

Device Manager, Release 4.1.1

Table of Contents

New and changed information . . . 1
Physical . . . 2
- Inventory . . . 2
- Modules - Status and Config . . . 2
- Power Supplies . . . 3
- Temperature Sensors . . . 4
- Fan . . . 4
- Switches . . . 4
- ISLs . . . 5
- NP Link . . . 6
- ISLs Statistics . . . 6
- Hosts . . . 7
- Enclosures . . . 7
- Device Manager - Preferences . . . 8

Interface . . . 9
- Virtual Interface Groups . . . 11
- Virtual FC Interfaces . . . 11
- Ethernet Interfaces . . . 12
- Virtual FC Ethernet . . . 13
- Quick Configuration Tool . . . 13
- Ethernet Interface . . . 14
- Ethernet Interfaces iSCSI . . . 15
- Ethernet Interfaces iSCSI TCP . . . 15
- Ethernet Interfaces VLAN . . . 16
- Ethernet VLAN . . . 17
- FC Interface Monitor Traffic . . . 17
- FC Interface Monitor Protocol . . . 17
- FC Interface Monitor Discards . . . 18
- FC Interface Monitor Link Errors . . . 18
- FC Interface Monitor Frame Errors . . . 19
- FC Interface Monitor Class 2 Traffic . . . 19
- FC Interface Monitor Class 2 Errors . . . 20
- FC Interface Monitor FICON . . . 20
- Check Oversubscription . . . 20
- Virtual FC Interface Monitor Traffic . . . 21
- Virtual FC Interface Monitor Discards . . . 21
- Virtual FC Interface Monitor Errors . . . 21
- Ethernet Interface Dot3Stats . . . 21
- Interface Monitor . . . 22
- Ethernet PortChannels . . . 23
- Ethernet Interface Monitor iSCSI Connections . . . 23

Ethernet Interface Monitor TCP . . . 23
FCIP Monitor . . . 24
Monitor SVC Interface . . . 24
Monitor SVC NPorts . . . 25
Monitor SVC Session FCP . . . 25
Monitor SVC Session Other . . . 26
FCIP Interfaces . . . 26
System Timeout . . . 27
Interface License . . . 27
General . . . 27
FC Interfaces General . . . 28
FC Interfaces Rx BB Credit . . . 30
FC Interfaces Other . . . 31
FC Interfaces FLOGI . . . 32
FC Interfaces ELP . . . 32
FC Interfaces Trunk Config . . . 34
FCIP Interfaces Trunk Failures . . . 34
FC Interfaces IP . . . 34
FC Interfaces Physical . . . 35
FC Interfaces Capability . . . 35
FC Interfaces FICON Peer . . . 36
Interfaces NPorts (SVC) . . . 36
Interfaces Sessions . . . 37
IP Statistics TCP . . . 37
Port Channels Ethernet Interfaces . . . 37
Port Channels FC Interfaces . . . 38
Port Channels General . . . 38
FlexAttach Global . . . 39
FlexAttach Virtual PWWN . . . 39
FlexAttach Physical to Virtual WWNs . . . 40
FIPS . . . 40
FCIP FICON Configuration . . . 40
Port Channels AutoCreate . . . 41
SPAN Sessions . . . 41
Span Global . . . 41
SPAN Source Interfaces . . . 41
Port Tracking Dependencies . . . 41
Port Tracking Force Shut . . . 42
Port Guard . . . 42
Bandwidth Reservation: 48-Port 96-Gbps Fibre Channel module . . . 42
Bandwidth Reservation: 48-Port 48-Gbps Fibre Channel module . . . 43
Bandwidth Reservation: 24-Port 48-Gbps Fibre Channel module . . . 43
Bandwidth Reservation: 48-Port 256-Gbps Fibre Channel module . . . 43

Bandwidth Reservation: 32-Port 256-Gbps Fibre Channel module . . . 44
DS-X9448-768K9 (Luke) Line Card Bandwidth Reservation . . . 45
FC . . . 46
VSAN General . . . 48
VSAN Membership . . . 49
VSAN Interop-4 WWN . . . 49
VSAN Timers . . . 49
VSAN Default Zone Policies . . . 50
IVR Local Topology . . . 50
IVR Fabric ID . . . 50
IVR Default Fabric ID . . . 50
IVR Action . . . 50
IVR RDI VSANs . . . 51
IVR Active Topology . . . 51
IVR Zoneset Status . . . 51
IVR Discrepancies . . . 52
IVR Domains . . . 53
IVR FCID . . . 53
IVR Zoneset Active Zones . . . 53
IVR Zoneset Active Zones Attributes . . . 53
IVR Zoneset Name . . . 53
DPVM Actions . . . 54
DPVM Config Database . . . 54
DPVM Active Database . . . 55
Domain Manager Running . . . 55
Domain Manager Configuration . . . 55
Domain Manager Domains . . . 57
Domain Manager Statistics . . . 57
Domain Manager Interfaces . . . 57
Domain Manager Persistent FcIds . . . 58
Domain Manager Allowed DomainIds . . . 58
Zoneset Active Zones . . . 58
Zoneset Unzoned . . . 59
Zoneset Status . . . 59
Zoneset Policies . . . 59
Zoneset Active Zones Attributes . . . 60
Zoneset Enhanced . . . 60
Zoneset Read Only Violations . . . 61
Zoneset Statistics . . . 61
Zoneset LUN Zoning Statistics . . . 62
Zoneset Members . . . 62
Fabric Config Server Discovery . . . 62
Fabric Config Server Interconnect Elements . . . 63

Fabric Config Server Platforms (Enclosures) . . . 63
Fabric Config Server Fabric Ports . . . 63
FC Routes . . . 64
FDMI HBAs . . . 64
FDMI Ports . . . 64
FDMI Versions . . . 65
Flow Statistics . . . 65
FCC . . . 65
Diagnostics . . . 66
FSPF General . . . 66
FSPF Interfaces . . . 67
FSPF Interface Stats . . . 68
SDV Virtual Devices . . . 68
SDV Real Devices . . . 69
LUN Discover . . . 69
LUN Targets . . . 69
LUNs . . . 70
Device Alias . . . 70
Device Alias Configuration . . . 70
Device Alias Mode . . . 70
Device Alias Discrepancies . . . 70
Name Server General . . . 71
Name Server Advanced . . . 71
Name Server Proxy . . . 72
Name Server Statistics . . . 72
Preferred Path Maps and Routes . . . 72
Preferred Path Maps Active . . . 73
Preferred Path All Match Criteria . . . 73
Preferred Path Active Match Criteria . . . 73
Preferred Path All Sets . . . 74
RSCN Nx Registrations . . . 74
RSCN Multi-PID Support . . . 74
RSCN Event . . . 74
RSCN Statistics . . . 74
Multicast Root . . . 75
QoS Policy Maps . . . 75
QoS Class Maps . . . 75
QoS Match Statements . . . 75
QoS Class Maps by Policy Maps . . . 76
QoS Policy Maps by VSAN . . . 76
QoS DWRR . . . 76
QoS Rate Limit . . . 76
Timers and Policies . . . 76

WWN Manager . . . 77
NPV Traffic Map . . . 78
NPV Load Balance . . . 78
NPV External Interface Usage . . . 78
NP Link . . . 78
FCoE . . . 80
Config . . . 80
VSAN-VLAN Mapping . . . 80
VLAN-VSAN Mapping . . . 80
FCoE Statistics . . . 80
FICON . . . 82
FICON VSANs . . . 82
FICON VSANs Files . . . 83
Global . . . 83
FICON Port Attributes . . . 83
FICON Port Configuration . . . 84
FICON Port Numbers . . . 84
FICON VSANs Director History . . . 85
Fabric Binding Actions . . . 85
Fabric Binding Config Database . . . 86
Fabric Binding Active Database . . . 86
Fabric Binding Database Differences . . . 86
Fabric Binding Violations . . . 86
Fabric Binding Statistics . . . 87
Fabric Binding EFMD Statistics . . . 87
IP Storage . . . 89
FCIP Profiles . . . 89
FCIP Tunnels . . . 90
FCIP Tunnels (Advanced) . . . 91
FCIP Tunnels (FICON TA) . . . 91
FCIP Tunnels Statistics . . . 91
FCIP XRC Statistics . . . 92
iSCSI Connection . . . 92
iSCSI Initiators . . . 93
iSCSI Session Initiators . . . 94
Module Control . . . 94
iSCSI Global . . . 94
iSCSI Session Statistics . . . 94
iSCSI Targets . . . 95
iSCSI iSLB VRRP . . . 95
iSCSI Initiator Access . . . 95
Initiator Specific Target . . . 96
iSCSI Initiator PWWN . . . 96

iSCSI Sessions . . . 96
iSCSI Sessions Detail . . . 97
IP Services . . . 98
IP Routes . . . 98
IP Statistics ICMP . . . 99
IP Statistics IP . . . 99
IP Statistics SNMP . . . 101
IP Statistics UDP . . . 102
mgmt0 Statistics . . . 102
TCP UDP TCP . . . 103
TCP UDP UDP . . . 103
VRRP General . . . 103
VRRP IP Addresses . . . 104
VRRP Statistics . . . 104
CDP General . . . 104
CDP Neighbors . . . 105
iSNS Profiles . . . 105
iSNS Servers . . . 105
iSNS Entities . . . 106
iSNS Cloud Discovery . . . 106
iSNS Clouds . . . 107
iSNS Cloud Interfaces . . . 107
Monitor Dialog Controls . . . 107
iSNS Details iSCSI Nodes . . . 108
iSNS Details Portals . . . 108
Security . . . 110
Security Roles . . . 111
Security Role Rules . . . 111
Feature Group Manager . . . 112
AAA LDAP Servers . . . 112
AAA Server Groups . . . 113
AAA Search Map . . . 113
AAA Applications . . . 113
AAA Defaults . . . 114
AAA General . . . 114
AAA Statistics . . . 115
iSCSI User . . . 117
Common Roles . . . 117
SNMP Security Users . . . 118
SNMP Security Communities . . . 118
Security Users Global . . . 118
FC-SP General/Password . . . 119
FC-SP Interfaces . . . 119

FC-SP Local Passwords . . . 120
FC-SP Remote Passwords . . . 120
FC-SP Statistics . . . 120
FC-SP SA (Security Association) . . . 120
FC-SP ESP Interfaces . . . 120
PKI General . . . 121
PKI RSA Key-Pair . . . 121
PKI Trust Point . . . 122
PKI Trust Point Actions . . . 122
PKI LDAP . . . 123
PKI Certificate Map . . . 123
PKI Certificate Map - Application . . . 123
PKI Trust Point Detail . . . 124
IKE Global . . . 124
IKE Pre-Shared AuthKey . . . 125
IKE Policies . . . 125
IKE Initiator Version . . . 125
IKE Tunnels . . . 126
IPSEC Global . . . 126
IPSEC Transform Set . . . 126
IPSEC CryptoMap Set Entry . . . 127
IPSEC Interfaces . . . 127
IPSEC Tunnels . . . 127
IP ACL Profiles . . . 128
IP ACL Interfaces . . . 128
IP Filter Profiles . . . 128
SSH/Telnet . . . 130
Port Security Actions . . . 130
Port Security Config Database . . . 132
Port Security Active Database . . . 132
Port Security Database Differences . . . 132
Port Security Violations . . . 133
Port Security Statistics . . . 133
IPsec . . . 133
Events . . . 134
Call Home General . . . 134
Call Home Destinations . . . 135
Call Home Email Setup . . . 135
Call Home Alerts . . . 135
Call Home HTTP Proxy Server . . . 136
Call Home SMTP Servers . . . 136
Call Home User Defined Command . . . 136
Delayed Traps . . . 136

Call Home Profiles . . . 137
Event Destinations Addresses . . . 137
Event Destinations Security (Advanced) . . . 137
Event Filters General . . . 138
Event Filters Interfaces . . . 139
Event Filters Control . . . 139
Link Incident History . . . 139
RMON Thresholds Controls . . . 139
RMON Thresholds 64bit Alarms . . . 139
RMON Thresholds 32bit Alarms . . . 140
RMON Thresholds Events . . . 141
RMON Thresholds Log . . . 141
Admin . . . 143
Copy Configuration . . . 144
Flash Files . . . 144
Compact Flash . . . 144
License Features . . . 144
License Manager Keys . . . 145
License Manager Install . . . 145
License Manager Usage . . . 146
Port Licensing . . . 146
Feature Set . . . 147
Feature Control . . . 147
NTP Servers . . . 147
NTP General . . . 148
Running Processes . . . 148
Show Startup/Running Config . . . 148
Show EPLD Version . . . 149
Copy Flash Files . . . 149
Generate TAC Pac File . . . 149
Show Tech Support . . . 150
Show Image Version . . . 150
Show Onboard Log . . . 150
Summary View . . . 150
RLIR ERL . . . 151
Preferred Host . . . 151
Preferred Path . . . 152
Edit iSCSI Advertised Interfaces . . . 152
DNS General . . . 152
DNS Servers . . . 152
Cisco Fabric Services (CFS) Features . . . 152
Cisco Fabric Services (CFS) IP Multicast . . . 154
Cisco Fabric Service (CFS) IP Static Peers . . . 154

Cisco Fabric Services (CFS) Feature by Region . . . 155
Cisco Fabric Services (CFS) All Region . . . 155
Cisco Fabric Services (CFS) Owner . . . 155
Cisco Fabric Services (CFS) Merge . . . 155
Logs . . . 156
SysLog (Since Reboot) . . . 156
SysLog (Severe Events) . . . 156
Accounting Log . . . 156
Switch Logging . . . 157
Syslog Severity Levels . . . 157
Syslog Servers . . . 157
End Devices – Hosts . . . 158
Intelligent Features – Summary . . . 159
Data Mobility Manager – Modules . . . 160
Storage Media Encryption . . . 161
Members . . . 161
Interfaces . . . 161
Hosts . . . 161
SSM Features . . . 162
Summary . . . 162
FCWA . . . 162
SSM . . . 163
MSM . . . 163
SANTap CVT . . . 163
SANTap DVT . . . 164
NASB . . . 164
NASB Target . . . 164
Virtual Initiator . . . 165
DMM Rate . . . 165
FCWA Config Status . . . 165
Statistics Status . . . 165
Statistics I/O Traffic . . . 166
Statistics I/O Traffic Details . . . 166
Statistics SCSI Commands . . . 167
Statistics SCSI Errors . . . 167
Statistics SCSI Sense Errors . . . 167
Compact . . . 168

New and changed information

The following table provides an overview of the significant changes up to this current release. The table does not provide an exhaustive list of all changes or of the new features up to this release.

Release Version	Feature	Description
Nexus Dashboard 4.1.1	Improved navigation and workflow when working with Device Manager	Beginning with Nexus Dashboard 4.1.1, Nexus Dashboard enhanced the navigation and the workflow when working with Device Manager.

Physical

This section includes the physical attributes for the 4.1.1 SAN setup:

- Inventory
- Modules - Status and Config
- Power Supplies
- Temperature Sensors
- Fan
- Switches
- ISLs
- NP Link
- ISLs Statistics
- Hosts
- Enclosures
- Device Manager - Preferences

Inventory

Field	Description
Name	Field Replaceable Unit (FRU) name.
ModelName	Model name identifier.
SerialNumber	Primary and secondary serial numbers.
HardwareRevision	Hardware revision.
SoftwareRevision	The release version of Cisco NX-OS software.
Alias	Alias name as specified by a network manager.
AssetID	User-assigned asset tracking identifier as specified by a network manager.

Modules - Status and Config

Field	Description
Name	Module description.
Module	Module name identifier.
OperStatus	Module's operational state.
Reset	Click to reboot the module.
RateModeOverSubscriptionLimit	Select this option to control the restriction on the oversubscription ratio on modules that support it. By default, the restriction is enabled. If you disable this option, all the interfaces on the module are capable of operating at maximum admin speed, regardless of the available bandwidth.

Field	Description
BandwidthFairnessConfig	Select this option to control bandwidth fairness on modules that support it. By default, bandwidth fairness is enabled.
BandwidthFairnessOper	Shows if bandwidth fairness is enabled or disabled. By default, bandwidth fairness is enabled.
X2 xcvrFrequency Config	Specifies the transceiver frequency of the module. • notApplicable – Select this when the module does not support this configuration. • xcvrFreqX2FC – Select this to set the module's FC transceiver frequency to10 Gigabyte. • xcvrFreqX2Eth – Select this to set the module's Ethernet transceiver frequency to10 Gigabyte.
ResetReasonDescription	Why module was last reset.
Local Switching Mode	Shows the status of the local switching modules.
StatusLastChangeTime	When OperStatus was changed.
Power Admin	Allows you to power on and off the Field Replaceable Unit (FRU).
Power Oper	Field Replaceable Unit (FRU) operational power state.
Current	Current supplied by the Field Replaceable Unit (FRU).

Power Supplies

Field	Description
Name	Power supply location.
TotalPowerAvailable	Shows the available power. In combined mode, the total available power is twice the lesser of the two power supplies.
Redundant/Combined	Select to determine how the power supplies are configured. Redundant mode provides a backup power supply if one should fail, but the total power available is less.
ModelName	The model identifier.
OperStatus	Operational power state.
TotalAvailable	Total power available for power supply usage. When Mode is redundant, the total power available will be the lesser power capacity of the power supplies. When Mode is combined, the total power available will be twice the lesser of the power capacities of the operating power supplies.
TotalReserved	Total current drawn by powered-on FRUs



If the power supply to the Uros and Paradise is either interrupted or turned off, the OperStatus in the power supply table displays "offEnvOther". However, the corresponding entry for the powered down device the inventory table will remain.

Temperature Sensors

Field	Description
Name	Sensor location.
Threshold Major	Major temperature threshold.
Threshold Minor	Minor temperature threshold.
Current	Most recent measurement seen by the sensor.
Status	The present operational status of the sensor.

Fan

Field	Description
Name	Fan location.
ModelName	The model identifier.
OperStatus	The current operating status.

Switches

Field	Description
Description	A description of the switch and software.
UpTime	The time since the network management portion of the system was last re-initialized.
Name	An administratively-assigned name for this switch.
Location	The physical location of this switch (e.g., `telephone closet, 3rd floor').
Contact	The contact person for this switch, together with information on how to contact this person.
SwitchWWN	The World-Wide Name of this switch.
ClockDateAndTime	The current local date and time for the system. Setting this is equivalent to setting an automated clock and calendar.
TimeZone	The current local time zone for the system. The time zone must be entered in the format GMT, which is the number of hours difference between your time zone and GMT (Greenwich Mean Time).
ProcessorRAM	Total number of bytes of RAM available on the Processor.

Field	Description
NVRAM	This field provides two sets of values: • 1st value: Number of bytes of NVRAM in use. • 2nd value: Total number of bytes of NVRAM in the entity.  There's a known issue where the information shown in the GUI should be updated based on the switch model and platform type, but it may not be properly updated. However, you can get the correct NVRAM information for your switch model and platform type by loading the debug plugin (dplug) and using the following command from the Linux prompt: `cat /proc/isan/sw/nvram | grep length`
FIPSModeActivation	Enable or disable FIPS mode on the device. FIPS 140-2 is a set of security requirements for cryptographic modules and it details the U.S. Government requirements for cryptographic modules. A module will comprise both hardware and software such as a data center switching or routing module. The module is said to be in FIP- enabled mode when a request is recieved to enable the FIPS mode and a set of self-tests are successfully run in response to the request. If the self-tests fail, then an appropriate error is returned.
CPUUtilization	The average utilization of CPU on the active supervisor.
MemoryUtilization	The average utilization of memory on the active supervisor.
FlashPartitionSize	Flash partition size.
FlashPartitionFreeSpace	Free space within a Flash partition.
Status	The overall status of the switch.
Vendor	Switch vendor's name, such as Cisco, McData, or Brocade.
Model	Switch model name, such as MDS 9134 or MDS 9124.
Release	Switch software version.
NumFCPorts	Number of physical FC ports in the switch.
WWN	MAC address for the Ethernet VDCs that are discovered.
VDCId	Unique IDs for the Ethernet VDCs that are discovered.
FCoE Enabled	If true, FCoE is enabed for the Ethernet VDCs that are discovered.

ISLs

Field	Description
From Switch	The source switch of the link.
From Interface	The port index of source E_port of the link.

Field	Description
To Switch	The switch on the other end of the link.
To Interface	The port index of destination E_port of the link.
Status	The operational status of the link.

NP Link

Field	Description
NPIV (Core)	The NPIV core switch.
F Port	The connected F Port on the NPIV core switch.
NPV	NPV Switch.
NP Port	The connected port on the NPV switch.
Status	The operational status of the link.

ISLs Statistics

Field	Description
Description	An alias name for the interface, as specified by a network manager. For Port Channel and FCIP, this field will always show members if they are available. For FCIP, this field will show compress if compressed.
VSAN(s)	VSAN membership.
Mode	Operating mode of the port> (See Legend).
Connected To	Attached port. This could be a host, storage, or switch port.
Speed	Maximum bandwidth in Gbps.
Rx	One of the following: Utilization % Number of Bytes Number of Frames Average Frame Size
Rx Comp	The IP Copmression ratio for received packets on the FCIP device.
Tx	One of the following: Utilization % Number of Bytes Number of Frames Average Frame Size
Tx Comp	The IP Copmression ratio for transmitted packets on the FCIP device
Errors	Total number of Rx and Tx errors on the interface. Types of Rx errors include CRC errors, fragmented framed, unsupported class frames, runt frames, jabber frames, and giant Frames. Types of Tx errors are generally CRC errors, but these are rare. If the Errors field is not empty, there are probably Rx errors. For a more detailed breakdown of the error count, check the Monitor dialog box for appropriate interface.

Discards	Total number of Rx and Tx discards on the interface. Rx frames discarded are generally due to protocol errors. On rare occasions, a frame is received without any hardware errors, but a filtering rule set for the MAC address discards the frame due to a mismatch. Discarded Tx frames can be timeout frame discards (port is offline or not up), or timeout frames that are not sent back to the supervisor (class F/2 frames). If the Discards field is not empty, it is probably due to timeout frames.
Log	If checked, writes the record into the message log on each poll interval.

Hosts

Field	Description
Enclosure Name	The name of the enclosure.
Alias	The device alias of this entry.
Port WWN	The assigned PWWN for this host.
FcId	The FC ID assigned for this host.
Link Status	The operational status of the link.
Serial Number	Serial number.
Model	Model name.
Firmware Ver	The version of the firmware executed by this HBA.
Driver Ver	The version of the firmware executed by this HBA.
Information	The information list corresponding to this HBA.
Switch Interface	Interface on the switch that is connected with the end device.

Enclosures

Field	Description
IP Address	The IP address of the enclosure.
Elem. Mgr Use HTTP	Use HTTP to launch the local enclosure.
Elem. Mgr URL/Path	Use a URL to launch the local enclosure
Device Type	If host, it is HBA. If storage, it is the SCSI target.
Vendor	If host, it is HBA. If storage, it is the SCSI target.
Model	If host, it is HBA. If storage, it is the SCSI target.
Firmware Ver	The version of the firmware executed by this HBA.
Driver Ver	The version level of the driver software controlling this HBA.
OS	The type and version of the operating system controlling this HBA
Other Info	The information list corresponding to this HBA.

Device Manager - Preferences

Field	Description
Retry Requests # time(s) after #sec timeout	The number of retries to be attempted after time out (seconds).
Enable Status Polling	Check to enables status polling in every (specified number of) seconds
Trace SNMP packets in Message Log	Check to enable tracing SNMP packets in the message log.
Register for Events after Open, listen on Port 1163	Check to automatically register for events.
Show WWN Vendor	Check to enable showing the WWN vendor name. • Replace - Replace the existing vendor name with the new one. • Prepend - Attach the new vendor name to the beginning of the current vendor name.
Show Timestamps as Date/Time	Check for displaying the time stamp in the Date/Time format.
Telnet Path	Path to the telnet client.
Use Secure Shell instead of Telnet	Check to use secure shell.
CLI Session Timeout	Time interval for the CLI session (in seconds). Enter '0' to disable CLI timeout.
Show Tooltips in Physical View	Check to show tooltips.
Label Physical View Ports with	• FICON - Displays FICON as label for the ports on the device view. • Interface - Displays Interface as label for the ports on the device view.
Export Table	• Tab-Delimited - Exports the table to tab-delimited text file. • XML - Exports the table to xml file.

Interface

The following sections provide more information in these areas:

- Virtual Interface Groups
- Virtual FC Interfaces
- Ethernet Interfaces
- Virtual FC Ethernet
- Quick Configuration Tool
- Ethernet Interface
- Ethernet Interfaces iSCSI
- Ethernet Interfaces iSCSI TCP
- Ethernet Interfaces VLAN
- Ethernet VLAN
- FC Interface Monitor Traffic
- FC Interface Monitor Protocol
- FC Interface Monitor Discards
- FC Interface Monitor Link Errors
- FC Interface Monitor Frame Errors
- FC Interface Monitor Class 2 Traffic
- FC Interface Monitor Class 2 Errors
- FC Interface Monitor FICON
- Check Oversubscription
- Virtual FC Interface Monitor Traffic
- Virtual FC Interface Monitor Discards
- Virtual FC Interface Monitor Errors
- Ethernet Interface Dot3Stats
- Interface Monitor
- Ethernet PortChannels
- Ethernet Interface Monitor iSCSI Connections
- Ethernet Interface Monitor TCP
- FCIP Monitor
- Monitor SVC Interface
- Monitor SVC NPorts
- Monitor SVC Session FCP
- Monitor SVC Session Other
- FCIP Interfaces

- System Timeout
- Interface License
- General
- FC Interfaces General
- FC Interfaces Rx BB Credit
- FC Interfaces Other
- FC Interfaces FLOGI
- FC Interfaces ELP
- FC Interfaces Trunk Config
- FCIP Interfaces Trunk Failures
- FC Interfaces IP
- FC Interfaces Physical
- FC Interfaces Capability
- FC Interfaces FICON Peer
- Interfaces NPorts (SVC)
- Interfaces Sessions
- IP Statistics TCP
- Port Channels Ethernet Interfaces
- Port Channels FC Interfaces
- Port Channels General
- FlexAttach Global
- FlexAttach Virtual PWWN
- FlexAttach Physical to Virtual WWNs
- FIPS
- FCIP FICON Configuration
- Port Channels AutoCreate
- SPAN Sessions
- Span Global
- SPAN Source Interfaces
- Port Tracking Dependencies
- Port Tracking Force Shut
- Port Guard
- Bandwidth Reservation: 48-Port 96-Gbps Fibre Channel module
- Bandwidth Reservation: 48-Port 48-Gbps Fibre Channel module
- Bandwidth Reservation: 24-Port 48-Gbps Fibre Channel module
- Bandwidth Reservation: 48-Port 256-Gbps Fibre Channel module

- Bandwidth Reservation: 32-Port 256-Gbps Fibre Channel module
- DS-X9448-768K9 (Luke) Line Card Bandwidth Reservation

Virtual Interface Groups

The Bound Ethernet Interface field in the table can be modified. The remaining fields are for information only.

Field	Description
Switch	Name of the switch hosting this virtual interface group (VIG).
VIG Id	Virtual interface group identifier.
Bound Eth Interface	Physical Ethernet interface associated with this VIG.
Virtual Eth Interfaces	The virtual Ethernet interface bound to this VIG.
Virtual FC Interfaces	The virtual FC interface bound to this VIG.
Operational Status	The current operational state of the VIG.
CreationTime	Date and time when the VIG was created.



This table applies only to N5k switches running version less than 4.0(1a).

Virtual FC Interfaces

The following fields in the table can be modified: Description, Bind Type, Bind Interface, Bind MAC Address, FCF Priority, VSAN ID Port, Mode Admin, Status Admin. The remaining fields are for information only.

Field	Description
Switch	Name of the switch hosting this interface.
Interface	Interface name.
Description	Text description of the interface as specified by a network manager.
VIG Id	Virtual interface group to which this virtual FC interface is bound.
Bind Type	The type of interface associated with this virtual FC interface - physical Ethernet interface or MAC address of the FCoE Node (ENode).
Bind Interface	Physical Ethernet interface or Ethernet port channel associated with this virtual FC interface.
Bind MACAddress	MAC address of an FCoE Node (ENode) or a remote Fibre Channel Forwarder (FCF) identified by the virtual FC interface.
FCF Priority	The FCoE Initialization Protocol (FIP) priority value advertised by the FCF to ENodes.
VSAN ID Port	VSAN ID to which this interface is statically assigned.
VSAN Id Dynamic	Index of the VSAN to which this interface is statically assigned.

Field	Description
Mode Admin	The port mode configured by the user. Virtual FC interfaces support only fabric port (F Port) mode.
Rate Mode	Specifies the interface as dedicated mode or shared mode.
Speed Oper	Operational speed.
Mode Oper	The current operating mode of the port.
Speed Admin	The port speed configured by the user.
Status Service	Specifies whether the interface is in service or out of service.
Status Admin	The desired state of the interface.
Status Oper	The current operational state of the interface.
Status FailureCause	The cause of current operational state of the port.
Status LastChange	When the interface entered its current operational state. If the current state was entered prior to the last re-initialization of the local network management subsystem, then this value is N/A.



VIG Id field applies only to N5k switches running version less than 4.0(1a).

Ethernet Interfaces

The Description and Admin fields in the table can be modified. The remaining fields are for information only.

Field	Description
Switch	Name of the switch hosting this interface.
Interface	Interface name.
Description	Text description of the interface as specified by a network manager.
VIG Id	Virtual interface group to which this virtual interface is bound.
Bound Eth Interface	Physical Ethernet interface associated with this virtual Ethernet interface.
Admin	The desired state of the interface.
Oper	The current operational state of the interface.
LastChange	When the interface entered its current operational state. If the current state was entered prior to the last re-initialization of the local network management subsystem, then this value is N/A.
CDP (Enable)	Indicates whether the Cisco Discovery Protocol is currently running on this interface.
Duplex Status	The current mode of operation of the MAC entity. The status 'unknown' indicates that the current duplex mode could not be determined.
Enable Link Trap	Specifies whether Link Up or Link Down traps should be generated for this interface.

This table applies only to N5k switches running version less than 4.0(1a).

Virtual FC Ethernet

Field	Description
Switch	Name of the switch hosting this interface.
Interface	Displays the name of the vFC interface and its association with other interfaces.
Description	Text description of the interface as specified by a network manager.
Status Admin	The desired state of the interface.
Status Oper	The current operational state of the interface.
Speed Oper	Operational speed of the interface
LastChange	When the interface entered its current operational state. If the current state was entered prior to the last re-initialization of the local network management subsystem, then this value is N/A.

Quick Configuration Tool

Field	Description
Show All Interfaces	Check this checkbox to show all the available interfaces including the interfaces that are not available for binding to a vFC.
Auto Assigin vFC Id	Check this checkbox to select vFC Id automatically. If you do not select this option you must manually enter a valid vFC Id.
Switch Operational Type	Click **Ethernet Switch** if you are not configuring any Fibre Channel interfaces on the switch. Click **FCoE Switch** if you are configuring Fibre Channel and FCoE interfaces.
Interface	Name of the physical Ethernet interface. If you hover the cursor over a physical Ethernet interface, any associated virtual interfaces are displayed in the tooltip.
FCoE VLAN(VSAN)	FCoE VLAN (VSAN) mapping to be used by the interface.
Admin Mode	Admin mode of the vFC interface, i.e. F or E
Eth Only	Configures the physical Ethernet without any virtual interfaces. Click the **Eth Only** button in the column header to set all the interfaces to this value.
vEth Only	Configures the physical Ethernet to have an associated VIG and a virtual Ethernet interface. Click the **vEth Only** button in the column header to set all the interfaces to this value.
vFC Only	Configures the physical Ethernet to have an associated VIG and a virtual FC interface. Click the **vFC Only** button in the column header to set all the interfaces to this value.

