Cambium Networks

cnMatrix Parameters and Commands

Table of Contents

L2 Features

cnMatrix VLAN Parameters and Commands

Commands	Description	CLI Mode
`vlan <vlan-id>`	Creates a VLAN and enters into the config-VLAN mode in which VLAN specific configurations are done and sets the VLAN in active mode.	Global Configuration
`name <vlan name string>`	Configures name for the VLAN.	Config-VLAN
`protocol-vlan`	Enables protocol-VLAN based membership classification on all ports of the switch.	Global Configuration

`map protocol {ip | novell | netbios | appletalk | other <aa:aa or aa:aa:aa:aa:aa>} {enet-v2 | snap | llcOther | snap8021H | snapOther} protocols-group <Group id integer(0-2147483647)>`
`TBD`
	Creates a protocol group with a specific protocol and encapsulation frame type combination.	Global Configuration

`ports [add] [(gigabitethernet/extreme-ethernet/port-channel)]`	Configures a VLAN entry with the required member ports, untagged ports and/or forbidden ports, and activates the VLAN.	Config-VLAN
`ports [add] ([<interface-type> <0/a-b,0/c,...>] [<interface-type> <0/a-b,0/c,...>] [port-channel <a,b,c-d>]) [untagged <interface-type> <0/a-b,0/c,...> [<interface-type> <0/a-b,0/c,...>] [port-channel <a,b,c-d>][all])] [forbidden <interface-type> <0/a-b,0/c,...> [<interface-type> <0/a-b,0/c,...>] [port-channel <a,b,c-d>]` The `<interface-type>` parameter can have the following values: • gigabitethernet • extreme-ethernet • port-channel	Configures a VLAN entry with the required member ports, untagged ports and/or forbidden ports, and activates the VLAN. The VLAN can also be activated using the vlan active command.	Config-VLAN
`vlan active`	Activates a VLAN in the switch.	Config-VLAN
`switchport access vlan <vlanid (1-4094)>`	Configures the PVID (Port VLAN Identifier) on a port.	Interface Configuration (Physical /

cnMatrix Parameters and Commands

Commands	Description	CLI Mode
		Port Channel)
switchport acceptable-frame-type {all | tagged | untaggedAndPrioritytagged } Available options: • all - configures the acceptable frame type as all. • tagged - configures the acceptable frame type as tagged. • untaggedAndPrioritytagged - configures the acceptable frame type as untagged and priority tagged.	Configures the type of VLAN dependent BPDU frames such as GMRP BPDU that the port should accept during the VLAN membership configuration.	Interface Configuration (Physical / Port Channel)
switchport ingress-filter	Enables ingress filtering feature on the port.	Interface Configuration (Physical / Port Channel)
port protocol-vlan	Enables protocol-VLAN based membership classification in a port.	Interface Configuration (Physical Interface)
switchport map protocols-group <Group id integer(0-2147483647)> vlan <vlan-id> Available options: • <Group id integer(0-2147483647)> - configures a unique group ID that is already created with the specified protocol type and encapsulation frame type.	Maps the configured protocol group to a particular VLAN ID for an interface.	Interface Configuration (Physical / Port Channel)
switchport mode { access | trunk | hybrid | {private-vlan {promiscuous | host }} |{dynamic {auto | desirable}} } Available options: • access - configures the port as access port that accepts and sends only untagged. • trunk - configures the port as trunk port that accepts and sends only tagged frames. • hybrid - configures the port as hybrid port that accepts and sends both tagged and untagged frames.	Configures the mode of operation for a switch port.	Interface Configuration (Physical / Port Channel)
debug vlan { [{fwd | priority | redundancy}([initshut] [mgmt] [data] [ctpl] [dump] [os] [failall] [buffer] [all])] [switch <context_name>] }[{ <short (0-7)> | alerts | critical | debugging | emergencies | errors | informational | notification | warnings }] Available options:	Enables the tracing of the VLAN sub module as per the configured debug levels.	Privileged Exec

cnMatrix Parameters and Commands

Commands	Description	CLI Mode
• `fwd` - sets the submodule as VLAN forward module, for which the tracing is to be done as per the configured debug levels. • `priority` - sets the submodule as VLAN priority module, for which the tracing is to be done as per the configured debug levels. • `redundancy` - sets the submodule as VLAN redundancy module, for which the tracing is to be done as per the configured debug levels. • `initshut` - generates debug statements for init and shutdown traces. • `switch <context_name>` - configures the tracing of the VLAN submodule for the specified context. • `mgmt` - generates debug statements for management traces. • `dump` - Generates debug statements for packet dump traces. • `failall` - generates debug statements for all kind of failure traces. • `buffer` - generates debug statements for VLAN buffer related traces. • `ctpl` - generates debug statements for control path traces. • `os` - generates debug statements for OS resource related traces. • `data` - generates debug statements for data path traces.		
`show vlan [brief | id <vlan-range> | summary | ascending]`	Displays VLAN entry related information of all active VLANs and VLANs (that are not active) for which the port details are configured.	Privileged Exec
`show vlan device info`	Displays the VLAN global information that is applicable to all VLANs created in the switch / all contexts.	Privileged Exec
`show vlan protocols-group`	Displays all entries in the protocol group table.	Privileged Exec
`show protocol-vlan`	Displays all entries in the port protocol table.	Privileged Exec
`show mac-address-table [vlan <vlan-range>]`	Displays all static / dynamic unicast and multicast MAC entries created in the MAC address table for the specified VLANs alone.	Privileged Exec
`show mac-address-table static unicast [vlan <vlan-range>] [address <aa:aa:aa:aa:aa:aa>] [{interface <interface-type> <interface-id>` Available options:	Displays all static unicast MAC address entries created in the FDB table.	Privileged Exec

cnMatrix Parameters and Commands

Commands	Description	CLI Mode
• vlan <vlan-range> - displays all static unicast MAC address entries created in the FDB table for the specified VLANs alone. • address <aa:aa:aa:aa:aa:aa> - displays all static unicast MAC address entries created in the FDB table for the specified unicast MAC address. • interface - displays all static unicast MAC address entries for the specified interface.		
show mac-address-table dynamic unicast [vlan <vlan-range>] [address <aa:aa:aa:aa:aa:aa>] [{interface <interface-type> <interface-id> Available options: • vlan <vlan-range> - displays all dynamically learnt unicast entries from the MAC address table for the specified VLANs alone. • address <aa:aa:aa:aa:aa:aa> - displays all dynamically learnt unicast entries from the MAC address table for the specified unicast MAC address. • interface - displays all dynamically learnt unicast entries from the MAC address table for the specified interface.	Displays all dynamically learnt unicast entries from the MAC address table.	Privileged Exec
show mac-address-table dynamic multicast [vlan <vlan-range>] [address <aa:aa:aa:aa:aa:aa>] [{interface <interface-type> <interface-id>}] Available options: • vlan <vlan-range> - displays all dynamically learnt multicast entries from the MAC address table for the specified VLANs alone. • address <aa:aa:aa:aa:aa:aa> - displays all dynamically learnt multicast entries from the MAC address table for the specified unicast MAC address. • interface - displays all dynamically learnt multicast entries from the MAC address table for the specified interface.	Displays all dynamically learnt multicast entries from the MAC address table.	Privileged Exec
show mac-address-table aging-time	Displays the ageing time configured for the MAC address table.	Privileged Exec
clear mac-address-table dynamic [interface {port-channel <port-channel-id (1-65535)> |	Clears the dynamically learnt MAC Addresses.	Global Configuration

cnMatrix Parameters and Commands

Commands	Description	CLI Mode
`<interface-type> <interface-id>}] [vlan <vlan_>]` Available options: • `port-channel <port-channel-id (1-65535)>` - Clears the FDB entries for the specified port channel interface. • `<interface-type>` - Clears the FDB entries for the specified type of interface. • `gigabitethernet` • `<vlan -id>` - VLAN ID is a unique value that represents the specific VLAN.		
`debug vlan global`	Enables tracing in VLAN sub module and generates debug statements for global traces for the specified severity levels.	Privileged Exec

cnMatrix RSTP Parameters and Commands

Commands	Description	CLI Mode
`spanning-tree mode` Available options: • `mst` • `rst` • `pvrst`	Sets the type of spanning tree to be executed, enables spanning tree operation and starts spanning tree functionality in the switch.	Global Configuration
`no spanning-tree`	Disables the spanning tree operation in the switch.	Global Configuration
`spanning-tree compatibility {stp | rst | mst}` Available options: • `stp` • `rst` • `mst` ⚡ The STP compatibility version cannot be set as mst, if the spanning tree Mode is set as rst.	Sets the STP compatibility version in the switch for all ports. The compatibility version allows the switch to temporarily operate (that is, till this configuration is reset manually) in other STP version even though the spanning tree Mode is set as some other version. ⚡ This configuration is useful during cases where spanning tree Mode itself is not required to be changed.	Global Configuration
`spanning-tree {forward-time <seconds(4-30)> | hello-time <seconds(1-2)> | max-age <seconds(6-40)>}` Available options: • `forward-time` • `hello-time`	Sets the spanning tree timers such as hello time used for controlling the transmission of BPDUs during the computation of loop free topology.	Global Configuration

