native VLAN ID interface in the running configuration. |

# show vlan all-ports

To display the status of all VLANs and the ports that are configured on them, use the **show vlan all-ports** command.

**show vlan all-ports**

## 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. |

## Examples

This example shows how to display the status of all VLANs and the ports that are configured on them:

```
n1000v# show vlan all-ports

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Po1, Po2, Po12, Veth1, Veth2
                                                Veth3, Veth10, Veth100
2    VLAN0002                         active
100  VLAN0100                         active
101  VLAN0101                         active
102  VLAN0102                         active
103  VLAN0103                         active
104  VLAN0104                         active
105  VLAN0105                         active
106  VLAN0106                         active
107  VLAN0107                         active
108  VLAN0108                         active
109  VLAN0109                         active
115  VLAN0115                         active
260  cp_control                       active
261  cp_packet                        active
n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **show vlan id** | Displays the VLAN configuration |

| Command | Description |
|---|---|
| **show vlan summary** | Displays a summary of VLAN information. |
| **show vlan private-vlan** | Displays the Private VLAN (PVLAN) configuration. |

# show vlan brief

To display only a brief summary of the status for all VLANs, use the **show vlan brief** command.

**show vlan brief**

## 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 display the aging time in the MAC address table:

```
n1000v# show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Po1, Po2, Po12, Veth1, Veth2
                                                Veth3, Veth10, Veth100
2    VLAN0002                         active
100  VLAN0100                         active
101  VLAN0101                         active
102  VLAN0102                         active
103  VLAN0103                         active
104  VLAN0104                         active
105  VLAN0105                         active
106  VLAN0106                         active
107  VLAN0107                         active
108  VLAN0108                         active
109  VLAN0109                         active
115  VLAN0115                         active
260  cp_control                       active
261  cp_packet                        active
n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **show vlan id** | Displays the VLAN configuration |

| Command | Description |
|---|---|
| **show vlan summary** | Displays a summary of VLAN information. |
| **show vlan private-vlan** | Displays the PVLAN configuration. |

# show vlan id

To display the configuration for a specified VLAN, use the **show vlan id** command.

**show vlan id** *vlan-id*

## Syntax Description

| | |
|---|---|
| *vlan-id* | Number identifying an existing VLAN, or range of VLANs, from 1–3967 and 4048–4093. You can specify groups of VLANs or individual VLANs; for example, 1–5, 10 or 2–5, 7–19. |

## 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 display the configuration for VLAN 462:

```
nexus1000v# show vlan id 462

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
462  VLAN0462                         active    Veth3, Veth5

VLAN Type
---- -----
462  enet

Remote SPAN VLAN
----------------
Disabled

Primary  Secondary  Type             Ports
-------  ---------  ---------------  ------------------------------------------
```

## Related Commands

| Command | Description |
|---|---|
| **vlan** | Creates a VLAN and enters the VLAN configuration mode. |

| Command | Description |
|---|---|
| **show vlan private-vlan** | Displays private VLAN information. |
| **show vlan summary** | Displays VLAN summary information. |

# show vlan private-vlan

To display the PVLAN configuration, use the **show vlan private-vlan** command.

**show vlan private-vlan** [**type**]

## Syntax Description

| | |
|---|---|
| **type** | (Optional) Specifies the display of only the PVLAN type information. |

## 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 display the PVLAN configuration:

```
1000v(config)# show vlan private-vlan
Primary  Secondary  Type             Ports
-------  ---------  ---------------  ------------------------------------------
202      303        community        Eth3/2, Veth1

n1000v(config)#
```

## Related Commands

| Command | Description |
|---|---|
| **show vlan id** | Displays the VLAN configuration. |
| **show vlan brief** | Displays only a brief summary of the status for all VLANs. |
| **show vlan summary** | Displays a summary of VLAN information. |

# show vlan summary

To display a summary of VLAN information, use the **show vlan summary** command.

**show vlan summary**

## 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 display the aging time in the MAC address table:

```
n1000v# show vlan summary

Number of existing VLANs           : 15
 Number of existing user VLANs     : 15
 Number of existing extended VLANs : 0


n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **show vlan id** | Displays the VLAN configuration |
| **show vlan brief** | Displays only a brief summary of the status for all VLANs. |
| **show vlan private-vlan** | Displays the PVLAN configuration. |

# show vmware vc extension-key

To display the extension key of the Virtual Supervisor Module (VSM), use the **show vmware vc extension-key** command.

**show vmware vc extension-key**

## 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

The VSM uses the extension key when communicating with the vCenter Server. Each VSM has its own unique extension key, such as Cisco_Nexus_1000V_32943215.

You can also locate the extension key in the .xml file. The extension key registered on the vCenter Server can be found through the Managed Object Browser (MOB).

## Examples

This example shows how to display the extension key of the VSM:

```
n1000v# show vmware vc extension-key
Extension ID: Cisco_Nexus_1000V_1193126422
n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **show vmware vem upgrade status** | Monitors the upgrade of a Virtual Ethernet Module (VEM) to a new software version. |
| **vmware vem upgrade notify** | Notifies the vCenter Server that the software on the VSM has been upgraded. |
| **vmware vem upgrade proceed** | Begins the upgrade of the virtual machine (VM). |
| **vmware vem upgrade complete** | Clears the upgrade status. |

# show vmware vem upgrade status

To monitor the upgrade of the Virtual Ethernet Module (VEM) to a new software version, use the **show vmware vem upgrade status** command.

**show vmware vem upgrade status**

## 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 monitor the upgrade of the VEMs to a new software version:

```
n1000v# show vmware vem upgrade status

Upgrade Status: Upgrade Complete in vCenter
Upgrade Notification Sent Time: Tue Sep  8 17:37:23 2009
Upgrade Status Time(vCenter): Tue Sep  8 17:45:05 2009
Upgrade Start Time: Tue Sep  8 17:42:02 2009
Upgrade End Time(vCenter): Tue Sep  8 17:45:02 2009
Upgrade Error:
n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **vmware vem upgrade notify** | Notifies the vCenter Server that the software on the Virtual Supervisor Module (VSM) has been upgraded. |
| **vmware vem upgrade proceed** | Begins the upgrade of the Virtual Machine (VM). |
| **vmware vem upgrade complete** | Clears the upgrade status. |

# show xml server status

To display information about XML server settings and any active XML server sessions, use the **show xml server status** command.

**show xml server status**

## 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. |

## Examples

This example shows how to display information about XML server settings and any active XML server sessions:

```
n1000v# show xml server status
operational status is enabled
maximum session configured is 8
n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **xml server max-session** | Sets the number of allowed XML server sessions. |
| **xml server terminate session** | Terminates the specified XML server session. |

# T Commands

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

## tacacs+ enable

To enable TACACS+, use the **tacacs+ enable** command. To disable it, use the **no** form of this command.