Field	Description
vFC	Configures the physical Ethernet to have an associated VIG and a virtual FC interface. Click the **vFC** button in the column header to set all the interfaces to this value.
vEth + vFC	Configures the physical Ethernet to have an associated VIG, a virtual Ethernet interface and a virtual FC interface. Click the **vEth + vFC** button in the column header to set all the interfaces to this value.
Configure Action Status	Displays the current status of the requested configuration changes.



vEth only, vFC only, vEth + vFC columns are not applicable for N5K switches running version 4.0(1a)N1 NOTE: vFC column is applicable only for N5K switches running version 4.0(1a)N1 NOTE: For earlier configured ports, mapping details will not be displayed in VLAN(VSAN) Mapping column.

Ethernet Interface

Field	Description
Description	An `alias' name for the interface as specified by a network manager.
Mtu	The size of the largest frame which can be sent/received on the interface, specified in bytes.
Speed Oper	Operational speed of the interface.
Speed Admin	▪ notApplicable – The Speed change is not applicable for that port. ▪ oneGigSpeed – The IPStorage port is configured as 1G. ▪ tenGigSpeed – The IPStorage port is configured as 10G.
Failure Cause	Causes of the failures.
PhysAddress	The interface's MAC address.
Status Admin	The desired state of the interface.
Status Oper	The current operational state of the interface.
LastChange	When the interface entered its current operational state. If the current state was entered prior to the last re-initialization of the local network management subsystem, then this value is N/A.
ConnectorPresent	True if the connector is detected.
CDP (Enable)	An indication of whether the Cisco Discovery Protocol is currently running on this interface.
IscsiAuthMethod	The authentication method.
Promiscuous Mode	Checking or unchecking this option dictates the destination of the packets/frames. If this option is checked, then this interface accepts packets/frames that are addressed to this station. If this option is not selected, then packets accepted by the station are transmitted on the media. Checking or unchecking this option does not affect the reception of broadcast and multicast packets/frames by the interface.

Field	Description
AutoNegotiate	Select this option to enable auto negotiation.
Beacon Mode	In beacon mode, an interface LED is assigned a flashing mode for identification. Select this option to enable beacon mode.
IPAddress/Mask	IP address and subnet mask for the interface.



SAN Admin users cannot change the ethernet interfaces settings in Cisco Nexus 5000 Series switches using Device Manager.

Ethernet Interfaces iSCSI

Field	Description
Description	An `alias' name for the interface as specified by a network manager.
Speed	Operational speed.
PhysAddress	The interface’s WWN.
Admin	The desired state of the interface.
Oper	The current operational state of the interface.
LastChange	When the interface entered its current operational state. If the current state was entered prior to the last re-initialization of the local network management subsystem, then this value contains a N/A value.
PortVSAN	The VSAN that the interface belongs to.
ForwardingMode	Use Store and Forward if the HBA has problems with Passthrough.
Initiator ID Mode	How the initiator is identified on this interface, either by its iSCSI name (name) or by its IP address (ipaddress).
Enable	The intiator proxy mode for this interface. If true, then all the initiators coming on this interface would use the intiator configuration provided by this interface. The initiator configuration include port WWN and node WWN.
Assignment	How the initiator proxy mode FC addresses are assigned. If `auto', then the FC addresses are automatically assigned. If it is `manual', then they have to be manually configured.
Port WWN	The Port FC address used by the intiators on this interface when the intiator proxy mode is on.
Node WWN	The Node FC address used by the initiators on this interface when the initiator proxy mode is on.

Ethernet Interfaces iSCSI TCP

Field	Description
Local Port	Local interface TCP port.

Field	Description
SACK	Indicates if the Selective Acknowledgement (SACK) option is enabled or not.
KeepAlive	The TCP keep alive timeout for this iSCSI interface. If the value is 0, the keep-alive timeout feature is disabled.
MinTimeout	The TCP minimum retransmit time.
Max	The TCP maximum retransmissions.
SendBufferSize	The TCP send buffer size.
MinBandwidth	The TCP minimum bandwidth.
MaxBandwidth	The TCP maximum bandwidth.
Estimated Round Trip	The estimated round trip delay of network pipe used for B-D product computation. The switch can use this to derive the TCP window to advertise.
QoS	The TCP QoS code point.
PMTU Enable	Indicates if the Path MTU discovery option is enabled or not.
PMTU Reset Timeout	The PMTU reset timeout.
Connections Normal	The number of normal iSCSI connections.
Connections Discovered	The number of discovery iSCSI connections.
CWM Enable	If true, congestion window monitoring is enabled. If false, it is disabled.
CWM Burst Size	The maximum burst sent after a TCP sender idle period.
Max Jitter	The maximum delay variation (not due to congestion) that can be experienced by TCP connections on this interface.
Port	The local TCP port of this interface.

Ethernet Interfaces VLAN

Field	Description
Switch	Name of the switch.
Interface	Name of the interface.
VLAN mode	The mode in which this VLAN is configured. Static-A port with static VLAN membership directly assigned to a single VLAN. Dynamic-A port with dynamic VLAN membership assigned to a single VLAN based on the content of packets received on the port via VQP queries to VMPS. multiVLAN-A port with multiple VLAN memberships that are directly assigned to one or more VLANs.
VLAN list	The list of VLANs which are allowed on the switch.

Ethernet VLAN

Field	Description
Switch	Name of the switch.
ID	Switch ID
Trunk Mode	Specifies whether the mode is access or trunk.
Trunk Status	Ttrunking status of the port.
Native VLAN	Native VLANs
Allowed VLAN List	The list of VLANs which are allowed to be received/transmitted on the port.
Active VLAN List	The list or range of VLANs that are active on the switch.

FC Interface Monitor Traffic

The Monitor dialog boxes have special Monitor Dialog Controls.

Field	Description
C3 Rx Bytes	The number of Class 3 bytes, including the frame delimiters, received by this port from its attached Nx_Port.
C3 Rx Frames	The number of Class 3 frames, including the frame delimiters, received by this port from its attached Nx_Port.
C3 Tx Bytes	The number of Class 3 bytes, including the frame delimiters, transmitted by this port to its attached Nx_Port.
C3 Tx Frames	The number of Class 3 frames, including the frame delimiters, transmitted by this port to its attached Nx_Port.
CF Rx Bytes	The number of Class F bytes, including the frame delimiters, received by this port from its attached Nx_Port.
CF Rx Frames	The number of Class F frames, including the frame delimiters, received by this port from its attached Nx_Port.
CF Tx Bytes	The number of Class F bytes, including the frame delimiters, transmitted by this port to its a attached Nx_Port.
CF Tx Frames	The number of Class F frames, including the frame delimiters, transmitted by this port to its attached Nx_Port.

FC Interface Monitor Protocol

The Monitor dialog boxes have special Monitor Dialog Controls.

Field	Description
LRRIn	The number of Link reset responses received by the FC-port.
LRROut	The number of Link reset responses transmitted by the FC-port.

Field	Description
OlsIns	The number of Offline Sequence errors received by the FC-Port.
OlsOuts	The number of Offline Sequence errors issued by the FC-Port.
NOSIn	The number of Non-Operational Sequences received by the FC-port.
NOSOut	The number of Non-Operational Sequences transmitted by the FC-port.
LinkResetIns	The number of link reset protocol errors received by the FC-Port from the attached FC-port.
LinkResetOuts	The number of link reset protocol errors issued by the FC-Port to the attached FC-Port.
TxWaitCount	The number of times the FC-port waited due to lack of transmit credits.
RxBBCredit	The maximum number of receive buffers available for holding Class 2, Class 3 received from the logged-in Nx_Port. It is for buffer-to-buffer flow control in the incoming direction from the logged-in Nx_Port to FC-port.
TxBBCredit	The total number of buffers available for holding Class 2, Class 3 frames to be transmitted to the logged-in Nx_Port. It is for buffer-to-buffer flow control in the direction from FC-Port to Nx_Port.
BBCreditTransitionFromZero	The number of transitions of BB credit out of zero state.

FC Interface Monitor Discards

The Monitor dialog boxes have special Monitor Dialog Controls.

Field	Description
Class2	The number of Class 2 frames discarded by this port.
Class3	The number of Class 3 frames discarded by this port.
ClassF	The number of Class F frames discarded by this port.
EISL	The number of Enhanced Inter Switch Link (EISL) frames discarded by the FC-port. EISL frames carry an EISL header containing VSAN among other information.
InDiscards	The total number of inbound frames which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol.
OutDiscards	The total number of outbound frames which were chosen to be discarded even though no errors had been detected to prevent their being transmitted.

FC Interface Monitor Link Errors

The Monitor dialog boxes have special Monitor Dialog Controls.

Field	Description
LinkFailures	The number of link failures detected by the FC-Port.
SigLosses	The number of signal losses detected by the FC-Port.
SyncLosses	The number of loss of synchronization failures detected by the FC-Port.
InvalidTxWords	The number of invalid transmission words detected by the FC-Port.
DelimiterErrors	The number of Delimiter Errors detected by the FC-Port.
AddressIdErrors	The number of address identifier errors detected by the FC-Port.

FC Interface Monitor Frame Errors

The Monitor dialog boxes have special Monitor Dialog Controls.

Field	Description
InvalidCrcs	The number of invalid CRCs detected by the FC-Port. Loop ports should not count CRC errors passing through when monitoring.
ELPFailures	The number of Exchange Link Parameters Switch Fabric Internal Link service request failures detected by the FC-Port. This is applicable to only Interconnect_Port, which are E_Port or B_Port.
Frags	The number of fragmented frames received by the FC-port.
Runts	The number of frames received by the FC-port that are shorter than the minimum allowable frame length regardless if the CRC is good or not.
Jabbers	The number of frames received by the FC-port that are longer than a maximum frame length and also have a CRC error.
TooLongs	The number of frames received by the FC-port where the frame length was greater than what was agreed to in FLOGI/PLOGI. This could be caused by losing the end of frame delimiter.
TooShorts	The number of frames received by the FC-port where the frame length was less than the minimum indicated by the frame header (normally 24 bytes), but it could be more if the DFCTL field indicates an optional header should be present.
Unknowns	The number of unknown class frames received by FC-port.
EOFa	The number of frames received by FC-port with EOF aborts.
Framing	The number of framing errors. This denotes that the FC-port detected an inconsistency of frame structure.

FC Interface Monitor Class 2 Traffic

The Monitor dialog boxes have special Monitor Dialog Controls.

Field	Description
In Octets/In Frames	The number of Class 2 frame bytes and frames, including the frame delimiters, received by this port from its attached Nx_Port.

Field	Description
Out Octets/Out Frames	The number of Class 2 frame bytes and frames, including the frame delimiters, delivered through this port to its attached Nx_Port.

FC Interface Monitor Class 2 Errors

The Monitor dialog boxes have special Monitor Dialog Controls.

Field	Description
FBSY	The number of busy frame responses.
FRJT	The number of F_RJT frames generated by this port against Class 2 frames.
PBSY	The number of times that port busy was returned to this port as result of a class 2 frame that could not be delivered to the other end of the link. This occurs if the destination Nx_Port is temporarily busy. PBSY can only occur on SOFc1 frames (the frames that establish a connection).
PRJT	The number of times that port reject was returned to this port as a result of a class 2 frame that was rejected at the destination Nx_Port.

FC Interface Monitor FICON

The Monitor dialog boxes have special Monitor Dialog Controls.

Field	Description
FramePacingTime	Number of 2.5 microsecond units that frame transmission is blocked due to zero credit.
DispErrorsInFrame	Number of frames with disparity errors.
EOFErrs	Number of frames with EOF errors.
DispErrsOutOfFrame	Number of frames with OOF errors.
InvalidOrderSets	Number of invalid or unrecognizable Order Sets outside of frames.

Check Oversubscription

Field	Description
Interval	
Elapsed	Time elapsed.
Interface	Name of the interface
InOctectRate	
OutOctectRate	

Virtual FC Interface Monitor Traffic

The Monitor dialog boxes have special Monitor Dialog Controls.

Field	Description
RxBytes	The number of bytes, including the frame delimiters, received by this port from its attached N_Port.
RxFrames	The number of frames, including the frame delimiters, received by this port from its attached N_Port.
TxBytes	The number of bytes, including the frame delimiters, transmitted by this port to its attached N_Port.
TxFrames	The number of frames, including the frame delimiters, transmitted by this port to its attached N_Port.

Virtual FC Interface Monitor Discards

The Monitor dialog boxes have special Monitor Dialog Controls.

Field	Description
InDiscards	The total number of inbound frames which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol.
OutDiscards	The total number of outbound frames which were chosen to be discarded even though no errors had been detected to prevent their being transmitted.

Virtual FC Interface Monitor Errors

The Monitor dialog boxes have special Monitor Dialog Controls.

Field	Description
InErrors	The number of incoming errors detected by the virtual FC port.
OutErrors	The number of outgoing errors detected by the virtual FC port.

Ethernet Interface Dot3Stats

Field	Description
Interface	Name of the interface.
Alignment Errors	The count of frames received on a particular interface that are an integral number of octets in length but do not pass the FCS check.
FCS Errors	The count of frames received on a particular interface that are an integral number of octets in length but do not pass the FCS check. This count does not include frames received with frame-too-long or frame-too-short error.

Field	Description
Single Collision Frames	The count of successfully transmitted frames on a particular interface for which transmission is inhibited by a single collision.
Multiple Collision Frames	The count of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collisions.
SQE Test Errors	The number of times the PLS sublayer generated the SQE TEST ERROR message for a particular interface.
Deferred Transmissions	The count of the number of frames for which the first transmission attempt on a particular interface is delayed because the medium is busy.
Late Collisions	The number of times that a collision is detected on a particular interface later than one slot time into the transmission of a packet.
Excessive Collisions	The count of the number of frames for which transmission on a particular interface failes because of excessive collisions. This counter does not increment when the interface is operating in full-duplex mode.
Internal Mac Transmit Errors	The count of the number of frames for which transmission on a particular interface fails because of an internal MAC sublayer transmit error.
Carrier Sense Errors	The number of times that a carrier sense condition was lost or never asserted when attempting to transmit a frame on a particular interface.
Frame Too Longs	The count of number of frames received on a particular interface that exceed the maximum permitted frame size.
Internal Mac Receive Errors	The count of number of frames for which reception on a particular interface fails because of an internal MAC sublayer receive error.
Symbol Errors	For an interface operating at 100 Mb/s, the number of times there was an invalid data symbol when a valid carrier was present

Interface Monitor

The Monitor dialog boxes have special Monitor Dialog Controls.

Field	Description
Rx Bytes	The total number of bytes received on the interface, including framing characters.
RxFrames	The number of frames received on the interface.
Rx Multicast Frames	(Nexus 5000 Series only) The number of multicast frames received on the interface.
Rx Broadcast Frames	(Nexus 5000 Series only) The number of broadcast frames received on the interface.
TxBytes	The total number of bytes transmitted out of the interface, including framing characters.
TxFrames	The total number of frames transmitted out of this interface.
Tx Multicast Frames	(Nexus 5000 Series only) The number of multicast frames transmitted out of this interface.

Field	Description
Tx Broadcast Frames	(Nexus 5000 Series only) The number of multicast frames transmitted out of this interface.
RxErrors	The number of inbound frames that contained errors preventing them from being deliverable to a higher-layer protocol.
TxErrors	The number of outbound frames that could not be transmitted because of errors.
RxDiscards	The number of inbound frames which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol.
TxDiscards	The number of outbound frames which were chosen to be discarded even though no errors had been detected to prevent their being transmitted.

Ethernet PortChannels

Field	Description
Description	Alias name for the interface as specified by a network manager.
Members	Members of this Ethernet port channel.
Oper Speed	Operational speed of the interface.
Mtu	The size of the largest frame which can be sent/received on the interface, specified in bytes.
PhysAddress	The interface's MAC address.
Status Admin	The desired state of the interface.
Status Oper	The current operational state of the interface.
LastChange	When the interface entered its current operational state. If the current state was entered prior to the last re-initialization of the local network management subsystem, then this value is N/A.

Ethernet Interface Monitor iSCSI Connections

Field	Description
RxBytes	Total number of bytes received on an iSCSI session.
TxBytes	Total number of bytes transmitted on an iSCSI session.
IPSEC	A collection of objects for iSCSI connection statistics.

Ethernet Interface Monitor TCP

Field	Description
Opens	The number of times connections have been opened.
Accepts	The number of times connections have been accepted.

Field	Description
Failed	The number of times connections have failed.
RxResets	The number of times connections have been reset.
Est	The number of connections that have been established.
RxSegs	The total number of segments received on established connections, including those received in error.
TxSegs	The total number of segments sent, except for those containing retransmitted bytes.
ReTxSegs	The total number of segments retransmitted.
BadSegs	The total number of segments received in error (e.g., bad checksums).
TxSegResets	The number of segments sent containing the "reset" flag.
SplitSeg	The number of segments sent which were less than the minimum.
DupACKs	The number of duplicate ACKs received.
RxBytes	The number of header and data bytes received.
TxBytes	The number of header and data bytes sent.

FCIP Monitor

The Monitor dialog boxes have special Monitor Dialog Controls.

Field	Description
C3 Rx Bytes	The number of incoming bytes of data traffic.
C3 Tx Bytes	The number of outgoing bytes of data traffic.
CF Rx Bytes	The number of incoming bytes of control traffic.
CF Tx Bytes	The number of outgoing bytes of control traffic.
Rx Error	The number of inbound frames that contained errors preventing them from being deliverable to a higher-layer protocol.
Tx Error	The number of outbound frames that could not be transmitted because of errors.
RxDiscard	The number of inbound frames which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol.
TxDiscard	The number of outbound frames which were chosen to be discarded even though no errors had been detected to prevent their being transmitted.

Monitor SVC Interface

The Monitor dialog boxes have special Monitor Dialog Controls.

Field	Description
Rx Bytes	Number of incoming bytes.
Rx Frames	Number of incoming frames.
Tx Bytes	Number of outgoing bytes.
Tx Frames	Number of outgoing frames.
Rx Errors	Number of incoming errors.
Tx Errors	Number of outgoing errors.
Rx Discards	Number of incoming discards.
Tx Discards	Number of outgoing discards.

Monitor SVC NPorts

The Monitor dialog boxes have special Monitor Dialog Controls.

Field	Description
Rx Bytes	Number of incoming bytes on this virtual N-port.
Rx Frames	Number of incoming frames on this virtual N-port.
Tx Bytes	Number of outgoing bytes on this virtual N-port.
Tx Frames	Number of outgoing frames on this virtual N-port.
Rx Bytes	Number of incoming bytes on this virtual N-port.
Rx Frames	Number of incoming frames on this virtual N-port.
Tx Bytes	Number of outgoing bytes on this virtual N-port.
Tx Frames	Number of outgoing frames on this virtual N-port.

Monitor SVC Session FCP

The Monitor dialog boxes have special Monitor Dialog Controls.

Field	Description
Cmds	Number of incoming FCP Command frames in this session.
XferRdys	Number of incoming FCP Transfer Ready frames in this session.
DataFrames	Number of incoming FCP Data frames.
Status	Number of incoming FCP status frames.
DataBytes	Number of incoming FCP Data bytes.
OverRuns	Number of incoming FCP Overrun frames in this session.
UnderRuns	Number of incoming FCP Underrun frames in this session.
Cmds	Number of outgoing FCP Command frames in this session.
XferRdys	Number of outgoing FCP Transfer Ready frames in this session.

Field	Description
DataFrames	Number of outgoing FCP Data frames.
Status	Number of outgoing FCP status frames.
DataBytes	Number of outgoing FCP Data bytes.
OverRuns	Number of outgoing FCP OverRun frames in this session.
UnderRuns	Number of outgoing FCP UnderRun frames in this session.

Monitor SVC Session Other

The Monitor dialog boxes have special Monitor Dialog Controls.

Field	Description
InELSFrames	Number of incoming Extended Link Service frames in this session.
InBLSFrames	Number of incoming Basic Link Service frames in this session.
OutELSFrames	Number of outgoing Extended Link Service frames in this session.
OutBLSFrames	Number of outgoing Basic Link Service frames in this session.
InAborts	Number of incoming aborted frames in this session.
OutAborts	Number of outgoing aborted frames in this session.
OpenXchanges	Number of Open Exchanges in this session.
InBadFc2Drops	Number of FC2 dropped frames in this session.
InBadFcPDrops	Number of FCP dropped frames.
InFCPDataExcess	Number of FCP Data Excess frames in this session.

FCIP Interfaces

Field	Description
Description	Alias name for the interface as specified by a network manager.
PortVsan	The VSAN ID to which this interface is statically assigned.
Oper Mode	The current operating mode of the port.
AutoChannelCreate	If checked, automatically create the PortChannel.
Admin	The desired state of the interface.
Oper Status	The current operational state of the interface.
FailureCause	The cause of current operational state of the port.
LastChange	When the interface entered its current operational state. If the current state was entered prior to the last re-initialization of the local network management subsystem, then this value is N/A.
FICON Address	The FICON port address of this port.

System Timeout

If frames residing in the switch for a long time, they should be regarded as congestion drop. If there is continuously no tx/rx credits received, it should be regarded as no credit drop. You can configure the timeout value of congestion drop and no credit drop in the Device Manager client. To configure the slow port monitor timeout, please go to **Admin > System Timeout**.

Field	Description
E port Congestion Drop	Specify the time for E port congestion drop. Or click on default to input a default value. The unit is ms.
F port Congestion Drop	Specify the time for F port congestion drop. Or click on default to input a default value. The unit is ms.
F port NoCredit Drop	Specify the time for no credit drop. Click on disable if you do not want to drop the frames without tx/rx credits or click on default to input a default value. The unit is ms.
E Port slowport-monitor	Specify the slowport-monitor timeout value for E port. Click on disable to disable slowport monitoring. Or click on default to input a default value. The unit is ms.
F Port slowport-monitor	Specify the slowport-monitor timeout value for F port. Click on disable to disable slowport monitoring. Or click on default to input a default value. The unit is ms.



To configure the slow port monitor time out values from SAN client, go to **Physical Attributes > Switches > System> Timeout**.

Interface License

Field	Description
Type	Specifies the license that can be acquired for a given interface. Currently, the Port Activation license can be defined.
Config	Displays the license for which an interface is eligible. An interface which is not eligible for any type of license will not be displayed.
Oper	The current state of port license on the interface is displayed.

General

Field	Description
Description	An `alias' name for the interface as specified by a network manager.
Mtu	The size of the largest frame which can be sent/received on the interface, specified in bytes.
Oper	Operational speed
PhysAddress	The interface's MAC address.
Admin	State of the admin.

Field	Description
Oper	The current operational state of the interface.
LastChange	When the interface entered its current operational state.
CDP	Enable or disable CDP.
Default Gateway	The IP address of the default gateway.

FC Interfaces General

The following variables are not supported by all interfaces: PortVSAN, Port Mode Admin and Oper, Admin Speed, and FailureCause.

Field	Description
Description	Alias name for the interface as specified by a network manager.
VSAN Id Port	VSAN ID to which this interface is statically assigned.
VSAN Id Dynamic	The VSAN ID that this interface has been dynamically assigned (see DPVM).
CDP (Enable)	An indication of whether the Cisco Discovery Protocol is currently running on this interface.
Promiscuous Mode	Checking or unchecking this option dictates the destination of the packets/frames. If this option is checked, then this interface accepts packets/frames that are addressed to this station. If this option is not selected, then packets accepted by the station are transmitted on the media. Checking or unchecking this option does not affect the reception of broadcast and multicast packets/frames by the interface9.
Auto Negotiate	An indication of whether auto-negotiation of speed and duplex mode should be used on this interface.
Beacon Mode	In beacon mode, an interface LED is assigned a flashing mode for identification. Select this option to enable beacon mode.

Field	Description
Mode Admin	The port mode configured by the user. Modes are: • auto - If the user configured the port as auto, then the port initialization scheme determines the mode of the port. • F Port - In fabric port mode, an interface functions as a fabric port. This port may be connected to a peripheral device (host or disk) operating as an N port. • FL Port - In fabric loop port mode, an interface functions as a fabric loop port. This port may be connected to one or more NL ports (including FL ports in other switches) to form a public arbitrated loop. • E Port - In expansion port mode, an interface functions as a fabric expansion port. This port may be connected to another E port to create an Inter-Switch Link (ISL) between two switches. E ports carry frames between switches for configuration and fabric management. • FX Port - Interfaces configured as Fx ports can operate in either F port or FL port mode. The Fx port mode is determined during interface initialization depending on the attached N port or NL port. This administrative configuration disallows interfaces to operate in any other mode-for example, preventing an interface to connect to another switch. • SD Port - In SPAN destination port mode, an interface functions as a switched port analyzer (SPAN). The SPAN feature is specific to switches in the Cisco MDS 9000 Family. It monitors network traffic that passes though a Fibre Channel interface. • TL Port - In translative loop port mode, an interface functions as a translative loop port. It may be connected to one or more private loop devices. TL port mode is specific to Cisco MDS 9000 family switches and have similar properties as FL ports. • ST Port - In the SPAN tunnel port (ST port) mode, an interface functions as an entry point port in the source switch for the RSPAN Fibre Channel tunnel. The ST port mode and the remote SPAN (RSPAN) feature are specific to switches in the Cisco MDS 9000 Family. When configured in ST port mode, the interface cannot be attached to any device, and thus cannot be used for normal Fibre Channel traffic. • TE Port - In trunking E port mode, an interface functions as a trunking expansion port. It may be connected to another TE port to create an Extended ISL (EISL) between two switches. TE ports are specific to Cisco MDS 9000 family switches. • B Port - While E ports typically interconnect Fibre Channel switches, some SAN extender devices, such as Cisco's PA-FC-1G Fibre Channel port adapter, implement a bridge port model to connect geographically dispersed fabrics. The oper mode on this port type is " read only" and it cannot be set. • TF Port - Trunking f_Port • TNP Port - Trunking N Proxy port mode applicable only to N-port Virtualizer (NPV) • NP Port - N Proxy port mode applicable only to N-port Virtualizer (NPV)
Mode Oper	The current operating mode of the port.

Field	Description
SpeedGroup	Specifies the current speed group configuration on the given interface. • None-The interface speed group configuration on this interface is not applicable. It is a read-only value. • 10G-The interface speed group configuration on this interface is 10G. • 1/2/4/8G-The interface speed group configuration on this interface as 1G-2G-4G-8G.
Speed Admin	The port speed configured by the user. The port speed values are auto, 1Gb, 2Gb, 4Gb, 8Gb, 10Gb, autoMax2G, and autoMax4G. **Note** On a Cisco Nexus 5000 Series switch that runs Cisco NX-OS Release 4.2(2), you can configure the 8-Gbps administrative speed only on an M1060 switch module. You can configure the speed to 1 Gbps, 2 Gbps, or 4 Gbps on all switch modules on a Cisco Nexus 5000 Series switch that runs Cisco NX-OS Release 4.2(2) or earlier releases.
Speed Oper	Operational speed.
RateMode	Specifies the interface as dedicated mode or shared mode.
Status Service	Specifies whether the interface is in service or out of service.
Status Admin	The desired state of the interface.
Status Oper	The current operational state of the interface.
Status FailureCause	The cause of current operational state of the port.
StatusWasEnabled	If true, this port successfully completed a link initialization.
Status LastChange	When the interface entered its current operational state. If the current state was entered prior to the last re-initialization of the local network management subsystem, then this value is N/A.
Port Owner	Administratively assigned name of the current owner of the interface resource.

FC Interfaces Rx BB Credit

Field	Description
Oper	The receive buffer-to-buffer credits configured for the operational port mode.
Model	The BB_Credit model used by the FC-port. The alternate BB_Credit management model can be used in the arbitrated loop topology to manage the flow of frames between the two ports participating in the current loop circuit. Since this is a characteristic of a physical port, this is not applicable for Port Channel ports.

Field	Description
Admin	The receive buffer-to-buffer credits configured for this port.
Extended	The extended BB credits that can be configured on an FC port (in the range 256 through 4095). The acceptable value depends on the BB credit configuration of other ports on the module. This value can only be modified on modules that support the extended BB credit feature.
AdminISL	The receive buffer-to-buffer credits configured for this port to be used if it is operating in xE_port mode.
AdminFx	The receive buffer-to-buffer credits configured for this port to be used if it is operating in Fx mode.
PerfBuffer Admin	The performance buffers configured for this port. These buffers in addition to the buffer-to-buffer credits are used to improve the performance of a port. If a value of 0 is set, then the module uses the built-in algorithm to calculate the number of performance buffers to be used.
PerfBuffer Oper	The performance buffers presently operational on this port.
Oper Rx	The maximum number of receive buffers available for holding Class 2, Class 3, Class F frames received from the peer Interconnect_Port.
Oper Tx	The total number of buffers available for holding Class 2, Class 3, Class F frames to be transmitted to the peer Interconnect_Port.
Current Rx	The current value of receive buffer-to-buffer credits for this port.
Current Tx	The current value of transmit buffer-to-buffer credits for this port.
BbScn Notify	Indicates whether the Buffer-to-buffer State Change Number (BB_SC_N) mode is enabled. If checked, BB_SC_N mode is enabled. If unchecked, BB_SC_N mode is disabled.

FC Interfaces Other

Field	Description
PortChannel Id	The port channel that this interface belongs to.
Fabric WWN	The world wide name given to this interface.
Mtu bytes	The size of the largest frame which can be sent/received on the interface, specified in bytes.
RxDataFieldSize bytes	The largest Data_Field size for an FT_1 frame that can be received by this port.
HoldTime us	The maximum time that the FC-Port shall hold a frame in the transmitter buffer before discarding it, if it is unable to deliver the frame.
Auto Port Channel	Check if you want the PortChannel to be created automatically.
FEC Admin	Specifies the port FEC state configured.
FEC Oper	Specifies the current operating FEC state of the port.

FC Interfaces FLOGI

Field	Description
FcId	The address identifier that has been assigned to the logged-in Nx_Port.
PortName	The world wide name of the logged-in Nx_Port.
NodeName	The world wide name of the Remote Node the logged-in Nx_Port belongs to.
Original PWWN	The original port WWN for this interface
Version	The version of FC-PH that the Fx_Port has agreed to support from the Fabric Login.
BBCredit Rx	The maximum number of receive buffers available for holding Class 2, Class 3 received from the logged-in Nx_Port. It is for buffer-to-buffer flow control in the incoming direction from the logged-in Nx_Port to FC-port.
BBCredit Tx	The total number of buffers available for holding Class 2, Class 3 frames to be transmitted to the logged-in Nx_Port. It is for buffer-to-buffer flow control in the direction from FC-Port to Nx_Port. The buffer-to-buffer flow control mechanism is indicated in the respective BbCreditModel.
CoS	The classes of services that the logged-in Nx_Port has requested the FC-Port to support and the FC-Port has granted the request.
Class2 RxDataSize	The Class 2 Receive Data Field Size of the logged-in Nx_Port. Specifies the largest Data Field Size for an FT_1 frame that can be received by the Nx_Port.
Class2 SeqDeliv	Whether the FC-Port has agreed to support Class 2 sequential delivery during the Fabric Login. This is meaningful only if Class 2 service has been agreed. This is applicable only to Fx_Ports.
Class3 RxDataSize	The Class3 Receive Data Field Size of the logged-in Nx_Port. Specifies the largest Data Field Size for an FT_1 frame that can be received by the Nx_Port.
Class3 SeqDeliv	Whether the FxPort has agreed to support Class 3 sequential delivery during the Fabric Login. This is meaningful only if Class 3 service has been agreed. This is applicable only to Fx_Ports.

FC Interfaces ELP

Field	Description
Neighbor Port	The port world wide name of the peer Interconnect_Port.
Neighbor Switch	The node world wide name of the peer Node.
BBCredit Rx	The maximum number of receive buffers available for holding Class 2, Class 3, Class F frames received from the peer Interconnect_Port. It is for buffer-to-buffer flow control in the incoming direction from the peer Interconnect_Port to local Interconnect_Port. The buffer-to-buffer flow control mechanism is indicated in the respective BbCreditModel.