Commands	Description	CLI Mode
- `max-age`		
`spanning-tree transmit hold-count <value (1-10)>` ⚡ If the spanning tree mode is set as mst, the default values is 6 and if the spanning tree mode is set as rst or pvrst, the default value is 3.	Sets the transmit hold-count value for the switch, where the value is a counter that is used to limit the maximum transmission rate of the switch and to avoid flooding. This value specifies the maximum number of packets that can be sent in a given hello time interval. This value ranges from 1 to 10.	Global Configuration
`clear spanning-tree counters[interface <interface-type> <interface-id>]`	Deletes all bridge and port level spanning tree statistics information.	Global Configuration
`spanning-tree pathcost dynamic [lag-speed]` The following parameter is available for this command: - `lag-speed` - Calculates the path cost for change in speed of the port.	Enables dynamic pathcost calculation feature in the switch.	Global Configuration
`spanning-tree priority <value(0-61440)>` Available options: - `mst <instance-id>` - Configures the ID of MSTP instance already created in the switch. - `priority <value(0-61440)>` - Configures the priority value for the switch and for the MSTI, in RSTP and MSTP respectively.	Configures the priority value that is assigned to the switch.	Global Configuration
`spanning-tree auto-edge`	Enables the automatic detection of the Edge port parameter of an interface.	
`spanning-tree [{cost <value(0-200000000)>|disable|link-type{point-to-point|shared}|portfast|port-priority <value(0-240)>}]` Available options: - `cost <value(0-200000000)>` - port's path cost value. - `disable` - Disables the spanning tree operation on the port. - `link-type` - Configures the link status of the LAN segment attached to the port. The following options are available: - `point-to-point` – The port is treated as if it is connected to a point-to-point link. - `shared` - The port is treated as if it is using a shared media connection. - `portfast` - `port-priority <value(0-240)>` - Configures the priority value assigned to the port.	Configures the port related spanning tree information for all kinds of STPs.	Interface Configuration (Physical Interface)

cnMatrix Parameters and Commands

Commands	Description	CLI Mode
`spanning-tree portfast {bpdufilter default | default}` Available options: - `bpdufilter default` - Enables BPDU filtering on all PortFast ports. - `default` - Enables PortFast by default on all access ports.	Configures the portfast of the non-trunk ports as bpdufilter default or bpduguard default or default.	Global Configuration
`spanning-tree restricted-role`	Enables the restricted role feature for a port.	Interface Configuration (Physical Interface)
`spanning-tree restricted-tcn`	Enables the topology change guard / restricted TCN feature on a port.	Interface Configuration (Physical Interface)
`spanning-tree layer2-gateway-port`	Configures a port to operate as a L2GP.	Interface Configuration (Physical Interface)
`spanning-tree bpdu-receive {enabled | disabled}` Available options: - `enabled` - Allows the normal processing of the BPDUs received on the port. - `disabled` - Discards the BPDUs received on the port.	Configures the processing status of the BPDUs received in a port.	Interface Configuration (Physical Interface)
`spanning-tree bpdu-transmit {enabled | disabled}` Available options: - `enabled` - Allows the transmission of BPDUs from the port. - `disabled` - Blocks the transmission of BPDUs from the port.	Configures the BPDU transmission status of a port. ⚡ The BPDU transmission status cannot be enabled on the port that is configured as L2GP.	Interface Configuration (Physical Interface)
`spanning-tree loop-guard` ⚡ This feature can be configured, only if the spanning tree functionality is not shut down in the switch.	Enables the loop guard feature in a port.	Interface Configuration (Physical Interface)
`spanning-tree [mst <instance-id>] pseudoRootId priority <value(0-61440)> mac-address <ucast_mac>` Available options: - `mst <instance-id>/ mst <instance-id(1-64)>` - `priority <value(0-61440)>` - `mac-address`	Configures the pseudo root related information for a port set as L2GP.	Interface Configuration (Physical Interface)
`clear spanning-tree detected protocols [{interface <interface-type> <interface-id>}]` Available options: - `interface <interface-type> <interface-id>` - Restarts the protocol migration process on the specified interface.	Restarts the protocol migration process on all interfaces in the switch and forces renegotiation with the neighboring switches.	Privileged EXEC

cnMatrix Parameters and Commands

Commands	Description	CLI Mode
`show spanning-tree detail`	Displays detailed spanning tree related information of the switch and all ports enabled in the switch.	Privileged EXEC
`show spanning-tree active [detail]` Available options: • `detail`	Displays spanning tree related information available in the switch for the current STP enabled in the switch.	Privileged EXEC
`show spanning-tree interface <interface-type> <interface-id> [{cost | encapsulationtype | priority | portfast | rootcost | restricted-role | restricted-tcn | state | stats | detail }]`	Displays the port related spanning tree information for the specified interface.	Privileged EXEC
show spanning-tree root [{ address | cost | forward-time | id | max-age | port | priority | detail }] Available options: • `address` - Displays the MAC address of the root bridge. • `cost` - Displays the cost of the root bridge. • `forward-time` - Displays the forward delay time of the root bridge. • `id` - Displays the ID of the root bridge. • `max-age` - Displays the maximum age time of the root bridge. • `port` - Displays the ID of the root port. • `priority` - Displays the priority of the root bridge. • `detail` - Displays the root priority, root address, root cost, root port, forward delay time and maximum age time.	Displays the spanning tree root information.	Privileged EXEC
`show spanning-tree bridge [{ address | forward-time | hello-time | id | max-age | protocol | priority | detail }]`	Displays the spanning tree bridge information.	Privileged EXEC
`show spanning-tree [interface <interface-type> <interface-id>] layer2-gateway-port` Available options: • `<interface-type>` • `<interface-id>`	Displays the spanning tree information for all L2GPs enabled in the switch.	Privileged EXEC
`spanning-tree forwarddelay optimization alternate-role {enabled | disabled}`	Enables or disables the optimization for spanning-tree related protocol during transition from alternate to designated port role.	Global Configuratio
`show spanning-tree interface <ifnum> bpduguard` Available options:	Displays the spanning-tree bpduguard configuration for RSTP, MSTP and PVRST	Privileged EXEC

cnMatrix Parameters and Commands

Commands	Description	CLI Mode
• `<ifnum>` - The spanning-tree bpduguard configuration for the specified interface identifier. • `Bpduguard` - The status of the BPDU guard feature for the interface.		
`show spanning-tree performance-data [interface <interface-type> <interface-id>]`	Displays the spanning-tree performance data for RSTP and MSTP.	Privileged EXEC
`spanning-tree bpduguard {disable | enable | none}`	Configures the status of the BPDU guard feature in an interface.	Interface Configuration (Physical Interface)
`show spanning-tree interface <ifnum> inconsistency`	Displays the spanning-tree root and loop inconsistent state information for RSTP, MSTP & PVRST.	Privileged EXEC
`set performance-data-status {enable | disable}`	Enables or disables the collection of performance data for the for RSTP and MSTP protocol.	Privileged EXEC
`spanning-tree bpdufilter {disable | enable }`	Configures the status of the BPDU filter feature in an interface.	Interface Configuration (Physical Interface)

cnMatrix MSTP Parameters and Commands

Commands	Description	CLI Mode
`spanning-tree mst configuration`	Enters the MSTP configuration Mode, where instance specific and MST region configuration can be performed.	Global Configuration
`spanning-tree mst max-instance <short(0-7)>`	Configures the maximum number of active MSTIs that can be created. This value ranges from 0 to 7.	Global Configuration
`spanning-tree mst {instance-id <instance-id(0-7)>} root {primary | secondary}`	Enables BPDU (Bridge Protocol Data Unit) transmission and reception on the interface.	Global Configuration
`spanning-tree mst forward-time <seconds(4-30)>`	Configures the forward timer of the spanning tree and the no form of the command sets the forward timer to the default value.	Global Configuration
`spanning-tree mst max-age <seconds(6-40)>`	Configures the max-age timer of the spanning tree.	Global Configuration
`spanning-tree mode mst`	Enables the spanning tree operating mode.	Global Configuration
`name <string(optional max Length)>`	Configures the name for the MST region.	MSTP Configuration
`revision <value(0-65535)>`	Configures the revision number for the MST region. This value ranges from 0 to 65535.	MSTP Configuration

`instance <instance-id(0-7|4094)> vlan <vlan-range>` Available options: • `<instance-id(0-7|4094)>` - Configures the ID of MSTP instance to be created / deleted and mapped with / unmapped from VLAN. • `vlan <vlan-range>` - Configures a VLAN ID or list of VLAN IDs that should be mapped with / unmapped from the specified MST instance.	Creates an MST instance and maps it to VLANs.	MSTP Configuration
`spanning-tree mst hello-time<value(1-2)>`	Configures the spanning tree hello time.	Interface Configuration (Physical Interface)
`show spanning-tree mst [<instance-id(0-7|4094)>] [detail]`	Displays the multiple spanning tree information for all MSTIs in the switch.	Privileged EXEC
`show spanning-tree mst configuration`	Displays multiple spanning tree instance related information.	Privileged EXEC

cnMatrix PVRST Parameters and Commands

Commands	Description	CLI Mode
`spanning-tree vlan <vlan-id > {forward-time <seconds(4-30)>	hello-time <seconds(1-10)>	max-age <seconds(6-40)>	hold-count <integer(1-10)>	brg-priority <integer(0-61440)>	root {primary	secondary}}`	Configures spanning tree related information on a per VLAN basis.	Global Configuration
`spanning-tree encap {dot1q	ISL}`	Configures the encapsulation type to be used in an interface.	Interface Configuration (Physical Interface)
`spanning-tree vlan <vlan-id > status {disable	enable}`	Configures the status of PVRST on a port for the specified VLAN.	Interface Configuration (Physical Interface)
`show spanning-tree vlan <vlan-id> [{blockedports		pathcost-method	summary }]` Available options: • `vlan <vlan-id >` - Displays the PVRST related information for the specified VLAN / VFI ID. This value ranges from 1 to 65535. • `<vlan -id>` - VLAN ID is a unique value that represents a specific	Displays PVRST related information for the specified VLAN.	Privileged EXEC