**tacacs+ enable**

**no tacacs+ enable**

**Syntax Description** This command has no arguments or keywords.

**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 enable TACACS+:

```
n1000v(config)# tacacs+ enable
n1000v(config)#
```

This example shows how to disable TACACS+:

```
n1000v(config)# no tacacs+ enable
n1000v(config)#
```

## Related Commands

| Command | Description |
|---|---|
| **tacacs-server key** | Designates the global key shared between the Cisco Nexus 1000V and the TACACS+ server hosts. |
| **tacacs-server host** | Designates the key shared between the Cisco Nexus 1000V and this specific TACACS+ server host. |
| **show tacacs-server** | Displays the TACACS+ server configuration. |
| **tacacs-server deadtime** | Sets a periodic time interval where a nonreachable (nonresponsive) TACACS+ server is monitored for responsiveness. |
| **test aaa** | Tests for AAA on a TACACS+ or RADIUS server or server group. |

# tacacs-server deadtime

To set a periodic time interval where a nonreachable (nonresponsive) TACACS+ server is monitored for responsiveness, use the **tacacs-server deadtime** command. To disable the monitoring of the nonresponsive TACACS+ server, use the **no** form of this command.

**tacacs-server deadtime** *minutes*

**no tacacs-server deadtime** *minutes*

## Syntax Description

| | |
|---|---|
| *time* | Specifies the time interval in minutes. The range is from 1 to 1440. |

## 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

Setting the time interval to zero disables the timer. If the dead-time interval for an individual TACACS+ server is greater than zero (0), that value takes precedence over the value set for the server group.

When the dead-time interval is 0 minutes, TACACS+ server monitoring is not performed unless the TACACS+ server is part of a server group and the dead-time interval for the group is greater than 0 minutes.

In global configuration mode, you must first enable the TACACS+ feature, using the **tacacs+ enable** command, before you can use any of the other TACACS+ commands to configure the feature.

## Examples

This example shows how to configure the dead-time interval and enable periodic monitoring:

```
n1000v# config terminal
n1000v(config)# tacacs-server deadtime 10
```

This example shows how to revert to the default dead-time interval and disable periodic monitoring:

```
n1000v# config terminal
n1000v(config)# no tacacs-server deadtime 10
```

## Related Commands

| Command | Description |
|---|---|
| **deadtime** | Sets a dead-time interval for monitoring a nonresponsive TACACS+ server. |
| **show tacacs-server** | Displays TACACS+ server information. |
| **tacacs+ enable** | Enables TACACS+. |
| **tacacs-server key** | Designates the global key shared between the Cisco Nexus 1000V and the TACACS+ server hosts. |
| **tacacs-server host** | Designates the key shared between the Cisco Nexus 1000V and this specific TACACS+ server host. |
| **test aaa** | Tests for AAA on a TACACS+ or RADIUS server or server group. |

# tacacs-server directed-request

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

**tacacs-server directed-request**

**no tacacs-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 must enable TACACS+ with the **tacacs+ enable** command before you can configure TACACS+.

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

**Note** If you enable the directed-request option, the NX-OS device uses only the RADIUS method for authentication and not the default local method.

## Examples

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

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

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

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

## Related Commands

| Command | Description |
|---|---|
| **show tacacs-server directed request** | Displays a directed request TACACS+ server configuration. |
| **tacacs-server key** | Designates the global key shared between the Cisco Nexus 1000V and the TACACS+ server hosts. |
| **tacacs-server host** | Designates the key shared between the Cisco Nexus 1000V and this specific TACACS+ server host. |
| **tacacs-server deadtime** | Sets a periodic time interval where a nonreachable (nonresponsive) TACACS+ server is monitored for responsiveness. |
| **tacacs+ enable** | Enables TACACS+. |
| **test aaa** | Tests for AAA on a TACACS+ or RADIUS server or server group. |

# tacacs-server host

To configure TACACS+ server host parameters, use the **tacacs-server host** command in configuration mode. To revert to the defaults, use the **no** form of this command.

**tacacs-server host** {*hostname* | *ipv4-address* | *ipv6-address*}
[**key** [**0** | **7**] *shared-secret*] [**port** *port-number*]
[**test** {**idle-time** *time* | **password** *password* | **username** *name*}]
[**timeout** *seconds*]

**no tacacs-server host** {*hostname* | *ipv4-address* | *ipv6-address*}
[**key** [**0** | **7**] *shared-secret*] [**port** *port-number*]
[**test** {**idle-time** *time* | **password** *password* | **username** *name*}]
[**timeout** *seconds*]

## Syntax Description

| | |
|---|---|
| *hostname* | TACACS+ server Domain Name Server (DNS) name. The name is alphanumeric, case sensitive, and has a maximum of 256 characters. |
| *ipv4-address* | TACACS+ server IPv4 address in the *A.B.C.D* format. |
| *ipv6-address* | TACACS+ server IPv6 address in the *X*:*X*:*X*::*X* format. |
| **key** | (Optional) Configures the TACACS+ server's shared secret key. |
| **0** | (Optional) Configures a preshared key specified in clear text (indicated by 0) to authenticate communication between the TACACS+ 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 TACACS+ client and server. |
| *shared-secret* | Preshared key to authenticate communication between the TACACS+ client and server. The preshared key is alphanumeric, case sensitive, and has a maximum of 63 characters. |
| **port** *port-number* | (Optional) Configures a TACACS+ server port for authentication. The range is from 1 to 65535. |
| **test** | (Optional) Configures parameters to send test packets to the TACACS+ server. |
| **idle-time** *time* | (Optional) Specifies the time interval (in minutes) for monitoring the server. The time range is 1 to 1440 minutes. |
| **password** *password* | (Optional) Specifies a user password in the test packets. The password is alphanumeric, case sensitive, and has a maximum of 32 characters. |
| **username** *name* | (Optional) Specifies a user name in the test packets. The username is alphanumeric, case sensitive, and has a maximum of 32 characters. |
| **timeout** *seconds* | (Optional) Configures a TACACS+ server timeout period (in seconds) between retransmissions to the TACACS+ server. The range is from 1 to 60 seconds. |

## Defaults

| Parameter | Default |
|---|---|
| Idle-time | disabled |
| Server monitoring | disabled |
| Timeout | 1 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

You must enable TACACS+ with the **tacacs+ enable** command before you can configure TACACS+.