Field	Description
BBCredit Tx	The total number of buffers available for holding Class 2, Class 3, Class F frames to be transmitted to the peer Interconnect_Port. It is for buffer-to-buffer flow control in the direction from the local Interconnect_Port to peer Interconnect_Port. The buffer-to-buffer flow control mechanism is indicated in the corresponding BbCreditModel.
CoS	The classes of services that the peer Interconnect_Port has requested the local Interconnect_Port to support and the local Interconnect_Port has granted the request.
Class2 SeqDeliv	Whether the local Interconnect_Port has agreed to support Class 2 sequential delivery during the Exchange Link Parameters Switch Fabric Internal Link Service request. This is meaningful only if Class 2 service has been agreed.
Class2 RxDataSize	The Class 2 Receive Data Field Size of the peer Interconnect_Port. Specifies the largest Data Field Size for an FT_1 frame that can be received by the Interconnect_Port. This is meaningful only if Class 2 service has been agreed.
Class3 SeqDeliv	Whether the local Interconnect_Port has agreed to support Class 3 sequential delivery during the Exchange Link Parameters Switch Fabric Internal Link Service request. This is meaningful only if Class 3 service has been agreed.
Class3 RxDataSize	The Class 3 Receive Data Field Size of the peer Interconnect_Port. Specifies the largest Data Field Size for an FT_1 frame that can be received by the Interconnect_Port. This is meaningful only if Class 3 service has been agreed.
ClassF X_ID	When true indicates that the peer Interconnect_Port supplying this parameter requires that an interlock be used during X_ID assignment in Class F. This is meaningful only if Class F service has been agreed.
ClassF RxDataSize	The Class F Receive Data Field Size of the peer Interconnect_Port. Class F service is always agreed between two Interconnect_Ports. Specifies the largest Data Field Size for an FT_1 frame that can be received by the Interconnect_Port.
ClassF ConSeq	The number of sequence status blocks provided by the Interconnect_Port supplying the parameters for tracking the progress of a sequence as a sequence recipient. The maximum number of concurrent sequences that can be specified is 255. A value of N/A in this field is reserved.
ClassF EECredit	The maximum number of Class F data frames which can be transmitted by an Interconnect_Port without receipt of accompanying ACK or Link_Response frames. The minimum value of end-to-end credit is one. The end-to-end credit field specified is associated with the number of buffers available for holding the Data_Field of a Class F frame and processing the contents of that Data_Field by the Interconnect_Port supplying the parameters.

Field	Description
ClassF OpenSeq	The open sequences per exchange shall specify the maximum number of sequences that can be open at one time at the recipient between a pair of Interconnect_Ports for one exchange. This value is used for exchange and sequence tracking.

FC Interfaces Trunk Config

Field	Description
Admin	The trunking mode configured by the user. • When set to nonTrunk, the port negotiates and converts the link into non-trunking mode. This port and the peer port's OperTrunkMode will not carry multiple VSAN traffic. • When set to trunk, the port negotiates and converts the link into trunking mode only if the peer port is trunk or auto. • When set to auto, the port is willing to convert the link to a trunk link only if the peer port is trunk.
Oper	The current trunking mode of the port.
Allowed VSANs	The list of VSANs which are allowed to be received/transmitted on the port when the port is operating in trunking mode. Only ports operating in trunk mode can belong to multiple VSANs.
Up VSANs	The list of VSANs whose operational state is up, that this port is associated with. Only ports operating in trunk mode can be associated to multiple VSANs. This is applicable to only ports operating in trunk mode.

FCIP Interfaces Trunk Failures

Field	Description
FailureCause	An entry is shown in this table if there is an error in the trunk status for the given VSAN.

FC Interfaces IP

Field	Description
Switch	The name of the switch.
Ethernet Interface	A unique value that identifies the ethernet interface.
Ethernet Status	The current operational state of the ethernet interface.
Ethernet IP Address	The Internet address for this entity.
Peer IP Address	The Internet address for this entity
Port	The Port ID string as reported in the most recent CDP message.

Field	Description
Peer Interface	A unique value that identifies the peer interface on this device to which this link pertains.
Peer Device Id	The Peer Device ID string as reported in the most recent CDP message.
IP Security Enabled	Specifies whether the IP Security is turned on or not.

FC Interfaces Physical

Field	Description
BeaconMode	If enabled, an interface LED is put into flashing mode for easy identification of a particular interface.
ConnectorPresent	If true, there is a physical connector.
ConnectorType	The module type of the port connector.
TransmitterType	The technology of the port transceiver.
Vendor	The connector unit vendor.
PartNumber	The connector unit part number.
Revision	The port revision of the connector unit.
SerialNo	The serial number of the connector unit.

FC Interfaces Capability

Field	Description
FC-PH Vers Low	The lowest version of FC-PH that the FC-Port is capable of supporting.
FC-PH Vers High	The highest version of FC-PH that the FC-Port is capable of supporting.
RxDataSize Min	The minimum size in bytes of the Data Field in a frame that the FC-Port is capable of receiving from its attached FC-port.
RxDataSize Max	The maximum size in bytes of the Data Field in a frame that the FC-Port is capable of receiving from its attached FC-port.
HoldTime Min	The minimum holding time (in microseconds) that the FC-Port is capable of supporting.
HoldTime Max	The maximum holding time (in microseconds) that the FC-Port is capable of supporting.
CoS	The Bit mask indicating the set of Classes of Service that the FC-Port is capable of supporting.
ServiceStateCapable	Indicates whether this interface is capable of handling service state change.
PortRateMode Capable	Indicates whether this interface is capable of being configured as dedicated or shared port rate modes.

Field	Description
AdminRxBbCreditExtendedCapable	If true, it is capable of changing the extended buffer-to-buffer credits on the interface. The user can configure the object fcIfAdminRxBbCreditExtended on this interface
Class2Seq Deliv	The flag indicating whether or not the FC-Port is capable of supporting Class 2 Sequential Delivery.
Class3Seq Deliv	The flag indicating whether or not the FC-Port is capable of supporting Class 3 Sequential Delivery.

FC Interfaces FICON Peer

Field	Description
TypeNumber	The type number of the peer node. For example, the type number could be 002105.
SerialNumber	The sequence number assigned to the peer node during manufacturing. For example, the serial number could be 000000023053.
Tag	The identifier of the port in the peer node connected to this port.
FcId	Address Identifier assigned to NX-Port
Status	Specifies the status of the row, is valid, invalid or old.
Name	Name of this port.
Manufacturer	The name of the company that manufactured the peer node. For example, the manufacturer info could be HTC.
ModelNumber	The model number of the peer node. For example, the model number could be F20.
PlantOfMfg	The plant code that identifies the plant of manufacture of the peer node. For example, the plant code of manufacture could be 00.
UnitType	The type of the peer node that this port is communicating.
Alert	The type of link incident that occurred on this interface.

Interfaces NPorts (SVC)

Field	Description
Pwwn	The WWN (Worldwide Name) of the virtual N-port.
FcId	Fibre Channel Identifier of the virtual N-port.
State	The operational state of the virtual N-port.
DownReason	If the state of the N-port is 'down' as depicted by the instance of State, this value denotes the reason why this N-port is 'down'.

Interfaces Sessions

Field	Description
NportPwwn	The WWN of the N-port that belongs to this session.
PeerPwwn	The WWN of the remote N-port for this session.
PeerNwwn	The WWN of the remote N-port for this session.
PeerFcId	Fibre Channel Identifier of the remote port for this session.

IP Statistics TCP

Field	Description
AttemptFails	The number of times TCP connections have made a direct transition to the CLOSED state from either the SYN-SENT state or the SYN-RCVD state, plus the number of times TCP connections have made a direct transition to the LISTEN state from the SYN-RCVD state.
InErrs	The total number of segments received in error (e.g., bad TCP checksums).
ActiveOpens	The number of times TCP connections have made a direct transition to the SYN-SENT state from the CLOSED state.
PassiveOpens	The number of times TCP connections have made a direct transition to the SYN-RCVD state from the LISTEN state.
EstabResets	The number of times TCP connections have made a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE-WAIT state.
InSegs	The total number of segments received, including those received in error. This count includes segments received on currently established connections.
OutSegs	The total number of segments sent, including those on current connections but excluding those containing only retransmitted bytes.
RetransSegs	The total number of segments retransmitted - that is, the number of TCP segments transmitted containing one or more previously transmitted bytes.
OutRsts	The number of TCP segments sent containing the RST flag.

Port Channels Ethernet Interfaces

Field	Description
Description	Alias name for the interface as specified by a network manager.
Mtu	The size of the largest frame which can be sent/received on the interface, specified in bytes.
PhysAddress	The interface's address at its protocol.
Admin	The desired state of the interface.

Field	Description
Oper	The current operational state of the interface.
LastChange	When the interface entered its current operational state. If the current state was entered prior to the last re-initialization of the local network management subsystem, then this value is N/A.
IPAddress/Mask	The IP address and mask of the interface.
iSCSI AuthMethod	The authentication method for this interface.
iSNS ProfileName	The iSNS server profile name for this interface.

Port Channels FC Interfaces

Field	Description
PortVsan	VSAN to which this interface is statically assigned.
Description	Alias name for the interface as specified by a network manager.
Admin Mode	The port mode configured by the user. If the user configured the port as auto(1), then the port initialization scheme determines the mode of the port. In this case the user can look at OperMode to determine the current operating mode of port. Only auto(1) or ePort(4) is allowed.
Oper Mode	The current operating mode of the port.
Admin Speed	The port speed configured by the user.
Oper Speed	The interface's current bandwidth per second.
Admin Status	The desired state of the interface.
Oper Status	The current operational state of the interface.
FailureCause	The cause of current operational state of the port.
LastChange	The time the interface entered its current operational state. If the current state was entered prior to the last re-initialization of the switch, then this is a zero or N/A value.

Port Channels General

Field	Description
Admin Mode	The channel mode desired by the network manager.
Oper Mode	The current operating channel mode of the port.

Field	Description
Force	The method to add port(s) to a Port Channel port. ▪ If unchecked, then a compatibility check is done on the parameters of the port(s) being added to this Port Channel. The port(s) being added must have the same physical and configured parameters as the Port Channel port. ▪ If checked, a compatibility check is done on only physical parameters. The port(s) being added to this Port Channel port must have same physical parameters. The operation will fail only if the physical parameters are not same. The configured parameters of the port(s) being added are overwritten by configured parameters of this Port Channel port.
MemberList By Interface	The list of the E_ports that are members of this Port Channel port.
MemberList By FICON	The list of the E_ports that are members of this Port Channel port.
MemberList LoadBalanced	Those ports which are actively participating in the PortChannel.
LastAction Status	The status of the last operation (add or remove a member) done to change the member list of a Port Channel Port. When no ports are added or the last operation is successful then this value is successful. If this value is failed then the user can look at LastAddStatusCause to find the reason of failure.
LastAction FailureCause	The cause of failure to last operation (add or remove a member) done to change the member list of a Port Channel port.
LastAction Time	The timestamp indicating the time of last action performed on this entry.
CreationTime	The timestamp of this entry’s creation time.
FICON Address	The FICON port address. If empty, then this channel is not used by FICON. (This column is displayed if FICON is enabled. This column is grayed out if the Port Channel is auto-created.)

FlexAttach Global

Field	Description
VirtualPwwnauto	Enables automatic generation of Virtual WWNs on all the F_port interfaces. If the value of VirtualPWWNauto is set to 'true', the value of VirtualWWN Auto of all the entries in the VirtualWWN table is implicitely set to true.

FlexAttach Virtual PWWN

Field	Description

virtual pWWN	This is the virtual port WWN for this interface. If the value of VirtualWwnAuto is 'true', then value of this virtual pWWWN is automatically generated by the device.If value of this pWWWN is set explicitely, then value of VirtualWwnAuto is implicitely set to 'false'. If length of pWWWN is zero, then automatic virtual WWN generation is disabled. This pWWWN can not be set to length zero
Auto	Enable automatic generation of Virtual WWNs on this interface.If the value of VirtualWwnPwwn is set explicitely, then the value of Auto will be implicitely set to false. Also, if this Auto is set to 'true', then value of VirtualWwnPwwn is overwritten with auto generated virtual port WWN.
LastChange	The value of sysUpTime at the time of the last change to this Virtual WWN Entry.

FlexAttach Physical to Virtual WWNs

Field	Description
virtual pWWN	This is the virtual port WWN for this device port WWN. In order to minimize WWN collision, no two instances of this Virtual pWWN can have same value. **Note** :The Virtual pWWN cannot be changed when corresponding device is logged in.
LastChange	The value of sysUpTime at the time of the last change to this Virtual WWN Entry.

FIPS

Field	Description
ModeActivation	To enable/disable FIPS mode on the device. FIPS 140-2 is a set of security requirements for cryptographic modules and it details the U.S. Government requirements for cryptographic modules. A module will comprise both hardware and software, eg a datacenter switching or routing module. The module is said to be in FIPS enabled mode when a request is recieved to enable the FIPS mode and a set of self-tests are successfully run in response to the request. If the self-tests fail, then an appropriate error is returned

FCIP FICON Configuration

Field	Description
Interface	This is a unique value that identifies the interface on this FCIP device to which this link pertains.
VSAN List Admin	This is the list of VSANs (in the range 1 through 2047) for which Ficon Tape Acceleration is configured. Only VSANs with a cficonVsanEntry of CISCO-FICON-MIB present can be configured for Ficon Tape Acceleration.

Field	Description
VSAN List Oper	This is the list of VSANs (in the range 1 through 2047) for which Ficon Tape Acceleration is operationally " ON" .

Port Channels AutoCreate

Field	Description
Channel	The channel group mode of this PortChannel.
Persistent	True if the PortChannel is persistent.

SPAN Sessions

Field	Description
Dest Interface	The Span Destination port interface.
Filter VSAN List	The VSANs that are assigned to this session.
Status Admin	Suspend an active session or activate an inactive session.
Status Oper	The current state of the session.
Description	The description of the session status.
VSAN List	The VSANs that are assigned to this session.
Or Interface (Direction)	The destination port ID to be configured for the session.
Inactive Reason	Description of the reason why this session is not active.

Span Global

Field	Description
MaxQueuedSpanPackets	This field specifies the drop threshold packets for all span sessions.The MaxQueuedSpanPackets field is only available when no session is active.

SPAN Source Interfaces

Field	Description
Interface, Direction	The destination port ID configured for the session, and the direction of traffic.

Port Tracking Dependencies

Field	Description
Linked, Destination Interfaces	The interfaces that are doing the tracking.

Field	Description
VSAN Type	Whether a single VSAN or all VSANs are being tracked.
VSAN ID	If a single VSAN is being tracked, the ID of that VSAN.

Port Tracking Force Shut

Field	Description
Interface	The interface of the port to be configured for the forced-shut mode.
Force Shut	If true, the port is brought down administratively, and you must bring the port up manually. If false, the port is brought down operationally only, and is brought up again as soon as any one of the tracked ports comes up.

Port Guard

Field	Description
Interface	Name of the interface
Enable	Specifies whether an interface can be stopped from changing between up and down states or allowed to change states continuously.
Duration (sec)	Specifies the time duration in which a port is allowed to change states.
Number of Flaps	Specifies the number of times the port can flap in the time specified in the Duration.
Oper	Operational state of the interface.

Bandwidth Reservation: 48-Port 96-Gbps Fibre Channel module

RateMode Config Macro	Description
Dedicated 4 Gbps on the first port of each group and the remaining ports 8 Gbps shared	Allocates a rate mode and admin speed of 4 Gbps on the first port of each group and the remaining ports share 8 Gbps depending on the operational speed of the ports
Dedicated 8 Gbps on the first port of each group and the remaining ports 8 Gbps shared	Allocates a rate mode and admin speed of 8 Gbps on the first port of each group and the remaining ports share 8 Gbps depending on the operational speed of the ports
Shared 8 Gbps on all ports (initial & default settings)	Allocates a rate mode and admin speed of 8 Gbps on all the available ports. This is the default setting.

Bandwidth Reservation: 48-Port 48-Gbps Fibre Channel module

RateMode Config Macro	Description
Dedicated 2 Gbps on the first port of each group and the remaining ports 4 Gbps shared	Allocates a rate mode and admin speed of 2Gbps on the first port of each group and the remaining ports share 4 Gbps depending on the operational speed of the ports
Dedicated 8 Gbps on the first port of each group and the remaining ports 4 Gbps shared	Allocates a rate mode and admin speed of 8 Gbps on the first port of each group and the remaining ports share 4 Gbps depending on the operational speed of the ports
Shared Auto with Maximum of 4 Gbps on all ports (initial & default settings)	Allocates a maximum rate mode and admin speed of 4Gbps on all the available ports. This is the default setting.

Bandwidth Reservation: 24-Port 48-Gbps Fibre Channel module

RateMode Config Macro	Description
Dedicated 8 Gbps on the first port of each group and the remaining ports 8G shared	Allocates a rate mode and admin speed of 8Gbps on the first port of each group and the remaining ports share 8 Gbps depending on the operational speed of the ports
Shared Auto on all ports (initial & default settings)	Allocates a rate mode and admin speed of 8 Gbps on all the available ports. This is the default setting.

Bandwidth Reservation: 48-Port 256-Gbps Fibre Channel module

RateMode Config Macro	Description
Dedicated 8 Gbps on the first 4 ports in each 6-port port group and the remaining ports 8G shared	Allocates a rate mode and admin speed of 8Gbps on the first 4 ports in each 6-port port group and the remaining ports share 8 Gbps depending on the operational speed of the ports.

RateMode Config Macro	Description
Dedicated 8 Gbps on the first port of each group and the remaining ports 8G shared	Allocates a rate mode and admin speed of 8 Gbps on the first port of each group and the remaining ports share 8 Gbps depending on the operational speed of the ports.
Shared 8G 0n all ports	Allocates a rate mode and admin speed of 8 Gbps on all the available ports. This is the default setting.
Dedicated 4G 0n all ports	Allocates a rate mode and admin speed of 4Gbps on all the available ports.
Dedicated 10G on following ports: • 4,5,6,7,8,10 (ports 1,2,3,9,11,12 disabled) • 16, 17, 18, 19, 20, 22 (ports 13,14,15, 21,23,24 disabled) • 28,29,30,31,32,34 (ports 25,26,27,33,35,36 disabled) • 40,41,42,43,44,46 (ports 37,38, 39 45, 47, 48 disabled)	Allocates a rate mode and admin speed of 10Gbps on the following ports.

Bandwidth Reservation: 32-Port 256-Gbps Fibre Channel module

RateMode Config Macro	Description
Dedicated 8 Gbps on on all ports	Allocates a rate mode and admin speed of 8 Gbps on all the available ports.
Shared 8 Gbps on on all ports – initial and default settings.	Allocates a rate mode and admin speed of shared 8 Gbps on all the available ports.

RateMode Config Macro	Description
Dedicated 10G on following ports: • 2,3,4,5,6,8 (ports 1 and 7 disabled) • 10,11,12,13,14,16 (ports 9 and 15 disabled) • 18,19,20,21,22,24 (ports 17 and 23 disabled) • 26,27,28,29,30,32 (ports 25 and 31 disabled)	Allocates a rate mode and admin speed of 10Gbps on the specified ports.

DS-X9448-768K9 (Luke) Line Card Bandwidth Reservation

RateMode Config Macro	Description
Dedicated 10G on the following ports: • Ports 1-8 • Ports 9-16 • Ports 17-24 • Ports 25-32 • Ports 33-40 • Ports 41-48	Allocates dedicated rate mode and admin speed of 10 Gbps on the specified ports.
Unconfigure 10G on the following ports: • Ports 1-8 • Ports 9-16 • Ports 17-24 • Ports 25-32 • Ports 33-40 • Ports 41-48	Reverts to default rate mode and admin speed on the specified ports. Transceiver frequencey is set to FC. This operation is disruptive.

FC

This section provides information on the following areas:

- VSAN General
- VSAN Membership
- VSAN Interop-4 WWN
- VSAN Timers
- VSAN Default Zone Policies
- IVR Local Topology
- IVR Fabric ID
- IVR Default Fabric ID
- IVR Action
- IVR RDI VSANs
- IVR Active Topology
- IVR Zoneset Status
- IVR Discrepancies
- IVR Domains
- IVR FCID
- IVR Zoneset Active Zones
- IVR Zoneset Active Zones Attributes
- IVR Zoneset Name
- DPVM Actions
- DPVM Config Database
- DPVM Active Database
- Domain Manager Running
- Domain Manager Configuration
- Domain Manager Domains
- Domain Manager Statistics
- Domain Manager Interfaces
- Domain Manager Persistent FcIds
- Domain Manager Allowed DomainIds
- Zoneset Active Zones
- Zoneset Unzoned
- Zoneset Status
- Zoneset Policies
- Zoneset Active Zones Attributes

- Zoneset Enhanced
- Zoneset Read Only Violations
- Zoneset Statistics
- Zoneset LUN Zoning Statistics
- Zoneset Members
- Fabric Config Server Discovery
- Fabric Config Server Interconnect Elements
- Fabric Config Server Platforms (Enclosures)
- Fabric Config Server Fabric Ports
- FC Routes
- FDMI HBAs
- FDMI Ports
- FDMI Versions
- Flow Statistics
- FCC
- Diagnostics
- FSPF General
- FSPF Interfaces
- FSPF Interface Stats
- SDV Virtual Devices
- SDV Real Devices
- LUN Discover
- LUN Targets
- LUNs
- Device Alias
- Device Alias Configuration
- Device Alias Mode
- Device Alias Discrepancies
- Name Server General
- Name Server Advanced
- Name Server Proxy
- Name Server Statistics
- Preferred Path Maps and Routes
- Preferred Path Maps Active
- Preferred Path All Match Criteria
- Preferred Path Active Match Criteria

- Preferred Path All Sets
- RSCN Nx Registrations
- RSCN Multi-PID Support
- RSCN Event
- RSCN Statistics
- Multicast Root
- QoS Policy Maps
- QoS Class Maps
- QoS Match Statements
- QoS Class Maps by Policy Maps
- QoS Policy Maps by VSAN
- QoS DWRR
- QoS Rate Limit
- Timers and Policies
- WWN Manager
- NPV Traffic Map
- NPV Load Balance
- NPV External Interface Usage
- NP Link

VSAN General

Field	Description
Name	The name of the VSAN. Note that default value will be the string VSANxxxx where xxxx is value of vsanIndex expressed as 4 digits. For example, if vsanIndex is 23, the default value is VSAN0023.
Mtu	The MTU of the VSAN. Normally, this is 2112.
LoadBalancing	The type of load balancing used on this VSAN. • srcdst - use source and destination ID for path selection • srcdst 0xId - use source, destination, and exchange IDs
InterOp	The interoperability mode of the local switch on this VSAN. • standard • interop-1 • interop-2 • interop-3
AdminState	The state of this VSAN.
OperState	The operational state of the VSAN.

Field	Description
InOrderDelivery	The InorderDelivery guarantee flag of device. If true, then the inorder delivery is guaranteed. If false, it is not guaranteed.
DomainId	Specifies an insistent domain ID.
FICON	True if the VSAN is FICON-enabled.
Network Latency	Network latency of this switch on this VSAN. This is the time interval after which the frames are dropped if they are not delivered in the order they were transmitted.

VSAN Membership

Field	Description
Switch	Name of the switch
Ports	FC Ports in VSAN
Channels	PortChannels in VSAN
FCIP	FCIP Interfaces in VSAN
iSCSI	iSCSI Interfaces in VSAN
FICON	Interfaces in VSAN by FICON
FC Virtual Interface	Virtual FC interfaces in VSAN

VSAN Interop-4 WWN

Field	Description
VSAN ID	The ID of the VSAN containing the McData switch.
WWN	The WWN of the McData switch.

VSAN Timers

Field	Description
VSAN Id	The ID of the VSAN.
R_A_TOV	The Resource_Allocation_Timeout Value used for FxPorts as the timeout value for determining when to reuse an NxPort resource such as a Recovery_Qualifier. It represents E_D_TOV plus twice the maximum time that a frame may be delayed within the Fabric and still be delivered. Note that all switches in a fabric should be configured with the same value of this timeout.
D_S_TOV	The Distributed_Services_Timeout Value which indicates that how long a distributed services requestor will wait for a response.

Field	Description
E_D_TOV	The Error_Detect_Timeout Value used for FxPorts as the timeout value for detecting an error condition. Note that all switches in a fabric should be configured with the same value of this timeout. Note that value must be less than value of D_S_TOV.
NetworkDropLatency	Network latency of this switch on this VSAN.

VSAN Default Zone Policies

Field	Description
Zone Behavior	Represents the initial value for default zone behavior on a VSAN when it is created. If a VSAN were to be deleted and re-created again, the default zone behavior will be set to the value specified for this object.
Propagation Mode	Represents the initial value for zone set propagation mode on a VSAN when it is created. If a VSAN were to be deleted and re-created again, the zone set propagation mode will be set to the value specified for this object.

IVR Local Topology

Field	Description
VSAN List	The list of configured VSANs that are part of IVR topology on this device.

IVR Fabric ID

Field	Description
VSAN List	The list of configured VSANs that are part of IVR topology on this device.

IVR Default Fabric ID

Field	Description
Fabric Id	The configured Default Autonomous Fabric ID of this switch.

IVR Action

Field	Description
Activate Local Topology	Setting this object to activate is a request for the configured IVR topology to be activated on this device. i.e., for the current configuration of IVR topology to be cloned, with the clone becoming the active IVR topology.
IsActive	This object indicates of IVR topology is active or not. If true, the IVR topology is active. If false, the IVR topology is not active.

Field	Description
Activation Time	When the IVR topology was most recently activated. If the IVR topology has not been activated prior to the last re-initialization of the local network management system, then this value will be N/A.
Enable IVR NAT	Enable FCID and VSAN identifier translation across VSAN boundaries. If true, the VSAN identifier as well as the entire FCID of the end devices would be modified as frames cross VSAN boundaries.
Auto Discover Topology	Enable automatic VSAN topology discovery. If true, automatic VSAN topology discovery is turned on. IVR processes would communicate with each other to provide a global view of the physical topology to all the IVR enabled switches. If false, automatic VSAN topology discovery is turned off.

IVR RDI VSANs

Field	Description
Add Virtual Domain to FC Domain List	This object lists VSANs in which the virtual domains in a VSAN are added to the domain list in that VSAN.

IVR Active Topology

Field	Description
VSAN List	The list of VSANs that are part of IVR topology on this device.

IVR Zoneset Status

Field	Description
Status	Status of the active IV Zoneset on this VSAN.

- idle – Idle
- active – Active
- deactive – Deactive
- defaultZoneDeny – Activation failed because of default zone behavior is deny and there is no regular active zoneset.
- activationFailed – Activation failed
- deactivationFailed – Deactivation failed
- activationNotInitiated – Activation not initiated
- activationFailedFabricChgFailed – Activation failed because of fabric change failed.
- deactivationNotInitiated – Deactivation not initiated.
- deactivationFailedFabChgFailed – Deactivation failed because of fabric change failed.
- deactivationNotInitiated – Deactivation not initiated.
- deactivationFailedFabChgFailed – Deactivation failed because of fabric changing.
- activating – Activation in progress.
- activatingWaitForLowestSwwn – Activation in progress; waiting for the lowest switch WWN switch to add IV zoneset to the regular active zoneset.
- activatingFabricChanging – Activation in progress; fabric is changing.
- deactivating – Deactivation in progress.
- deactivatingWaitForLowestSwwn – Deactivation in progress; waiting for the lowest switch WWN switch to delete IVR zoneset from the regular active zoneset.
- deactivatingFabricChanging – Deactivation in progress; fabric is changing.
- defaultZonePermit – Activation failed because of default zone behavior is permit.
- defaultZonePermitNoForce – Activation failed because of default zone behavior is permit with no force option.
- defaultZonePermitActZsNoForce – Activation failed because of default zone behavior is permit and with regular activate zoneset and no force option.
- denyNoActiveZoneset – Activation failed because there is no active zoneset.
- activationFailedLowestWwnWait – Activation failed waiting for the switch with lowest wwn to activate this zoneset.
- deactivationFailedLowestWwnWait – Deactivation failed waiting for switch with lowest wwn to deactivate this zoneset.
- activationFailedZoneNmCtnsIlChar – Activation fails because one of the zone names in zoneset that is being activated contains illegal character.

IVR Discrepancies

Field	Description
Discrepancy	The checksum of the enforced (active) IV zoneset.
RegionID	Identifies the CFS configuration supported region.

IVR Domains

Field	Description
Domain Id	The FC domain ID that will be used to represent the VSAN.

IVR FCID

Field	Description
FCID	The FCID to be used by IVR to represent the device.

IVR Zoneset Active Zones

Field	Description
VSAN Id	IVR VSAN ID.
Zone	Active IVR zone name.
Fabric Id	Autonomous fabric ID.
Switch Interface	Switch interface to which the zone member is connected to.
Name	Zone member name.
WWN	Zone member WWN.
FcId	Zone member FC ID.
LUNs	Zone member LUN.
Status	• Not in Fabric: If zone member is not in the fabric. • Not in VSAN: If zone member is not present in the VSAN. • n/a: Cannot determine status. • Empty: Member is present in fabric and correct VSAN and can communicate with other members of the zone.

IVR Zoneset Active Zones Attributes

Field	Description
Zone	Active IVR zone name.
QoS	True if QoS enabled, otherwise false.
QoS Priority	QoS priority value (Low, Medium, or High).
Broadcast	Specifies if broadcast zoning is enabled on this default zone on this VSAN. If true, then it is enabled. If false, then it is disabled.

IVR Zoneset Name

Field	Description
VSAN Id	IVR VSAN ID.
Zone	Active IVR zone name.
Fabric Id	Autonomous fabric ID.
Switch Interface	Switch interface to which the zone member is connected to.
Name	Zone member name.
WWN	Zone member WWN.
FcId	Zone member FC ID.
Luns	Zone member LUN.
Status	• Not in Fabric: If zone member is not in the fabric. • Not in VSAN: If zone member is not present in the VSAN. • n/a: Cannot determine status. • Empty: Member is present in fabric and correct VSAN and can communicate with other members of the zone.

DPVM Actions

Field	Description
Action	Helps in activating the set of bindings.
Result	Indicates the outcome of the activation.
Status	Indicates the state of activation. If true, then activation has been attempted as the most recent operation. If false, then an activation has not been attempted as the most recent operation.
CopyActive to Config	When set to copy(1), results in the active (enforced) binding database to be copied on to the configuration binding database. The learned entries are also copied.
Auto Learn Enable	Helps to learn the configuration of devices logged into the local device on all its ports and the VSANs to which they are associated.
Auto Learn Clear	Assists in clearing the auto-learnt entries.
Clear WWN	Represents the Port WWN (pWWN) to be used for clearing its corresponding auto-learnt entry.

DPVM Config Database

Field	Description
Switch	Name of the switch.
Type	Specifies the type of the corresponding instance of device.
WWN or Name or MAC	Represents the logging in device. The value depends on the corresponding device type (PWWN, NWWN or MAC).

Field	Description
VSAN Id	Represents the VSAN to be associated to the port on the local device on which the device represented by cdpvmLoginDev logs in.
Switch Interface	Represents the device alias.

DPVM Active Database

Field	Description
Type	Specifies the type of the corresponding instance of cdpvmEnfLoginDev.
WWN or Name or MAC	Represents the logging in device. The value depends on the corresponding device type (PWWN, NWWN or MAC).
VSAN Id	Represents the VSAN of the port on the local device through which the device represented by cdpvmEnfLoginDev logs in.
Interface	Represents the device alias.
IsLearnt	Indicates whether this is a learnt entry or not. If true, then it is a learnt entry. If false, then it is not.