Commands	Description	CLI Mode
VLAN. This value ranges from 1 to 4094. • `blockedports` - Displays the list of ports in blocked state and the total number of blocked ports, for the specified VLAN. • `pathcost-method` - Displays the pathcost method configured for the specified VLAN. • `summary` - Displays the currently used STP, applied path cost method and port details such as port ID, port role, port state and port status.		
`show spanning-tree vlan <vlan-id> bridge [{address | detail | forward-time | hello-time | id | max-age | priority [system-id] | protocol}]` Available options: • `vlan <vlan-id >` - Displays the PVRST related information of the bridge for the specified VLAN. • `address` - Displays the address of the bridge. • `detail` - Displays the detailed PVRST related information for the bridge. • `forward-time` - Displays the forward delay value of the bridge. • `hello-time` - Displays the hello time value of the bridge. • `id` - Displays the ID of the bridge. • `max-age` - Displays the maximum age of the bridge. • `priority [system-id]` - Displays the priority of the bridge. • `protocol` - Displays the type of STP executed in the bridge.	Displays PVRST related information of the bridge for the specified VLAN ID.	Privileged EXEC
`show spanning-tree vlan <vlan-id> root [{address | cost | detail | forward-time | hello-time | id | max-age | port | priority [system-id] }]` Available options: • `vlan <vlan-id >` - Displays the PVRST related information of the root for the specified VLAN / VFI ID. • `address` - Displays the address of the root. • `detail` - Displays the detailed PVRST related information for the root. • `forward-time` - Displays the forward delay value of the root.	Displays PVRST related information of the root, for the specified VLAN ID.	Privileged EXEC

cnMatrix Parameters and Commands

Commands	Description	CLI Mode
• `hello-time` - Displays the hello time value of the root. • `id` - Displays the ID of the bridge. • `max-age` - Displays the maximum age of the root. • `priority [system-id]` - Displays the priority of the root. • `protocol` - Displays the type of STP executed in the root.		
`show spanning-tree vlan <vlan-id> interface <ifnum> [{ cost | detail | priority | rootcost | state | stats }]` Available options: • `vlan <vlan-id>` - Displays the interface PVRST related information for the specified VLAN. • `cost` - Displays the cost of the specified port. • `detail` - Displays detailed interface specific PVRST related information for the port. • `priority` - Displays the priority of the specified port. • `rootcost` - Displays the root cost of the port. • `state` - Displays the state of the port. • `stats` - Displays the port level spanning tree statistics information.	Displays interface specific PVRST information for the specified VLAN.	Privileged EXEC
`show spanning-tree vlan <vlan-id> active [detail]`	Displays PVRST related information for the specified active VLAN.	Privileged EXEC
`show spanning-tree vlan <vlan-id> detail [active]`	Displays detailed PVRST related information for the specified VLAN.	Privileged EXEC

cnMatrix LLDP Parameters and Commands

Commands	Description	CLI Mode
`set lldp {enable | disable | management-address | tag| version}` Available options: • `disable` • `enable` • `management-address` • `tag` • `version`	Transmits or receives LLDP frames from the server to the LLDP module.	Global Configuration

cnMatrix Parameters and Commands

Commands	Description	CLI Mode
`lldp transmit-interval <seconds(5-32768)>`	Sets the transmission interval in which the server sends the LLDP frames to the LLDP module.	Global Configuration
`lldp holdtime-multiplier <value(2-10)>`	Sets the holdtime-multiplier value, which is the amount of time, the server should hold the LLDP.	Global Configuration
`lldp reinitialization-delay <seconds(1-10)>`	Sets the reinitialization delay time which is the minimum time an LLDP port will wait before reinitializing LLDP transmission.	Global Configuration
`lldp tx-delay <seconds(1-8192)>`	Sets the transmit delay which is the minimum amount of delay between successive LLDP frame transmissions.	Global Configuration
`lldp notification-interval <seconds(5-3600)>`	Sets the time interval in which the local system generates a notification-event.	Global Configuration
`lldp chassis-id-subtype { chassis-comp <string(255)> | if-alias | port-comp <string(255)> | mac-addr | nw-addr | if-name | local <string(255)> }` Available options: • `chassis-comp <string(255)>` - Represents a chassis identifier based on the value of entPhysicalAlias object for a chassis component • `if-alias` - Represents a chassis identifier based on the value of ifAlias for an interface on the containing chassis. • `port-comp <string(255)>` - Represents a chassis identifier based on the value of entPhysicalAlias object for a port or backplane within the chassis. • `mac-addr` - Represents a chassis identifier based on the value of a unicast source address, of a port on the chassis. • `nw-addr` - Represents a chassis identifier based on a network address, associated with a particular chassis. • `if-name` - Represents a chassis identifier based on the value of ifName object for an interface on the containing chassis. • `local <string(255)>` - Represents a chassis identifier based on a locally defined value.	Configures an ID for LLDP chassis subtype which is a unique address of any module.	Global Configuration
`clear lldp counters`	Clears the inbuilt counter which has the total count of LLDP frames that are transmitted/ received.	Global Configuration
`clear lldp table`	Clears all the LLDP information about the neighbors.	Global Configuration
`lldp {transmit | receive} [mac-address <mac_addr>]` Available options: • `transmit` - Enables transmission of LLDPDUs.	Transmits or receives LLDP frames from the one of the ports of the server to the LLDP module	Interface Configuration (Physical Interface)

cnMatrix Parameters and Commands

Commands	Description	CLI Mode
• receive - Enables reception of LLDPDUs • mac-address <mac_addr> - Configures the MAC address to be used as destination MAC address by the LLDP agent on the specified port		
lldp notification ([remote-table-chg][mis-configuration]) [mac-address <mac_addr>]	Controls the transmission of LLDP notifications.	Interface Configuration (Physical Interface)
lldp port-id-subtype { if-alias | if-name | local <local port description> | mac-addr | port-comp <port component description> Available options: • if-alias - Represents a port identifier based on the value of interface alias. • if-name - Represents a port identifier based on the value of Slot0/<interface_number>. • local - Represents a port identifier based on the value of local port description. • mac-addr - Represents a port identifier based on the value of port MAC address. • port-comp - Represents a port identifier based on the value of port component description.	Configures an ID for LLDP port subtype.	Interface Configuration (Physical Interface)
(no) lldp tlv-select basic-tlv { mgmt-addr <ipv4/ipv6/all> | port-descr | sys-capab | sys-descr | sys-name } Available options: • mgmt-addr - Sends ipv4 / ipv6 / both addresses TLVs. • port-descr - Sends port description TLVs. • sys-capab - Sends system capabilities TLV. • sys-descr - Sends system description TLV. • sys-name - Sends hostname TLV.	Enables/Disables transmission on basic LLDP TLVs (these are enabled by default).	Interface Configuration (Physical Interface)
(no) lldp tlv-select dot1tlv { link-aggregation | mgmt-vid | port-vlan-id | protocol-vlan-id | vid-usage-digest | vlan-name } Available options: • link-aggregation - Sends link aggregation dot1 TLV. • mgmt-vid - Sends vid 1 TLV. • port-vlan-id - Sends pvid TLV. • protocol-vlan-id – Sends protocol based VLAN IDs TLVs. • vid-usage-digest - Sends VLAN digest TLV. • vlan-name - Sends VLANs name TLVs.	Enables/Disables transmission on dot1 LLDP TLVs.	Interface Configuration (Physical Interface)
(no) lldp tlv-select dot3tlv { link-aggregation | macphy-config | max-framesize } Available options: • link-aggregation - Sends link aggregation dot3 TLV.	Enables/Disables transmission on dot3 LLDP TLVs.	Interface Configuration (Physical Interface)

cnMatrix Parameters and Commands

Commands	Description	CLI Mode
• `macphy-config` - Sends port auto-negotiation capabilities TLV. • `max-framesize` - Sends maximum frame size TLV.		
Starting with version 2.1 `(no) lldp pba-tlv-select authentication`	Enables/Disables auto attach TLV transmission on a specific interface.	Interface Configuration (Physical Interface)
Starting with version 2.1 `(no) lldp med-tlv-select { ex-power-via-mdi | inventory-management | location-id | med-capability | network-policy }` Available options: • `ex-power-via-mdi` - Sets the transmission of the PoE LLDP MED TLV information. • `inventory-management` - Sets the transmission of Inventory (system information) LLDP MED TLV. • `location-id` - Sets the transmission of the Emergency Call Service Number LLDP MED TLV. • `med-capability` - Sets the transmission of the LLDP MED Capabilities TLV information (this is enabled by default). • `network-policy` - Sets the transmission of the LLDP MED Policies TLV information.	Enables/Disables LLDP MED TLVs.	Interface Configuration (Physical Interface)
Starting with version 2.1 `(no) lldp med-app-type { guestVoice | guestVoiceSignaling | softPhoneVoice | streamingVideo | videoSignaling | videoconferencing | voice | voiceSignaling }` Available options: • `guestVoice` - Sets the transmission of the Guest Voice LLDP MED policy TLV. • `guestVoiceSignaling` - Sets the transmission of the Guest Voice Signaling LLDP MED policy TLV. • `softPhoneVoice` - Sets the transmission of the softPhone Voice LLDP MED policy TLV. • `streamingVideo` - Sets the transmission of the Video Streaming LLDP MED policy TLV. • `videoSignaling` - Sets the transmission of the Video Signaling LLDP MED policy TLV. • `videoconferencing` - Sets the transmission of the Video Conferencing LLDP MED policy TLV. • `voice` – Sets the transmission of the Voice LLDP MED policy TLV. • `voiceSignaling` - Sets the transmission of the Voice Signaling LLDP MED policy TLV.	Enables/Disables transmission of LLDP MED policies TLVs set by enabling the lldp med-tlv-select network-policy	Interface Configuration (Physical Interface)
Starting with version 2.1 `lldp med-location elin-location location-id <string(10-25)>`	Sets an Emergency Call Service Number to be sent by enabling the lldp med-tlv-select location-id.	Interface Configuration (Physical Interface)