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

## Examples

This example shows how to configure TACACS+ server host parameters:

```
n1000v# config terminal
n1000v(config)# tacacs-server host 10.10.2.3 key HostKey
n1000v(config)# tacacs-server host tacacs2 key 0 abcd
n1000v(config)# tacacs-server host tacacs3 key 7 1234
n1000v(config)# tacacs-server host 10.10.2.3 test idle-time 10
n1000v(config)# tacacs-server host 10.10.2.3 test username tester
n1000v(config)# tacacs-server host 10.10.2.3 test password 2B9ka5
```

## Related Commands

| Command | Description |
|---|---|
| **show tacacs-server** | Displays TACACS+ server information. |
| **tacacs-server key** | Designates the global key shared between the Cisco Nexus 1000V and the TACACS+ server hosts. |
| **tacacs-server deadtime** | Sets a periodic time interval where a nonreachable (nonresponsive) TACACS+ server is monitored for responsiveness. |
| **tacacs+ enable** | Enables TACACS+. |
| **test aaa** | Tests for AAA on a TACACS+ or RADIUS server or server group. |

# tacacs-server key

To configure a global TACACS+ shared secret key, use the **tacacs-server key** command. To removed a configured shared secret, use the **no** form of this command.

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

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

## Syntax Description

| | |
|---|---|
| **0** | (Optional) Configures a preshared key specified in clear text to authenticate communication between the TACACS+ client and server. This is the default. |
| **7** | (Optional) Configures a preshared key specified in encrypted text to authenticate communication between the TACACS+ client and server. |
| *shared-secret* | Preshared key to authenticate communication between the TACACS+ client and server. The preshared key is alphanumeric, case sensitive, and has a maximum of 63 characters. |

## Defaults

None

## 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 TACACS+ preshared key to authenticate the device on the TACACS+ 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 TACACS+ server configurations on the device. You can override this global key assignment by using the **key** keyword in the **tacacs-server host** command.

You must enable TACACS+ with the **tacacs+ enable** command before you can configure TACACS+.

## Examples

The following example shows how to configure TACACS+ server shared keys:

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

## Related Commands

| Command | Description |
|---|---|
| **show tacacs-server** | Displays TACACS+ server information. |
| **tacacs-server deadtime** | Sets a periodic time interval where a nonreachable (nonresponsive) TACACS+ server is monitored for responsiveness. |
| **tacacs-server host** | Designates the key shared between the Cisco Nexus 1000V and this specific TACACS+ server host. |
| **tacacs+ enable** | Enables TACACS+. |
| **test aaa** | Tests for AAA on a TACACS+ or RADIUS server or server group. |

# tacacs-server timeout

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

**tacacs-server timeout** *seconds*

**no tacacs-server timeout** *seconds*

## Syntax Description

| | |
|---|---|
| *seconds* | Seconds between retransmissions to the TACACS+ 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. |

## Usage Guidelines

You must enable TACACS+ with the **tacacs+ enable** command before you can configure TACACS+.

## Examples

This example shows how to configure the TACACS+ server timeout value:

```
n1000v# config terminal
n1000v(config)# tacacs-server timeout 3
```

This example shows how to revert to the default TACACS+ server timeout value:

```
n1000v# config terminal
n1000v(config)# no tacacs-server timeout 3
```

## Related Commands

| Command | Description |
|---|---|
| **show tacacs-server** | Displays TACACS+ server information. |
| **tacacs+ enable** | Enables TACACS+. |
| **tacacs-server key** | Designates the global key shared between the Cisco Nexus 1000V and the TACACS+ server hosts. |
| **tacacs-server host** | Designates the key shared between the Cisco Nexus 1000V and this specific TACACS+ server host. |

| Command | Description |
|---|---|
| **tacacs-server deadtime** | Sets a periodic time interval where a nonreachable (nonresponsive) TACACS+ server is monitored for responsiveness. |
| **test aaa** | Tests for AAA on a TACACS+ or RADIUS server or server group. |

# tail

To display the last lines of a file, use the **tail** command.

**tail** [*filesystem*:[*//module/*]][*directory/*]*filename lines*]

## 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/* | (Optional) Name of a directory. The name is case sensitive. |
| *filename* | Name of the command file. The name is case sensitive. |
| *lines* | (Optional) Number of lines to display. The range is from 0 to 80. |

## Defaults

10 lines

## 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 display the last 10 lines of a file:

```
n1000v# tail bootflash:startup.cfg
ip arp inspection filter marp vlan 9
ip dhcp snooping vlan 13
ip arp inspection vlan 13
ip dhcp snooping
ip arp inspection validate src-mac dst-mac ip
ip source binding 10.3.2.2 0f00.60b3.2333 vlan 13 interface Ethernet2/46
ip source binding 10.2.2.2 0060.3454.4555 vlan 100 interface Ethernet2/10
logging level dhcp_snoop 6
logging level eth_port_channel 6
```

This example shows how to display the last 20 lines of a file:

```
n1000v# tail bootflash:startup.cfg 20
area 99 virtual-link 1.2.3.4
router rip Enterprise
router rip foo
  address-family ipv4 unicast
router bgp 33.33
event manager applet sdtest
monitor session 1
monitor session 2
```

```
ip dhcp snooping vlan 1
ip arp inspection vlan 1
ip arp inspection filter marp vlan 9
ip dhcp snooping vlan 13
ip arp inspection vlan 13
ip dhcp snooping
ip arp inspection validate src-mac dst-mac ip
ip source binding 10.3.2.2 0f00.60b3.2333 vlan 13 interface Ethernet2/46
ip source binding 10.2.2.2 0060.3454.4555 vlan 100 interface Ethernet2/10
logging level dhcp_snoop 6
logging level eth_port_channel 6
```

## Related Commands

| Command | Description |
|---|---|
| **cd** | Changes the current working directory. |
| **copy** | Copies files. |
| **dir** | Displays the directory contents. |
| **pwd** | Displays the name of the current working directory. |

# telnet

To create a Telnet session, use the **telnet** command.