Domain Manager Running

Field	Description
State	The state of the Domain Manager on the local switch on this VSAN.
DomainId	The Domain ID of the local switch on this VSAN or 0 if no Domain ID has been assigned.
Local Switch WWN	The WWN of the local switch on this VSAN.
Local Priority	The running priority of the local switch on this VSAN.
Principal Switch WWN	The WWN of the principal switch on this VSAN, or empty string if the identity of the principal switch is unknown.
Principal Priority	The running priority of the principal switch on this VSAN.

Domain Manager Configuration

Field	Description
Enable	Enables the Domain Manager on this VSAN. If enabled on an active VSAN, the switch will participate in principal switch selection. If disabled, the switch will participate in neither the principal switch selection nor domain allocation. Thus, Domain ID needs to be configured statically.

Field	Description
Running DomainId	The configured Domain ID of the local switch on this VSAN or 0 if no Domain ID has been configured. The meaning depends on DomainIdType. If Type is 'preferred', then domain ID configured is called 'preferred Domain ID'. The valid values are between 0 and 239. In a situation where this domain could not be assigned, any domain ID would be acceptable. The value '0' means any domain ID. • If Type is 'static' (insistent), then domain ID is called 'static Domain ID' and valid values are between 1 and 239. In a situation where this domain was non-zero but could not be assigned, no other domain ID would be acceptable. • If the Domain Manager is enabled on the VSAN, then a RDI (Request Domain ID) will be sent requesting this Domain ID. • If no Domain ID can be granted in the case of 'preferred' or if the configured 'static' (insistent) domain ID cannot be not granted then, it is an error condition. When this error occurs, the E_ports on that VSAN will be isolated. If the domain manager is not enabled, then the static (insistent) Domain ID is assumed to be granted, if it has been configured (to a valid number). • If either of the domain IDs are not configured with a non-zero value on this VSAN and if the domain manager is not enabled, then - switch will isolate all of its E_ports on this VSAN.
DomainId Type	Type of configured Domain ID.
FabricName	The WWN that is used for fabric logins on this VSAN. This is used only if Enable is false. If Enable is true, then principal switch WWN is used. It is automatically set to the default value when set to zero-length value.
Priority	Priority of the switch to be used in principal switch selection process.
Contiguous Allocation	Determines how the switch behaves when elected as the principal switch. If true, switch won't accept non-contiguous domain IDs in RDIs and will try to replace all the Domain IDs in the list with contiguous domain IDs if a RDI for a contiguous Domain ID can not be fulfilled. If false, then the switch acts normally in granting the Domain IDs even if they are not contiguous.
Auto Reconfigure	Determines how the switch responds to certain error conditions. The condition that can cause these errors is merging of two disjoint fabrics that have overlapping Domain ID list. If true, the switch will send a RCF (ReConfigureFabric) to rebuild the Fabric. If false, the switch will isolate the E_ports on which the errors happened.
Persistent FcId	If true, then all the FC ID assigned on this VSAN are made persistent on this VSAN. If false, then all the entries on VSAN in PersistencyTable are deleted.
Purge FcIds?	Tells the Domain Manager to purge the FC IDs on this VSAN in the FC ID persistency database.

Field	Description
Restart?	Tells the Domain Manager to rebuild the Domain ID tree all over again. If 'disruptive', then a RCF (ReConfigure Fabric) is generated in the VSAN in order for the fabric to recover from the errors. If nonDisruptive, then a BF (Build Fabric) is generated in the VSAN.
Optimization	You need to click the field to select one of the following. To disable turbo mode, do not select anything. • Fast-Restart- Set the optimization type to fast restart. • Selective-Restart- Set the optimization type to selective restart.

Domain Manager Domains

Field	Description
SwitchWWN	The WWN of the switch to which the corresponding value of DomainId is currently assigned for the particular VSAN.

Domain Manager Statistics

Field	Description
Prin. Sel Total	The number of principal switch selections on this VSAN.
Prin. Sel Local	The number of times the local switch became the principal switch on this VSAN.
Fabric Builds (BF)	The number of BuildFabrics (BFs) that have occurred on this VSAN.
Fabric Reconfigures (Rcf)	The number of ReconfigureFabrics (RCFs) that have occurred on this VSAN.
FcIds Free	The number of FC IDs that are unassigned on this VSAN.
FcIds Assigned	The number of FC IDs that are assigned on this VSAN.
FcIds Reserved	The number of FC IDs that are reserved on this VSAN.

Domain Manager Interfaces

Field	Description
Role	One of the following: • nonPrincipal - non-principal interface • principalUpstream - upstream principal interface • principalDownsteam - downstream principal interface • isolated - isolated interface • down - down interface unknown • unknown - unknown interface

Field	Description
RcfReject	Determines if the incoming ReConfigure Fabric (RCF) messages on this interface on this VSAN is accepted or not. If true, then the incoming RCF is rejected. If false, incoming RCF is accepted. Note that this does not apply to the outgoing RCFs generated by this interface.

Domain Manager Persistent FcIds

Field	Description
FcId	The FC ID assigned for this WWN on this VSAN. The third octet must be 0x00 if value of PersistencyNum is area.
Mask	The number of FC IDs starting from PersistencyFcId which are assigned either statically or dynamically for this WWN on this VSAN. The value one means just one FC ID is assigned. The value area means all the FC IDs in the area that is specified in the second octet of FcId are assigned. Typically, 256 FC IDs are assigned for an area. This value cannot be changed if the value of Used is true.
Used	Indicates if this FC ID is used or not.
Assignment	The type of persistency of this FC ID.

Domain Manager Allowed DomainIds

Field	Description
List	Provides the lists of domains that are allowed. A domain is allowed in this VSAN if the corresponding bit has a value of 1. If it has a value which is less than 32 bytes long, then the domains which are not represented are not considered to be in the list. If this object is a zero-length string, then no domains are allowed in this VSAN.

Zoneset Active Zones

Field	Description
Zone	Zone name.
Type	Zone member type.
Switch Interface	Switch interface to which the zone member is connected to.
Name	Zone member name.
WWN	Zone member WWN.
FcId	Zone member FC ID.
LUNs	Zone member LUN.

Field	Description
Status	• Not in Fabric: If zone member is not in the fabric. • Not in VSAN: If zone member is not present in the VSAN. • n/a: Cannot determine status. • Empty: Member is present in fabric and correct VSAN and can communicate with other members of the zone.

Zoneset Unzoned

Field	Description
Name	Zone member name.
WWN	Zone member WWN.
FcId	Zone member FC ID.

Zoneset Status

Field	Description
Status	Indicates the outcome of the most recent activation/deactivation.
Activation Time	When this entry was most recently activated. If this entry has been activated prior to the last re-initialization of the local network management system, then this value will be N/A.
FailureCause	The reason for the failure of the zoneset activation/deactivation.
FailedSwitch	The domain ID of the device in the fabric that has caused the Change Protocol to fail.
Active == Local?	Indicates whether the enforced database is the same as the local database on this VSAN. If true, then they are the same. If false, then they are not the same.
Active Zoneset	The name of the enforced IV zoneset.
Hard Zoning	Indicates whether the hard zoning is enabled on this VSAN. Hard zoning is a mechanism by which zoning is enforced in hardware. If true, then hard zoning is enabled on this VSAN. If false, then hard zoning is not enabled on this VSAN.

Zoneset Policies

Field	Description
Default Zone Behavior	Controls the behavior of the default zone on this VSAN. If it is set to permit, then the members of the default zone on this VSAN can communicate with each other. If it is set to deny, then the members of the default zone on this VSAN cannot communicate with each other.

Field	Description
Default Zone ReadOnly	Indicates whether SCSI read operations are allowed on members of the default zone which are SCSI targets, on this VSAN. If true, then only SCSI read operations are permitted. So, this default zone becomes a read-only default zone on this VSAN. If false, then both SCSI read and write operations are permitted.
Default Zone QoS	Specifies whether the QoS attribute for the default zone on this VSAN is enabled. If true, then QoS attribute for the default zone on this VSAN is enabled. If false, then the QoS attribute for the default zone on this VSAN is disabled.
Default Zone QoS Priority	Specifies the QoS priority value.
Default Zone Broadcast	Specifies if broadcast zoning is enabled on this default zone on this VSAN. If true, then it is enabled. If false, then it is disabled.
Propagation	Controls the way zoneset information is propagated during Merge/Change protocols on this VSAN
Read From	Specifies whether the management station wishes to read from the effective database or from the copy database.

Zoneset Active Zones Attributes

Field	Description
Name	Zone name.
Read Only	Indicates if only SCSI read operations are allowed on members of the default zone which are SCSI targets on this VSAN. If true, then only SCSI read operations are permitted. So, this default zone becomes a read-only default zone on this VSAN. If false, then both SCSI read and write operations are permitted.
QoS	Specifies whether the QoS attribute for the default zone on this VSAN is enabled. If true, then QoS attribute for the default zone on this VSAN is enabled. If false, then the QoS attribute for the default zone on this VSAN is disabled.
QoS Priority	Specifies QoS priority value (Low, Medium, or High).
Broadcast	Specifies if broadcast zoning is enabled on this default zone on this VSAN. If true, then it is enabled. If false, then it is disabled.

Zoneset Enhanced

Field	Description
Action	When set to basic(1), results in the zone server operating in the basic mode as defined by FC-GS4 standards. When set to enhanced(2), results in the zone server operating in the enhanced mode as defined by FC-GS4 standards.

Field	Description
Result	The outcome of setting the mode of operation of the local Zone Server on this VSAN.
Config DB Locked By	Specifies the owner for this session.
Config DB Discard Changes	Assists in committing or clearing the contents of the copy database on this session.
Config DB Result	Indicates the outcome of setting the corresponding instance of czseSessionCntl to commitChanges(1).
Enforce Full DB Merge	Controls the zone merge behavior. If this object is set to allow, then the merge takes place according to the merge rules. If set to restrict, then if the merging databases are not exactly identical, the Inter-Switch Link (ISL) between the devices is isolated.
Read From	Specifies whether the management station wishes to read from the effective database or from the copy database.

Zoneset Read Only Violations

Field	Description
Violations	The number of Data protected Check Condition error responses sent by the local Zone Server.

Zoneset Statistics

Field	Description
Merge Req Tx	The number of Merge Request Frames sent by this Zone Server to other Zone Servers in the fabric on this VSAN.
Merge Req Rx	The number of Merge Request Frames received by this Zone Server from other Zone Servers in the fabric on this VSAN.
Merge Acc Tx	The number of Merge Accept Frames sent by this Zone Server to other Zone Servers in the fabric on this VSAN.
Merge Acc Rx	The number of Merge Accept Frames received by this Zone Server from other Zone Servers in the fabric on this VSAN.
Change Req Tx	The number of Change Requests sent by this Zone Server to other Zone Servers in the fabric on this VSAN.
Change Req Rx	The number of Change Requests received by this Zone Server from other Zone Servers in the fabric on this VSAN.
Change Acc Tx	The number of Change Responses sent by this Zone Server to other Zone Servers in the fabric on this VSAN.
Change Acc Rx	The number of Change Responses received by this Zone Server from other Zone Servers in the fabric on this VSAN.
GS3 Rej Tx	The number of GS3 requests rejected by this Zone Server on this VSAN.

Field	Description
GS3 Req Rx	The number of GS3 requests received by this Zone Server on this VSAN.

Zoneset LUN Zoning Statistics

Field	Description
INQUIRY	The number of SCSI INQUIRY commands that have been received by the local zone server.
REPORT LUN	The number of SCSI Report LUNs commands that have been received by the local zone server. Typically the Report LUNs command is sent only for LUN 0.
SENSE	The number of SCSI SENSE commands that have been received by the local zone server.
Other Cmds	The number of SCSI Read, Write, Seek, etc., commands received by the local zone server.
BadInquiry Errors	The number of No LU error responses sent by the local zone server.
Illegal Errors	The number of Illegal Request Check Condition responses sent by the local zone server.

Zoneset Members

Field	Description
Zone	Default zone.
Type	FCID.
Switch Interface	Switch interface to which the zone member is connected to.
Name	Zone member name.
WWN	Zone member WWN.
FcId	Zone member FC ID.
Luns	Zone member LUN.
Status	• Not in Fabric: If zone member is not in the fabric. • Not in VSAN: If zone member is not present in the VSAN. • n/a: Cannot determine status. • Empty: Member is present in fabric and correct VSAN and can communicate with other members of the zone.

Fabric Config Server Discovery

Field	Description
Status	The status of the discovery on the local switch. Initially when the switch comes up, this will be set to databaseInvalid state on all VSANs. This indicates that a discovery needs to be done. The state will be set to inProgress for this VSAN during the discovery. Once the discovery is completed on this VSAN, this will be set to completed. After the discovery is completed for the specified list of VSANs, the data is cached for an interval of time. Once this interval of time expires, the data is lost and this will be set to databaseInvalid state for the specified list of VSANs.
CompleteTime	When the last discovery was completed on this VSAN. This value is N/A before the first discovery on this VSAN.

Fabric Config Server Interconnect Elements

Field	Description
Type	The type of this Interconnect Element.
DomainId	The Domain Id of this Interconnect Element. If the Domain Id has not been configured, then this value is 0.
MgmtId	The management identifier of this Interconnect Element. If the Interconnect Element is a switch, then this will be the Domain Controller identifier of the switch.
FabricName	The fabric name of this Interconnect Element.
LogicalName	The logical name of this Interconnect Element.
Vendor, Model, Release, WWN	The information list corresponding to this Interconnect Element.
MgmtAddrList	The management address list corresponding to this Interconnect Element.

Fabric Config Server Platforms (Enclosures)

Field	Description
Name	The name of this platform.
Type	The type of this platform.
ConfigSource	The source of configuration of this entry. Note that an entry which is configured via GS3 cannot be deleted through SNMP.
NodeList	The node name list corresponding to this platform.
MgmtAddrList	The management address list corresponding to this Platform.

Fabric Config Server Fabric Ports

Field	Description
Type	The type of this port.

Field	Description
TXType	The TX type of this port.
ModuleType	The module type of this port.
Interface	The physical number corresponding to this port entry.
State	The state of this port.
AttachedPortList	The attached port name list corresponding to this port.

FC Routes

Field	Description
Preference	The value used to select one route over another when more than one route to the same destination is learned from different protocols, peers, or static routes. The preference value is an arbitrarily assigned value used to determine the order of routes to the same destination in a single routing database (RIB). The active route is chosen by the lowest preference value.
LastChangeTime	The last time a row was created, modified, or deleted in the FC route table.
DomainId	The domain ID of next hop switch. However, when read, this value could be N/A if the value of fcRouteProto is local.
Metric	The routing metric for this route. The use is dependent on fcRouteProto used.
Type	The type of route. ▪ local(1): refers to a route for which the next hop is the final destination. ▪ remote(2): refers to a route for which the next hop is not the final destination. This is not relevant for multicast and broadcast route entries.

FDMI HBAs

Field	Description
Sn	The serial number of this HBA.
Model	The model of this HBA.
ModelDescr	The model description.
OSInfo	The type and version of the operating system controlling this HBA.
MaxCTPayload	The maximum size of the Common Transport (CT) payload including all CT headers but no FC frame header(s), that may be send or received by application software resident in the host containing this HBA.

FDMI Ports

Field	Description
SupportedFC4Type	The supported FC-4 types attribute registered for this port on this VSAN.
SupportedSpeed	The supported speed registered for this port on this VSAN.
CurrentSpeed	The current speed registered for this port on this VSAN.
MaxFrameSize	The maximum frame size attribute registered for this port on this VSAN.
OsDevName	The OS Device Name attribute registered for this port on this VSAN.
HostName	The name of the host associated with this port.

FDMI Versions

Field	Description
Hardware	The hardware version of this HBA.
DriverVer	The version level of the driver software controlling this HBA.
OptROMVer	The version of the Option ROM or the BIOS of this HBA.
Firmware	The version of the firmware executed by this HBA.

Flow Statistics

Field	Description
Type	The matching criteria by which flows are selected to be included in the traffic which is instrumented by the ingress traffic counters.
VsanId	The id of VSAN.
DestId	The destination fibre channel address ID.
SrcId	The source fibre channel address ID.
Mask	The mask for source and destination fibre channel address ID.
Frames	The number of received frames for the flow created by the network manager.
Bytes	The number of received frame bytes for the flow created by the network manager.
CreationTime	The timestamp indicating the time the row was created or modified.

FCC

Field	Description
Enable	Enable Fabric Congestion Control
Priority	Specifies the priority level for the frames.
EdgeQuenchPktsRecd	The number of Edge Quench packets received and processed on this port.

Field	Description
EdgeQuenchPktsSent	The number of Edge Quench packets generated on this Port as result of congestion.
PathQuenchPktsRecd	The number of Path Quench packets received and processed on this port.
PathQuenchPktsSent	The number of Path Quench packets generated on this Port as result of congestion.
CurrentCongestionState	The current FCC congestion state of this Port indicating the severity of the congestion.
LastCongestedTime	When the congestion state of the Port changed to noCongestion from some other value. N/A if the congestion state of the Port has never transitioned to noCongestion since the last restart of the device.
LastCongestionStartTime	When the congestion state of the port changed from noCongestion to some other value.
IsRateLimitingApplied	If true, rate limiting is currently being applied on this port.

Diagnostics

Field	Description
Value	Displays the most recent measurement seen by the sensor.
Alarms High and Low	Represents the severity level of the SFP diagnostic information of an interface for temperature, voltage, current, optical transmit and receive power. It ranges from 1 to 6, with 6 being highest severity.
Warnings High and Low	

FSPF General

Field	Description
AdminStatus	The desired state of FSPF on this VSAN.
OperStatus	State of FSPF on this VSAN.
SetToDefault	Enabling this changes each value in this row to its default value. If all the configuration parameters have their default values and if the VSAN is suspended, then the row is deleted automatically.
RegionId	The autonomous region of the local switch on this VSAN.
DomainId	The Domain Id of the local switch on this VSAN.
SpfHoldTime	The minimum time between two consecutive SPF computations on this VSAN. The smaller value means that routing will react to the changes faster but the CPU usage is greater.
SpfDelay	The time between when FSPF receives topology updates and when it starts the Shortest Path First (SPF) computation on this VSAN. The smaller value means that routing will react to the changes faster but the CPU usage is greater.

Field	Description
MinLsArrival	The minimum time after accepting a Link State Record (LSR) on this VSAN before accepting another update of the same LSR on the same VSAN. An LSR update that is not accepted because of this time interval is discarded.
MinLsInterval	The minimum time after this switch sends an LSR on this VSAN before it will send another update of the same LSR on the same VSAN.
LsRefreshTime	The interval between transmission of refresh LSRs on this VSAN.
LSRMaxAge	The maximum age an LSR will be retained in the FSPF database on this VSAN. It is removed from the database after MaxAge is reached.
CreateTime	When this entry was last created.
CheckSum	The total checksum of all the LSRs on this VSAN.

FSPF Interfaces

Field	Description
SetToDefault	Enabling this changes each value in this row to its default value. If all the configuration parameters have their default values and if the interface is down, then the row is deleted automatically.
Cost	The administrative cost of sending a frame on this interface on this VSAN. The value 0 means that the cost has not been configured. Once the value has been configured, the value can not again be 0; so, obviously the value can not be set to 0. If the value is 0 and the corresponding interface is up, the agent sets a value calculated using the ifSpeed of the interface. Otherwise, the value is used as the cost. Note that following formula is used to calculate the link cost. Link Cost = { fspfIfCost if fspfIfCost > 0 {(1.0625e12 / Baud Rate) if fspfIfCost == 0 where Baud Rate is the ifSpeed of the interface.
AdminStatus	The desired state of FSPF on this interface on this VSAN.
HelloInterval	Interval between the periodic HELLO messages sent on this interface on this VSAN to verify the link health. Note that this value must be same on both the interfaces on each end of the link on this VSAN.
DeadInterval	Maximum time for which no HELLO messages can be received on this interface on this VSAN. After this time, the interface is assumed to be broken and removed from the database. Note that this value must be greater than the HELLO interval specified on this interface on this VSAN.
RetransmitInterval	Time after which an unacknowledged link update is retransmitted on this interface on this VSAN.
Neighbour State	The state of FSPF's neighbor state machine, which is the operational state of the interaction with the neighbor's interface which is connected to this interface.
Neighbour DomainId	The Domain ID of the neighbor on this VSAN.
Neighbour PortIndex	The index, as known by the neighbor, of the neighbor's interface which is connected to this interface on this VSAN.

Field	Description
CreateTime	When this entry was last created.

FSPF Interface Stats

Field	Description
CreateTime	When this entry was last created.
ErrorRxPkts	Number of invalid FSPF control frames received on this interface on this VSAN since the creation of the entry.
InactivityExpirations	Number of times the inactivity timer has expired on this interface on this VSAN since the creation of the entry.
LsuRxPkts	Number of Link State Update (LSU) frames received on this interface on this VSAN since the creation of the entry.
LsuTxPkts	Number of Link State Update (LSU) frames transmitted on this interface on this VSAN since the creation of the entry.
RetransmittedLsuTxPkts	Number of LSU frames retransmitted on this interface on this VSAN since the creation of the entry.
LsaRxPkts	Number of Link State Acknowledgement (LSA) frames received on this interface on this VSAN since the creation of the entry.
LsaTxPkts	Number of Link State Acknowledgement (LSA) frames transmitted on this interface on this VSAN since the creation of the entry.
HelloTxPkts	Number of HELLO frames transmitted on this interface on this VSAN since the creation of the entry.
HelloRxPkts	Number of HELLO frames received on this interface on this VSAN since the creation of the entry.

SDV Virtual Devices

Field	Description
Name	Represents the name of this virtual device.
Virtual Domain	The user preference for a persistent Domain ID for this virtual device to indicate a specific partition (domain) of the fabric that this virtual device should belong to.
Virtual FCID	The user preference for a persistent FCID for this virtual device.
Port WWN	The assigned PWWN for this virtual device. The agent assigns this value when the configuration is committed.
Node WWN	The assigned NWWN for this virtual device. The agent assigns this value when the configuration is committed.
Assigned FCID	The assigned FCID of this virtual device. The agent assigns this value when the configuration is committed and the real device that this virtual device virtualizes is on-line.

Field	Description
Real Device Map List	The set of real device(s) that this virtual device virtualizes in this VSAN.

SDV Real Devices

Field	Description
Type	The type of real device identifier represented by the value of the corresponding instance of cFcSdvVirtRealDeviceId that this virtual device virtualizes to.
Name	Represents a real device(s) identifier that this virtual device virtualizes.
Map Type	The mapping association type of the real device(s) (initiator/target).

LUN Discover

Field	Description
StartDiscovery	If Local, then only the directly attached SCSI target devices/ports and LUNs associated with them on all VSANs will be discovered. If Remote, then all SCSI target devices/ports and LUNs associated with them on all VSANs in the whole fabric, except the directly attached ones, will be discovered.
Type	Selecting targets results in only targets being discovered, without the NS results in both targets and LUNs being discovered.
OS	Specifies the operating system on which the LUNs need to be discovered.
Status	Indicates the outcome of the LUN discovery on the local switch. Contains the status of the most recent discovery. • inProgress(1) – indicates that the discovery is still in progress. • completed(2) – indicates that the discovery is complete. • failure(3) – indicates that the discovery encountered a failure.
CompleteTime	When the last discovery was completed. The value will be zero or N/A, if discovery has not been performed since the last system restart.

LUN Targets

Field	Description
VsanId	The VSAN to which this target belongs to.
Port WWN	The name of this authorized/discovered target device or port.
DevType	The device type of the SCSI target.
VendorId	The vendor Id of the SCSI target.
ProductId	The product Id of the SCSI target.
RevLevel	The product revision level of the SCSI target.

Field	Description
OtherInfo	The bytes from 0 to 7 in the INQUIRY command response data.

LUNs

Field	Description
Id	The number of this LUN.
Capacity (MB)	The capacity of this LUN.
SerialNum	The serial number of this LUN.
OS	The operating system for which this LUN was discovered.
FC ID	The Fibre Channel ID for this LUN.

Device Alias

Field	Description
Alias	The device alias of this entry. A device can have only one alias configured.
WWN	The Fibre Channel device which is given a device alias.

Device Alias Configuration

Field	Description
Device Alias	The device alias of this entry. A device can have only one alias configured.
WWN	The Fibre Channel device which is given a device alias.

Device Alias Mode

Field	Description
ConfigMode	Specifies the mode in which the device aliases can be configured. When it is set to basic, the device aliases operate in basic mode of operation. When basic mode is turned on, all MIBs which are using device aliases should internally convert them to their equivalent pWWNs and use the pWWNs. The mechanism to be followed for this conversion is implementation specific. When it is set to enhanced, the Device aliases operate in enhanced mode of operation. When enhanced mode is turned on, all MIBs which are using device aliases should use them as is without any conversion. Since the device aliases are used directly without any conversion, this is the native mode of operation of device aliases.

Device Alias Discrepancies

Field	Description

Discrepancy	Represents the checksum computed over the database represented by cfdaConfigTable and the cfdaConfigMode object. This object is used by a network manager to check if the above mentioned objects have changed on the local device. The method used to compute the checksum is implementation specific.

Name Server General

Field	Description
VSAN Id / FcId	The ID of the VSAN or FC.
Type	The port type of this port.
PortName	The fibre channel Port_Name (WWN) of this Nx_port.
NodeName	The fibre channel Node_Name (WWN) of this Nx_port.
FC4Type/Features	The FC-4 Features associated with this port and the FC-4 Type. Refer to FC-GS3 specification for the format.
FC4 Features	The FC-4 Features associated with this port.
ProcAssoc	The Fibre Channel initial process associator.
FabricPortName	The Fabric Port Name (WWN) of the Fx_port to which this Nx_port is attached.

Name Server Advanced

Field	Description
ClassOfSvc	The class of service indicator.
PortIpAddress	Contains the IP address of the associated port.
NodeIpAddress	The IP address of the node of this Nx_port, as indicated by the Nx_Port in a GS3 message that it transmitted.
SymbolicPortName	The user-defined name of this port.
SymbolicNodeName	The user-defined name of the node of this port.
HardAddress	Extended Link Service (FC-PH-2). Hard Address is the 24-bit NL_Port identifier which consists of - the 8-bit Domain Id in the most significant byte - the 8-bit Area Id in the next most significant byte - the 8-bit AL-PA(Arbitrated Loop Physical Address) which an NL_port attempts acquire during FC-AL initialization in the least significant byte. If the port is not an NL_Port, or if it is an NL_Port but does not have a hard address, then all bits are reported as 0s.
ProcAssoc	The Fibre Channel initial process associator (IPA).
PermanentPortName	The Permanent Port Name of this Nx port. If multiple port names are associated with this Nx port via FDISC (Discover F Port Service Parameters), the Permanent Port Name is the original port name associated with this Nx port at login.

Name Server Proxy

Field	Description
PortName	Name of the proxy port which can register/de-register for other ports on this VSAN. Users can enable third party registrations by setting this value.

Name Server Statistics

Field	Description
Queries Rx	The total number of Get Requests received by the local switch on this VSAN.
Queries Tx	The total number of Get Requests sent by the local switch on this VSAN.
Requests Rx Reg	The total number of Registration Requests received by the local switch on this VSAN.
Requests Rx DeReg	The total number of De-registration Requests received by the local switch on this VSAN.
RSCN Rx	The total number of RSCN commands received by the local switch on this VSAN.
RSCN Tx	The total number of RSCN commands sent by the local switch on this VSAN.
Rejects Tx	The total number of requests rejected by the local switch on this VSAN.

Preferred Path Maps and Routes

Field	Description
VSAN Id, Route Id	The VSAN ID of this FC route map. An arbitrary integer value that identifies a route in this FC route map.
Map Active	Allows the activation/de-activation of all the routes within an FC route map. If true, then all the routes within this FC route map will be activated. If false, then all routes within this FC route map will be de-activated.
Route Strict Preference	Allows changes to the way the preferred path selection logic will select the preferred path. Setting it to true makes the preferred path to select the outgoing interface strictly based on the preference set using the cPrefPathRMapSetIntfPref. When it is set to false, then the preferred path selection logic only performs selection only when the current outgoing interface goes down.
Route Active	Allows the activation/de-activation of the route within an FC route map. If true, then the route will be activated. If false, then the route will be de-activated.
RouteActive	Allows the activation/de-activation of the route within an FC route map. If true, then the route will be activated. If false, then the route will be de-activated.

Preferred Path Maps Active

Field	Description
VSAN Id	The VSAN ID of this FC route map.
GlobalActive	Allows the activation/de-activation of all the routes within an FC route map.

Preferred Path All Match Criteria

Field	Description
VSAN Id, Route Id	The VSAN ID of this FC route map. An arbitrary integer value that identifies a route in this FC route map.
Source FcId	The FC ID that needs to be matched with a source address in a frame for flow classification.
Source Information	Represents the mask associated with the source address.
Source Serial Number	Represents the source serial number.
Source Unit Type	The unit type of the source.
Source Tag	Unique identifier for the source address.
Dest FcId	The FC ID that needs to be matched with a destination address in a frame for flow classification.
Dest Information	Represents the mask associated with the destination address.
Dest Serial Number	Represents the destination serial number.
Dest Unit Type	The unit type of the destination.
Dest Tag	Unique identifier for the destination address.

Preferred Path Active Match Criteria

Field	Description
VSAN Id, Route Id	The VSAN ID of this FC route map. An arbitrary integer value that identifies a route in this FC route map.
Source FcId	The FC ID that needs to be matched with a source address in a frame for flow classification.
Source Information	Represents the mask associated with the source address.
Source Serial Number	Represents the source serial number
Source Unit Type	The unit type of the source.
Source Tag	Unique identifier for the source address.
Dest FcId	The FC ID that needs to be matched with a destination address in a frame for flow classification.
Dest Information	Represents the mask associated with the destination address.

Field	Description
Dest Serial Number	Represents the destination serial number.
Dest Unit Type	The unit type of the source.
Dest Tag	Unique identifier for the destination address.

Preferred Path All Sets

Field	Description
VSAN Id, Route Id, Preference	The VSAN ID of this FC route map. An arbitrary integer value that identifies a route in this FC route map. Preference level, which indicates the metric or cost of the preferred path. The lower the number the higher the preference.
Interface	Represents an interface on the local device on which the matched or classified frame will be forwarded.
IVR Nexthop VSAN	Represents the IVR next hop VSAN ID.

RSCN Nx Registrations

Field	Description
RegType	Indicates the type of registration desired by the subscriber. • 'fromFabricCtrlr' indicates RSCNs generated by the Fabric Controller. • 'fromNxPort' indicates RSCNs generated by Nx_Ports. • 'fromBoth' indicates RSCNs generated by Fabric Controller and Nx_Ports.

RSCN Multi-PID Support

Field	Description
Enable	Specifies whether the multi-pid option is enabled on this VSAN.

RSCN Event

Field	Description
TimeOut (msec)	The time (in seconds) before the RSCN event times out.

RSCN Statistics

Field	Description
SCR Rx	The number of SCRs received from Nx_Ports on this VSAN.

Field	Description
SCR RJT	The number of SCR rejected on this VSAN.
RSCN Rx	The number of RSCNs from Nx_Ports received on this VSAN.
RSCN Tx	The total number of RSCNs transmitted on this VSAN.
RSCN RJT	The number of RSCN requests rejected on this VSAN.
SW-RSCN Rx	The number of Inter-Switch Registered State Change Notifications (SW_RSCN) received on this VSAN from other switches.
SW-RSCN Tx	The number of Inter-Switch Registered State Change Notifications (SW_RSCN) transmitted on this VSAN to other switches.
SW-RSCN RJT	The number of SW_RSCN requests rejected on this VSAN.

Multicast Root

Field	Description
DomainId	The domain ID of the multicast root on this VSAN.
ConfigMode	The configured multicast root mode on this VSAN.
OperMode	The operational multicast root mode on this VSAN.