cnMatrix Parameters and Commands

Commands	Description	CLI Mode
`show lldp` Available options: • `errors` • `interface` • `local` • `neighbors` • `peers` • `statistics` • `traffic`	Displays the LLDP global configuration details.	Privileged EXEC
`show lldp interface [<interface-type> <interface-id>] [mac-address <mac_addr>]` Available options: • <interface-type> - displays the information about the specified type of interface: - `gigabitethernet` - A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. - `extreme-ethernet` – A version of Ethernet that supports data transfer up to 10 Gigabits per second.	Displays the information about interfaces where LLDP is enabled.	Privileged EXEC
`show lldp neighbors [chassis-id <string(255)> port-id <string(255)>] [<interface-type> <interface-id>][detail]` Available options: • chassis-id <string(255)> - Displays LLDP Neighbor information for the specified chassis identifier value. • <interface-type> - Displays the information about the specified type of interface. • detail - Displays the information obtained from all the received TLVs .	Displays the information about neighbors on an interface or all interfaces.	Privileged EXEC
show lldp traffic [<iftype> <ifnum>[mac-address <mac_addr>]] Available options: • <interface-type> - Displays the LLDP counters for specified type of interface.	Displays the LLDP counters on all interfaces or on a specific interface.	Privileged EXEC
show lldp local {[<interface-type> <interface-id> [mac-address <mac_addr>]] | [mgmt-addr]} Available options: • <interface-type> - Displays the current switch information for the specified type of interface. • mgmt-addr - All the management addresses configured in the system and the Tx enabled ports.	Displays the current switch information that will be used to populate outbound LLDP advertisements for a specific interface or all interfaces.	Privileged EXEC
show lldp errors	Displays the information about the errors such as memory allocation failures, queue overflows and table overflow.	Privileged EXEC

cnMatrix Parameters and Commands

Commands	Description	CLI Mode
show lldp statistics	Displays the LLDP remote table statistics information.	Interface Configuration (Physical Interface)
set lldp version {v1 | v2} Available options: • v1 - Enables LLDP 2005 version 1 on the port. • v2 -Eenables LLDP 2009 version 2 on the port.	Enables the lldp version to be used on the system.	Global Configuration
lldp txCreditMax <value (1-10)>	Configures the maximum number of consecutive LLDPDUs that can be transmitted any time.	Global Configuration
lldp MessageFastTx <seconds(1-3600)>	Configures the interval at which LLDP frames are transmitted on behalf of this LLDP agent during fast transmission period.	Global Configuration
lldp txFastInit <value (1-8)>	Configures the value used to initialize the txFast variable which determines the number of transmissions that are made in fast transmission mode.	Global Configuration
show lldp peers [chassis-id <string(255)> port-id <string(255)>] <interface-type> <interface-id>[[mac-address <mac_addr>] [detail]] • <interface-type> - displays the information about the specified type of interface: - gigabitethernet - A version of LAN standard architecture that supports data transfer up to 1 Gigabit per second. - extreme-ethernet – A version of Ethernet that supports data transfer up to 10 Gigabits per second. • chassis-id <string(255)> - Displays the LLDP peer information for the specified chassis identifier.	Displays the information about the peers on an interface or all interfaces.	Privileged EXEC

cnMatrix RMON Parameters and Commands

Commands	Description	CLI Mode
`rmon {enable | disable}`	Enables or disables the RMON feature.	Global Configuration
`rmon collection history <index (1-65535)> [buckets <bucket-number (1-65535)>] [interval <seconds (1-3600)>] [owner <ownername (127)>]`	Enables the history collection of interface/ VLAN statistics in the buckets for the specified time interval.	Interface Configuration / Config-VLAN
`rmon collection stats <index (1-65535)> [owner <ownername (127)>]`	Enables RMON statistic collection on the interface/ VLAN.	Interface Configuration / Config-VLAN

rmon event <number (1-65535)> [description <event-description (127)>] [log] [owner <ownername (127)>] [trap <community (127)>]	Adds an event to the RMON event table.	Global Configuration
rmon alarm <alarm-number> <mib-object-id (255)> <sample-interval-time (1-65535)> {absolute | delta} rising-threshold <value (0-2147483647)> [rising-event-number (1-65535)] falling-threshold <value (0-2147483647)> [falling-event-number (1-65535)] [owner <ownername (127)>]	Sets an alarm on a MIB object.	Global Configuration
show rmon [statistics [<stats-index (1-65535)>]] [alarms] [events] [history [history-index (1-65535)] [overview]]	Displays the RMON statistics, alarms, events, and history configured on the interface.	Privileged EXEC

cnMatrix SNTP Parameters and Commands

Commands	Description	CLI Mode
sntp	Enters to SNTP configuration mode which allows the user to execute all the commands that supports SNTP configuration mode.	Global Configuration
set sntp client {enabled | disabled}	Enables or disables SNTP client module.	SNTP Configuration
set sntp client version { v1 | v2 | v3 | v4 }	Sets the operating version of the SNTP for the client.	SNTP Configuration
set sntp client addressing-mode { unicast | broadcast | multicast | manycast }	Sets the addressing mode of SNTP client.	SNTP Configuration
set sntp client port <portno(123|1025-65535)>	Modifies the Client Port setting.	SNTP Configuration
set sntp client clock-format {ampm | hours}	Sets the system clock as either AM / PM format or HOURS format.	SNTP Configuration
set sntp client time-zone <UTC-offset value as (+HH:MM /-HH:MM)(+00:00 to +14:00)/ (-00:00 to -12:00)> Eg: +05:30	Sets the system time zone with respect to UTC.	SNTP Configuration
set sntp client clock-summer-time <week-day-month,hh:mm> <week-day-month,hh:mm>	Enables the DST (Daylight Saving Time).	SNTP Configuration
set sntp client authentication-key <key-id> md5 <key>	Sets the authentication parameters for the key.	SNTP Configuration

cnMatrix Parameters and Commands

Commands	Description	CLI Mode
`set sntp unicast-server auto-discovery {enabled | disabled}`	Enables / Disables the auto discovery of the server.	SNTP Configuration
`set sntp unicast-poll-interval <value (16-16384) seconds>`	Sets the SNTP unicast poll interval.	SNTP Configuration
`set sntp unicast-max-poll-timeout <value (1-30) seconds>`	Configures SNTP client maximum poll interval timeout which is the maximum interval to wait for the poll to complete.	SNTP Configuration
`set sntp unicast-max-poll-retry <value (1-10) times>`	Configures SNTP client maximum retry poll count which is the maximum number of unanswered polls.	SNTP Configuration
`set sntp unicast-server {ipv4 <ucast_addr> |ipv6 <ip6_addr> | domain-name < dns_host_name>} [{primary | secondary}] [version { 3 | 4 }] [port <integer(1025-36564)>]` Available options: • `domain-name < dns_host_name>` - Sets the domain name for the unicast server. • `ipv4 <ucast_addr>` - Sets the address type of the unicast server as Internet Protocol Version 4. • `ipv6 <ip6_addr>` - Sets the address type of the unicast server as Internet Protocol Version 6.	Configures the SNTP unicast server.	SNTP Configuration
`set sntp broadcast-mode send-request {enabled | disabled}`	Enables or disables the SNTP to send status request.	SNTP Configuration
`set sntp broadcast-poll-timeout [<value (1-30) seconds>]`	Configures the SNTP client poll interval in broadcast mode which is the maximum interval to wait for a poll to complete. This value ranges from 1 to 30 seconds.	SNTP Configuration
`set sntp broadcast-delay-time [<value (1000-15000) microseconds>]`	Configures the SNTP delay time in broadcast mode which is the time interval the SNTP client needs to wait for a response from the server.	SNTP Configuration
`set sntp multicast-mode send-request {enabled | disabled}`	Sets the status of sending the request to the multicast server to calculate the delay time.	SNTP Configuration
`set sntp multicast-poll-timeout [<value (1-30) seconds>]`	Configures the SNTP client poll interval in multicast mode which is the maximum interval to wait for the poll to complete.	SNTP Configuration
`set sntp multicast-delay-time [<value (1000-15000) microseconds>]`	Configures the SNTP delay time in which there is no response from the multicast server.	SNTP Configuration
`set sntp multicast-group-address {ipv4 {<mcast_addr> | default} | ipv6 {<ipv6_addr> | default}}`	Configures a group address for the SNTP so that all the SNTP client servers can be connected to this address.	SNTP Configuration