**telnet** {*ipv4-address* | *hostname*} [*port-number*] [**vrf** *vrf-name*]

## Syntax Description

| | |
|---|---|
| *ipv4-address* | IPv4 address of the remote device. |
| *hostname* | Hostname of the remote device. The name is alphanumeric, case sensitive, and has a maximum of 64 characters. |
| *port-number* | (Optional) Port number for the Telnet session. The range is from 1 to 65535. |
| **vrf** *vrf-name* | (Optional) Specifies the virtual routing and forwarding (VRF) name to use for the Telnet session. The name is case sensitive. |

## Defaults

Port 23

Default VRF

## Command Modes

Any

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

To use this command, you must enable the Telnet server using the **telnet server enable** command.

## Examples

This example shows how to start a Telnet session using an IPv4 address:

```
n1000v# telnet 10.10.1.1 vrf management
```

## Related Commands

| Command | Description |
|---|---|
| **clear line** | Clears Telnet sessions. |
| **telnet server enable** | Enables the Telnet server. |

# telnet server enable

To enable the Telnet server, use the **telnet server enable** command. To disable the Telnet server, use the **no** form of this command.

**telnet server enable**

**no telnet server enable**

## Syntax Description

This command has no arguments or keywords.

## Defaults

Enabled

## 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 enable the Telnet server:

```
n1000v# config t
n1000v(config)# telnet server enable
```

This example shows how to disable the Telnet server:

```
n1000v# config t
n1000v(config)# no telnet server enable
XML interface to system may become unavailable since ssh is disabled
```

## Related Commands

| Command | Description |
|---|---|
| **show telnet server** | Displays the Telnet server configuration. |
| **telnet** | Creates a Telnet session. |

# template data timeout

To designate a timeout period for resending NetFlow template data, use the **template data timeout** command. To remove the timeout period, use the **no** form of this command.

**template data timeout** *time*

**no template data timeout**

## Syntax Description

| | |
|---|---|
| *time* | A time period between 1 and 86400 seconds. |

## Defaults

None

## Command Modes

Netflow flow exporter version 9 configuration (config-flow-exporter-version-9)

## SupportedUserRoles

network-admin

## Command History

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

## Examples

This example shows how to configure a 3600-second timeout period for resending NetFlow flow exporter template data:

```
n1000v# config t
n1000v(config)# flow exporter ExportTest
n1000v(config-flow-exporter)# version 9
n1000v(config-flow-exporter-version-9)# template data timeout 3600
```

This example shows how to remove the timeout period for resending NetFlow flow exporter template data:

```
n1000v# config t
n1000v(config)# flow exporter ExportTest
n1000v(config-flow-exporter)# version 9
n1000v(config-flow-exporter-version-9)# no template data timeout
n1000v(config-flow-exporter)#
```

## Related Commands

| Command | Description |
|---|---|
| **flow exporter** | Creates a Flexible NetFlow flow exporter. |
| **flow record** | Creates a Flexible NetFlow flow record. |
| **flow monitor** | Creates a Flexible NetFlow flow monitor. |
| **show flow exporter** | Displays information about the NetFlow flow exporter. |
| **show flow record** | Displays information about NetFlow flow records. |
| **show flow monitor** | Displays information about the NetFlow flow monitor. |
| **version 9** | Designates NetFlow export version 9 in the NetFlow exporter. |

# terminal event-manager bypass

To bypass the CLI event manager, use the **terminal event-manager bypass** command.

**terminal event-manager bypass**

## Syntax Description

This command has no arguments or keywords.

## Defaults

Event manager is enabled.

## Command Modes

Any

## SupportedUserRoles

network-admin
network-operator

## CommandHistory

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

## Examples

This example shows how to disable the CLI event manager:

```
n1000v# terminal event-manager bypass
n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **show terminal** | Displays terminal configuration. |

# terminal length

To set the number of lines that appear on the screen, use the **terminal length** command.

**terminal length** *number*

## Syntax Description

| | |
|---|---|
| *number* | Number of lines. The range of valid values is 0 to 511. |

## Defaults

28 lines

## Command Modes

Any

## SupportedUserRoles

network-admin
network-operator

## Command History

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

## Usage Guidelines

Set *number* to 0 to disable pausing.

## Examples

This example shows how to set the number of lines that appear on the screen:

```
n1000v# terminal length 60
n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **show terminal** | Displays the terminal configuration. |

# terminal monitor

To enable logging for Telnet or Secure Shell (SSH), use the **terminal monitor** command.

**terminal monitor**

## 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. |

## Examples

This example shows how to enable logging for Telnet or SSH:

```
n1000v# terminal monitor
n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **show terminal** | Displays the terminal configuration. |
| **terminal length** | Sets the number of lines that appear on the screen. |
| **terminal width** | Sets the terminal width. |
| **terminal type** | Specifies the terminal type. |
| **terminal session-timeout** | Sets the session timeout. |

# terminal session-timeout

To set session timeout, use the **terminal session-timeout** command.

**terminal session-timeout** *time*

## Syntax Description

| | |
|---|---|
| *time* | Timeout time, in seconds. The range of valid values is 0 to 525600. |

## 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

Set *time* to 0 to disable timeout.

## Examples

This example shows how to set session timeout:

```
n1000v# terminal session-timeout 100
n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **show terminal** | Displays the terminal configuration. |

# terminal terminal-type

To specify the terminal type, use the **terminal terminal-type** command.

**terminal terminal-type** *type*

## Syntax Description

| | |
|---|---|
| *type* | Terminal type. |

## 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 specify the terminal type:

```
n1000v# terminal terminal-type vt100
n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **show terminal** | Displays the terminal configuration. |

# terminal tree-update

To update the main parse tree, use the **terminal tree-update** command.

**terminal tree-update**

## 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 update the main parse tree:

```
n1000v# terminal tree-update
n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **show terminal** | Displays the terminal configuration. |

# terminal width

To set terminal width, use the **terminal width** command.

**terminal width** *number*

| Syntax Description | | |
|---|---|---|
| | *number* | Number of characters on a single line. The range of valid values is 24 to 511. |

**Defaults**

102 columns

**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 set terminal width:

```
n1000v# terminal width 60
n1000v#
```

**Related Commands**

| Command | Description |
|---|---|
| **show terminal** | Displays the terminal configuration. |

# test aaa

To test for AAA on a TACACS+ or RADIUS server or server group, use the **test aaa** command.