QoS Policy Maps

Field	Description
Name	The name of this classifier entry. The name should be unique.

QoS Class Maps

Field	Description
Name	The name of this filter entry. The name should be unique.
Match	Specifies how the filter should be applied. If true, then all the match statements associated with this filter must be satisfied in order for this filter match to be considered successful. If false, then even if any one of the criteria associated with this filter is satisfied, then the filter match is considered successful.

QoS Match Statements

Field	Description
SrcAddr	An FC address that needs to be matched with the source address in a FC frame.
DstAddr	An FC address that needs to be matched with the destination address in a FC frame.

Field	Description
Interface	An FC interface on the local device on which a frame should arrive in order to be classified by this filter. A value of zero indicates that no interface is configured.
WildCard	Specifies whether the wild-card option has been set. If true, then the wild-card option is set and all the FC traffic will be considered to match the corresponding multi-field classifier. If false, then the wild-card option is not set.

QoS Class Maps by Policy Maps

Field	Description
Class Map ID	Identifies a Fibre Channel filter.
Priority	Specifies priority value.

QoS Policy Maps by VSAN

Field	Description
VSAN Id, Direction	Specifies the direction of traffic flow on this VSAN.
Policy Map Id	Selects the first Differentiated Services Classifier Element to handle traffic on this VSAN.

QoS DWRR

Field	Description
Weight	The weight associated with this queue.

QoS Rate Limit

Field	Description
Percent	Specifies the rate-limit factor on this interface.

Timers and Policies

Field	Description
R_A_TOV	The Resource_Allocation_Timeout Value used for FxPorts as the timeout value for determining when to reuse an NxPort resource such as a Recovery_Qualifier.
D_S_TOV	The Distributed_Services_Timeout Value which indicates how long a distributed services requester will wait for a response.

Field	Description
E_D _TOV	The Error_Detect_Timeout Value used for FxPorts as the timeout value for detecting an error condition.
F_S_TOV	The Fabric_Stability_Timeout Value used to ensure that fabric stability has been achieved during fabric configuration.
Network Drop Latency	Network latency of this switch. This is the time interval after which the frames are dropped if they are not delivered in the order they were transmitted. Note that network latency is always greater than switch latency.
Switch Drop Latency	The switch latency of this switch. This is the time interval after which a switch drops the undelivered frames on a link which went down after delivering some frames to the next hop. This way the undelivered frames can be transmitted on a new link if there is one available.
InOrderDelivery	The InOrderDelivery guarantee flag of device. If true, then the InOrder Delivery is guaranteed. If false, it is not guaranteed.
TrunkProtocol	Enables or disables the trunking protocol for the device. The trunking protocol is used for negotiating trunk mode and calculating operational VSANs on an EISL link. It also performs port VSAN consistency checks. On non-trunking ISL links, if the port VSANs are different, the E ports will be isolated. To avoid this isolation, this should be set to disable.

WWN Manager

Field	Description
SwitchWWN	The World-Wide Name of this fabric element. It's a 64-bit identifier and is unique worldwide.
Type 1 WWNs	
Max	Maximum number of NAA Type 1 WWNs that are available for assignment to internal entities.
Available	Number of NAA Type 1 WWNs that are currently available for assignment to internal entities.
Reserved	Number of NAA Type 1 WWNs that are reserved for internal purposes.
Type 2 & 5 WWNs	
Max	Maximum number of total WWNs of types NAA Type 2 and Type 5 WWNs available for assignment to internal entities.
Available	Sum of number of NAA Type 2 and Type 5 WWNs currently available for assignment to the internal entities.
Reserved	Number of total WWNs of types NAA Type 2 and Type 5 WWNs reserved for internal purposes.
Enable Secondary when more WWWNs needed	

Field	Description
BaseMacAddress	The first MAC address used for generating World Wide Names (WWNs) when the default range of WWNs generated from supervisor MAC address are exhausted.
MacAddressRange	The number of secondary MAC Addresses starting from and including the wwnmSecondayBaseMacAddress.

NPV Traffic Map

Field	Description
Switch	Name of the switch
Server Interface	Name of the server interface.
External Interface List	The list of interfaces to which the traffic needs to be mapped to.

NPV Load Balance

Field	Description
Switch	Name of the switch.
Enable	Enable or disable displaying NPV related per server interface information

NPV External Interface Usage

Field	Description
Switch	Name of the switch
Server Interface	Interface on the NPV Device that connects to end devices such as hosts or disks. It is also known as F-port, as it operates in F port mode.
External Interface In Use	Interface on the NPV Device that connects to the NPV Core Switch. It is also known as NP-port as it operates in NP port mode.

NP Link

Field	Description
NPIV (core)	Name of the NPIV core switch.
F port	The F port that is connected to the NPIV core switch
NPV	Name of the NPV switch
Speed	An estimate of the interface's current bandwidth in units of 1,000,000 bits per second. If this object reports a value of `n' then the speed of the interface is between `n-500,000' to `n+499,999'.

Field	Description
Rx Util%	Received traffic Utilization %, total number of octets received on the interface over the speed configured on the interface, including framing characters
Rx Bytes	The total number of octets received on the interface, including framing characters.
Tx Util%	Recetransmittedived traffic Utilization %, total number of octets transmitted out of the interface over the speed configured on the interface, including framing characters.
Tx Bytes	The total number of octets transmitted out of the interface, including framing characters.

FCoE

The following sections provide more information in these areas:

- Config
- VSAN-VLAN Mapping
- VLAN-VSAN Mapping
- FCoE Statistics

Config

Field	Description
FC Map	The FCoE Mac Address Prefix used to associate the FCoE Node (ENode).
Default FCF Priority	The default FCoE Initialization Protocol (FIP) priority value advertised by the Fibre Channel Forwarder (FCF) to ENodes.
FKA Adv. Period (sec)	The time interval at which FIP Keep Alive (FKA) messages are transmitted to the MAC address of the ENode.

VSAN-VLAN Mapping



This table applies only to N5k switches running version 4.0(1a) and greater.

Field	Description
VSAN Id	The ID of the VSAN.
VLAN Id	The ID of the VLAN.
Oper State	Shows the operational state of this VLAN-VSAN association entry.

VLAN-VSAN Mapping

Field	Description
VSAN Id	The ID of the VSAN.
VLAN Id	The ID of the VLAN.
Oper State	Shows the operational state of this VLAN-VSAN association entry.

FCoE Statistics

Field	Description
Alignment Errors	The count of frames received on a particular interface that are an integral number of octets in length but do not pass the FCS check.

Field	Description
FCS Errors	The count of frames received on a particular interface that are an integral number of octets in length but do not pass the FCS check. This count does not include frames received with frame-too-long or frame-too-short error.
Single Collision Frames	The count of successfully transmitted frames on a particular interface for which transmission is inhibited by a single collision.
Multiple Collision Frames	The count of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collisions.
SQE Test Errors	The number of times the PLS sublayer generated the SQE TEST ERROR message for a particular interface.
Deferred Transmissions	The count of the number of frames for which the first transmission attempt on a particular interface is delayed because the medium is busy.
Late Collisions	The number of times that a collision is detected on a particular interface later than one slot time into the transmission of a packet.
Excessive Collisions	The count of the number of frames for which transmission on a particular interface failes because of excessive collisions. This counter does not increment when the interface is operating in full-duplex mode.
Internal Mac Transmit Errors	The count of the number of frames for which transmission on a particular interface fails because of an internal MAC sublayer transmit error.
Carrier Sense Errors	The number of times that a carrier sense condition was lost or never asserted when attempting to transmit a frame on a particular interface.
Frame Too Longs	The count of number of frames received on a particular interface that exceed the maximum permitted frame size.
Internal Mac Receive Errors	The count of number of frames for which reception on a particular interface fails because of an internal MAC sublayer receive error.
Symbol Errors	For an interface operating at 100 Mb/s, the number of times there was an invalid data symbol when a valid carrier was present

FICON

The following sections provide more information in these areas:

- FICON VSANs
- FICON VSANs Files
- Global
- FICON Port Attributes
- FICON Port Configuration
- FICON Port Numbers
- FICON VSANs Director History
- Fabric Binding Actions
- Fabric Binding Config Database
- Fabric Binding Active Database
- Fabric Binding Database Differences
- Fabric Binding Violations
- Fabric Binding Statistics
- Fabric Binding EFMD Statistics

FICON VSANs

Field	Description
VSAN ID	Uniquely identifies a VSAN within a fabric.
Host Can Offline SW	If true, it allows the host to put the system offline.
Host Can Sync Time	If true, the host can set the system time.
Port Control by Host	If true, the host is allowed to alter FICON Director connectivity parameters.
Port Control by SNMP	If true, SNMP manager is allowed to alter FICON director connectivity parameters.
CUP Name	The name of the Control Unit Device.
CUP Enable	Indicates whether the Control Unit Device is enabled.
Domain ID	Specifies the domain ID of the switch.
CodePage	The Code Page used in this VSAN.
Character Set	Character set for the code page used in this VSAN.
Active=Saved	If true, the active to saved mode is enabled. All changes will be saved to NVRAM.
User Alert Mode	If true, FICON management stations will prompt on changes.

Field	Description
Device Allegiance	If CUP is in allegiance state with a channel, it cannot accept any commands from any logical paths. A CUP goes in an allegiance state when it accepts command from a channel and forms 'an allegiance' with it until the successful completion of the channel program, at which point the CUP goes in a an 'unlocked' mode.
VSAN Time	The system time in the VSAN. This could be set either by the host or be the default global time in the FICON Director. The default global time is the local time in the FICON Director.
VSAN State	Controls the state of the ports belonging to a VSAN in the context of the FICON functionality.
VSAN Serial Number	The serial number of the FICON director for this VSAN.

FICON VSANs Files

Field	Description
Description	Configuration file description.
CUP Name	The name of the Control Unit Device.
Status	Locked indicates no change allowed. Unlocked indicates change allowed.
LastAccessed	The time this file was last accessed.
UserAlertMode	If true, director user alert mode is enabled.

Global

Field	Description
Default Port Prohibited	Check this option to block the default port.

FICON Port Attributes

Field	Description
TypeNumber	The type number for this FICON Director.
SerialNumber	The sequence number assigned to this FICON Director during manufacturing.
Tag	This is the identifier of the peer port. • If the peer port’s unit type is channel, then PortId will be the CHPID (Channel Path Identifier) of the channel path that contains this peer port. • If the peer port is controlUnit, then PortId will be 0. • If the peer port is fabric, then PortId will be port address of the interface on the peer switch.

Field	Description
FcId	The fabric Id of the other side port (initiator /target). This will be filled only in the case of Fabric ports.
Status	'valid' – if this information is current. 'old' – if this information is cached. Click Clear Old Attributes to clear the cache.
Name	The FICON port name.
Manufacturer	The name of the company that manufactured this FICON Director.
ModelNumber	The model number for this FICON Director.
PlantOfMfg	The plant code that identifies the plant of manufacture of this FICON Director.
UnitType	The peer type of the port that this port is communicating. ==Channel – host ==Control Unit – disk == Fabric – ISL
Alert	Displays one of the following: • bitErrThreshExceeded • lossOfSignalOrSync • nosReceived • primitiveSeqTimeOut • invalidPrimitiveSeq Click Clear to acknowledge and clear this alert.

FICON Port Configuration

Field	Description
Show Installed Ports Only	If true, only physically available ports will be listed in the table.
ESCON Style	ESCON Style Port Configuration display is the Port Configuration table in DM displaying the ESCON Style Ports. In the table, A represents the available ports and P represents the prohibited ports.
Port/ Prohibit	Enter the FICON address of the port and the prohibited list. (This is an alternative to the table grid.)
Name	The port name of this port.
Block	If true, this port will be isolated.
Prohibit Grid	Click on the grid to add or remove the ability of ports to communicate with each other.

FICON Port Numbers

Field	Description
Module	The number of the module in the chassis.

Field	Description
Reserved Port Numbers (Physical)	The reserved port numbers for the module.
NumPorts	The number of ports reserved for that module.
Module Name	The name of the module.
Reserved Port Numbers (Logical)	Chassis slot port numbers. Reserved port numbers for one chassis slot. There can be up to 64 port numbers reserved for each slot in the chassis.

FICON VSANs Director History

To view the latest FICON information, you must click the Refresh button.

Field	Description
KeyCounter	The key counter.
Ports Address Changed	The list of ports that have configuration change for a value of KeyCounter.

Fabric Binding Actions

Field	Description
VSANId	Specifies the unique identifier for a VSAN within a fabric.
Activate	• activate - results in the valid fabric bindings on this VSAN/VLAN being activated. • force activate - results in forced activation, even if there are errors during activation and the activated fabric bindings will be copied to the active database. • deactivate - results in deactivation of currently activated valid fabric bindings (if any), on this VSAN/VLAN. Currently active entries (if any), which would have been present in the active database, will be removed. • no-selection -
Enabled	The state of activation on this VSAN/VLAN. If true, then an activation has been attempted as the most recent operation on this VSAN/VLAN. If false, then an activation has not been attempted as the most recent operation on this VSAN/VLAN.
Result	Indicates the outcome of the most recent activation/deactivation.
LastChange	When the valid fabric bindings on this VSAN/VLAN were last activated. If the last activation took place prior to the last re-initialization of the agent, then this value will be N/A.
CopyActToConfig	If enabled, results in the active fabric binding database to be copied on to the configuration database on this VSAN/VLAN. Note that the learned entries are also copied.

Fabric Binding Config Database

Field	Description
VSAN Id	Specifies the unique identifier for a VSAN within a fabric.
Peer WWN (Name)	Specifies the switch WWN of a switch that can be part of the fabric.
DomainId	Specifies an insistent domain ID.

Fabric Binding Active Database

Field	Description
VSAN Id	Specifies the unique identifier for a VSAN within a fabric.
Peer WWN	Specifies the switch WWN of a switch that can be part of the fabric.
DomainId	Specifies the insistent domain ID of the switch represented by the corresponding instance of the WWN of a switch.

Fabric Binding Database Differences

Field	Description
VSAN	From the drop down list, select the number VSANs to be compared.
Compare With	Choose the database for comparison: • Active – compares the fabric bind active database with respect to configuration database on this VSAN/VLAN. So, the configuration database will be the reference database and the results of the difference operation will be with respect to the configuration database. • Config – compares the fabric bind configuration database with respect to active database on this VSAN/VLAN. So, the active database will be the reference database and the results of the difference operation will be with respect to the active database.
VSAN Id	Specifies the unique identifier for a VSAN within a fabric.
Peer WWN	Specifies the device WWN of a device that can be part of the fabric.
DomainId	Specifies the insistent domain ID of the switch represented by the corresponding instance of the WWN of a switch.
Reason	Indicates the reason for the difference between the databases being compared, for this entry.

Fabric Binding Violations

Field	Description
VSAN Id	Specifies the unique identifier for a VSAN within a fabric.

Field	Description
Peer WWN	The sWWN (switch WWN) of the device that was denied entry into the fabric on one of the local device's ports.
DomainId	The domain ID of the device that was denied entry into the fabric on one of the local device's ports. A value of zero indicates that the switch WWN of the device was not present in the enforced fabric bindings.
DenialTime	When the denial took place.
DenialCount	The number of times this switch has been denied entry into the fabric on one of the local device's ports.
DenialReason	The reason for which the device was denied entry into the fabric on one of the local device's ports.

Fabric Binding Statistics

Field	Description
AllowedReqs	The number of requests from switches to become part of the fabric that have been allowed on this VSAN/VLAN.
DeniedReqs	The number of requests from switches to become part of the fabric that have been denied on this VSAN/VLAN.
Clear	When set to clear, it results in fabric bind statistic counters being cleared on this VSAN/VLAN.

Fabric Binding EFMD Statistics

Field	Description
TxMergeReqs	The number of EFMD Merge Requests transmitted on this VSAN by the local device.
RxMergeReqs	The number of EFMD Merge Requests received on this VSAN by the local device.
TxMergeAccs	The number of EFMD Merge accepts transmitted on this VSAN by the local device.
RxMergeAccs	The number of EFMD Merge accepts received on this VSAN by the local device.
TxMergeRejs	The number of EFMD Merge rejects transmitted on this VSAN by the local device.
RxMergeRejs	The number of EFMD Merge rejects received on this VSAN by the local device.
TxMergeBusys	The number of EFMD Merge Busys transmitted on this VSAN by the local device.
RxMergeBusys	The number of EFMD Merge Busys received on this VSAN by the local device.

Field	Description
TxMergeErrs	The number of EFMD Merge Errors transmitted on this VSAN by the local device.
RxMergeErrs	The number of EFMD Merge Errors received on this VSAN by the local device

IP Storage

The following sections provide more information in these areas:

- FCIP Profiles
- FCIP Tunnels
- FCIP Tunnels (Advanced)
- FCIP Tunnels (FICON TA)
- FCIP Tunnels Statistics
- FCIP XRC Statistics
- iSCSI Connection
- iSCSI Initiators
- iSCSI Session Initiators
- Module Control
- iSCSI Global
- iSCSI Session Statistics
- iSCSI Targets
- iSCSI iSLB VRRP
- iSCSI Initiator Access
- Initiator Specific Target
- iSCSI Initiator PWWN
- iSCSI Sessions
- iSCSI Sessions Detail

FCIP Profiles

Field	Description
IP Address	The Internet address for this entity.
Port	A TCP port other than the FCIP well-known port on which the FCIP entity listens for new TCP connection requests.
SACK	Whether the TCP Selective Acknowledgement Option is enabled to allow the receiver end to acknowledge multiple lost frames in a single ACK, enabling faster recovery.
KeepAlive (s)	The TCP keep alive timeout for all links within this entity.
ReTrans MinTimeout (ms)	The TCP minimum retransmit timeout for all the links on this entity.
ReTrans Max	The Maximum number of times that the same item of data will be retransmitted over a TCP connection. If delivery is not acknowledged after this number of retransmissions then the connection is terminated.

Field	Description
Send BufSize (KB)	The aggregate TCP send window for all TCP connections on all Links within this entity. This value is used for Egress Flow Control. When the aggregate of the data queued on all connections within this entity reaches this value, the sender is flow controlled.
Bandwidth Max (Kb)	This is an estimate of the Bandwidth of the network pipe used for the B-D product computation, which lets us derive the TCP receive window to advertise.
Bandwidth Min (Kb)	The minimum available bandwidth for the TCP connections on the Links within this entity.
Est Round Trip Time (us)	This is an estimate of the round trip delay of the network pipe used for the B-D product computation, which lets us derive the TCP receive window to advertise.
PMTU Enable	The path MTU discovery.
PMTU ResetTimeout (sec)	The time interval for which the discovered pathMTU is valid, before MSS reverts back to the negotiated TCP value.
CWM Enable	If true, congestion window monitoring is enabled.
CWM BurstSize (KB)	The maximum burst sent after a TCP sender idle period.
Max Jitter	The maximum delay variation (not due to congestion) that can be experienced by TCP connections on this interface.

FCIP Tunnels

Field	Description
Interface	This identifies the interface on this FCIP device to which this link pertains.
Attached	The interface on which this FCIP link was initiated.
B Port Enable	If true, the B port mode is enabled on the local FCIP link.
B Port KeepAlive	If true, a message is sent in response to a (Fibre Channel) ELS Echo frame received from the peer. Some B Port implementations use ELS Echo request/response frames as Link Keep Alive.
Remote IP Address	The Internet address for the remote FCIP entity.
Remote TCP Port	The remote TCP port to which the local FCIP entity will connect if and when it initiates a TCP connection setup for this link.
Spc Frames Enable	If true, the TCP active opener initiates FCIP special frames and the TCP passive opener responds to the FCIP special frames. If it is set to false, the FCIP special frames are neither generated nor responded to.
Spc Frames RemoteWWN	The World Wide Name of the remote FC Fabric Entity. If this is a zero length string then this link would accept connections from any remote entity. If a WWN is specified then this link would accept connections from a remote entity with this WWN.
Spc Frames Remote Profile Id	The remote FCIP entity's identifier.

FCIP Tunnels (Advanced)

Field	Description
Interface	The interface on which this FCIP link was initiated.
Timestamp Enable	If true, the timestamp in FCIP header is to checked.
Timestamp Tolerance	The accepted time difference between the local time and the timestamp value received in the FCIP header. By default this value will be EDTOV/2. EDTOV is the Error_Detect_Timeout Value used for Fibre channel Ports as the timeout value for detecting an error condition.
Number Connections	The maximum number of TCP connections allowed on this link.
Passive	If false, this link endpoint actively tries to connect to the peer. If true, the link endpoint waits for the peer to connect to it.
QoS Control	The value to be set for the ToS field in IP header for the TCP control connection.
QoS Data	The value to be set for the ToS field in IP header for the TCP Data connection.
IP Compression	What algorithm is used, if any.
Write Accelerator	The Write accelerator allows for enhancing SCSI write performance.
Tape Accelerator	If true, the tape accelerator (which allows for enhancing Tape write performance) is enabled.
Tape Accelerator Oper	Write Acceleration is enabled for the FCIP link.
TapeRead Accelerator Oper	Enabled automatically when the Tape Accelerator Oper is active.
FlowCtrlBufSize Tape (KB)	The size of the flow control buffer (64K to 32MB). If set to 0, flow control buffer size is calculated automatically by the switch.
IPSec	Indicates whether the IP Security has been turned on or off on this link.
XRC Emulator	Check to enable XRC Emulator. It is disabled by default.
XRC Emulator Oper	Indicates the operational status of XRC Emulator.

FCIP Tunnels (FICON TA)

Field	Description
Interface	A unique value that identifies the interface on this FCIP device to which this link pertains.
VSAN List Admin	The list of VSANs for which FICON Tape Acceleration is configured.
VSAN List Oper	The list of VSANs for which FICON Tape Acceleration is operationally on.

FCIP Tunnels Statistics

Field	Description
Interface	A unique value that identifies the interface on this FCIP device to which this link pertains.
Rx IPCompRatio	The IP compression ratio for received packets on the FCIP device. The value of this object will be presented as a floating point number with two digits after the decimal point.
Tx IPCompRatio	The IP compression ratio for transmitted packets on the FCIP device. The value of this object will be presented as a floating point number with two digits after the decimal point.

FCIP XRC Statistics

Field	Description
ProfileId	Unique ID of the profile.
Interface	Name of the interface.
RRSAccelerated	The number of read record set IUs accelerated.
RRSForwarded	Number of read record set IUs forwarded.
BusyStatus	Number of instances of busy status received from the control unit.
UnitCheckStatus	Number of instances of unit check status received from the control unit.
cfmFcipLinkExtXRCEStatsSelReset	Number of selective resets processed.
BufferAllocErrors	Number of buffer allocation errors.

iSCSI Connection

Field	Description
LocalAddr	The local Internet Network Address used by this connection.
RemoteAddr	The remote Internet Network Address used by this connection.
CID	The iSCSI Connection ID for this connection.
State	The current state of this connection, from an iSCSI negotiation point of view. • login – The transport protocol connection has been established, but a valid iSCSI login response with the final bit set has not been sent or received. • full – A valid iSCSI login response with the final bit set has been sent or received. • logout – A valid iSCSI logout command has been sent or received, but the transport protocol connection has not yet been closed.

Field	Description
MaxRecvDSLen	The maximum data payload size supported for command or data PDUs in use within this connection. Note that the size of reported in bytes even though the negotiation is in 512k blocks.
SendMarker	Indicates whether or not this connection is inserting markers in its outgoing data stream.
HeaderDigest	The iSCSI header digest scheme in use within this connection.
DataDigest	The iSCSI data digest scheme in use within this connection.

iSCSI Initiators

Field	Description
Name or IP Address	A character string that is a globally unique identifier for the node represented by this entry.
VSAN Membership	The list of configured VSANs the node represented by this entry can access.
Dynamic	If true, then the node represented by this entry is automatically discovered.
Initiator Type	Indicates whether the node is a host that participates in iSCSI load-balancing.
Persistent Node WWN	If true, then the same FC address is assigned to the node if it were to be represented again in the FC domain with the same node name. Note that the node FC address is either automatically assigned or manually configured.
SystemAssigned Node WWNN	If true, the FC address is automatically assigned to this node. If false, then the FC address has to be configured manually.
Node WWN	The persistent FC address of the node.
Persistent Port WWN	If true, then the same FC address is assigned to the ports of the node if it were to be represented again in the FC domain with the same node name.
Port WWN	All the FC port addresses associated with this node.
AuthUser	This is the only CHAP user name that the initiator is allowed to log in with.
Target UserName	(Optional) The user name to be used for login. If you do not supply a username, the global user name is used.
Target Password	(Optional) The password to be used for login. If you do not supply a password, the global password is used.
Load Metric	A configured load metric of this iSCSI initiator for the purpose of iSCSI load balancing.
Auto Zone Name	The zone name that is used when the system creates automatic zone for this initiator's specific list of targets.

iSCSI Session Initiators

Field	Description
Name or IP Address	The name or IP address of the initiator port.
Alias	The initiator alias acquired at login.

Module Control

Field	Description
Module Id	ID of the module.
Admin Status	Enables or disables the iSCSI feature for the module.
OperStatus	Shows whether the iSCSI interface is enabled or disabled for the module.

iSCSI Global

Field	Description
AuthMethod	The authentication method.
InitiatorIdleTimeout	The time for which the gateway (representing a FC target) waits from the time of last iSCSI session to a iSCSI initiator went down, before purging the information about that iSCSI initiator.
iSLB ZonesetActivate	Checking this option performs automatic zoning associated with the initiator targets
DynamicInitiator	This field determines how dynamic iSCSI initiators are created. Selecting the iSCSI option (default) creates dynamic iSCSI initiators. If you select iSLB then the an iSLB dynamic initiator is created. Selecting the deny option does not allow dynamic creation of the initiators.
Target UserName	The default user name used for login. If an initiator user name is specified, that user name is used instead.
Target Password	The default password used for login. If an initiator password is specified, that password is used instead.

iSCSI Session Statistics

Field	Description
PDU Command	The count of Command PDUs transferred on this session.
PDU Response	The count of Response PDUs transferred on this session.
Data Tx	The count of data bytes that were transmitted by the local iSCSI node on this session.
Data Rx	The count of data bytes that were received by the local iSCSI node on this session.

Field	Description
Errors Digest	Authentication errors.
Errors CxnTimeout	Connection timeouts.

iSCSI Targets

Field	Description
Dynamically Import FC Targets	Check this option to dynamically import FC targets into the iSCSI domain. A target is not imported if it already exists in the iSCSI domain.
iSCSI Name	The iSCSI name of the node represented by this entry.
Dynamic	Indicates if the node represented by this entry was either automatically discovered or configured manually.
Primary Port WWN	The FC address for this target.
Secondary Port WWN	The optional secondary FC address for this target. This is the FC address used if the primary cannot be reached.
LUN Map iSCSI	The configured default Logical Unit Number of this LU.
LUN Map FC Primary	The Logical Unit Number of the remote LU for the primary port address.
LUN Map FC Secondary	The Logical Unit Number of the remote LU for the secondary port address.
Initiator Access All	If true, then all the initiators can access this target even those which are not in the initiator permit list of this target. If false, then only initiators which are in the permit list are allowed access to this target.
Initiator Access List	Lists all the iSCSI nodes that are permitted to access the node represented by this entry. If AllAllowed is false and the value of List is empty, then no initiators are allowed to access this target.
Advertised Interfaces	Lists all the interfaces on which the target could be advertised.
Trespass Mode	The trespass mode for this node. Every iSCSI target represents one or more port(s) on the FC target. If true, the node instructs the FC node to present all LUN I/O requests to secondary port if the primary port is down.
RevertToPrimaryPort	Indicates if it is required to revert back to primary port if the FC target comes back online.

iSCSI iSLB VRRP

Field	Description
Vrld, IpVersion	The virtual router number and the IP version (IPv4, IPv6, or DNS).
Load Balance	Indicates whether load balancing is enabled.

iSCSI Initiator Access

Field	Description
Initiator Name	The iSCSI node name.

Initiator Specific Target

Field	Description
Name	A globally unique identifier for the node.
Port WWN(s) Primary	The Fibre-Channel target's port addresses associated with this iSCSI initiator-specific target.
Port WWN(s) Secondary	The Fibre-Channel target's port addresses associated with this iSCSI initiator-specific target.
LUN Map (Hex) iSCSI	The Fibre-Channel target's port addresses associated with this iSCSI initiator-specific target.
LUN Map (Hex) FC Primary	The Fibre-Channel target's port addresses associated with this iSCSI initiator-specific target.
LUN Map (Hex) FC Secondary	The Fibre-Channel target's port addresses associated with this iSCSI initiator-specific target.
No AutoZone Creation	Indicates if a FibreChannel zone is automatically created for this iSCSI initiator-target and the iSCSI initiator. If true the zone is not automatically created. If false (default) the zone is automatically created.
Trespass Mode	The trespass mode for this node. If true the FC node instance presents all LUN I/O requests to the secondary port (fcSecondaryAddress) if the primary port (fcAddress) is down.
Revert to Primary Port	The revert to primary mode for this node. If true the FC node instance presents all LUN I/O requests to the primary port fcAddress) when the primary port comes back online.
Primary PWWN VSAN	Indicates the VSAN into which the auto zone is placed for this initiator target. If this object is not set then the VSAN is determined by querying the name server.
Secondary PWWN VSAN	Indicates the VSAN into which the auto zone is placed for this initiator target. If this object is not set then the VSAN is determined by querying the name server.

iSCSI Initiator PWWN

Field	Description
Port WWN	The FC address for this entry.

iSCSI Sessions

Field	Description
Type	Type of iSCSI session: • normal - session is a normal iSCSI session • discovery - session is being used only for discovery.
TargetName	If Direction is Outbound, this will contain the name of the remote target.
Vsan ID	The VSAN to which this session belongs to.
ISID	The initiator-defined portion of the iSCSI Session ID.
TSIH	The target-defined identification handle for this session.

iSCSI Sessions Detail

Field	Description
ConnectionNumber	The number of transport protocol connections that currently belong to this session.
ImmediateData	Whether the initiator and target have agreed to support immediate data on this session.
Initial	If true, the initiator must wait for a Ready-To-Transfer before sending to the target. If false, the initiator may send data immediately, within limits set by FirstBurstSize and the expected data transfer length of the request.
MaxOutstanding	The maximum number of outstanding Ready-To-Transfers per task within this session.
First	The maximum length supported for unsolicited data sent within this session.
Max	The maximum number of bytes which can be sent within a single sequence of Data-In or Data-Out PDUs.
Sequence	If false, indicates that iSCSI data PDU sequences may be transferred in any order. If true indicates that data PDU sequences must be transferred using continuously increasing offsets, except during error recovery.
PDU	If false, iSCSI data PDUs within sequences may be in any order. If true indicates that data PDUs within sequences must be at continuously increasing addresses, with no gaps or overlay between PDUs.

IP Services

The following sections provide more information in these areas:

- IP Routes
- IP Statistics ICMP
- IP Statistics IP
- IP Statistics SNMP
- IP Statistics UDP
- mgmt0 Statistics
- TCP UDP TCP
- TCP UDP UDP
- VRRP General
- VRRP IP Addresses
- VRRP Statistics
- CDP General
- CDP Neighbors
- iSNS Profiles
- iSNS Servers
- iSNS Entities
- iSNS Cloud Discovery
- iSNS Clouds
- iSNS Cloud Interfaces
- Monitor Dialog Controls
- iSNS Details iSCSI Nodes
- iSNS Details Portals

IP Routes

Field	Description
Routing Enabled	When this check box is enabled, the switch is acting as in IP router.
Destination, Mask, Gateway	The value that identifies the local interface through which the next hop of this route should be reached.
Metric	The primary routing metric for this route.
Interface	The local interface through which the next hop of this route should be reached.
Active	Indicates whether the route is active.