cnMatrix Parameters and Commands

Commands	Description	CLI Mode
`set sntp manycast-poll-interval [<value (16-16384) seconds>]`	Configures SNTP client poll interval which is the maximum interval between successive messages.	SNTP Configuration
`set sntp manycast-poll-timeout [<value (1-30) seconds>]`	Configures the SNTP client poll timeout which is the maximum interval to wait for a poll to complete.	SNTP Configuration
`set sntp manycast-poll-retry-count [<value (1-10)>]`	Configures SNTP poll retries count, which is the maximum number of unanswered polls that cause a slave to identify the server as dead.	SNTP Configuration
`set sntp manycast-server { broadcast | multicast }`	Configures the SNTP multicast or broadcast server address in manycast mode.	SNTP Configuration
`show sntp clock`	Displays the current time.	Privileged EXEC
`show sntp status`	Displays the SNTP status.	Privileged EXEC
`show sntp unicast-mode status`	Displays the status of SNTP in unicast mode.	Privileged EXEC
`show sntp broadcast-mode status`	Displays the status of SNTP in broadcast mode.	Privileged EXEC
`show sntp multicast-mode status`	Displays the status of SNTP in multicast mode.	Privileged EXEC
`show sntp manycast-mode status`	Displays the SNTP manycast mode status.	Privileged EXEC
`debug sntp ([init-shut] [mgmt] [data-path] [control] [resource] [all-fail] [buff])` Available options: • `init-shut` - Generates debug statements for init and shutdown traces. • `mgmt` - Generates debug statements for management traces. • `data-path` - Generates debug statements for data path traces. • `control` - Generates debug statements for control path traces. • `all-fail` - Generates debug statements for all failure traces of the above mentioned traces. • `buff` - Generates debug statements for SNTP buffer related traces.	Enables tracing in the SNTP module as per the configured debug levels.	Privileged EXEC
`show sntp statistics`	Displays the SNTP packet statistics.	Privileged EXEC
`debug sntp all`	Enables tracing in SNTP module for all debug levels.	Privileged EXEC

cnMatrix Port Settings Features Parameters and Commands

Negotiation

Commands	Description	CLI Mode
`Negotiation {10full | 10half | 100full | 100half | 1000full | 2500full}` Available options: • 10full - Port advertises 10Mbps, full duplex. • 10half - Port advertises 10Mbps, half duplex. • 100full - Port advertises 100Mbps, full duplex. • 100half - Port advertises 100Mbps, half duplex. • 1000full - Port advertises 1000Mbps, full duplex. • 1000half - Port advertises 1000Mbps, half duplex. • 2500full - Port advertises 2500Mbps, full duplex. Note: If the command is issued without any parameters, all of the supported advertisements will be set.	Enables auto-negotiation on the interface and sets advertisements.	Interface Configuration (Physical Interface)
`no negotiation`	Disables auto-negotiation on the interface.	Interface Configuration (Physical Interface)

Speed

Commands	Description	CLI Mode
`speed { 10 | 100 | 1000 | 10000 }` Available options: • `10` - Port runs at 10Mbps. • `100` - Port runs at 100Mbps. • `1000` - Port runs at 1000Mbps. • `10000` - Port runs at 10000Mbps. • `auto` - Port automatically configures it's speed based on the peer switch. • `nonegotiate` - Disables negotiation on the ports.	Sets the speed of the interface.	Interface Configuration (Physical Interface)

Duplex

Commands	Description	CLI Mode
`duplex { full | half }` Available options:	Configures the duplex operation.	Interface Configuration (Physical Interface)

• full - Port is in full-duplex mode, that is data simultaneously communicates in both directions. • half - Port is in half-duplex mode, that is data can communicate in both directions, but only in one direction at a time. • auto - Port is in auto mode.		

MTU

Commands	Description	CLI Mode
`mtu <frame-size(46-9216)>`	Configures the maximum transmission unit frame size for all the frames transmitted and received on all the interfaces in a switch.	Interface Configuration (Physical Interface)

cnMatrix Link Aggregation Parameters and Commands

Commands	Description	CLI Mode
`lacp system-priority <0-65535>`	Configures the LACP priority.	Global Configuration
`lacp system-identifier <aa:aa:aa:aa:aa:aa>`	Configures the unicast MAC address value.	Global Configuration
`lacp port-priority <0-65535>`	Configures the LACP port priority.	Interface Configuration (Physical Interface)
`lacp port-identifier <1-65535>`	Configures the port identifier.	Interface Configuration (Physical Interface)
`channel-group <channel-group-number(1-65535)> Mode { on | active | passive }` Available options: • `<channel-group-number(1-65535)>` - Adds the port as a member of the specified port channel. • `active` - Starts LACP negotiation un-conditionally. • `passive` - Starts LACP negotiation only when LACP packet is received from peer. • `on` - Forces the interface to channel without LACP.	Adds the port as a member of the specified port channel that is already created in the switch.	Interface Configuration (Physical Interface)
`lacp wait-time <0-10>`	Configures the LACP wait-time for an interface.	Interface Configuration (Physical Interface)
`lacp timeout {long | short }` Available options:	Configures the LACP timeout period.	Interface Configuration (Physical Interface)

cnMatrix Parameters and Commands

Commands	Description	CLI Mode
• `long` - Configures the LACP timeout period as 90 seconds. • `short` - Configures the LACP timeout period as 3 seconds.		
`lacp rate {normal | fast }` Available options: • `normal` - LACP PDU should be received every 30 seconds and the timeout value (no packet is received from peer) is set as 90 seconds. • `fast` - LACP PDU should be received every 1 second and timeout value is set as 3 seconds.	Configures the LACP rate.	Interface Configuration (Physical Interface)
`lacp admin-key <(Admin Key)1-65535> [Mode {active | passive}]` Available options: • `admin-key` - Configures the LACP actor admin key that is used while port participates in dynamic aggregation selection. • `[Mode {active | passive}]` - active - Starts LACP negotiation un-conditionally / passive - Starts LACP negotiation only when LACP packet is received from peer.	Configures the LACP actor admin key and LACP Mode for a port.	Interface Configuration (Physical Interface)
`port-channel max-ports <integer (2-8)>`	Configures the maximum number of ports that can be attached to a port channel.	Interface Configuration (Physical Interface)
`debug lacp [ { init-shutdown | mgmt | data | events | packet | os | failall | buffer | all } ]` Available options: • `init-shutdown` - Generates debug statements for init and shutdown traces. • `mgmt` - Generates debug statements for management traces. • `data` - Generates debug statements for data path traces. • `events` - Generates debug statements for event traces. • `packet` - Generates debug statements for packet dump traces. • `os` - Generates debug statements for OS resource related traces. • `buffer` - Generates debug statements for buffer related traces. • `all` - Generates debug statements for all kinds of traces.	Enables the tracing of the LACP as per the configured debug levels.	Privileged EXEC
`debug etherchannel {[all] [detail] [error] [event] [idb]}` Available options: • `all` - Generates debug statements for all kinds of traces.	Enables the tracing of the link aggregation module as per the configured debug levels.	Privileged EXEC

cnMatrix Parameters and Commands

Commands	Description	CLI Mode
• `detail` - Generates detailed debug statements for traces. • `error` - Generates debug statements for all failure traces. • `event` - Generates debug statements for event traces. • `idb` - Generates debug statements for interface descriptor block traces.		
`show etherchannel <channel-group-number(1-65535)> { detail | load-balance | port | port-channel | summary | protocol }` Available options: • `detail` - Displays detailed Etherchannel information. • `port` - Displays the status of protocol operate Mode and port details for each group. • `port-channel` - Displays the admin and operational status of port channel module, and port channel details. • `protocol` - Displays the status of protocol operate Mode for each port-channel group. • `summary` – Displays the admin and operational status of port channel module, number of channel groups used, number of aggregators, group IDs, and port channel ID, status of protocol operate Mode and member ports for each group.	Displays etherchannel information for the specified port-channel groups created in the switch.	Privileged EXEC
`show etherchannel`	Displays etherchannel information for port-channels created in the switch.	Privileged EXEC
`show interfaces [<interface-type> <interface-id> ] etherchannel`	Displays etherchannel details for all aggregated ports and port channels.	Privileged EXEC
`show lacp [<port-channel(1-65535)>] { counters | neighbor [detail] }` Available options: • `<port-channel(1-65535)>` - Displays LACP counter / neighbor information for the specified port-channel. • `counters` - Displays the LACP counter information. • `neighbor [detail] –` `neighbor` - Displays LACP neighbor information.	Displays LACP counter / neighbor information for all port-channels.	Privileged EXEC

cnMatrix Private VLAN Edge Parameters and Commands

Commands	Description	CLI Mode
`switchport protected`	Enables the protected feature of a port.	Interface Configuration (Physical Interface)
`no switchport protected`	Disables the protected feature of a port.	Interface Configuration (Physical Interface)
`show vlan port <interface>`	Displays the protected features of a port.	Privileged EXEC

cnMatrix PoE Parameters and Commands

Commands	Description	CLI Mode
`set poe {enable | disable}` Available options: • enable - enables the Power Over Ethernet module in the switch. • disable - disables the Power Over Ethernet module and releases all the resources allocated to the POE module to the system and the power is shut off on all POE enabled ports.	Enables or disables the Power Over Ethernet module in the switch.	Global Configuration
show power detail	Displays the Power Over Ethernet power supply status information such as PoE Global admin state, PSE operational status and Maximum power supply.	Privileged EXEC
`show power inline [{<interface-type> <interface-id> | <measurements>}]` Available options: • Gigabitethernet - gigabit Ethernet interface. • Extreme-Ethernet - Extreme Ethernet interface. • measurements - Power inline measurements.	Displays the power status and per port power measurements for all or the specified Power Over Ethernet interface.	Privileged EXEC
power inline priority { critical | high | low }	Sets the Power Over Ethernet priority per port.	Interface Configuration (Physical Interface)
power inline {auto | never}	Enables / Disables the Power Over Ethernet per port.	Interface Configuration (Physical Interface)