**test aaa** {**group** *group-name user-name password* | **server radius** *address* {*user-name password* | **vrf** *vrf-name user-name password*]}}

## Syntax Description

| | |
|---|---|
| **group** | Specifies an AAA server group. |
| *group-name* | AAA server group name. The range of valid values is 1 to 32. |
| *user-name* | User name. The range of valid values is 1 to 32. |
| *password* | User password. The range of valid values is 1 to 32. |
| **server** | Specifies an AAA server. |
| **radius** | Specifies a RADIUS server. |
| *address* | IP address or DNS name. |
| **vrf** | Specifies a virtual route. |
| *vrf-name* | Virtual route.name. |

## 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 test for AAA on RADIUS server:

```
n1000v# test aaa server radius ts1 vrf route1 user1 9w8e7r
n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **show aaa** | Displays AAA information. |
| **aaa group server radius** | Creates a RADIUS server group. |
| **aaa group server tacacs+** | Creates a TACACS+ server group. |

| Command | Description |
|---|---|
| **aaa authentication login default** | Configures the default AAA authentication methods. |
| **aaa authentication login error-enable** | Configure an AAA authentication failure message to display on the console. |
| **aaa authentication login mschap** | Enables Microsoft Challenge Handshake Authentication Protocol (MSCHAP) authentication at login. |
| **show aaa authentication** | Displays AAA authentication information. |
| **show aaa group** | Displays the AAA server groups. |
| **radius-server host** | Configures RADIUS servers. |
| **tacacs-server host** | Configures TACACS+ servers. |
| **tacacs+ enable** | Enables the TACACS+ feature. |

# traceroute

To discover the routes that packets take when traveling to an IPv4 address, use the **traceroute** command.

**traceroute** {*dest-ipv4-addr* | *hostname*} [**vrf** *vrf-name*] [**show-mpls-hops**] [**source** *src-ipv4-addr*]

## Syntax Description

| | |
|---|---|
| *dest-ipv4-addr* | IPv4 address of the destination device. The format is *A.B.C.D*. |
| *hostname* | Name of the destination device. The name is case sensitive. |
| **vrf** *vrf-name* | (Optional) Specifies the virtual routing and forwarding (VRF) to use. The name is case sensitive. |
| **show-mpls-hops** | (Optional) Displays the Multiprotocol Label Switching (MPLS) hops. |
| **source** *src-ipv4-addr* | (Optional) Specifies a source IPv4 address. The format is *A.B.C.D*. |

## Defaults

Uses the default VRF.
Does not show the MPLS hops.
Uses the management IPv4 address for the source address.

## Command Modes

Any

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

To use IPv6 addressing for discovering the route to a device, use the **traceroute6** command.

## Examples

This example shows how to discover a route to a device:

```
n1000v# traceroute 172.28.255.18 vrf management
traceroute to 172.28.255.18 (172.28.255.18), 30 hops max, 40 byte packets
 1  172.28.230.1 (172.28.230.1)  0.746 ms  0.595 ms  0.479 ms
 2  172.24.114.213 (172.24.114.213)  0.592 ms  0.51 ms  0.486 ms
 3  172.20.147.50 (172.20.147.50)  0.701 ms  0.58 ms  0.486 ms
 4  172.28.255.18 (172.28.255.18)  0.495 ms  0.43 ms  0.482 ms
```

## Related Commands

| Command | Description |
|---|---|
| **traceroute6** | Discovers the route to a device using IPv6 addressing. |

# transport udp (NetFlow)

To add a destination UDP port from the NetFlow exporter to the collector, use the **transport udp** command. To remove the port, use the **no** form of this command.

**transport udp** *portnumber*

**no transport udp**

| | |
|---|---|
| *portnumber* | Destination UDP number from 1 to 65535. |

**Command History**

**Defaults**

None

**Command Modes**

Netflow flow exporter configuration (**config-flow-exporter**)

**SupportedUserRoles**

network-admin

**Command History**

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

**Usage Guidelines**

Avoid using well-known ports 1-1024 when possible.

**Examples**

This example shows how to add UDP 200 to the flow exporter:

```
n1000v(config)# flow exporter ExportTest
n1000v(config-flow-exporter)# transport udp 200
```

This example shows how to remove UDP 200 from the flow exporter:

```
n1000v(config)# flow exporter ExportTest
n1000v(config-flow-exporter)# no transport udp 200
```

**Related Commands**

| Command | Description |
|---|---|
| **flow exporter** | Creates a Flexible NetFlow flow exporter. |
| **flow record** | Creates a Flexible NetFlow flow record. |
| **flow monitor** | Creates a Flexible NetFlow flow monitor. |
| **show flow exporter** | Displays information about the NetFlow flow exporter. |
| **show flow record** | Displays information about NetFlow flow records. |
| **show flow monitor** | Displays information about the NetFlow flow monitor. |

# U Commands

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

## use-vrf

To specify the virtual routing and forwarding instance (VRF) to use to contact this server group, use the **use-vrf** command.

**use-vrf** *vrf-name*

| Syntax Description | | |
|---|---|---|
| | *vrf-name* | Name of the VRF to use to contact this server group. |

**Defaults**

None

**Command Modes**

RADIUS server group configuration submode for the specified group (config-radius)

**SupportedUserRoles**

network-admin
network-operator

**Command History**

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

**Examples**

This example shows how to specify the VRF to use to contact the server group called management:

```
n1000v# configure terminal
n1000v(config)# aaa group server radius fred
n1000v(config-radius)# use-vrf management
n1000v(config-radius)#
```

## Related Commands

| Command | Description |
|---|---|
| **aaa group server tacacs+** | Creates a TACACS+ server group with the specified name and puts you into the TACACS+ configuration mode for that group. |
| **aaa group server radius** | Creates a RADIUS server group and enters the RADIUS server group configuration submode for that group. |
| **server** | Configures the RADIUS server as a member of the RADIUS server group. |
| **deadtime** | Configures the monitoring dead time. |
| **show radius-server groups** | Displays the RADIUS server group configuration. |

# username

To create and configure a user account, use the **username** command. To remove a user account, use the **no** form of this command.

**username** *user-id* [**expire** *date* [**past**] ] [**password** [**0** | **5**] *password*] [**role** *role-name*] [ **sshkey** {**file** *uri* | *key* }]

**no username** *user-id* **[ role** *role-name***]**

## Syntax Description

| | |
|---|---|
| *user-id* | User identifier, a case-sensitive, alphanumeric character string with a maximum length of 28 characters.<br>**Note** The following characters are not permitted in usernames:<br>#<br>@ |
| **expire** *date* | (Optional) The expiration date for the user account in the format: YYYY-MM-DD. |
| **password** | (Optional) Specifies a password for the account. The default is no password. |
| **0** | (Optional) Specifies that the password is in clear text. Clear text passwords are encrypted before they are saved to the running configuration.\ |
| **5** | (Optional) Specifies that the password is in encrypted format. Encrypted passwords are not changed before they are saved to the running configuration. |
| *password* | Password string. The password is alphanumeric, case sensitive, and has a maximum of 64 characters.<br>**Note** Clear text passwords cannot contain dollar signs ($) or spaces anywhere in the password. Also, they cannot include these special characters at the beginning of the password: quotation marks (" or '), vertical bars (\|), or right angle brackets (>). |
| **role** *role-name* | (Optional) Specifies the user role. The *role-name* is case sensitive. |
| **sshkey** | (Optional) Specifies an SSH key for the user account. |
| *key* | SSH public key string. |
| **file** *filename* | Specifies the location of the file that contains the SSH public key string.<br>bootflash: file containing host public key for the user<br>volatile: file containing host public key for the user |

## Defaults

No expiration date, password, or SSH key.

The default role is the network-operator user role.

## Command Modes

Global configuration (config)

**SupportedUserRoles**

network-admin
network-operator

**Command History**

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

**Usage Guidelines**

You cannot delete the default admin user role.

You cannot change the expiration date for the the default admin user role.

You cannot remove the network-admin role for the default admin user role.

In you have enabled password-strength checking, you can only assign strong passwords. The following are the characteristics of a strong password:

- At least eight characters long
- Does not contain many consecutive characters (such as “abcd”)
- Does not contain many repeating characters (such as “aaabbb”)
- Does not contain dictionary words
- Does not contain proper names
- Contains both uppercase and lowercase characters
- Contains numbers

**Caution** If you do not specify a password for the user account, the user might not be able to log in.

**Examples**

This example shows how to create a user account with a password and a user role:

```
n1000v# config t
n1000v(config)# username user1 password Ci5co321 role network-admin
```

This example shows how to configure the SSH key for a user account:

```
n1000v# config t
n1000v(config)# username user1 sshkey file bootflash:key_file
```

**Related Commands**

| Command | Description |
|---|---|
| **password strength-check** | Checks the password security strength. |
| **show user-account** | Displays the user account configuration. |

# username admin password

To change the network admin password in the running configuration, use the **username admin password** command.

**username admin password** [*new-password*]

## Syntax Description

| | |
|---|---|
| *new-password* | (Optional) Password string, which is alphanumeric, case sensitive, and has a maximum of 64 characters. |

## 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 change the network admin password in the running configuration:

```
n1000v# config t
n1000v(config)# username admin password <new-password>
n1000v(config)#
```

## Related Commands

| Command | Description |
|---|---|
| **username** | Creates and configures a user account. |
| **show user-account** | Displays usernames and their roles. |

# V Commands

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

## vem

To configure a Virtual Ethernet Module (VEM), use the **vem** command. To remove a VEM configuration, use the **no** form of this command.

**vem** *module-number* [- *module-number*]

**no vem** *module-number* [- *module-number*]

**Syntax Description**

| | |
|---|---|
| *module-number* | Specifies a module number. The range of valid values is 3 to 66. |

**Defaults**

None

**Command Modes**

Global configuration (config)

**SupportedUserRoles**

network-admin

**Command History**

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

**Usage Guidelines**

Specify a range of VEMs by using a dash. For example, 3-9 or 20-30.

**Examples**

This example shows how to create a VEM and enter the VEM slot configuration mode:

```
n1000v# configure terminal
n1000v(config)# vem 10
```

```
n1000v(config-vem-slot)#
```

This example shows how to remove a VEM:

```
n1000v# configure terminal
n1000v(config)# no vem 10
n1000v(config)#
```

**Related Commands**

| Command | Description |
|---|---|
| **show module vem** | Displays information about the VEM module. |

# version 9

To designate NetFlow export version 9 in the NetFlow exporter, use the **version 9** command. To remove version 9, use the **no** form of this command.

**version 9**

**no version 9**

## Syntax Description

This command has no arguments or keywords.

## Defaults

None

## Command Modes

NetFlow flow exporter configuration (config-flow-exporter)

## SupportedUserRoles

network-admin

## Command History

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

## Examples

This example shows how to configure version 9 for a Netflow flow exporter:

```
n1000v# config t
n1000v(config)# flow exporter ExportTest
n1000v(config-flow-exporter)# version 9
n1000v(config-flow-exporter-version-9)#
```

This example shows how to remove version 9 from the Netflow flow exporter:

```
n1000v# config t
n1000v(config)# flow exporter ExportTest
n1000v(config-flow-exporter)# version 9
n1000v(config-flow-exporter-version-9)# no version 9
n1000v(config-flow-exporter)#
```

## Related Commands

| Command | Description |
|---|---|
| **option exporter-stats timeout** | Specifies a timeout period for resending NetFlow flow exporter data. |
| **option interface-table timeout** | Specifies a timeout period for resending the NetFlow flow exporter interface table. |
| **template data timeout** | Specifies a timeout period for resending NetFlow flow exporter template data. |

| Command | Description |
|---|---|
| **flow exporter** | Creates a Flexible NetFlow flow exporter. |
| **flow record** | Creates a Flexible NetFlow flow record. |
| **flow monitor** | Creates a Flexible NetFlow flow monitor. |
| **show flow exporter** | Displays information about the NetFlow flow exporter. |
| **show flow record** | Displays information about NetFlow flow records. |
| **show flow monitor** | Displays information about the NetFlow flow monitor. |

# virtual-service-domain

To classify and separate traffic for network services, use the **virtual-service-domain** command. To remove a virtual service domain, use the **no** form of this command.

**virtual-service-domain** *vsd-name*

**no virtual-service-domain**

## Syntax Description

| | |
|---|---|
| *vsd-name* | Creates and names a virtual service domain. |

## Defaults

None

## Command Modes

Port profile configuration (config-port-prof)

## SupportedUserRoles

network-admin

## Command History

| Release | Modification |
|---|---|
| 4.0(4)SV1(2) | This command was introduced. |

## Examples

This example shows how to configure a port profile for a VSD:

```
n1000v# config t
n1000v(config)# port-profile vsd1_member
n1000v(config-port-prof)# vmware port-group
n1000v(config-port-prof)# switchvport access vlan 315
n1000v(config-port-prof)# virtual-service-domain vsd1
n1000v(config-port-prof)# no shutdown
n1000v(config-port-prof)# state enabled
```

This example shows how to remove the virtual service domain configuration:

```
n1000v# config t
n1000v(config)# port-profile vsd1_member
n1000v(config-port-prof)# no virtual-service-domain vsd1
```

## Related Commands

| Command | Description |
|---|---|
| **show virtual-service-domain** | Displays a list of the VSDs currently configured in the VSM, including VSD names and port profiles. |

# vlan

To create a VLAN and enter the VLAN configuration mode, use the **vlan** command. To remove a VLAN, use the **no** form of this command.

**vlan** {*id* | **dot1Q tag native**}

**no vlan** {*id* | **dot1Q tag native**}

## Syntax Description

| | |
|---|---|
| *id* | VLAN identification number. The range of valid values is 1 to 4094. |
| **dot1Q tag native** | Specifies an IEEE 802.1Q virtual LAN. |

## Defaults

The default VLAN is VLAN 1.

## Command Modes

Global configuration (config)

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

Specify a VLAN range by using a dash. For example, 1-9 or 20-30.

## Examples

This example shows how to create a VLAN and enter the VLAN configuration mode:

```
n1000v# configure terminal
n1000v(config)# vlan 10
n1000v(config-vlan)#
```

This example shows how to remove a VLAN:

```
n1000v# configure terminal
n1000v(config)# no vlan 10
n1000v(config)#
```

## Related Commands

| Command | Description |
|---|---|
| **show vlan** | Displays VTP VLAN status. |

# vlan policy deny

To enter the VLAN configuration mode and deny all VLAN access for the role, use the **vlan policy deny** command.

To remove the policy restrictions, use the **no** form of this command.

**vlan policy deny**

**no vlan policy deny**

## Syntax Description

This command has no arguments or keywords.

## 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

After executing this command, access to any VLAN must be explicitly defined for this role by using the **permit vlan** command.

## Examples

This example shows how to enter the VLAN configuration mode and deny all VLAN access for the role:

```
n1000v# config t
n1000v(config)# role name network-observer
n1000v(config-role)# vlan policy deny
n1000v(config-role-vlan)#
```

This example shows how to remove policy restrictions:

```
n1000v# config t
n1000v(config)# role name network-observer
n1000v(config-role)# no vlan policy deny
n1000v(config-role-vlan)#
```

## Related Commands

| Command | Description |
|---|---|
| **role name** | Specifies a user role and enters role configuration mode. |

| Command | Description |
|---|---|
| **permit vlan** | Specifies the VLAN that users assigned to this role can access. |
| **show role** | Displays the role configuration. |

# vmware dvs datacenter-name

To create a VMware virtual switch, use the **vmware dvs datacenter-name** command. To remove the virtual switch, use the **no** form of this command.

**vmware dvs datacenter-name** *name*

**no vmware dvs**

## Syntax Description

| | |
|---|---|
| *name* | Switch name. |

## 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. |

## Usage Guidelines

To create a virtual switch, you must be in the SVS connection configuration mode. Use the **svs connection** command to create a connection and enter that mode. The number of SVS connections that can be created is limited to one.

## Examples

This example shows how to create a VMware virtual switch:

```
n1000v# configure terminal
n1000v(config)# svs connect s1
n1000v(config-svs-conn)# vmware dvs datacenter-name dc1
n1000v(config-svs-conn)#
```

This example shows how to remove a VMware virtual switch:

```
n1000v# configure terminal
n1000v(config)# svs connect s1v
n1000v(config-svs-conn)# no vmware dvs datacenter-name dc1
n1000v(config-svs-conn)#
```

## Related Commands

| Command | Description |
|---|---|
| **show svs** | Displays SVS information. |
| **show vmware** | Displays VMware information. |

# vmware max-ports

To create the maximum number of ports for the VMware port profile, use the **vmware max-ports** command. To remove the maximum port configuration, use the **no** form of this command.

**vmware max-ports** *number*

**no vmware max-ports** *number*

## Syntax Description

| | |
|---|---|
| *number* | Specifies the maximum number of ports. The range of valid values is 1 to 1024. |

## Defaults

32 ports

## Command Modes

Port profile configuration (config-port-prof)

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

To specify the maximum number of VMware ports to configure, you must be in port profile configuration mode.

## Examples

This example shows how to set the maximum number of VMware ports in a port profile:

```
n1000v# configure terminal
n1000v(config)# port-profile testprofile
n1000v(config-port-prof)# vmware max-ports 100
n1000v(config-port-prof)#
```

This example shows how to remove the maximum VMware ports configuration:

```
n1000v# configure terminal
n1000v(config)# port-profile testprofile
n1000v(config-port-prof)# no vmware max-ports 100
n1000v(config-port-prof)#
```

## Related Commands

| Command | Description |
|---|---|
| **show port-profile name** | Displays configuration information about a particular port-profile. |

# vmware port-group

To create a VMware port group, use the **vmware port-group** command. To remove the VMware port group, use the **no** form of this command.

**vmware port-group** *name*

**no vmware port-group** *name*

## Syntax Description

| | |
|---|---|
| *name* | Specifies the name of the VMware port group. |

## Defaults

None

## Command Modes

Port profile configuration (config-port-prof)

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

To create the VMware port group, you must be in port profile configuration mode.

## Examples

This example shows how to create a VMware port group:

```
n1000v# configure terminal
n1000v(config)# port-profile testprofile
n1000v(config-port-prof)# vmware port-group testgroup
n1000v(config-port-prof)#
```

This example shows how to remove the VMware port group:

```
n1000v# configure terminal
n1000v(config)# port-profile testprofile
n1000v(config-port-prof)# no vmware port-group testgoup
n1000v(config-port-prof)#
```

## Related Commands

| Command | Description |
|---|---|
| **show port-profile name** | Displays configuration information about a particular port-profile. |

# vmware vc extension-key

To create an extension key, use the **vmware vc extension-key** command.

**vmware vc extension-key** *key*

## Syntax Description

| | |
|---|---|
| *key* | Extension key number. The range of valid values is 1 to 80. |

## Defaults

The key does not exist.

## Command Modes

Global configuration (config)

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

An extension key is used to connect to an instance of Virtual Center.

## Examples

This example shows how to create an extension key:

```
n1000v# configure terminal
n1000v(config)# vmware vc extension-key 10
n1000v(config)#
```

## Related Commands

| Command | Description |
|---|---|
| **show vmware vc extension-key** | Displays extension key information. |

# vmware vem upgrade complete

To clear the upgrade status, use the **vmware vem upgrade complete** command.

**vmware vem upgrade complete**

## 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

Once you have cleared the upgrade status, you cannot repeat this procedure.

## Examples

This example shows how to clear the upgrade status:

```
n1000v# vmware vem upgrade complete
n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **show vmware vem upgrade status** | Monitors the upgrade of the Virtual Ethernet Module (VEM) to a new software version. |
| **vmware vem upgrade notify** | Notifies the vCenter Server that the software on the Virtual Supervisor Module (VSM) has been upgraded. |
| **vmware vem upgrade proceed** | Begins the upgrade of the virtual machine (VM). |

# vmware vem upgrade notify

To notify the vCenter Server that the software on the Virtual Supervisor Module (VSM) has been upgraded, and that a Virtual Ethernet Module (VEM) upgrade is available, use the **vmware vem upgrade notify** command.

**vmware vem upgrade notify**

## 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 notify the vCenter Server that the software on the Virtual Supervisor Module (VSM) has been upgraded, and that a VEM upgrade is available:

```
n1000v# vmware vem upgrade notify
n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **show vmware vem upgrade status** | Monitors the upgrade of the VEMs to a new software version. |
| **vmware vem upgrade proceed** | Begins the upgrade of the virtual machine (VM). |
| **vmware vem upgrade complete** | Clears the upgrade status. |

# vmware vem upgrade proceed

To begin the upgrade of the virtual machine (VM), use the **vmware vem upgrade proceed** command.

**vmware vem upgrade proceed**

## 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 begin the upgrade of the VM:

```
n1000v# vmware vem upgrade proceed
n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **show vmware vem upgrade status** | Monitors the upgrade of the Virtual Ethernet Module (VEM) to a new software version. |
| **vmware vem upgrade notify** | Notifies the vCenter Server that the software on the Virtual Supervisor Module (VSM) has been upgraded. |
| **vmware vem upgrade complete** | Clears the upgrade status. |

# W Commands

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

## where

To display your current context in the command-line interface (CLI), use the **where** command.

**where** [**detail**]

| Syntax Description | | |
|---|---|---|
| | **detail** | (Optional) Displays detailed context information. |

**Defaults**

Displays summary context information.

**Command Modes**

Any

**SupportedUserRoles**

network-admin

**Command History**

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

**Usage Guidelines**

This command helps you track where you are in the CLI and how you got there.

**Examples**

This example shows how to display summary context information:

```
n1000v(config-if)# where
  ?conf; interface Ethernet2/3      admin@switch%default
```

This example shows how to display detailed context information:

```
n1000v(config-if)# where detail
  ?conf; interface Ethernet2/3      admin@switch%default
  mode:                conf
                         interface Ethernet2/3
  username:            admin
  routing-context vrf: default
```

# write erase

To erase configurations in persistent memory areas, use the **write erase** command.

**write erase** [**boot** | **debug**]

## Syntax Description

| | |
|---|---|
| **boot** | (Optional) Erases only the boot variable and mgmt0 interface configuration. |
| **debug** | (Optional) Erases only the debug configuration. |

## Defaults

Erases all configuration in persistent memory except for the boot variable, mgmt0 interface, and debug configuration.

## Command Modes

Any

## SupportedUserRoles

network-admin

## Command History

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

## Usage Guidelines

You can use this command to erase the startup configuration in the persistent memory when information is corrupted or otherwise unusable. Erasing the startup configuration returns the device to its initial state, except for the boot variable, mgmt0 interface, and debug configurations. You have to explicitly erase those configurations with the **boot** and **debug** options.

## Examples

This example shows how to erase the startup configuration:

```
n1000v(config)# write erase
Warning: This command will erase the startup-configuration.
Do you wish to proceed anyway? (y/n)  [n] y
```

This example shows how to erase the boot variable and mgmt0 interface configuration in the persistent memory:

```
n1000v(config)# write erase boot
```

This example shows how to erase the debug configuration in the persistent memory:

```
n1000v(config)# write erase debug
```

**Related Commands**

| Command | Description |
|---|---|
| **copy running-config startup-config** | Copies the running configuration to the startup configuration. |
| **show running-config** | Displays the startup configuration. |

# X Commands

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

## xml server max-session

To set the number of allowed XML server sessions, use the **xml server max-session** command.

**xml server max-session** *sessions*

**Syntax Description**

| | |
|---|---|
| *sessions* | Maximum number of XML sessions permitted at one time. The range is 1–8. |

**Defaults**

The default maximum number of sessions is eight.

**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 set the number of allowed XML server sessions to 6:

```
n1000v# config t
n1000v# xml server max-session 6
n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **show xml server status** | Displays information about XML server settings and any active XML server sessions. |
| **xml server terminate session** | Displays information about XML server settings and any active XML server sessions. |
| **xml server timeout** | Sets the number of seconds after which an inactive XML server session is terminated. |

# xml server terminate session

To terminate the specified XML server session, use the **xml server terminate session** command.

**xml server terminate session** *session-number*

| Syntax Description | | |
|---|---|---|
| | *session-number* | Identifier for an existing XML server session. The range is 0–214748364. |

**Defaults**

None

**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 terminate the XML server session 8665:

```
n1000v# xml server terminate 8665
n1000v#
```

**Related Commands**

| Command | Description |
|---|---|
| **show xml server status** | Displays information about XML server settings and any active XML server sessions. |
| **xml server max-session** | Sets the number of allowed XML server sessions. |
| **xml server timeout** | Sets the number of seconds after which an inactive XML server session is terminated. |

# xml server timeout

To set the number of seconds after which an inactive XML server session is terminated, use the **xml server timeout** command.

**xml server timeout** *seconds*

## Syntax Description

| | |
|---|---|
| *seconds* | Maximum time that the XML server can remain inactive before session termination. The range is 0–1200 seconds. |

## 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 set the XML server timeout to 600 seconds:

```
n1000v# config t
n1000v# xml server timeout 600
n1000v#
```

## Related Commands

| Command | Description |
|---|---|
| **show xml server status** | Displays information about XML server settings and any active XML server sessions. |
| **xml server max-session** | Sets the number of allowed XML server sessions. |
| **xml server terminate session** | Displays information about XML server settings and any active XML server sessions. |