IP Statistics ICMP

Field	Description
InParmProbs	The number of ICMP Parameter Problem messages received.
OutParmProbs	The number of ICMP Parameter Problem messages sent.
InSrcQuenchs	The number of ICMP Source Quench messages received.
InRedirects	The number of ICMP Redirect messages received.
InEchos	The number of ICMP Echo (request) messages received.
InEchoReps	The number of ICMP Echo Reply messages received.
InTimestamps	The number of ICMP Timestamp (request) messages received.
InTimestampReps	The number of ICMP Timestamp Reply messages received.
InAddrMasks	The number of ICMP Address Mask Request messages received.
InAddrMaskReps	The number of ICMP Address Mask Reply messages received.
InDestUnreachs	The number of ICMP Destination Unreachable messages received.
InTimeExcds	The number of ICMP Time Exceeded messages received.
OutSrcQuenchs	The number of ICMP Source Quench messages sent.
OutRedirects	The number of ICMP Redirect messages sent. For a host, this value will always be N/A, since hosts do not send redirects.
OutEchos	The number of ICMP Echo (request) messages sent.
OutEchoReps	The number of ICMP Echo Reply messages sent.
OutTimestamps	The number of ICMP Timestamp (request) messages sent.
OutTimestampReps	The number of ICMP Timestamp Reply messages sent.
OutAddrMasks	The number of ICMP Address Mask Request messages sent.
OutAddrMaskReps	The number of ICMP Address Mask Reply messages sent.
OutDestUnreachs	The number of ICMP Destination Unreachable messages sent.
OutTimeExcds	The number of ICMP Time Exceeded messages sent.

IP Statistics IP

Field	Description
InHdrErrors	The number of input data grams discarded due to errors in their IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, etc.
InAddrErrors	The number of input data grams discarded because the IP address in their IP header's destination field was not a valid address to be received at this entity. For entities which are not IP routers and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.

Field	Description
InUnknownProtos	The number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.
InDiscards	The number of input IP data grams for which no problems were encountered to prevent their continued processing, but which were discarded (e.g., for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly.
OutDiscards	The number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (e.g., for lack of buffer space). Note that this counter would include datagrams counted in ipForwDatagrams if any such frames met this (discretionary) discard criterion.
OutNoRoutes	The number of IP datagrams discarded because no route could be found to transmit them to their destination. Note that this counter includes any frames counted in ipForwDatagrams which meet this `no-route' criterion. Note that this includes any datagrams which a host cannot route because all of its default routers are down.
FragFails	The number of IP datagrams that have been discarded because they needed to be fragmented at this entity but could not be, e.g., because their Don't Fragment flag was set.
ReasmFails	The number of failures detected by the IP re-assembly algorithm (for whatever reason: timed out, errors, etc). Note that this is not necessarily a count of discarded IP fragments since some algorithms (notably the algorithm in RFC 815) can lose track of the number of fragments by combining them as they are received.
InReceives	The total number of input datagrams received from interfaces, including those received in error.
InDelivers	The total number of input datagrams successfully delivered to IP user-protocols (including ICMP).
OutRequests	The total number of IP datagrams which local IP user- protocols (including ICMP) supplied to IP in requests for transmission. Note that this counter does not include any data grams counted in ipForwDatagrams.
ForwDatagrams	The number of input datagrams for which this entity was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination. In entities which do not act as IP routers, this counter will include only those frames which were Source-Routed via this entity, and the Source-Route option processing was successful.
FragOKs	The number of IP datagrams that have been successfully fragmented at this entity.
FragCreates	The number of IP datagram fragments that have been generated as a result of fragmentation at this entity.
ReasmReqds	The number of IP fragments received which needed to be reassembled at this entity.
ReasmOKs	The number of IP datagrams successfully re-assembled.

IP Statistics SNMP

Field	Description
BadVersions	The total number of SNMP messages which were delivered to the SNMP entity and were for an unsupported SNMP version.
BadCommunityNames	The total number of SNMP messages delivered to the SNMP entity which used a SNMP community name not known to said entity.
BadCommunityUses	The total number of SNMP messages delivered to the SNMP entity which represented an SNMP operation which was not allowed by the SNMP community named in the message.
ASNParseErrs	The total number of ASN.1 or BER errors encountered by the SNMP entity when decoding received SNMP messages.
TooBigs	The total number of SNMP PDUs which were delivered to the SNMP protocol entity and for which the value of the error-status field is tooBig.
SilentDrops	The total number of GetRequest-PDUs, GetNextRequest-PDUs, GetBulkRequest-PDUs, SetRequest-PDUs, and InformRequest-PDUs delivered to the SNMP entity which were silently dropped because the size of a reply containing an alternate Response-PDU with an empty variable-bindings field was greater than either a local constraint or the maximum message size associated with the originator of the request.
ProxyDrops	The total number of GetRequest-PDUs, GetNextRequest-PDUs, GetBulkRequest-PDUs, SetRequest-PDUs, and InformRequest-PDUs delivered to the SNMP entity which were silently dropped because the transmission of the (possibly translated) message to a proxy target failed in a manner (other than a time-out) such that no Response-PDU could be returned.
NoSuchNames	The total number of SNMP PDUs which were delivered to the SNMP protocol entity and for which the value of the error-status field is noSuchName.
BadValues	The total number of SNMP PDUs which were delivered to the SNMP protocol entity and for which the value of the error-status field is badValue.
ReadOnlys	The total number valid SNMP PDUs which were delivered to the SNMP protocol entity and for which the value of the error-status field is readOnly. It should be noted that it is a protocol error to generate an SNMP PDU which contains the value readOnly in the error-status field, as such this is provided as a means of detecting incorrect implementations of the SNMP.
GenErrs	The total number of SNMP PDUs which were delivered to the SNMP protocol entity and for which the value of the error-status field is genErr.
Pkts	The total number of messages delivered to the SNMP entity from the transport service.
GetRequests	The total number of SNMP Get-Request PDUs which have been accepted and processed by the SNMP protocol entity.
GetNexts	The total number of SNMP Get-Next PDUs which have been accepted and processed by the SNMP protocol entity.

Field	Description
SetRequests	The total number of SNMP Set-Request PDUs which have been accepted and processed by the SNMP protocol entity.
OutTraps	The total number of SNMP Trap PDUs which have been generated by the SNMP protocol entity.
OutGetResponses	The total number of SNMP Get-Response PDUs which have been generated by the SNMP protocol entity.
OutPkts	The total number of SNMP Messages which were passed from the SNMP protocol entity to the transport service.
TotalReqVars	The total number of MIB objects which have been retrieved successfully by the SNMP protocol entity as the result of receiving valid SNMP Get-Request and Get-Next PDUs.
TotalSetVars	The total number of MIB objects which have been altered successfully by the SNMP protocol entity as the result of receiving valid SNMP Set-Request PDUs.

IP Statistics UDP

Field	Description
InErrors	The number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port.
InDatagrams	The total number of UDP datagrams delivered to UDP users.
OutDatagrams	The total number of UDP datagrams sent from this entity.
NoPorts	The total number of received UDP datagrams for which there was no application at the destination port.

mgmt0 Statistics

Field	Description
InErrors	Total number of received errors on the interface.
OutErrors	Total number of transmitted errors on the interface.
InDiscards	Total number of received discards on the interface.
OutDiscards	Total number of transmitted discards on the interface.
TotalRxBytes	Total number of bytes received.
TxBytes	Total number of bytes transmitted.
RxFrames	Total number of frames received.
TxFrames	Total number of frames transmitted.

TCP UDP TCP

Field	Description
State	The state of this TCP connection.

TCP UDP UDP

Field	Description
Port	The local port number for this UDP listener.

VRRP General

Field	Description
IP Address Type, Vrld, Interface	The IP address type (IPv4, IPv6, or DNS), the virtual router ID, and the interface.
Admin	The admin state of the virtual router (active or notInService).
Oper	The current state of the virtual router. There are three defined values: • `initialize', which indicates that all the virtual router is waiting for a startup event. • `backup', which indicates the virtual router is monitoring the availability of the master router. • master', which indicates that the virtual router is forwarding frames for IP addresses that are associated with this router.
Priority	Specifies the priority to be used for the virtual router master election process. Higher values imply higher priority. A priority of '0' is sent by the master router to indicate that this router has ceased to participate in VRRP and a backup virtual router should transition to become a new master. A priority of 255 is used for the router that owns the associated IP address(es).
AdvInterval	The time interval, in seconds, between sending advertisement messages. Only the master router sends VRRP advertisements.
PreemptMode	Controls whether a higher priority virtual router will preempt a lower priority master.
UpTime	When this virtual router transitioned out of `initialized'.
Version	The VRRP version on which this VRRP instance is running.
AcceptMode	Controls whether a virtual router in Master state will accept packets addressed to the address owner’s IPv6 address as its own if it is not the IPv6 address owner. If true, the virtual router in Master state will accept. If false, the virtual router in Master state will not accept.

VRRP IP Addresses

Field	Description
Interface, VRRP ID, IP Address	Interface, Virtual Router Redundancy Protocol ID, and associated IP address

VRRP Statistics

Field	Description
IP Address Type, VrId, Interface	The IP address type (IPv4, IPv6, or DNS), the virtual router ID, and the interface.
LastAdvRx	The total number of VRRP advertisements received by this virtual router.
Protocol Traffic MasterIpAddr	The master router's real (primary) IP address. This is the IP address listed as the source in VRRP advertisement last received by this virtual router.
Protocol Traffic BecomeMaster	The total number of times that this virtual router's state has transitioned to MASTER.
Priority 0 Rx	The total number of VRRP frames received by the virtual router with a priority of '0'.
Priority 0Tx	The total number of VRRP frames sent by the virtual router with a priority of '0'.
AuthErrors InvalidType	The total number of frames received with an unknown authentication type.
Other Errors dvIntervalErrors	The total number of VRRP advertisement frames received for which the advertisement interval is different than the one configured for the local virtual router.
Other Errors IpTtlErrors	The total number of VRRP frames received by the virtual router with IP TTL (Time-To-Live) not equal to 255.
Other Errors InvalidTypePktsRcvd	The number of VRRP frames received by the virtual router with an invalid value in the type field.
Other Errors AddressListErrors	The total number of frames received for which the address list does not match the locally configured list for the virtual router.
OtherErrors PacketLengthErrs	The total number of frames received with a frame length less than the length of the VRRP header.
RefreshRate	The interval of time between refreshes.

CDP General

Field	Description
Enable	Whether the Cisco Discovery Protocol is currently running. Entries in CacheTable are deleted when CDP is disabled.
MessageInterval sec	The interval at which CDP messages are to be generated. The default value is 60 seconds.

Field	Description
HoldTime sec	The time for the receiving device holds CDP message. The default value is 180 seconds.
LastChange	When the cache table was last changed.
Supported DeviceId Format	Indicates the Device-ID format capability of the device.
DeviceId Format	An indication of the format of Device-ID contained in the corresponding instance of the supported device.

CDP Neighbors

Field	Description
Switch	The Internet address for this entity.
Local Interface	A unique value that identifies the interface on this FCIP device to which this link pertains.
DeviceName	The remote device's name. By convention, it is the device's fully qualified domain name.
DeviceID	The device ID string as reported in the most recent CDP message.
DevicePlatform	The version string as reported in the most recent CDP message.
Interface	The port ID string as reported in the most recent CDP message.
IPAddress	The (first) network-layer address of the device's SNMP-agent as reported in the address TLV of the most recently received CDP message.
NativeVLAN	The remote device's interface's native VLAN, as reported in the most recent CDP message. The value 0 indicates no native VLAN field (TLV) was reported in the most recent CDP message.
PrimaryMgmtAddr	Indicates the (first) network layer address at which the device will accept SNMP messages as reported in the most recently received CDP message.
SecondaryMgmtAddr	Indicates the alternate network layer address at which the device will accept SNMP messages as reported in the most recently received CDP message.

iSNS Profiles

Field	Description
Addr	The address of the iSNS server.
Port	The TCP port of the iSNS server.

iSNS Servers

Field	Description
Name	The name of the iSNS Server.
TcpPort	The TCP port used for iSNS messages. If TCP is not supported by this server, the value is 0.
Uptime	The time the server has been active.
ESI Non Response Threshold	The number of ESI messages that will be sent without receiving a response before an entity is de-registered from the iSNS database.
Entities	The number of entities registered in iSNS on the server.
Portals	The number of portals registered in iSNS on the server.
Portal Groups	The number of portal groups registered in iSNS on the server.
iSCSI Devices	The number of iSCSI Nodes registered in iSNS on the server.

iSNS Entities

Field	Description
Entity ID	The iSNS entity identifier for the entity.
Last Accessed	The time the entity was last accessed.

iSNS Cloud Discovery

Field	Description
AutoDiscovery	Whether automatic cloud discovery is turned on or off.
DiscoveryDelay	Time duration between successive IP cloud discovery runs.
Discovery	The IP network discovery command to be executed. • all - Run IP network discovery for all the gigabit ethernet interfaces in the fabric. • noOp (default) - no operation is performed.

Field	Description
CommandStatus	The status of the license install / uninstall / update operation. • success – discovery operation completed successfully • nProgress – discovery operation is in progress • none – no discovery operation is performed • NoIpNetworkNameSpecified – ipCloud name not specified • invalidNetworkName – ipCloud is not configured • NoIPSPortNameSpecified – gigE port ifindex not specified • invalidIPSPortName – invalid gigE port interface • generalISNSFailure – General ISNS Server Failure

iSNS Clouds

Field	Description
Id	The ID of the IP cloud.
Switch WWN	The WWN of the switch in this table.

iSNS Cloud Interfaces

Field	Description
Name, Switch WWN, Interface, Address	The name, Switch WWN, interface, and address of the cloud.

Monitor Dialog Controls

Field	Description
Line Chart	Opens a new window with a line chart representation of the data.
Area Chart	Opens a new window with an area chart representation of the data.
Bar Chart	Opens a new window with a bar chart representation of the data.
Pie Chart	Opens a new window with a pie chart representation of the data.
Reset Cumulative Counters	Resets the counters to 0 if the Column Data display mode is set to Cumulative.
Export to File	Opens a standard Save dialog box. The data is saved as a.TXT file.
Print	Opens a standard Print dialog box.
Update Frequency	The interval at which the data is updated in the monitor dialog.

Field	Description
Column Data	Specifies the type of data that is displayed in the monitor dialog. • Absolute Value – Displays the total amount since the switch was booted. This is the default for error monitoring. • Cumulative – Displays the total amount since the dialog was opened. You can reset the counters by clicking the Reset Cumulative Counters button, to gather a new set of cumulative data. • Minimum/sec – Displays the minimum value per second at every refresh interval. • Maximum/sec – Displays the maximum value per second at every refresh interval. • Last Value/sec – Displays the most recent value per second at every refresh interval. This is the default setting for traffic monitoring.
Elapsed	The amount of time that has elapsed since the dialog was opened. You can reset this counter by clicking the Reset Cumulative Counters button, to gather a new set of cumulative data.

iSNS Details iSCSI Nodes

Field	Description
Name	The iSCSI Name of the initiator or target associated with the storage node.
Type	The Node Type bit-map defining the functions of this iSCSI node, where 31 is a Target, 30 is an Initiator, 29 is a Control, and all others are reserved.
Alias	The Alias name of the iSCSI node.
ScnBitmap	The State Change Notification (SCN) bitmap for a node.
WWN Token	An optional globally unique 64-bit integer value that can be used to represent the World Wide Node Name of the iSCSI device in a Fibre Channel fabric.
AuthMethod	The iSCSI authentication method enabled for this iSCSI Node.

iSNS Details Portals

Field	Description
Addr	The Internet address for this portal.
TcpPort	The port number for this portal.
SymName	The optional Symbolic Name for this portal.
EsiInterval	The Entity Status Inquiry (ESI) Interval for this portal.
TCP ESI	The TCP port number used for ESI monitoring.
TCP Scn	The TCP port used to receive SCN messages from the iSNS server.

Field	Description
SecurityInfo	Security attribute settings for the portal as registered in the Portal Security Bitmap attribute.

Security

The following sections provide more information in these areas:

- Security Roles
- Security Role Rules
- Feature Group Manager
- AAA LDAP Servers
- AAA Server Groups
- AAA Search Map
- AAA Applications
- AAA Defaults
- AAA General
- AAA Statistics
- iSCSI User
- Common Roles
- SNMP Security Users
- SNMP Security Communities
- Security Users Global
- FC-SP General/Password
- FC-SP Interfaces
- FC-SP Local Passwords
- FC-SP Remote Passwords
- FC-SP Statistics
- FC-SP SA (Security Association)
- FC-SP ESP Interfaces
- PKI General
- PKI RSA Key-Pair
- PKI Trust Point
- PKI Trust Point Actions
- PKI LDAP
- PKI Certificate Map
- PKI Certificate Map - Application
- PKI Trust Point Detail
- IKE Global
- IKE Pre-Shared AuthKey
- IKE Policies

- IKE Initiator Version
- IKE Tunnels
- IPSEC Global
- IPSEC Transform Set
- IPSEC CryptoMap Set Entry
- IPSEC Interfaces
- IPSEC Tunnels
- IP ACL Profiles
- IP ACL Interfaces
- IP Filter Profiles
- SSH/Telnet
- Port Security Actions
- Port Security Config Database
- Port Security Active Database
- Port Security Database Differences
- Port Security Violations
- Port Security Statistics
- IPsec

Security Roles

Field	Description
Name	Name of the role. Click the **Create** button to define a new role. Click the **Rules** button to define the rules for this role.
Description	Text description of the user role.
VSAN Scope Enable	Enables the ability to limit the role to specified VSANs.
VSAN Scope List	Specify a list of VSANs to which the role is allowed access.
Interface Scope Enable	(Nexus 5000 Series only) Enables the ability to limit the role to specified interfaces.
Interface Scope List	(Nexus 5000 Series only) Specify a list of interfaces to which the role is allowed access.

Security Role Rules



This table applies only to Nexus 5000 Series switches.

Field	Description
Rule Order	The rules are applied in numerical order.

Field	Description
Permit?	Indicates whether the rule will permit or deny the operation.
Rule Operation	The rule can specify read-only access or read-write access to the operation.
Rule Element Type	The rule can be applied to a command, a feature, feature group or all. Select **all** to apply the rule to all commands and features.
Rule Element	The rule element specifies the command, feature or feature group to which the rule applies.
Features/Groups	Click the **Features/Groups** button to open the feature group manager.

Feature Group Manager



This table applies only to Nexus 5000 Series switches.

Field	Description
Name	The name of the feature group.
Add	To create a new feature group, enter a new feature group name in the Name field, and click **Add**.
Add Feature	To add features to feature groups, select one or more feature group names in the Feature Groups panel, select features in the Features panel, and click **Add Feature**.
Apply	To save changes, click the **Apply** button

AAA LDAP Servers

Field	Description
IP Address Type	The IP address type (IPv4, IPv6, or DNS).
Name or IP Address	The name or IP address of the AAA server.
AuthPort	The Authentication port of the AAA server.
TimeOut(s)	The time in seconds between retransmissions to the AAA server.This value overrides value set in the timeout set in the Features tab for this server. If this value is zero, then the value set in the Features tab will be used.
Retransmits	The additional number of times the AAA server should be tried by the AAA client before giving up on the server. This value overrides value set in the Features tab. If this value is zero, then the value set in the Features tab will be used.
Idle Time (m)	The time interval in minutes, at which the system periodically tests the AAA Server by sending test packets to the server. The default value of 0 means that the AAA server is not tested periodically.
TestUser	The user name to be used in the test packets sent to the AAA Server, to test if the server responds to the requests.

Field	Description
TestPassword	The password to be used in test packets sent to the AAA Server to test if the server responds to the requests.
RootDN	The root name that is used for authenticating access to LDAP server database.
RootDNPasswordEncrType	Type of encryption that is used for the RootDNPassword password.
RootDNPassword	The RootDN password to use if you want to perform root binding. Anonymous bind will be performed if you do not enter a RoodDN password.
SSL Mode	Specifies whether the TLS tunnel needs be setup or not, before binding with the LDAP server.

AAA Server Groups

Field	Description
Name	The name of the server group.
Protocol	The AAA protocol to which this server group belongs to.
ServerIdList	This represents ordered list of AAA Servers which form this Server Group. The order in which servers occur within the value determines the Server priority in that group. The first one will be 'Primary' and the rest are secondary (others). A Server Group can not exist without any members.
DeadTime	The DeadTime setting for AAA Server Group. This indicates the length of time in minutes that the system will mark the server dead when a AAA server does not respond to an authentication request. During the interval of the dead time, any authentication request that comes up would not be sent to that AAA server that was marked as dead. The default value of 0 means that the AAA servers will not be marked dead if they do not respond.

AAA Search Map

Field	Description
BaseDN	Specifies the name of the base entry in the LDAP hierarchy from where the LDAP server begins the search while processing the authorization request.
Filter	Specifies the name of the LDAP filter to be used for searching the user entry in LDAP server database.
Attribute	Specifies the LDAP attribute to be used as user profile private attribute.

AAA Applications

Field	Description
ServerGroupIdList	This represents ordered list of AAA server groups that are configured for this application to perform AAA functions. The order in which server groups occur within the value determines the Server Group priority in the list.
Local	The 'Local' AAA means all the AAA functions are performed using the local AAA service provided in the device. If enabled, is used only after trying all the server groups in the server group list.
Trivial	'Trivial' AAA is used only after trying all the server groups and 'Local' AAA (if configured). Trivial AAA corresponds to one of the following based on the value of corresponding instance of AAAFunction. • User name based authentication, if 'AAAFunction' value is 'authentication' • No Authorization check, if 'AAAFunction' value is 'authorization' • No accounting, if 'AAAFunction' value is 'accounting'.

AAA Defaults

Field	Description
KeyEncrType	The encryption type of the server key.
AuthKey	The key used in encrypting the frames passed between the AAA server and the client.This key must match the one configured on the server.
TimeOut	The time in seconds between retransmissions to the AAA server.
Retransmits	The additional number of times the AAA server should be tried by the AAA client before giving up on the server.
DirectReq	Specifies whether you can choose an AAA server for authentication during login. If true, you can specify the remote AAA server for authentication during login. If you specify the login name as username@hostname, then the authentication request is sent to the remote AAA server hostname with the user name as user name. If false, you cannot specify the remote AAA server for authentication during login.
DeadTime (m)	The DeadTime setting for AAA server group. This indicates the length of time in minutes that the system will mark the server dead when a AAA server does not respond to an authentication request. During the interval of the dead time, any authentication request that comes up would not be sent to that AAA server that was marked as dead. The default value of 0 means that the AAA servers will not be marked dead if they do not respond.

AAA General

Field	Description
AuthTypeMSCHAP	Indicates whether the MSCHAP authentication mechanism should be used for authenticating the user through the remote AAA server during login. If true, MSCHAP authentication is used. If false, the default authentication mechanism is used.
AuthTypeMSCHAPv2	Indicates whether the MSCHAPv2 authentication mechanism should be used for authenticating the user through remote AAA Server during login. If true, MSCHAP authentication is used. If false, the default authentication mechanism is used.



You are recommended to change one authentication mechanism at a time otherwise there might be an error. For example, if you want to change MSCHAP to MSCHAPv2, please choose MSCHAP and apply, and then choose MSCHAPv2 and apply.

AAA Statistics

Field	Description
Authentication	
Requests	The number of authentication requests sent to this server since it was made active. Retransmissions due to request timeouts are counted as distinct requests.
Timeouts	The number of authentication requests which have timed out since the server was made active.
Unexpected	The number of unexpected authentication responses received from this server since it was made active.
Errors	The number of server ERROR authentication responses received from this server since it was made active.
Incorrect	The number of authentication responses which could not be processed since the server was made active.
ResponseTime	Average response time for authentication requests sent to this server, excluding timeouts, since system re-initialization.
Successes	The number of authentication transactions with this server which succeeded since it was made active. A transaction may include multiple request retransmissions if timeouts occur. A transaction is successful if the server responds with either an authentication pass or fail.
Failures	The number of authentication transactions with this server which failed since it was made active. A transaction may include multiple request retransmissions if timeouts occur. A transaction failure occurs if maximum resends have been met or the server aborts the transaction.
Authorization	
Requests	The number of authorization requests sent to this server since it was made active. Retransmissions due to request timeouts are counted as distinct requests.

Field	Description
Timeouts	The number of authorization requests which have timed out since the server was made active. A timeout results in a retransmission of the request. If the maximum number of attempts has been reached, no further retransmissions will be attempted.
Unexpected	The number of unexpected authorization responses received from this server since it was made active. An example is a delayed response to a request which had already timed out.
Errors	The number of server ERROR authorization responses received from this server since it was made active. These are responses indicating that the server itself has identified an error with its authorization operation.
Incorrect	The number of authorization responses which could not be processed since the server was made active. Reasons include inability to decrypt the response, invalid fields, or the response is not valid based on the request.
ResponseTime	Average response time for authorization requests sent to this server, excluding timeouts, since system re-initialization.
Successes	The number of authorization transactions with this server which succeeded since it was made active. A transaction may include multiple request retransmissions if timeouts occur. A transaction is successful if the server responds with either an authorization pass or fail.
Failures	The number of authorization transactions with this server which failed since it was made active. A transaction may include multiple request retransmissions if timeouts occur. A transaction failure occurs if maximum resends have been met or the server aborts the transaction.
Accounting	
Requests	The number of accounting requests sent to this server since system re-initialization. Retransmissions due to request timeouts are counted as distinct requests.
Timeouts	The number of accounting requests which have timed out since system re-initialization. A timeout results in a retransmission of the request If the maximum number of attempts has been reached, no further retransmissions are attempted.
Unexpected	The number of unexpected accounting responses received from this server since system re-initialization. An example is a delayed response to a request which had already timed out.
Errors	The number of server ERROR accounting responses received from this server since system re-initialization. These are responses indicating that the server itself has identified an error with its accounting operation.
Incorrect	The number of accounting responses which could not be processed since system re-initialization. Reasons include inability to decrypt the response, invalid fields, or the response is not valid based on the request.
ResponseTime	Average response time for accounting requests sent to this server, since system re-initialization excluding timeouts.

Field	Description
Successes	The number of accounting transactions with this server which succeeded since system re-initialization. A transaction may include multiple request retransmissions if timeouts occur. A transaction is successful if the server responds with either an accounting pass or fail.
Failures	The number of accounting transactions with this server which failed since system re-initialization. A transaction may include multiple request retransmissions if timeouts occur. A transaction failure occurs if maximum resends have been met or the server aborts the transaction.
Statistics	
State	Current state of the server. • up - Server responding to requests • dead - Server failed to respond A server is marked dead if it does not respond after maximum retransmissions. A server is marked up again either after a waiting period or if some response is received from it
Duration Current (csec)	The elapsed time the server has been in its current state.
Duration Previous (csec)	This object provides the elapsed time the server was been in its previous state prior to the most recent state. This value is zero if the server has not changed state.
TotalDeadTime	The total elapsed time this server's state has had the value dead since system re-initialization.
DeadCount	The number of times this server's state has transitioned to dead since system re-initialization

iSCSI User

Field	Description
iSCSI User	The name of the iSCSI user.
Password	The password of the iSCSI user.

Common Roles



Common Roles is not available in displayFCoE mode (use Security Roles).

Field	Description
Description	Description of the common role.
Enable	This specifies whether the common Role has a VSAN restriction or not.
List	List of VSANs user is restricted to.

SNMP Security Users

Field	Description
Role	The user in Security Model independent format.
Password	Password of the common user. For SNMP, this password is used for both authentication and privacy. For CLI and XML, it is used for authentication only.
Digest	The type of digest authentication protocol which is used.
Encryption	The type of encryption authentication protocol which is used.
ExpiryDate	The date on which this user will expire.
SSH Key File Configured	Specifies whether the user is configured with SSH public key.
SSH Key File	The name of the file storing the SSH public key. The SSH public key is used to authenticate the SSH session for this user. Note that this applies to only CLI user. The format can be one of the following: • SSH Public Key in OpenSSH format • SSH Public Key in IETF SECSH (Commercial SSH public key format) • SSH Client Certificate in PEM (privacy-enhanced mail format) from which the public key is extracted • SSH Client Certificate DN (Distinguished Name) for certificate based authentication
Creation Type	The type of the credential store of the user. When a row is created in this table by a user, the user entry is created in a credential store local to the device. In case of remote authentication mechanism like AAA Server based authentication, credentials are stored in other (remote) system/device.
Expiry Date	The date on which this user will expire.

SNMP Security Communities

Field	Description
Community	The community string.
Role	The Security Model name.

Security Users Global

Field	Description
Enforce SNMP Privacy Encryption	Specifies whether the SNMP agent enforces the use of encryption for SNMPv3 messages globally on all the users in the system.
Cache Timeout	This specifies maximum timeout value for caching the user credentials in the local system.

The privacy password and authentication password are required for an administrator to create a new user or delete an existing user in Device Manager. However, if the administrator does not provide these credentials at the time of creating a new user, Device Manager uses the authentication password of the administrator as the privacy password. If the privacy protocol defined for the user is not DES (default), the SNMP Agent in the MDS will not be able to decrypt the packet and the SNMP Agent times out. If the privacy protocol defined for the user is not DES, the user needs to provide both the privacy password and the protocol when logging in.

FC-SP General/Password

Field	Description
Timeout	Timeout period for FC-SP messages
HashList	Contains a proposed hash mechanism, in the order of preference. The first is the most preferred and the last contains the least preferred.
GroupList	Each ':' separated token contains a value, corresponding to a Diffie-Hellman group identifier.
GenericPasswd	Password for the switch

FC-SP Interfaces

Field	Description
Mode	The FC-SP mode on this interface. • If autoPassive, a port would not initiate any FC-SP authentication exchange; but would always take part in FC-SP authentication exchange initiated by the other side. • If autoActive, a port would always try to initiate FC-SP authentication exchange after ESC. If other side does not support FC-SP authentication, port will still be brought up. • If on, port would always try to initiate FC-SP authentication exchange and authentication is done before the port becomes up. If other side does not support FC-SP authentication, port will not be brought up. • If off, port would never initiate FC-SP authentication exchange and send reject to any FC-SP authentication message started from other end. If this is not 'off', then port has to support at least one FC-SP authentication protocol. You need to configure the FC-SP DHCHAP mode individually on each switch to avoid the timeout error from DCNM.
Reauthenticate Interval (hr)	The time (in hours) for which a port has to wait before trying to re-authenticate the other end.
Reauthenticate Start	Re-authenticate the other end, if this is set to enable.

Field	Description
Auth Successes	The number of times the FC-SP authentication succeeded on this interface.
Auth Fails	The number of times the FC-SP authentication failed on this interface.
Auth Bypasses	The number of times the FC-SP authentication was bypassed on this interface.

FC-SP Local Passwords

Field	Description
Local WWN	The World Wide Name of the local host.
Password	Password of the local switch.

FC-SP Remote Passwords

Field	Description
Remote WWN	The World Wide Name of the remote host.
Password	Password of the remote switch.

FC-SP Statistics

Field	Description
Auth Succeeded	The number of times the FC-SP authentication succeeded on this interface.
Auth Failed	The number of times the FC-SP authentication failed on this interface.
Auth ByPassed	The number of times the FC-SP authentication was bypassed on this interface.
EspSpiMismatch	The number of frames received with a mismatched SPI.
EspAuthFailed	The number of frames received that failed ESP authentication check.

FC-SP SA (Security Association)

Field	Description
SPI	Displays the Security Parameter Index value.
Salt	Salt used for encryption.
Key	Key used for encryption and authentication.

FC-SP ESP Interfaces

Field	Description
Interface	Name of the interface.
ESP Mode	Specifies the ESP mode as one of the following: • None-ESP is not running on the link. • Gcm- Link needs to be encrypted and authenticated. • Gmac-Link needs to be authenticated
EgressSA	Specifies the egress security association to be used. Valid values are between 256 and 65536.
IngressSA1	Specifies the ingress security association to be used. Valid values are between 256 and 65536.
IngressSA2	Specifies the ingress security association to be used. Valid values are between 256 and 65536.
EspFailureReason	Displays the reason of failure. "None" indicates that no error.