cnMatrix Port Mirroring Parameters and Commands

Commands	Description	CLI Mode

cnMatrix Parameters and Commands

`monitor session <session-id (1-7)> { source { interface <interface-type> <interface-id> [{ rx | tx | both }] | vlan <vlan_range> [ rx ] |mac-acl <acl-id> |ip-acl <acl-id>}}` Available options: • `session-id` - Configures the session number that is used to identify a session. • `interface` - Configures the source interface whose traffic to be mirrored. • `rx` - Mirrors received traffic. • `tx` - Mirrors transmitted traffic. • `both` – Mirrors both received and transmitted. • `mac-acl` - Specifies the ID of the MAC ACL (Access Control List) to be mirrored. • `ip-acl` - Specifies the ID of the IP ACL to be mirrored. • `vlan` - Specifies the VLAN for which traffic is to be mirrored in the mirroring session.	Configures a source port / VLAN for a mirroring session. A port that is a member of a port-channel cannot be a mirror-to port.	Global Configuration
`monitor session <session-id (1-7)> destination {interface <interface-type> <interface-id>}`	Configures a destination port for a mirroring session.	Global Configuration
`no monitor session { range | local | session-id (1-7)}`	Removes the mirroring configuration.	Global Configuration
`show monitor [{ session <session-id (1-7)> | local | range <session-list> | all }] [detail]`	Displays the mirroring information present in the system.	Privileged EXEC
`show monitor [ session (1-7) ] [ detail ]`	Displays port-monitoring information.	Privileged EXEC

cnMatrix Storm-Control Parameters and Commands

Commands	Description	CLI Mode
`storm-control { broadcast | multicast | dlf } level <rate-value>` Available options:	Sets the storm control rate for broadcast, multicast-broadcast, DLF_multicast-broadcast and all packets.	Interface Configuration ((Physical Interface))

cnMatrix Parameters and Commands

- `broadcast` - Configures the storm-control for broadcast packets. - `multicast` - Configures the storm-control for both multicast and broadcast packets. - `dlf` - Configures the storm-control for unicast, multicast and broadcast packets.		
show interfaces storm-control	Displays the storm-control status for the interfaces.	Privileged EXEC

cnMatrix Rate-Limit-Output Parameters and Commands

Commands	Description	CLI Mode
`rate-limit output [<rate-value>] [<burst-value>]` Available options: - `rate-value` - Configures the maximum rate (in kbps) at which packets can be sent out through the interface. - `burst-value` - Configures the burst size in kilobytes with which the rate is to be implemented.	Enables the rate limiting and burst size rate limiting by configuring the egress packet rate of an interface.	Interface Configuration (Physical Interface)

cnMatrix QoS Parameters and Commands

Commands	Description	CLI Mode
priority-map <priority-map-Id(1-65535)>	Adds a Priority Map entry. Configures the priority map index for the incoming packet received over ingress port with specified incoming priority. Returns the Priority Map Configuration mode. The no form of the command deletes a Priority Map entry.	Global Configuration

cnMatrix Parameters and Commands

Commands	Description	CLI Mode
map in-priority-type { vlanPri | dot1P <integer(0-1)> | ipDscp | vlanDEI } in-priority <integer(0-63)> regen-priority <integer(0-63)> [regen-color { green | yellow | red }] • in-priority-type - Configures the incoming priority type for the specified interface. The types are: - vlanPri – Sets the priority type to VLAN Priority. - dot1P <integer(0-1)> – VLAN Drop Eligibility Indicator. This value ranges from 0 to 1. - ipDscp – Sets the priority type to IP Differentiated Services Code Point. - vlanDEI – Sets the priority type to VLAN Drop Eligibility Indicator. **Starting with version 2.1**, this parameter has been removed. • in-priority <integer(0-63)> - Configures the Incoming priority value determined for the received frame. This value ranges from 0 to 63. • regen-priority <integer(0-63)> - Configures the Regenerated priority value determined for the received frame. This value ranges from 0 to 63. • regen-color - Sets the type of the regenerated color. **Starting with version 2.1**, this parameter has been removed. The types are: - green – Conform Action. - yellow – Exceed Action. - red – Violate Action.	Adds a Priority Map Entry for mapping an incoming priority to a regenerated priority	Priority Map Configuration
class-map <class-map-id(1-65535)>	Adds a Class Map entry. Configures an Index that enumerates the Classifier table entries. Returns the Class Map Configuration mode. The no form of the command deletes a Class Map entry.	Global Configuration
match access-group { mac-access-list <integer(0-65535)> | ip-access-list <integer(0-65535)> | priority-map <integer(0-65535)>} • mac-access-list <integer(0-65535)> - Identifier of the MAC ACL. • ip-access-list <integer(0-65535)> - Identifier of the IP ACL. • priority-map <integer(0-65535)>- Identifier of the priority map.	Sets the Class Map parameters using MAC ACL, IP ACL, or Priority Map.	Class Map Configuration
set class <integer(1-100)> [pre-color { green | yellow | red | none }] [regen-priority <integer(0-7)> group-name <string(31)>] • <class integer(1-65535)> – Traffic CLASS to which an incoming frame pattern is classified. • pre-color { green | yellow | red | none } - Color of the packet prior to metering. This can be any one of the following: - none – Traffic is not pre-colored. - green – Traffic conforms to SLAs (Service Level Agreements. - yellow – Traffic exceeds the SLAs. - red – Traffic violates the SLAs.	Sets the CLASS for L2and/or L3 filters or Priority Map ID and adds a class to Priority Map entry with regenerated priority. The no form of the command deletes a class to Priority Map Table entry.	Class Map Configuration

cnMatrix Parameters and Commands

Commands	Description	CLI Mode
• regen-priority <integer(0-7)> - Regenerated priority value determined for the input CLASS. • group-name <string(31)>- Unique identification of the group to which an input CLASS belongs.		
meter <integer(1-1000)>	Creates a Meter. Configures an Index that enumerates the Meter entries. Returns the Meter Configuration mode. The no form of the command deletes a Meter.	Global Configuration
meter-type { srTCM | trTCM } [cir <integer(0-10485760)>] [cbs <integer(0-10485760)>] [eir <integer(0-10485760)>] [ebs <integer(0-10485760)>] • srTCM - Configures the meter type as Single Rate Three Color Marker Metering as defined by RFC 2697. Valid value for Given Meter Type are CIR, CBS and EBS • trTCM - Configures the meter type as Two Rate Three Color Marker Metering as defined by RFC 2698. Valid value for Given Meter Type are CIR, CBS, EIR, and EBS • cir <integer(0-10485760)> - Committed information rate. • cbs <integer(0-10485760)> - Committed burst size. • eir <integer(0-10485760)> - Excess information rate. • ebs <integer(0-10485760)> - Excess burst size.	Sets the meter parameters: CIR, CBS, EIR, EBS, meter type.	Meter Configuration
policy-map <integer(1-65535)>	Creates a policy map. Configures an Index that enumerates the policy-map table entries. Returns the Policy Map Configuration mode. The no form of the command deletes a policy map.	Global Configuration
set policy [class<integer(0-100)>] [default-priority-type { none | { vlanPri <integer(0-7)>| ipDscp <integer(0-63)> }}] • class <integer(0-65535)> - Specifies the Traffic CLASS for which the policy-map needs to be applied. • default-priority-type { none | { vlanPri <integer(0-7)>| dot1P <integer(0-7)> <integer(0-1)> | ipDscp <integer(0-63)> }}]- Sets the Per-Hop Behvior (PHB) type to be used for filling the default PHB for the policy-map entry. The types are: - none – Sets the PHB type as none. - vlanPri – Sets the PHB type as VLAN Priority. - dot1P <integer(0-7)> <integer(0-1)> – Sets the PHB type as dot1P. This value ranges from 0 to 7 for vlanpri and ranges from 0 to 1 for default DEI. - ipDscp <integer(0-63)> – Sets the PHB type as IP Differentiated Services Code Point.	Sets the policy class. The no form of the command sets the default value for interface in this policy.	Policy Map Configuration