PKI General

Field	Description
Switch	Name of the switch.
CertStoreConfig	The certificate store configuration used by the system for authentication.

PKI RSA Key-Pair

Field	Description
Name	The name or label of a key-pair.
Size	The size of the key. The following modulus sizes are defined: • 512-bit, 768-bit, 1024-bit, 1536-bit and 2048-bit. Once created, the size cannot be changed. After a key-pair has been deleted through row deletion, the entry can be created again with another size.
FileName	The name of the file storing the RSA private key. This filename is automatically generated from the key-pair name. It is a unix style '/' separated string representing the absolute path of the file in the file system of the device.
Exportable	The key-pair is exportable through the exportpkcs12 PKI support action. Once created, the exportable flag value cannot be changed. After a key-pair has been deleted through row deletion, the entry can be created again with another value for the exportable flag.

PKI Trust Point

Field	Description
Name	The name or label of a trust point.
KeyPair Name	The name of the associated key-pair from a key-pair table. If a key-pair is not yet associated, the value will be a zero length string.
Revoke CheckMethods	Revocation checking methods list which is an ordered list of certificate revocation checking methods to be employed while verifying peer certificates issued by the CA corresponding to this trust point entry. The value of this object is a ordered list of one or more 1-octet values, where each 1-octet value corresponds to a method in the revocation checking method enumeration: • none (1) - No revocation status checking needed; instead consider the certificate as not revoked. • crl (2) - Use CRL for checking the revocation status of certificates. • ocsp (3) - Use OCSP for checking the revocation status of certificates. If none occurs in the list, it should be the last value. The octets after the last value in the ordered list should be zero octets. The order in which the revocation checking methods occur within the value of this object determines the order the revocation checking methods are attempted during the verification of a peer certificate. The default value (after row creation) contains only the revocation checking method crl.
OCSPurl	The contact http url of the external OCSP server for certificate revocation checking using OCSP protocol. The default value (after row creation) s a zero length string.

PKI Trust Point Actions

Field	Description
Name	The name or label of the trust point action.
Command	The PKI support action to be triggered for this trust point entry.
Url	Indicates the file name containing the input or output certificate data needed for the PKI support action being triggered on this entry. The file name should be specified as bootflash:<filename> and it should be available on bootflash or get created on bootflash depending upon the action being triggered.
Password	Indicates the password required to perform the PKI support action being triggered. This password is required to be specified only for certreq, importpkcs12 and exportpkcs12 actions. For security reasons, the value, whenever it is retrieved by the management protocol, is always the zero length string.

Field	Description
Last Command	The PKI support action attempted last. The value attempted to be set for cpkiAction object last. If no action has been triggered for the trust point after its creation, then retrieving the value of this object will return none.
Result	The result of the execution of the last PKI support action.

PKI LDAP

Field	Description
Switch	Name of the switch.
Store Type	The type of remote certificate store.
CRL Timer (hrs)	The time interval based on which the CRL's corresponding to the CA certificates are updated. The CA certificates and the corresponding CRL's are fetched from remote certstore for authenticaion are stored in local cache to avoid time delays for subsequent authentication.
Server Group Name	The name of the server group that is used for the remote certstore operations.

PKI Certificate Map

Field	Description
Switch	Name of the switch
Filter Name	The unique name of the mapping filter
Subject Name	The subject name of the CA certificate.
Alternate Name Email	AltNameEmail is another unique field and is a part of the subject name, that is used for authentication.
Alternate Name Universal Principal Name	UPN is another unique field and is a part of the subject name, that is used for authentication.

PKI Certificate Map - Application

Field	Description
Switch	Name of the switch.
Purpose / Issuer Name	The issuer name of the certificate
Map Name 1	The name of the first filtering map that will be applied to the certificate with a given purose and an issuer name.
Map Name 2	The name of the second filtering map that will be applied to the certificate with a given purose and an issuer name.

PKI Trust Point Detail

Field	Description
Name	The name or label of the key-pair.
IdCert FileName	The name of the file storing the identity certificate. It is a unix style '/' separated string representing the absolute path of the file in the file system of the device. If there is no identity certificate obtained as yet, the value will be a zero length string.
IdCert SubjName	The subject name of the identity certificate. If there is no certificate or no subject name in the certificate, the value of this object will be a zero length string.
IdCert SerialNum	The serial number of the identity certificate. If there is no certificate, the value of this object will be a zero length string.
IdCert StartDate	The time when the identity certificate starts to be valid, corresponding to the notBefore field in the certificate. If there is no certificate, the value of this object will be a zero length string.
IdCert EndDate	The time when the identity certificate validity ends, corresponding to the notAfter field in the certificate. If there is no certificate, the value of this object will be a zero length string.
IdCert FingerPrint	The MD5 fingerprint of the identity certificate in HEX string format. If there is no certificate, the value of this object will be a zero length string.
IssuerCert FileName	The name of the file storing the issuer certificate. It is a unix style '/' separated string representing the absolute path of the file in the file system of the device. If there is no issuer certificate obtained yet, the value of this object will be a zero length string.
IssuerCert SubjName	The issuer name (subject name in issuer certificate which will be the same as the issuer name in the identity certificate if present). If there is no certificate, the value will be a zero length string.
IssuerCert SerialNum	The serial number of the issuer certificate. If there is no certificate, the value will be a zero length string.
IssuerCert StartDate	The time when the issuer certificate starts to be valid, corresponding to the notBefore field in the certificate. If there is no certificate, the value will be a zero length string.
IssuerCert EndDate	The time when the issuer certificate validity ends, corresponding to the notAfter field on in the certificate. If there is no certificate, the value will be a zero length string.
IssuerCert FingerPrint	The MD5 fingerprint of the issuer's certificate in HEX string format. If there is no certificate, the value of this object will be a zero length string.

IKE Global

Field	Description
RemIdentity	Displays the keep alive interval in seconds used by the IKE entity on the managed device with all the peers for the DOI corresponding to this conceptual row.
Key	Displays the type of keep alives to be used by the IKE entity on the managed device with all the peers for the DOI corresponding to this conceptual row.

IKE Pre-Shared AuthKey

Field	Description
KeepAliveInterval (sec)	The Phase 1 ID identity of the peer for which this pre-shared key is configured on the local entity.
IdentityType	The pre-shared authorization key used in authenticating the peer corresponding to this conceptual row.

IKE Policies

Field	Description
Priority	The priority of this ISAKMP Policy entry. The policy with lower value would take precedence over the policy with higher value in the same DOI.
Encr	The encryption transform specified by this ISAKMP policy specification. The Internet KeyExchange (IKE) tunnels setup using this policy item would use the specified encryption transform to protect the ISAKMP PDUs.
Hash	The hash transform specified by this ISAKMP policy specification. The IKE tunnels setup using this policy item would use the specified hash transform to protect the ISAKMP PDUs.
Auth	The peer authentication method specified by this ISAKMP policy specification. If this policy entity is selected for negotiation with a peer, the local entity would authenticate the peer using the method specified by this object.
DHGroup	Specifies the Oakley group used for Diffie Hellman exchange in the Main Mode. If this policy item is selected to negotiate Main Mode with an IKE peer, the local entity chooses the group specified by this object to perform Diffie Hellman exchange with the peer.
Lifetime (sec)	Specifies the lifetime in seconds of the IKE tunnels generated using this policy specification.

IKE Initiator Version

Field	Description
Address	The address of the remote peer corresponding to this conceptual row. This object cannot be modified while the corresponding value of cicIkeCfgInitiatorStatus is equal to active.
Version	The IKE protocol version used when connecting to a remote peer specified in cicIkeCfgInitiatorPAddr. This object cannot be modified while the corresponding value of cicIkeCfgInitiatorStatus is equal to active.

IKE Tunnels

Field	Description
LocalAddress	The address of the local endpoint for the Phase-1 tunnel.
RemoteAddresss	The address of the remote endpoint of the Phase-1 tunnel.
AuthMethod	The authentication method used in Phase-1 negotiations on the control tunnel corresponding to this conceptual row.
Action	The action to be taken on this tunnel. If clear, then this tunnel is cleared. If re-key, then re-keying is forced on this tunnel. The value none would be returned on doing read of this object.

IPSEC Global

Field	Description
Lifetime (sec)	The default lifetime (in seconds) assigned to an IPSEC tunnel as a global policy (maybe overridden in specific cryptomap definitions).
Lifesize (KB)	The default life size in KBytes assigned to an IPSEC tunnel as a global policy (unless overridden in cryptomap definition).

IPSEC Transform Set

Field	Description
Id	This is the sequence number of the transform set that uniquely identifies the transform set. Distinct transform sets must have distinct sequence numbers.
Protocol	Represents the suite of Phase-2 security protocols of this transform set.
ESP Encryption	Represents the transform used for ESP encryption.
ESP Authentication	Represents the transform used to implement integrity check with ESP protocol.
Mode	Represents the encapsulation mode of the transform set.

IPSEC CryptoMap Set Entry

Field	Description
IpFilter	Specifies an IP protocol filter to be secured using this cryptomap entry. When it has a value of zero-length string, it is not valid/applicable.
TransformSetIdList	The list of cipsXformSetId that are members of this CipsStaticCryptomapEntry. The value of this object is a concatenation of zero ormore 4-octet strings, where each 4-octet string contains a 32-bit cipsXformSetId value in network byte order. A zero length string value means this list has no members.
AutoPeer	If true the destination address is taken as the peer address, while creating the tunnel.
Peer Address	The IP address of the peer to which this cryptomap entry is currently connected.
PFS	Identifies whether the tunnels instantiated due to this policy item should use Perfect Forward Secrecy (PFS) and if so, what group of Oakley they should use.
LifeTime	Specifies the lifetime of the IPsec Security Associations (SA) created using this IPsec policy entry.
Lifesize Value	Identifies the life size (maximum traffic in bytes that may be carried) of the IPSec SAs created using this IPSec policy entry. When a Security Association (SA) is created using this IPsec policy entry, its life size takes the value of this object.

IPSEC Interfaces

Field	Description
CryptomapName	The index of the static cryptomap table. The value of the string is the name string assigned by the NMS when defining a cryptomap set.
InterfaceList	Interfaces belong to the cryptomap.

IPSEC Tunnels

Field	Description
Local Address	The IP address of the local endpoint for the IPsec Phase-2 tunnel.
RemoteAdddress	The type of the IP address of the remote endpoint for the IPsec Phase-2 tunnel.
ESP Encryption	The encryption algorithm used by the outbound security association of the IPsec Phase-2 tunnel.
ESP Encryption KeySize	The key size in bits of the negotiated key to be used with the algorithm denoted by ceipSecTunOutSaEncryptAlgo. For DES and 3DES the key size is respectively 56 and 168. For AES, this will denote the negotiated key size.

Field	Description
ESP Authentication	The authentication algorithm used by the inbound encapsulation security protocol (ESP) security association of the IPsec Phase-2 tunnel.
LifeSize (KB)	The negotiated life size of the IPSEC Phase-2 tunnel in kilobytes.
LifeTime (sec)	The negotiated lifetime of the IPSEC Phase-2 tunnel in seconds. If the tunnel was setup manually, the value of this MIB element should be 0.
Action	The status of the MIB table row.

IP ACL Profiles

Field	Description
Name	This is the unique IP protocol filter profile identifier.
Type	This object determines the usage type for this filter profile. This usage type cannot be changed after the profile has been created.

IP ACL Interfaces

Field	Description
ProfileName	This is the unique IP protocol filter profile identifier.

IP Filter Profiles

Field	Description
Action	If it is set to deny, all frames matching this filter will be discarded and scanning of the remainder of the filter list will be aborted. If it is set to permit, all frames matching this filter will be allowed for further bridging or routing processing.
Protocol	This filter protocol value matches the Internet Protocol Number in the frames. These IP numbers are defined in the Network Working Group Request for Comments (RFC) documents. Setting this to '-1' will make the filtering match any IP number.
Address	The source IP address to be matched for this filter. A value of 0 causes all source address to match.
Mask	This is the wildcard mask for the SrcAddress bits that must match. 0 bits in the mask indicate the corresponding bits in the SrcAddress must match in order for the matching to be successful, and 1 bits are don’t care bits in the matching. A value of 0 causes only IP frames of source address the same as SrcAddress to match.
PortLow	If Protocol is UDP or TCP, this is the inclusive lower bound of the transport-layer source port range that is to be matched, otherwise it is ignored during matching. This value must be equal to or less than the value specified for this entry in SrcPortHigh.

Field	Description
PortHigh	If Protocol is UDP or TCP, this is the inclusive upper bound of the transport-layer source port range that is to be matched, otherwise it is ignored during matching. This value must be equal to or greater than the value specified for this entry in SrcPortLow. If this value is '0', the UDP or TCP port number is ignored during matching.
Address	The destination IP address to be matched for this filter. A value of 0 causes all source address to match.
Mask	This is the wildcard mask for the DestAddress bits that must match. 0 bits in the mask indicate the corresponding bits in the DestAddress must match in order for the matching to be successful, and 1 bits are don't care bits in the matching. A value of 0 causes only IP frames of source address the same as SrcAddress to match.
PortLow	If Protocol is UDP or TCP, this is the inclusive lower bound of the transport-layer destination port range that is to be matched, otherwise it is ignored during matching. This value must be equal to or less than the value specified for this entry in PortHigh.
PortHigh	If Protocol is UDP or TCP, this is the inclusive upper bound of the transport-layer destination port range that is to be matched, otherwise it is ignored during matching. This value must be equal to or greater than the value specified for this entry in DestPortLow. If this value is '0', the UDP or TCP port number is ignored during matching.
Precedence	The IP traffic precedence parameters in each frame are used to guide the selection of the actual service parameters when transmitting a datagram through a particular network. Most network treats high precedence traffic as more important than other traffic. The IP Precedence value ranges from '0' to '7', with '7' the highest precedence and '0' the lowest precedence. The value '-1' means to match frames of any IP precedence. In other words, the IP precedence parameter will not to checked if this value is '-1'. The precedence level are: • routine(0) - Routine traffic precedence • priority(1) - Priority traffic precedence • immediate(2) - Immediate traffic precedence • flash(3) - Flash traffic precedence • flashOverride(4) - Flash-override traffic precedence • critical(5) - Critical precedence • internet(6) - Internetwork control traffic precedence • network(7) - Network control traffic precedence.
TOS	The Type of Service (TOS) of the frame. The TOS values ranges from '0' to '15'. The value '-1' matches any TOS value.
ICMPType	This filter specifies the ICMP message type to be matched. Setting this value to '-1' will make the filtering match any ICMP message type.

Field	Description
ICMPCode	This filter specifies the ICMP message code to be matched. Setting this value to '-1' will make the filtering match any ICMP code.
TCPEstablished	This filter if true specifies that for TCP protocol, in an established connection, a match occurs if the TCP datagram has the ACK,FIN,PSH,RST,SYN or URG control bits set. If false, a match will occur for any TCP datagram.
LogEnabled	Specifies whether filtered frames will be logged by the filtering subsystem or not. If true, then all frames will be logged. If false, then no frame will be logged.

SSH/Telnet

Field	Description
Enable SSH/Telnet	Check to enable SSH and/or Telnet.
NumBits	The number of bits provided to generate the key. This determines the length of the key string generated by the SSH.
Key	The SSH key string that is generated.
LastCreationTime	The time of the last creation of the key.
Enable	Enables or disables the Secure Shell (SSH) service on the device.

Port Security Actions

Field	Description
Activation	

Field	Description
Action	• activate - results in the valid port bindings on this VSAN/VLAN being activated. • activate (Turn LearningOff) - results in the valid port bindings on this VSAN/VLAN being activated and copied to the active database and will also result in auto learn being turned off on this VSAN/VLAN, once the activation is complete. • force activate - results in forced activation, even if there are errors during activation and the activated port bindings will be copied to the active database. • force activate (Turn Learning Off) - results in forced activation along with turning auto learn off after activation and the activated port bindings will be copied to the active database. • deactivate - results in deactivation of currently activated valid port bindings (if any), on this VSAN/VLAN. Currently active entries (if any), which would have been present in the active database, will be removed. • Activation will not be allowed on a VSAN if auto-learn is enabled on that VSAN
Enabled	The state of activation on this VSAN/VLAN. If true, then an activation has been attempted as the most recent operation on this VSAN/VLAN. If false, then an activation has not been attempted as the most recent operation on this VSAN/VLAN.
Result	Indicates the outcome of the most recent activation/deactivation.
Last Change	When the valid port bindings on this VSAN/VLAN were last activated. If the last activation took place prior to the last re-initialization of the agent, then this value will be N/A.
CopyActiveToConfig	If enabled, results in the active port binding database to be copied on to the configuration database on this VSAN/VLAN. Note that the learned entries are also copied.
AutoLearn	Helps to learn the valid port binding configuration of devices/ports logged into the local device on all its ports and populate the above active database with the same. This mechanism of 'learning' the configuration of devices/ports logged into the local device over a period of time and populating the configuration is a convenience mechanism for users. If enabled on a particular VSAN, all subsequent logins (FLOGIs) on that VSAN will be populated in the enforced port binding database, provided it is not in conflict with existing enforced port bindings on that VSAN. When disabled, the mechanism of learning is stopped. The learned entries will however be in the active database.
Clear AutoLearned	
Action	• Clear VSAN results in port bind auto-learnt entries being cleared on this VSAN. • Clear Interface(s) results in port bind auto-learnt entries being cleared on the interface specified on this VSAN.

Field	Description
Interface	Specifies the interface(s) on which the port bind auto-learnt entries need to be cleared.

Port Security Config Database

Field	Description
Interface or fWWN	Represents the address of the port on the local device through which the device specified can FLOGI. • If fwwn, then the value is the fabric WWN of a port on the local device. • If intfIndex, then a port on the local device is being represented by its interface. • If wildCard, then it represents a wild-card entry. The wild-card represents any port on the local device.
Type	The mechanism to identify a switch port.
WWN	Represents the logging-in device address

Port Security Active Database

Field	Description
Interface or fWWN	The address of a port on the local device.
Type	The mechanism to identify a switch port.== fwwn - the local switch port is identified by Fabric WWN(fWWN). == intfIndex - the local switch port is identified by ifIndex. == wildCard - wild card (any switch port on local device).
WWN	Represents the logging in device address.
IsLearnt	Indicates if this entry is a learnt entry or not.

Port Security Database Differences

Field	Description
CompareWith	Specifies the database for the comparison. • configDb - compares the configuration database with respect to active database on this VSAN/VLAN. So, the active database will be the reference database and the results of the difference operation will be with respect to the active database. • activeDb - compares the active database with respect to configuration database on this VSAN/VLAN. So, the configuration database will be the reference database and the results of the difference operation will be with respect to the configuration database.

Field	Description
VSANId	The ID of the VSAN to compare against.
Interface/fWWN	The address of a port on the local device.
Type	The mechanism to identify a switch port. • fwwn – the local switch port is identified by Fabric WWN(fWWN). • intfIndex – the local switch port is identified by ifIndex. • wildCard – wild card (any switch port on local device).
WWN	Represents the logging in device address.
Reason	Indicates the reason for the difference between the databases being compared, for this entry.

Port Security Violations

Field	Description
Interface	The fWWN of the port on the local device where the login was denied.
End Device	The pWWN of the device that was denied FLOGI on one of the local device's ports.
Or Switch	The sWWN of the device (if the device happens to be a switch), that was denied entry on one of the local device's ports.
Time	When the login denial took place.
Count	The number of times this particular pWWN/nWWN or sWWN has been denied login on this particular local interface.

Port Security Statistics

Field	Description
AllowedLogins	The number of FLOGI requests that have been allowed on this VSAN/VLAN.
DeniedLogins	The number of FLOGI requests that have been denied on this VSAN/VLAN.
Clear	When set to clear, it results in port bind statistic counters being cleared on this VSAN/VLAN.

IPsec

Field	Description
Interface, CryptomapName	The binding of cryptomap sets to the interfaces of the managed entity.

Events

The following sections provide more information in these areas:

- Call Home General
- Call Home Destinations
- Call Home Email Setup
- Call Home Alerts
- Call Home HTTP Proxy Server
- Call Home SMTP Servers
- Call Home User Defined Command
- Delayed Traps
- Call Home Profiles
- Event Destinations Addresses
- Event Destinations Security (Advanced)
- Event Filters General
- Event Filters Interfaces
- Event Filters Control
- Link Incident History
- RMON Thresholds Controls
- RMON Thresholds 64bit Alarms
- RMON Thresholds 32bit Alarms
- RMON Thresholds Events
- RMON Thresholds Log

Call Home General

Field	Description
Contact	The contact person for this switch, together with information on how to contact this person.
PhoneNumber	The phone number of the contact person. The phone number must start with '+' and contains only numeric characters except for space and '-'. Some valid phone numbers are +44 20 8332 9091 +45 44886556 +81-46-215-4678 +1-650-327-2600.
EmailAddress	The email address of the contact person. Some valid email addresses are raj@helpme.com, bob@service.com, mtom@abc.caview.ca.us.
StreetAddress	The mailing address of this switch.
CustomerId	A string, in whatever format is appropriate, to identify the customer.

Field	Description
ContractId	A string, in whatever format is appropriate, to identify the support contract between the customer and support partner.
SiteId	A location identifier of this device.
DeviceServicePriority	The service priority of the device. This determines how fast the device has to be serviced.
Enable	Enables or disables the CallHome infrastructure on the local device.

Call Home Destinations

Field	Description
ProfileName,ID	The destination profile name and identifier.
Type	Transmission method type.
EmailAddress	The email address associated this destination profile. Some examples are raj@helpme.com, bob@service.com, mtom@abc.caview.ca.us.
Http Url	The HTTP URL associated with this destination profile.

Call Home Email Setup

Field	Description
From	The email address that is to be used in the From field when sending the email using SMTP. Some examples are raj@helpme.com, bob@service.com, mtom@abc.caview.ca.us.
ReplyTo	The email address that is to be used in the Reply-To field when sending the email using SMTP. Some examples are raj@helpme.com, bob@service.com, mtom@abc.caview.ca.us.
IP Address Type	The IP address type (IPv4, IPv6, or DNS).
Name or IP Address	Name or IP address of the SMTP server.
Port	TCP port of the SMTP server.

Call Home Alerts

Field	Description
Action	Test - sends a Call Home message TestWithInventory - sends a message with inventory details.
Status	The status of the last callhome action invocation.
FailureCause	The failure cause for the last callhome test invocation.
LastTimeSent	When the last CallHome alert was sent.
NumberSent	The number of CallHome alerts sent.

Field	Description
Every	Time frame for sending the periodic software inventory Call Home message.
Throttling Enable	If checked, enables the message throttling mechanism implemented on the system, to limit the number of callhome messages for a alert type within a time frame. The maximum is 30 in a 2-hour time frame, and any further messages for that alert type are discarded.
Enable	If checked, enables the sending of periodic software inventory callhome messages on the system.

Call Home HTTP Proxy Server

Field	Description
Master	Name of the switch.
Address Type	The type of the HTTP proxy server as represented by the value in the HTTP proxy server address.
Address	The address of the HTTP proxy server.
Port	The port of the HTTP proxy server.
Enable	Enable or disable the use of HTTP proxyserver configured for sending callhome messages over HTTP.

Call Home SMTP Servers

Field	Description
Address Type, Address	IP address of the SMTP server.
Port	TCP port of the SMTP server.
Priority	Priority value

Call Home User Defined Command

Field	Description
User Defined Command	Used to configure user defined commands for the callhome alert group types.

Delayed Traps

Field	Description
Enable	Enable or disable delay traps.
Delay	Delay interval in minutes (valid values are between 1 to 60)

Call Home Profiles

Field	Description
MsgFormat	XML, full text, or short text.
MaxMsgSize	Maximum message size that can be sent to destination pointed to by this destination profile.
MsgLevel	Threshold level, used for filtering alert messages sent to a destination. Callhome alert message with severity level lower than the configured threshold level would not be sent. The default threshold level is debug (1), which means all the alert messages will be sent.
AlertGroups	The list of configured alert groups for this destination profile.

Event Destinations Addresses

Field	Description
Address/Port	IP Address and Port to send event.
Security Name	The SNMP parameters to be used when generating messages to be sent to this address.
Security Model	Is used when generating SNMP messages using this entry.
Inform Type	• Trap - unacknowledged event • Inform - acknowledged event.
Inform Timeout	This expected maximum round trip time for communicating with the address.
RetryCount	The number of retries to be attempted when a response is not received for a generated message.
Status	• Active-Port is active. • NotInService-Port is out of service.

Event Destinations Security (Advanced)

Field	Description
MPModel	The Message Processing Model to be used when generating SNMP messages using this entry.
SecurityModel	The Security Model to be used when generating SNMP messages using this entry.
SecurityName	Identifies the Principal on whose behalf SNMP messages will be generated using this entry.
SecurityLevel	The Level of Security to be used when generating SNMP messages using this entry.

Event Filters General

Field	Description
FSPF – Nbr State Changes	Specifies whether or not the local switch should issue notification when the local switch learns of a change in the Neighbor's state (state in the FSPF Neighbor Finite State Machine) on an interface on a VSAN.
Domain Mgr – ReConfig Fabrics	Specifies whether or not the local switch should issue a notification on sending or receiving ReConfigureFabric (RCF) on a VSAN.
Zone Server – Request Rejects	Specifies if the Zone Server should issue a notification on rejects.
Zone Server – Merge Failures	Specifies if the zone server should issue a notification on merge failures.
Zone Server – Merge Successes	Specifies if the zone server should issue a notification on merge successes.
Zone Server – Default Zone Behavior Change	Specifies if the zone server should issue a notification if the propagation policy changes.
Zone Server – Unsupp Mode	Specifies if the zone server should issue a notification on unsupp mode changes
FabricConfigServer – Request Rejects	Specifies if the Fabric Configuration Server should issue a notification on rejects.
RSCN – ILS Request Rejects	Specifies if the RSCN module should generate notifications when a SW_RSCN request is rejected.
RSCN – ILS RxRequest Rejects	Specifies if the RSCN module should generate notifications when a SW_RSCN request is rejected.
RSCN – ELS Request Rejects	Specifies if the RSCN module should generate notifications when a SCR or RSCN request is rejected.
FRU Changes	A false value will prevent Field Replaceable Unit (FRU) notifications from being generated by this system.
SNMP – Community Auth Failure	Indicates whether the SNMP entity is permitted to generate authenticationFailure traps.
VRRP	Indicates whether the VRRP-enabled router will generate SNMP traps for events defined in this MIB.
FDMI	Specifies if the FDMI should generate notifications when a registration request is rejected.
License Manager	Indicates whether the system should generate notifications.
Port/Fabric Security	Specifies if the system should generate notifications when a port/fabric security issue arises.
FCC	Specifies whether the agent should generate notifications.
Name Server	If checked, the Name Server generates a notification when a request is rejected. If false, the notification is not generated.

Event Filters Interfaces

Field	Description
EnableLinkTrap	Indicates whether linkUp/linkDown traps should be generated for this interface.

Event Filters Control

Field	Description
Variable	Represents the notification to be controlled.
Descr	Description about the notification.
Enabled	Check to enable notification of the control. Shows the status of the control.



You see the Descr column only on switches that runs Cisco NX-OS release 5.0 or later.

Link Incident History

Field	Description
Host Time	The local time on the host.
Switch Time	The local time on the switch.
Port	The port number for the link incidents.
Interface	The Fibre Channel interface in the specified port.
Link Incident	The type of incident that occurred.

RMON Thresholds Controls

Field	Description
AlarmEnable	If true, the RMON alarm feature is enabled. If the RMON feature is disabled, all the RMON alarm related polling are stopped. Note that this is only intended for temporary disabling of RMON alarm feature to ensure that the CPU usage by RMON alarms is not detrimental. For permanent disabling on this feature, it suggested that all the entries in the alarmTable are removed.
MaxAlarms	The maximum number of entries allowed in the alarmTable.

RMON Thresholds 64bit Alarms

Field	Description
Interval	The interval in seconds over which the data is sampled and compared with the rising and falling thresholds. When setting this variable, care should be taken in the case of deltaValue sampling – the interval should be set short enough that the sampled variable is very unlikely to increase or decrease by more than 2^31 – 1 during a single sampling interval.
Variable	The variable to be sampled. Only variables that resolve to an ASN.1 primitive type of INTEGER (INTEGER, Integer32, Counter32, Counter64, Gauge, or TimeTicks) may be sampled.
SampleType	The method of sampling the selected variable and calculating the value to be compared against the thresholds. If the value is absoluteValue, the value of the selected variable will be compared directly with the thresholds at the end of the sampling interval. If the value is deltaValue, the value of the selected variable at the last sample will be subtracted from the current value, and the difference compared with the thresholds.
Value	The value of the statistic during the last sampling period. For example, if the sample type is deltaValue, this value will be the difference between the samples at the beginning and end of the period. If the sample type is absoluteValue, this value will be the sampled value at the end of the period. This is the value that is compared with the rising and falling thresholds. The value during the current sampling period is not made available until the period is completed and will remain available until the next period completes.
StartupAlarm	The alarm that may be sent when this entry is first set to valid.
Rising Threshold	A threshold for the sampled statistic. When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval was less than this threshold, a single event will be generated.
Rising EventId	The ID of the eventEntry that is used when a rising threshold is crossed.
Falling Threshold	A threshold for the sampled statistic. When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval was greater than this threshold, a single event will be generated.
Falling EventId	The ID of the eventEntry that is used when a falling threshold is crossed. The eventEntry identified by a particular value of this index is the same as identified by the same value of eventIndex. If there is no corresponding entry in the eventTable, then no association exists. In particular, if this value is N/A, no associated event will be generated, as N/A is not a valid event index.
FailedAttempts	The number of times the alarm variable was polled (in the active state) and no response was received.
Owner	The ID of the user who configured this entry.

RMON Thresholds 32bit Alarms

Field	Description
Interval	The interval in seconds over which the data is sampled and compared with the rising and falling thresholds. When setting this variable, care should be taken in the case of deltaValue sampling – the interval should be set short enough that the sampled variable is very unlikely to increase or decrease by more than 2^31 – 1 during a single sampling interval.
Variable	The variable to be sampled. Only variables that resolve to an ASN.1 primitive type of INTEGER (INTEGER, Integer32, Counter32, Counter64, Gauge, or TimeTicks) may be sampled.
SampleType	The method of sampling the selected variable and calculating the value to be compared against the thresholds.
Value	The value of the statistic during the last sampling period.
StartupAlarm	The alarm that may be sent when this entry is first set to valid.
Rising Threshold	A threshold for the sampled statistic. When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval was less than this threshold, a single event will be generated.
Rising EventId	The ID of the eventEntry that is used when a rising threshold is crossed.
Falling Threshold	A threshold for the sampled statistic. When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval was greater than this threshold, a single event will be generated.
Falling EventId	The ID of the eventEntry that is used when a falling threshold is crossed.
FailedAttempts	The number of times the alarm variable was polled (in the active state) and no response was received.
Owner	The ID of the user who configured this entry.

RMON Thresholds Events

Field	Description
Description	A comment describing this event entry.
Type	The type of notification that the probe will make about this event. In the case of log, an entry is made in the log table for each event. In the case of SNMP-trap, an SNMP trap is sent to one or more management stations.
Community	The community string.
LastTimeSent	When this event entry last generated an event. If this entry has not generated any events, this value will be N/A.
Owner	The entity that configured this entry and is therefore using the resources assigned to it.

RMON Thresholds Log

Field	Description
Time	When this log entry was created.
Description	A description of the event that activated this log entry.

Admin

The following sections provide more information in these areas:

- Copy Configuration
- Flash Files
- Compact Flash
- License Features
- License Manager Keys
- License Manager Install
- License Manager Usage
- Port Licensing
- Feature Set
- Feature Control
- NTP Servers
- NTP General
- Running Processes
- Show Startup/Running Config
- Show EPLD Version
- Copy Flash Files
- Generate TAC Pac File
- Show Tech Support
- Show Image Version
- Show Onboard Log
- Summary View
- RLIR ERL
- Preferred Host
- Preferred Path
- Edit iSCSI Advertised Interfaces
- DNS General
- DNS Servers
- Cisco Fabric Services (CFS) Features
- Cisco Fabric Services (CFS) IP Multicast
- Cisco Fabric Service (CFS) IP Static Peers
- Cisco Fabric Services (CFS) Feature by Region
- Cisco Fabric Services (CFS) All Region
- Cisco Fabric Services (CFS) Owner

- Cisco Fabric Services (CFS) Merge

Copy Configuration

Field	Description
From	Specifies the type of file to copy from.
To	Specifies the type of file to copy to.
ServerAddress	The IP address of the server from (or to) which to copy the configuration file.
FileName	The file name (including the path, if applicable) of the file.
Protocol	The protocol to be used for any copy.
UserName	Remote user name.
UserPassword	Remote user password
CopyState	Specifies the state of this config-copy request. The value of this object is instantiated only after the row has been instantiated. For example, after the CopyEntryRowStatus has been made active.
CopyFailCause	The reason why the config-copy operation failed. This object is instantiated only when the CopyState for this entry is in the failed state.

Flash Files

Field	Description
Name	Flash file name as specified by the user copying in the file.
Size (B)	Size of the file in bytes. Note that this size does not include the size of the file system file header.
Modified	Date and time the file was last modified.

Compact Flash

Field	Description
Device	Name of the device.
Partition	Flash partition name used to refer to a partition.
Size	Size of the partition.

License Features

Field	Description
Missing	Represents the number of missing usage licenses of this feature, when one or more installed license files containing this feature's license, are missing in the local system. Under normal condition, the value is 0.

Field	Description
Installed Type	A combination of demo, permanent, counted, unlicensed, inGracePeriod for that license.
Installed Count	Maximum number of concurrent usages of this license feature. This is the cumulative license usage count for this feature from all the installed license files, containing this feature's license information.
Status	Represents the number of current usages of this licensed feature.
ExpiryDate	Expiry date of the licensed feature.
GracePeriod	Represents the grace period left for this feature, in days/seconds. Grace period is the number of seconds either an unlicensed feature or a feature whose license has expired is allowed to run.
Errors	Errors, if any.
DefaultLicenses	The maximum number of concurrent usages of this license feature that is included by default.

License Manager Keys

Field	Description
LastModified	Represents the time when the license file contents was last modified.
Feature	Specifies the installed license file name.
Version	The version number of the license file.
Type	• permanent – Indicates permanent license
Count	• uncounted – Specified the uncounted license for this feature. • counted – Indicates the maximum number of concurrent uses of this licensed feature.

License Manager Install

Field	Description
HostId	Contains the License hostid of the local system. It is used to identify the local system when requesting license(s) for this system.
URI	Represents the location on the local system, from which the license file will be picked for installation. User should have copied the license file provided by CISCO-CCO, by some other means (for example, through CLI) to this location. For example, the value could be 'bootflash:licfile1'. This MUST be set to a valid value before 'install'. For uninstall operation the value is irrelevant.
Target Filename	Represents either the name with which the license file will be installed, or the name of the license file for uninstall.

Status	The status of the license install/uninstall operation: • success (1) – install/uninstall operation completed successfully. • InProgress (2) – License install/uninstall operation is in progress. • corruptedLicenseFile (3) – License file content is Invalid/Corrupted. • targetLicenseFileAlreadyExist (4) – Target license file name already exist. • invalidLicenseFileName (5) – License file does not exist. • duplicateLicense (6) – License file is already installed. • licenseInUse (7) – Can't uninstall a license file which is in use. • generalLicensingFailure (8) – General error from license Manager. • none (9) – no install/uninstall operation is performed. • licenseExpiryConflict(10) – License exist with a different expiration date for the feature. • invalidLicenseCount(11) – License count is invalid for the feature. • notThisHost (12) – License host-id in the license file doesn't match. • licenseInGraceMore (13) – Number of licenses in grace period exceeds the number in install license file. • licenseFileNotFound (14) – License file not found, for install / uninstall / update operation. • licenseFileMissing (15) – A previously installed license file is found missing. • invalidLicenseFileExtension (16) – License file does not have a.lic extension. • invalidURI (17) – Invalid license file URI, specified for install operation. • noDemoLicenseSupport (18) – Demo License Not Supported. • invalidPlatform (19) – Invalid Platform

License Manager Usage

Field	Description
Name	Represents the name of the application which has checked out the feature.
Application	The application which has checked out the feature.

Port Licensing

Field	Description
Id	Displays the License host ID of the local system. It is used to identify the local system when requesting licenses.
Max	Maximum number of concurrent usages of this license.

Field	Description
Used	Represents the current number of usages of this licensed feature.

Feature Set

Field	Description
Name	The name of the feature set.
OpStatus	The current operating status of the feature.
Action	The action executed against the feature set.
LastCommand	The last action triggered for the feature set.
Result	The result of the last action that was applied to the feature set.

Feature Control

Field	Description
Feature Name	The name of the feature.
Status	The current operating status of the feature.
Action	Enable or disable a feature.
LastCommand	The result of the last action for the feature.
Result	The failure reason description for the failed execution of last action triggered for the feature.

NTP Servers

Field	Description
IP Address Type	The IP address type (IPv4 or IPv6) of the peer.
Name or IP Address	The name or IP address of the peer.
Mode	The association mode of the NTP server, with values coded as follows: Peer – A host operating in this mode sends periodic messages regardless of the reachability state or stratum of its peer. By operating in this mode the host, usually a LAN workstation, announces its willingness to be synchronized by, but not to synchronize the peer. Server – This type of association is ordinarily created upon arrival of a client request message and exists only in order to reply to that request, after which the association is dissolved. By operating in this mode the host, usually a LAN time server, announces its willingness to synchronize, but not to be synchronized by the peer.

Field	Description
Preferred	Specifies whether this peer is the preferred one over the others. By default, NTP chooses the peer with which to synchronize the time on the local system. If true, NTP will choose the corresponding peer to synchronize the time with. If multiple entries are true, NTP will choose the first one to be set.

NTP General

Field	Description
Leap	Two-bit code warning of an impending leap second to be inserted in the NTP timescale.
RootDelay	A signed fixed-point number indicating the total round-trip delay in seconds, to the primary reference source at the root of the synchronization subnet.
RootDispersion	The maximum error in seconds, relative to the primary reference source at the root of the synchronization subnet.

Running Processes

Field	Description
Name	The name associated with this process. If the name is longer than 32 characters, it will be truncated to the first 31 characters, and a `*' will be appended as the last character to imply this is a truncated process name.
MemAllocated (B)	The sum of all the dynamically allocated memory that this process has received from the system. This includes memory that may have been returned.
CPU Time (us)	The amount of CPU time the process has used, in microseconds.

Show Startup/Running Config

Field	Description
Startup	Backs up startup configuration of the switch to another computer with the specified file name.
Running	Backs up running configuration of the switch to another computer with the specified file name.
TCP Timeout	The value (in seconds) to wait for establishing TCP connection before timing out. Valid values are 1 to 120. A timeout results in abortion of the back up action.
FileName	To specify the name of the file where backup details are stored.
Compress File	Check the **Compress File** check box to compress the backup log file.

Show EPLD Version

Field	Description
Image URI	URI of the image.
Result	Version of the the image specified in the URI.

Copy Flash Files

Field	Description
Direction	Specifies the direction for file transfer.
Protocol	The protocol to be used for copy.
ServerAddress	The server address to be used.
RemoteUserName	Remote user name for protocols FTP, SFTP, and SCP.
RemotePassword	Remote user password used by FTP, SFTP or SCP.
Server File	Server file name, either in Flash or on a server, depending on the type of copy command. Mandatory. For a copy from Flash: File name must be of the form [device>:][:] where is a value obtained from FlashDeviceName, is obtained from FlashPartitionName and is the name of a file in Flash. If you copy files using xFTP protocol, server files may need to be located in a path that is relative to xFTP root path.**Note** You may need to manually modify the file path if required.
Switch File	Switch file name. For a copy to Flash: File name must be of the form {device>:][:] where is a value obtained from FlashDeviceName, is obtained from FlashPartitionName and is any character string that does not have embedded colon characters.

Generate TAC Pac File

You can download Tac-Pac in .zip format file.

Field	Description
Protocol	
TCP Timeout	The value (in minutes) to wait for establishing TCP connection before timing out. Valid values are 1 to 60. A timeout results in abortion of the back up action.
Management Interface	Allows you to choose the type of interface. The available options are: • default • vrf management • vrf default
ServerAddress	The server address to be used.
UserName	Remote user name.

Field	Description
UserPassword	Remote user password
FileName	The name of the file where the show tech support information will be captured.

Show Tech Support

Field	Description
TCP Timeout	The number (in seconds) to wait for the CLI before timing out.
FileName	The name of the file where the show tech support information will be captured.
Compress File	Check this check box to compress the text file into a ZIP file.

Show Image Version

Field	Description
Image URL	The URL of the image.
Result	The version of the image at the specified URL.

Show Onboard Log

Field	Description
Filter Log By	Module Number
Slot number of the card in the chassis.	Start Date
Specify a start time.	End Date
Specify an end time.	**Capture Show Onboard Log Output to File**
TCP Timeout	Specify a time-out interval from the drop-down list.
FileName	Name of the log file.
Compress File	Check the **Compress File** check box to compress the log file.

Summary View

Field	Description
Description	An alias name for the interface, as specified by a network manager. For Port Channel and FCIP, this field will always show members if they are available. For FCIP, this field will show compress if compressed.
VSAN(s)	VSAN membership.
Mode	Operating mode of the port> (See Legend).

Field	Description
Connected To	Attached port. This could be a host, storage, or switch port.NOTE: Device Manager connects and manages one switch at a time. If the switch with NPV switch connection information is stored in the core switch and the NPV switch is selected to view, the **Connected To** information will not be displayed.
Speed	Maximum bandwidth in Gbps.
Rx	One of the following: Utilization % Number of Bytes Number of Frames Average Frame Size
Tx	One of the following: Utilization % Number of Bytes Number of Frames Average Frame Size
Errors	Total number of Rx and Tx errors on the interface. Types of Rx errors include CRC errors, fragmented framed, unsupported class frames, runt frames, jabber frames, and giant Frames. Types of Tx errors are generally CRC errors, but these are rare. If the Errors field is not empty, there are probably Rx errors. For a more detailed breakdown of the error count, check the Monitor dialog box for appropriate interface.
Discards	Total number of Rx and Tx discards on the interface. Rx frames discarded are generally due to protocol errors. On rare occasions, a frame is received without any hardware errors, but a filtering rule set for the MAC address discards the frame due to a mismatch. Discarded Tx frames can be timeout frame discards (port is offline or not up), or timeout frames that are not sent back to the supervisor (class F/2 frames). If the Discards field is not empty, it is probably due to timeout frames.
Log	If checked, writes the record into the message log on each poll interval.

RLIR ERL

Field	Description
Vsan ID	VSAN Identifier of the port.
FC ID	Fibre Channel identifier of the subscribing Nx_Port.
Format	The device type for which the Nx_Port receives RLIR ELS."
RegType	The subscriber’s registration type. • ConditionalRx – The Nx_Port will be the recipient of a link incident record only if no other recipients from the ERL on the VSAN is chosen. • AlwaysRx – The Nx_Port will be always chosen as the recipient of a link incident records.

Preferred Host

Field	Description
Vsan ID	VSAN Identifier of the port.

PreFcid	Preferred Fibre Channel identifier of the subscribing Nx_Port.

Preferred Path

Field	Description
Interface	Represents an interface on the local device on which the matched or classified frame will be forwarded.
VSAN Id	The VSAN ID of this FC route map. An arbitrary integer value that identifies a route in this FC route map. Preference level, which indicates the metric or cost of the preferred path. The lower the number the higher the preference.
DestinationDomain	
FCID	The FC ID that needs to be matched with a source address in a frame for flow classification.
Description	
Primary ISL	
Secondary ISL	

Edit iSCSI Advertised Interfaces

Field	Description
Num	The number of the iSCSI target.
Interface	The interface over which the target is to be advertised.

DNS General

Field	**Description**
Enable	Enables or disables DNS configuration.
Domain Name	The name of the domain where the DNS server is enabled.

DNS Servers

Field	**Description**
IP Address	The IP Address of the DNS server.

Cisco Fabric Services (CFS) Features

Field	**Description**
Globally Enabled	Check this box to allow CFS on this switch to distribute feature configurations to other switches. Uncheck the box to prevent CFS from distributing the configuration to other switches.

Field	Description
Feature	The name of the CFS-capable feature.
Status	Status of the CFS-capable feature.
Command	The action to be triggered for the feature. Actions include: • noop - No operation. • enable - Enable CFS distribution on the switch. • disable - Disable CFS distribution on the switch. • commit - Commit changes made since the session began. • abort - Discard changes made, and close the session. • clear - Discard changes made without closing the session.
Type	The last CFS feature scope type used.
VSAN Id	The ID of the VSAN on which this feature is running.
RegionId	The distribution region ID that this CFS capable feature maps to. This region is required to be defined prior to its usage.
View Config Changes As	Determines whether to view the changes as running or pending. A pending configuration exists until a Commit or Abort action is triggered for that feature. If the value is running then all subsequent configuration retrieval for this feature will be from the running configuration on the local device. If the value is pending then all subsequent configuration retrieval for this feature will be from the pending configuration on the local device.
LastCommand	The last action performed on this feature.
Result	Result of the action performed on the CFS-capable feature.
Scope	The value of this object represents the attributes of a CFS-capable feature as registered with the CFS infrastructure. • fcFabric - indicates that the CFS based distribution for a feature spans the entire FC (Fibre Channel) fabric • ipNetwork - indicates that the CFS based distribution for a feature spans the entire IP network • vsanScope - indicates that the CFS based distribution for a feature is done on per VSAN basis and restricted to a specific VSAN in a FC (Fibre Channel) fabric
PendingConfOwnerAddr	The address of the device in the fabric where the pending configuration exists for the feature.
Lock Owner Switch	The address of the device in the fabric where the pending configuration exists for the feature within this scope.
Lock Owner UserName	The name of the device in the fabric where the pending configuration exists for the feature within this scope.

Field	Description
Merge Status	The result of the last fabric merge for this feature within the context of the combination of scope type and scope value in the system. The following are the results: • Success-Fabric merge completed successfully. • InProgress-Fabric merge in progress. You may get this status when the local device that is a part of fabric engaged in the process of merging with another fabric. • Failure-Fabric merge failed. • Waiting-Waiting for existing merge to complete while the conflicts are being cleared. You may get this status when the local device that is a part of fabric waiting for any conflicts to be resolved before initiating a new instance of fabric merge. • Other-None of the other values of this enumeration.
Master	Select the CFS Master switch.

Cisco Fabric Services (CFS) IP Multicast

Field	Description
IP Address Type	The IP address type (IPv4, IPv6, or DNS).
Multicast Address Domain	The multicast address domain to which the CFS distribution is restricted. There is a default multicast address for both IPv4 and IPv6 through which the keep-alive messages are sent and received to discover the CFS capable switches over IP. All switches with similar multicast address form one CFS-over-IP fabric. The default multicast address for IPv4 is 239.255.70.83 and range supported is [239.255.0.0 - 239.255.255.255] The default multicast address for IPv6 is ff13::7743:4653 and the supported range is [ff13::0000:0000 - ff13::ffff:ffff]
Action	Specifies the current operating mode employed in CFS for distribution over the corresponding type of Internet address. By setting the value of this object to 'enable', CFS will enable its capability to distribute the application data across the fabric over the corresponding type of Internet address. By setting the value of this object to 'disable', CFS will disable its capability to distribute the data across the fabric over the corresponding type of Internet address.

Cisco Fabric Service (CFS) IP Static Peers

Field	Description
IP Static Peer	Specifies the address of a CFS peer device intended for distribution.
DiscStatus	Specifies a a user defined peer device intended for CFS distribution.

Cisco Fabric Services (CFS) Feature by Region

Field	Description
Feature	Identifies the name of a CFS-capable feature within a distribution region.
RegionId	Identifies a CFS distribution region.

Cisco Fabric Services (CFS) All Region

Field	Description
RegionId	Identifies a CFS distribution region.

Cisco Fabric Services (CFS) Owner

Field	Description
Feature, VSAN	The name of the CFS-capable feature, and the VSAN in which the feature is enabled or committed.
Name or IP Address	The name or IP address of the switch on which the feature is enabled or committed.
UserName	The name of the user who enabled or committed the feature.
Type	The last CFS feature scope type used.

Cisco Fabric Services (CFS) Merge

Field	Description
Feature	The name of the CFS-capable feature.
CFS Merge Status Value	The result of the last fabric merge that occurred.

Logs

The following sections provide more information in these areas:

- SysLog (Since Reboot)
- SysLog (Severe Events)
- Accounting Log
- Switch Logging
- Syslog Severity Levels
- Syslog Servers

SysLog (Since Reboot)



To see the latest logs, please close and launch the Log dialog. 'Refresh' option is not available for page by page dialog.

Field	Description
Switch Time	The local time on the switch.
Facility	Name of the facility that generated the message.
Severity	The severity of the message.
Event	The name of the event being logged
VSAN Id	The VSAN on which the event occurred.
Host Time	The local time on the host.
Description	A description of the event being logged.

SysLog (Severe Events)

Field	Description
Switch Time	The local time on the switch.
Facility	Name of the facility that generated the message.
Severity	The severity of the message.
Event	The name of the event being logged
VSAN Id	The VSAN on which the event occurred.
Host Time	The local time on the host.
Description	A description of the event being logged.

Accounting Log



To see the latest logs, please close and launch the Log dialog. 'Refresh' option is

not available for page by page dialog.

Field	Description
Switch Time	The local time on the switch.
Action	The action that occurred (start, stop, or update).
Protocol & Source	The protocol and the IP address of the source switch.
User	The name of the user.
Description	A description of the action, if applicable.

Switch Logging

Field	Description
ConsoleEnable	Indicate whether the Syslog messages should be sent to the console.
ConsoleMsgSeverity	Minimum severity of the message that are sent to the Console.
TerminalEnable	Indicate whether the Syslog messages should be sent to the terminals.
TerminalMsgSeverity	Minimum severity of the message that are sent to the terminals.
LinecardEnable	Indicate whether the Syslog messages should be generated at the line cards.
LinecardMsgSeverity	Minimum severity of the message that are sent from linecards.
LogFileMsgSeverity	Minimum severity of the message that are sent to the log file.
SyslogLogFileName	Name of file to which the Syslog messages are logged.

Syslog Severity Levels

Field	Description
Facility	Batch process that generates messages.
Severity	Minimum severity of the message that are generated by this Syslog message facility.

Syslog Servers

Field	Description
IPAddress Type	The IP address type (IPv4, IPv6, or DNS).
Name or IP Address	The address of the Syslog server.
MsgSeverity	Minimum severity of the message that are sent to this Syslog server.
Facility	The facility to be used when sending Syslog messages to this server.

End Devices - Hosts

Field	Description
Host Enclosure	Name of the host enclosure
Name	Name of the VMware
IP Address	IP Address of the VMware
CPU Count	CPU Count of the VMware
Memory Size	Memory Size of the VMware
Status	Current status of the VMware.
OS	OS of the VMware.
Data Store	Name of the VMware datastore.
Last Update Time	Time at which the DCNM-SAN Server last updated the VMware.

Intelligent Features - Summary

Field	Description
Switch	IP address of the switch.
Module	Name of the module.
Name	Name of the switch.
IOA	Display enabled if the IOA feature is enabled. The field will be blank if this feature is disabled.
DMM	Display enabled if the DMM feature is enabled. The field will be blank if this feature is disabled.
SANTap	Display enabled if the SANTap feature is enabled. The field will be blank if this feature is disabled.

Data Mobility Manager - Modules

Field	Description for a Job Row	Description for a Session Row
Name	The name of the job.	This field is blank.
ID	System-assigned unique identifier for the job.	The session number within the job.
Mode	Server mode or storage mode.	This field is blank.
Existing Storage	Alias name of the port on the existing storage.	LUN number on the existing storage.
New Storage	Alias name of the port on the new storage.	LUN number on the new storage.
Status	Status of the job. A created or scheduled job has not yet started. An in-progress job is currently performing the migration. A completed or verified job has finished successfully. A stopped, failed or reset job has finished unsuccessfully.	Status of the session.
Time	Date and time that the job is scheduled to start. This field is blank if the job has not been scheduled. If the job is in progress, this field displays the date and time that the job started.	If the session is in progress, this field displays the estimated duration remaining until the session completes. Otherwise, the field is blank.
SSM1	Switch number and slot of the SSM executing the migration job.	Displays **On SSM 1** if the session is executing on SSM 1.
SSM2	Switch number and slot of the SSM executing the migration job.	Displays **On SSM 2** if the session is executing on SSM 2.
Type	Online or offline migration.	This field is blank.
Rate	Best effort, slow, medium or fast. You set the rate when you configure the migration job.	This field is blank.

Storage Media Encryption

The following sections provide more information in these areas:

- Members
- Interfaces
- Hosts

Members

Field	Description
Cluster	SME cluster name.
State	The operational state of the SME cluster.
Master	Identifies the SME cluster master's IP address.
Members	Identifies the IP address of the switch that is a member of the SME cluster.
IsLocal?	Identifies if the switch is a local or remote member of this cluster.

Interfaces

Field	Description
Cluster	Identifies the cluster to which this SME interface belongs.
Interfaces	Identifies the SME interface.
State	Operational state of this SME interface.

Hosts

Field	Description
Host	Fibre-channel port name (P_WWN) of the host Nx_Port.
Cluster	Identifies the cluster to which this host port belongs.

SSM Features

The following sections provide more information in these areas:

- Summary
- FCWA
- SSM
- MSM
- SANTap CVT
- SANTap DVT
- NASB
- NASB Target
- Virtual Initiator
- DMM Rate
- FCWA Config Status
- Statistics Status
- Statistics I/O Traffic
- Statistics I/O Traffic Details
- Statistics SCSI Commands
- Statistics SCSI Errors
- Statistics SCSI Sense Errors
- Compact

Summary

Field	Description
Switch	Name of the switch on the intelligent module.
Module	Slot number of the intelligent module.
Name	Name of the intelligent module.
IOA	IOA state of the intelligent module.
DMM	DMM state of the intelligent module.
SANTap	SANTap state of the intelligent module.
SE	SE state of the intelligent module.

FCWA

Field	Description
Flow Id	Represents the flow identifier.

Field	Description
Init WWN	Represents the pWWN of the initiator in the flow.
Init VSAN	The VSAN ID of the initiator on which the flow is configured.
Target WWN	Represents the pWWN of the target in the flow.
TargetVSAN	The VSAN ID of the target on which the flow is configured.
WriteAcc	Specifies if write-acceleration feature is enabled for this flow. If set to true it is enabled. If set to false, it is disabled.
BufCount	It specifies the number of buffers to be used for write-acceleration.
Stats Enable	Specifies if the statistics gathering needs to be enabled for this flow. If set to true, then it is enabled. If it is set to false, then it is disabled.
Stats Clear	Assists in clearing the statistics for this flow.
Init Verification	The verification status of the initiator device corresponding to the SCSI flow.
Init Module	The status of the linecard where the SCSI flow initiator device is located.
Target Verification	The verification status of the target device corresponding to the SCSI flow.
Target Module	The status of the linecard where the SCSI flow target device is located.

SSM

Field	Description
StartPort, EndPort, Feature	A table containing feature related information for interfaces. This table gives a list of interfaces that are assigned to different features. The interfaces supported are of the type Fibre Channel.
PartnerImageURI	A collection of objects related to SSM Feature to interface mapping.

MSM

Field	Description
Switch	Name of the switch on the MSM module.
Module, StartNode, EndNode, Feature	A table containing the feature related information, such as the MSM module number, the node range that are assigned to different features.



The difference between MSM (Multiservice Modules) and SSM (Services Module) is that SSM could enable the features per port range on a card. For MSM you have to enabled it on the whole card.

SANTap CVT

Field	Description
Node WWN	Represents the node world wide name of the CVT created on the module.

Field	Description
Port WWN	Represents the port world wide name of the CVT created on the module.
Name	The administratively assigned name for this CVT.

SANTap DVT

Field	Description
VSAN Id, Port WWN	Represents the port world wide name of the created DVT. It will be the same as the port world wide name of the real target for which data is to be replicated.
Interface	Represents the port on the module where the DVT will be created.
Target VSAN Id	Represents the VSAN of the real target for which this DVT is being created.
Name	The administratively assigned name for this DVT.
LUNSize Handling	Indicates whether the DVT should use the real target LUN size for the virtual LUN or the max LUN size supported which is 2TB.
IO Timeout (sec)	Represents the IO timeout value associated with the DVT. This object should be set during the DVT creation time and cannot be modified later.
Target IO Timeout (sec)	Represents the target IO timeout value associated with the DVT.

NASB

Field	Description
Control	Specifies the device type for the LUNs exposed by the TPC target. A value of 1 sets the device type to the default value of disk. A value of 2 sets the device type to storage array controller. Other values are reserved for future changes.
Multiple	Specifies whether the TPC target is operating in a single LUN or multi-LUN mode. A value of 1 sets the default mode which is single LUN. A value of 2 sets multi LUN mode in which the TPC target exposes 10 LUNs.

NASB Target

Field	Description
Module, VSAN Id, Processor Id	The unique ID number associated with the TPC target. This ID number is unique within the VSAN in which the TPC target is configured.
Virtual Target Node WWN	The TPC target's node world wide name.
Virtual Target Port WWN	The TPC target's port world wide name.
State	The current state of the TPC target.

Field	Description
XCOPY Num	The total number of xcopy commands processed by the TPC target since the module on which this target has been configured has been online.
XCOPY MinData (KB)	The smallest amount of data in kilobytes transferred by the TPC target in a single xcopy command since the module on which this target has been configured has been online.
XCOPY MaxData (KB)	The largest amount of data in kilobytes transferred by the TPC target in a single xcopy command since the module on which this target has been configured has been online.
XCOPY Avgthruput (KBps)	The average kilobytes per second throughput of the TPC target in processing the xcopy commands.

Virtual Initiator

Field	Description
Processor Id	The DPP ID.
Control	If false, it’s the data path. If true, it’s the control path.

DMM Rate

Field	Description
Fast(MBps)	Specifies the migration rate value for the fast attribute for a specific module.
Medium(MBps)	Specifies the migration rate value for the medium attribute for a specific module.
Slow(MBps)	Specifies the migration rate value for the slow attribute for a specific module.

FCWA Config Status

Field	Description
Overall	The configuration status for write-acceleration feature for this flow.
Initiator	The initiator configuration status for write-acceleration feature for this flow.
Target	The target configuration status for write-acceleration feature for this flow.

Statistics Status

Field	Description
Overall	The configuration status for statistics feature for this flow.
Initiator	The initiator configuration status for statistics feature for this flow.

Field	Description
Target	The target configuration status for statistics feature for this flow.

Statistics I/O Traffic

Field	Description
IOs Read	The total number of SCSI read operations on this LUN on this flow.
IOs Write	The total number of SCSI write operations on this LUN on this flow.
Blocks Read	The total number of blocks that have been read on this LUN on this flow.
Blocks Write	The total number of blocks that have been written on this LUN on this flow.
Bytes Rx	The total number of octets received in link-level frames on this LUN on this flow.
Bytes Tx	The total number of octets transmitted in link-level frames on this LUN on this flow.
Frames Rx	The total number of link-level FC frames received on this LUN on this flow.
Frames Tx	The total number of link-level frames transmitted on this LUN on this flow.

Statistics I/O Traffic Details

Field	Description
Timeouts Read	The total number of SCSI read operations that have timed out on this LUN on this flow.
Timeouts Write	The total number of SCSI write operations that have timed out on this LUN on this flow.
MaxBlocks Read	The maximum number of blocks read across all read operations on this LUN on this flow.
MaxBlocks Write	The total number of blocks that have been written on this LUN on this flow.
MaxTime Read	The maximum response time over all read operations on this LUN on this flow.
MaxTime Write	The maximum response time over all write operations on this LUN on this flow.
MinTime Read	The minimum response time over all read operations on this LUN on this flow.
MinTime Write	The minimum response time over all write operations on this LUN on this flow.
Active Read	The number of read operations that are currently active on this LUN on this flow.
Active Write	The number of write operations that are currently active on this LUN on this flow.

Statistics SCSI Commands

Field	Description
TestUnitRdys	The number of test unit ready SCSI commands sent on this LUN on this flow.
RepLuns	The number of report LUN SCSI commands sent on this LUN on this flow.
Inquirys	The number of SCSI inquiry commands sent on this LUN on this flow.
RdCapacitys	The number of read capacity SCSI commands sent on this LUN on this flow.
ModeSenses	The number of mode sense SCSI commands sent on this LUN on this flow.
ReqSenses	The number of request sense SCSI commands sent on LUN on this flow.

Statistics SCSI Errors

Field	Description
BusyStatuses	The number of busy SCSI statuses received on this LUN on this flow.
StatusResvConfs	The number of reservation conflicts SCSI status received on this LUN on this flow.
TskSetFulStatuses	The number of task set full SCSI statuses received on this LUN on this flow.
AcaActiveStatuses	The number of ACA active statuses received on this LUN on this flow.

Statistics SCSI Sense Errors

Field	Description
NotRdyErrs	The number of NOT READY SCSI SENSE key errors received on this LUN on this flow. This indicates that the logical unit being addressed cannot be accessed.
MedErrs	The number of MEDIUM ERROR SCSI SENSE key errors received on this LUN on this flow. This indicates that the command terminated with a non-recovered error condition possibly caused by a flaw in the medium.
HwErrs	The number of HARDWARE ERROR SCSI SENSE key errors received on this LUN on this flow. This indicates that the target detected a non-recoverable hardware failure.
IllReqErrs	The number of ILLEGAL REQUEST SCSI SENSE key errors received on this LUN on this flow.
UnitAttErrs	The number of UNIT ATTENTION SCSI SENSE key errors received on this LUN on this flow.
DatProtErrs	The number of DATA PROTECT SCSI SENSE key errors received on this LUN on this flow.

Field	Description
BlankErrs	The number of BLANK CHECK SCSI SENSE key errors received on this LUN on this flow.
CpAbrtErrs	The number of COPY ABORTED SCSI SENSE key errors received on this LUN on this flow.
AbrtCmdErrs	The number of ABORTED COMMAND SCSI SENSE key errors received on this LUN on this flow.
VolFlowErrs	The number of VOLUME OVERFLOW SCSI SENSE key errors received on this LUN on this flow.
MiscmpErrs	The number of VOLUME OVERFLOW SCSI SENSE key errors received on this LUN on this flow.

Compact

Field	Description
Device	This is the flash device sequence number to index, used within the table of initialized flash devices. The lowest value should be 1. The highest should be less than or equal to the value of the ciscoFlashDevicesSupported object
Partition	This is the flash partition name used to refer to a partition by the system. This can be any alpha-numeric character string of the form AAAAAAAAnn, where A represents an optional alpha character and n a numeric character. Any numeric characters must always form the trailing part of the string. The system will use only the numeric portion to map to a partition index. Flash operations get directed to a device partition based on this name. The system has a concept of a default partition. This would be the first partition in the device. The system directs an operation to the default partition whenever a partition name is not specified. The partition name is therefore mandatory except when the operation is being done on the default partition, or the device has just one partition (is not partitioned).
Size	This is the flash partition size. It should be an integral multiple of ciscoFlashDeviceMinPartitionSize. If there is a single partition, this size will be equal to ciscoFlashDeviceSize.