cnMatrix Parameters and Commands

<table>
<tr><th>Commands</th><th>Description</th><th>CLI Mode</th></tr>
<tr><td>NOTE: This value can be overwritten by the meter used for the policy-map.</td><td></td><td></td></tr>
<tr><td>set meter <integer(1-65535)> [conform-action { cos-transmit-set <short(0-7)> | set-ip-dscp-transmit <short(0-63)> }] [exceed-action {drop | cos-transmit-set <short(0-7)> | set-ip-dscp-transmit <short(0-63)> }] [violate-action {drop | cos-transmit-set <short(0-7)> | set-ip-dscp-transmit <short(0-63)> }]
Available options:
• conform-action { set-cos-transmit <short(0-7)> set-de-transmit <short(0-1)> set-ip-dscp-transmit <short(0-63)> } – Configures action to be performed on the packet, when the packets are found to be In profile (conform). Options are:
- cos-transmit-set <short(0-7)> – Sets the VLAN priority of the outgoing packet.
- de-transmit-set <short(0-1)> – Sets the VLAN drop eligible indicator of the outgoing packet.
- set-cos-transmit <short(0-7)> - Sets the VLAN priority of the outgoing packet.
- set-de-transmit <short(0-1)> - Sets the VLAN drop eligible indicator of the outgoing packet.
- set-port <iftype> <ifnum> - Sets the new port value.
- inner-vlan-pri-set <short(0-7)> - Sets the inner VLAN priority of the outgoing packet.
- inner-vlan-de-set <short(0-1)> - Sets the inner VLAN DE of the outgoing packet.
- set-inner-vlan-pri <short(0-7)> - Sets the inner VLAN priority of the outgoing packet.
- set-inner-vlan-de <short(0-1)> - Sets the inner VLAN DE of the outgoing packet.
- set-ip-prec-transmit - Sets the new IP Type of Service.
.
- set-mpls-exp-transmit - Sets the MPLS experimental bits of the outgoing packet
- set-ip-dcp-transmit<short(0-63)> - Sets the new differentiated services code point value.
• exceed-action {drop | set-cos-transmit <short(0-7)> set-de-transmit <short(0-1)> | set-ip-dscp-transmit <short(0-63)> } – - Action to be performed on the packet, when the packets are found to be In profile (exceed). Options are:
- drop – Drops the packet.
- cos-transmit-set <short(0-7)>- Sets the VLAN priority of the outgoing packet.
- de-transmit-set <short(0-1)> - Sets the VLAN Drop Eligible indicator of the outgoing packet.
- set-cos-transmit<short(0-7)> – Sets the VLAN priority of the outgoing packet.</td><td>Sets the policy parameters, such as Meter and Meter Actions.

The no form of the command removes the Meter from the Policy and the Meter Actions.</td><td>Policy Map Configuration</td></tr>
</table>

Commands	Description	CLI Mode
- set-de-transmit<short(0-1)> – Sets the VLAN Drop Eligible indicator of the outgoing packet. - inner-vlan-pri-set <short(0-7) - Sets the inner VLAN priority of the outgoing packet. - set-inner-vlan-de <short(0-1)> - Sets the inner VLAN DE of the outgoing packet. - set-mpls-exp-transmit<short(0-7)> – Sets the MPLS Experimental bits of the outgoing packet. - set-ip-prec-transmit<short(0-7)> – Sets the new IP TOS value. - set-ip-dscp-transmit<short(0-63)> – Sets the new DSCP value. • violate-action {drop | set-cos-transmit <short(0-7)> set-de-transmit <short(0-1)> | set-ip-dscp-transmit <short(0-63)> } - Action to be performed on the packet, when the packets are found to be out of profile. • set-conform-newclass<integer(0-65535)> - Represents the Traffic CLASS to which an incoming frame pattern is classified after metering. • set-exceed-newclass<integer(0-65535)> - Represents the Traffic CLASS to which an incoming frame pattern is classified after metering. • set-violate-newclass<integer(0-65535)> - Represents the Traffic CLASS to which an incoming frame pattern is classified after metering.		
shape-template <integer(1-65535)> [cir <integer(1-1000000)>] [cbs <integer(0-4095)>] Available options: • shape-template <integer(1-65535)> - Configures the shape Template Table index. This value ranges from 1 to 65535. • cir <integer(1-1000000)> - Configures the Committed information rate for packets through the queue. • cbs <integer(0-4095)>)> - Configures the Committed burst size for packets through the queue.	Creates a Shape Template. The no form of the command deletes a Shape Template.	Global Configuration
scheduler <integer(1-8)> interface <iftype> <ifnum> [sched-algo {strict-priority | rr | wrr | strict-wrr}] Available options: • scheduler <integer(1-8)> - Scheduler identifier that uniquely identifies the scheduler in the system/egress interface. • interface <iftype> <ifnum> - Interface type and port number. • sched-algo {strict-priority | rr | wrr | strict-wrr}- Specifies the packet scheduling algorithm: - strict-priority – Packets from any source are matched. - rr – roundRobin - wrr – weightedRoundRobin - strict-wrr – strictWeightedRoundRobin	Creates a Scheduler and configures the Scheduler parameters. The no form of the command deletes a scheduler.	Global Configuration
queue-map class <integer(1-100)> queue-id <integer(1-8)> Available options:	Creates a Map for a Queue with a Class.	Global Configuration

Commands	Description	CLI Mode
• class <integer(1-100)> - Configures the Input CLASS (associated with an incoming packet) that needs to be mapped to an outbound queue. • queue-id <integer(1-8)> - Configures the Queue identifier. NOTE: Class needs to be created using the set class command to configure this parameter.		
set meter-stats {enable | disable} meter-id <integer(1-65535)> • enable - Enables counter status for the Meter Statistics • disable - Disables counter status for the Meter Statistics • meter-id <integer(1-65535)> - Specifies an Index that enumerates the Meter entries. NOTE: To enable or disable meter statistics to a specific meter-id, Meter id and Policy Map related configuration should be already created. **Starting with version 2.1**, this command has been removed.	Enables or disables the Meter Statistics counter status.	Global Configuration
show qos global info	Displays QoS related global configurations.	Privileged EXEC
show priority-map [<priority-map-id (1-65535)>] • <priority-map-id (1-65535)> - priority map id	Displays the Priority Map entry.	Privileged EXEC
show class-map [<class-map-id(1-65535)>] • <class-map-id (1-65535)> - class map id	Displays the Class Map entry.	Privileged EXEC
show meter [<meter-id(1-65535)>] • <meter-id (1-65535)> - meter id	Displays the Meter entry.	Privileged EXEC
show policy-map [<policy-map-id(1-65535)>] • <policy-map-id (1-65535)> - policy map id	Displays the Policy Map entry.	Privileged EXEC
show shape-template [<shape-template-id(1-65535)>] • <shape-template-id (1-65535)> - shape template id	Displays the Shape Template configurations.	Privileged EXEC
show scheduler [interface <iftype> <ifnum>]	Displays the configured Scheduler.	Privileged EXEC
show queue [interface <iftype> <ifnum>]	Displays the queue configuration.	Privileged EXEC
show qos meter-stats [<integer(1-65535)>]	Displays the Meters statistics for conform, exceed and violate packets count.	Privileged EXEC
clear meter-stats [meter-id <integer(1-65535)>]	Clears the Meter Statistics.	Privileged EXEC
show qos queue-stats [interface <iftype> <ifnum>]		Privileged EXEC
qos trust {none | dscp | dot1p} Available options:		Interface Configuration

cnMatrix Parameters and Commands

Commands	Description	CLI Mode
• none- The port's default 802.1p priority will be used to determine the packet's QoS attributes. • dscp - The DSCP field in the IP header will be used to determine the packet's QoS attributes. • dot1p - The 802.1p priority field in the frame will be used to determine the packet's QoS attributes.		
show queue-map interface	Displays the configured queue map.	Privileged EXEC

cnMatrix Auto Attach Parameters and Commands

Commands	Description	CLI Mode
debug auto-attach [trace { error | warning | info | debug }] [dump { rule | action | policy | prec | ifc }]	Enables debug options for the Auto-Attach module.	Privileged EXEC
no debug auto-attach	Disables the trace option for the Auto-Attach module.	Privileged EXEC
show auto-attach global	Displays the Auto-Attach global configuration details.	Privileged EXEC
show auto-attach interface [<iftype> <ifnum>]	Displays the Auto-Attach per-interface configuration details.	Privileged EXEC
show auto-attach action [name <string(20)>]	Displays the Auto-Attach action table contents.	Privileged EXEC
show auto-attach rule [name <string(20)>]	Displays Auto-Attach rule table contents.	Privileged EXEC
show auto-attach policy [name <string(20)>] [{detail | interface | statistics}]	Displays Auto-Attach policy table contents.	Privileged EXEC
show auto-attach script [{cnPilot}]	Displays configured Auto-Attach device script data.	Privileged EXEC
auto-attach	Enables the Auto-Attach feature on the system.	Global Configuration
no auto-attach	Disables the Auto-Attach feature on the system.	Global Configuration
auto-attach default (Starting with version 2.1)	Resets the Auto-Attach interface-specific settings for that one interface to their default values.	Interface Configuration
auto-attach default **Starting with version 2.1**, the interface parameter has been added so that you can reset all the Auto-Attach interface-specific settings for all interfaces to their default values.	Resets all the Auto-Attach settings to the default values for all interfaces and the following parameters: Auto-Attach Status, String Comparison and Update Port Description.	Global Configuration
auto-attach string-comparison { case-sensitive | ignore-case } Available options: • case-sensitive - Performs case-sensitive device data comparisons. • ignore-case - Ignores case for device data comparisons.	Configures the device data string comparison mode.	Global Configuration

cnMatrix Parameters and Commands

Commands	Description	CLI Mode
`auto-attach action <action-name(20)> ([vlan <vlan-list(99)>] [pvid <vlan(1-4094)>] [switch-port-mode hybrid])` Available options: • `<action-name(20)>` - Unique action set name. • `vlan` – Specifies the list of VLANs. • `<vlan-list(99)>` - List of 1..20 comma-separated VLANs. • `pvid` - Specifies default port VLAN. • `<vlan>` - Default VLAN from VLAN list. • `switch-port-mode` - Update switch port mode for the interface. • `hybrid` – Updates the switch port mode to Hybrid. **Starting with version 2.1:** • `access` – Updates the switch port mode to Access. • `trunk` – Updates the switch port mode to Trunk. **Starting with version 2.1**, the following parameters have been added: • `user-priority - 0..7`. • `qos-trust` – Updates the QoS trusted mode. • `dot1p` – Updates the trusted mode based on vlan priority value. • `dscp` - Updates the trusted mode based on dscp value. • `untrusted` - Sest as QoS untrusted. • `poe-priority` – Updates the PoE priority mode. • `critical` – Updates the PoE priority to critical. • `high` – Updates the PoE priority to high. • `low` – Updates the PoE priority to low. • `uplink` - Creates uplink ports (maximum 4 uplinks including physical ports and port-channels)	Configures the Auto-Attach action entries.	Global Configuration
`no auto-attach action <string(20)>`	Deletes the Auto-Attach action entries.	Global Configuration

`auto-attach rule <string(20)> { LLDP-ANY | LLDP-CAP | LLDP-SYS-NAME | LLDP-SYS-DESC | LLDP-CHASSIS | LLDP-PORT | LLDP-PORT-DESC } <string(60)>`
Starting with version 2.1:
`auto-attach rule <string(20)> { LLDP-ANY | LLDP-CAP | LLDP-CHASSIS | LLDP-IPV4-MGMT | LLDP-PORT | LLDP-PORT-DESC | LLDP-SYS-DESC | LLDP-SYS-NAME | MAC-FULL | MAC-OUI | MAC-RANGE} <string(60)>`
Available options:
• `<rule-name(20)>` - Unique rule name.
• `LLDP-ANY` – Searches in multiple LLDP TLVs for device ID data.
	Configures the Auto-Attach rule entries.	Global Configuration

cnMatrix Parameters and Commands

Commands	Description	CLI Mode
• `LLDP-CAP` - Matches LLDP Capabilities TLV data (comma-separated combination of 'bridge', 'wlan', 'router', 'phone', 'station', 'repeater', 'docsis', 'other'). • `LLDP-SYS-NAME` – Searches in the LLDP System Name TLV for device ID data. • `LLDP-SYS-DESC` – Searches in the LLDP System Description TLV for device ID data. • `LLDP-CHASSIS` – Searches in the LLDP Chassis ID TLV for device ID data. • `LLDP-PORT` - Search LLDP Port ID TLV for device ID data. • `LLDP-PORT-DESC` – Searches in the LLDP Port Description TLV for device ID data. • `<device-desc(60)>` - Targets the device identification data. **Starting with version 2.1**, the following parameters have been added: • `MAC-FULL` - Searches for full MAC address. • `MAC-OUI` - Searches for MAC OUI address. • `MAC-RANGE` - Searches for MAC range addresses. • `LLDP-IPV4-MGMT` - Search LLDP IPv4 ID TLV for device ID data.		
`no auto-attach rule <rule-name(20)>`	Deletes the Auto-Attach rule entries.	Global Configuration
`auto-attach policy <string(20)> match { rule <string(20)> | { LLDP-ANY | LLDP-CAP | LLDP-SYS-NAME | LLDP-SYS-DESC | LLDP-CHASSIS | LLDP-PORT | LLDP-PORT-DESC } <string(60)> } set { action <string(20)> | vlan <string(99)> [pvid <integer(1-4094)>] [switch-port-mode hybrid] | switch-port-mode hybrid } [precedence <integer(1-100)>] [{ enable | disable }]` **Starting with version 2.1:** `auto-attach policy <string(20)> match { rule <string(20)> | { LLDP-ANY | LLDP-CAP | LLDP-SYS-NAME | LLDP-SYS-DESC | LLDP-CHASSIS | MAC-FULL | MAC-OUI } <string(60)> } set { action <string(20)> | vlan <string(99)> [pvid <integer(1-4066)>] [switch-port-mode hybrid/access/trunk] } [precedence <integer(1-100)>] [{ enable | disable }]`  Available options: • `policy` – Configures the Auto-Attach policy data. • `<policy-name (20)>` - Unique policy name. • `match` – Specifies the device match criteria. • `rule` – Specifies the rule table entry. • `<rule-name(20)>` - Unique rule name. • `LLDP-ANY` - Search multiple LLDP TLVs for device ID data.	Configures the Auto-Attach policy entries.	Global Configuration

cnMatrix Parameters and Commands

Commands	Description	CLI Mode
• LLDP-CAP – Matches the LLDP Capabilities TLV data (comma-separated combination of 'bridge', 'wlan', 'router', 'phone', 'station', 'repeater', 'docsis', 'other'). • LLDP-SYS-NAME – Searches in the LLDP System Name TLV for device ID data. • LLDP-SYS-DESC – Searches in the LLDP System Description TLV for device ID data. • LLDP-CHASSIS – Searches in the LLDP Chassis ID TLV for device ID data. • LLDP-PORT – Searches in the LLDP Port ID TLV for device ID data. • LLDP-PORT-DESC – Searches in the LLDP Port Description TLV for device ID data. • <device-desc(60)> - Targets the device identification data. • set – Specifies the action criteria. • action – Specifies the action table entry. • <action-name(20)> - Unique action name vlan – Specifies the list of VLANs. • <vlan-list(99)> - List of 1..20 comma-separated VLANs. • pvid – Specifies the default port VLAN. • <vlan> - Default VLAN from VLAN list. • switch-port-mode – Updates the switch port mode for the interface. • switch-port-mode - Updates the switch port mode for the interface. • hybrid – Updates the switch port mode to Hybrid. • precedence - Policy precedence value. • <value(1-100)> - Precedence. • enable - Enables policy. • disable - Disables policy. **Starting with version 2.1**, the following parameters have been added: • MAC-FULL - Searches for the full MAC address. • MAC-OUI - Searches for the MAC OUI address.		
auto-attach policy <string(20)> ([precedence <integer(1-100)>] [{ enable | disable }]) Available options: • <policy-name(20)> - Unique policy name. • precedence - Policy precedence value. • <value(1-100)> - Precedence. • enable - Enables policy. • disable - Disables policy.	Updates the Auto-Attach policy information.	Global Configuration
no auto-attach policy <string(20)>	Deletes the Auto-Attach policy entries.	Global Configuration
clear auto-attach policy statistics [<string(20)>] Available options: • <policy-name(20)> - Unique policy name	Clears Auto-Attach policy-related statistics.	Global Configuration

cnMatrix Parameters and Commands

Commands	Description	CLI Mode
`auto-attach script {cnPilot} vlan <vlan-list(99)> [ pvid <vlan(1-4066)> ]` Available options: • `cnPilot` - Configures cnPilot device detection. • `vlan` – Specifies the list of VLANs. • `<vlan-list(99)>` - List of 1..20 comma-separated VLANs. • `pvid` – Specifies the default port VLAN. • `<vlan>` - Default VLAN from VLAN list.	Creates Auto-Attach device script configuration.	Global Configuration
`no auto-attach script {cnPilot}`	Deletes the Auto-Attach script configuration data.	Global Configuration
`(no) auto-attach msg-auth-status` (**Starting with version 2.1**)	Enables/Disables the authentication for the auto attach pushed policies.	Interface Configuration
`auto-attach msg-auth-key <private-key(32)>` (**Starting with version 2.1**)	Creates a custom authentication key for the auto attach pushed policy.	Interface Configuration
Starting with version 2.1 `auto-attach update-port-desc lldp-sys-description/lldp-sys-name/pba-policy-name` Available options: • `lldp-sys-description` - Changes the interface description based on LLDP System Description TLV information. • `lldp-sys-name` - Changes the interface description based on LLDP System Name TLV information. • `pba-policy-name` - Changes the interface description according to auto attach policy name.	Sets the interface description based on the auto attach information.	Global Configuration
`auto-attach`	Enables the Auto-Attach feature on the target interface.	Interface Configuration
`no auto-attach`	Disables the Auto-Attach feature on the target interface.	Interface Configuration
`clear auto-attach statistics`	Clears the Auto-Attach interface-related statistics.	Interface Configuration

cnMatrix Dynamic ARP Inspection Parameters and Commands (Starting with version 2.1)

Commands	Description	CLI Mode
`ip arp inspection vlan <VLAN ID>`	Enables the Dynamic ARP Inspection validation process on a particular VLAN	Global Configuration
`no ip arp inspection vlan <VLAN ID>`	Disables the Dynamic ARP Inspection validation process on a particular VLAN	Global Configuration

cnMatrix Parameters and Commands

Commands	Description	CLI Mode
`clear ip arp inspection statistics vlan <VLAN ID>`	Clears the Dynamic ARP Inspection statistics on a particular VLAN.	Global Configuration
`ip arp inspection`	Enables the Dynamic ARP Inspection validation process on the current VLAN	VLAN Configuration
`no ip arp inspection`	Disables the Dynamic ARP Inspection validation process on the current VLAN	VLAN Configuration
`ip arp inspection trust`	Configures the current interface as trusted.	Interface Configuration
`no ip arp inspection trust`	Configures the current interface as untrusted.	Interface Configuration
`show ip arp inspection vlan <VLAN ID>`	Displays the Dynamic ARP Inspection packet statistics on a particular VLAN	Privileged EXEC
`show ip arp inspection vlan`	Displays the Dynamic ARP Inspection packet statistics on all the VLAN	Privileged EXEC
`show ip arp inspection trust-state`	Displays the Dynamic ARP Inspection trust state for all the interfaces	Privileged EXEC

L3 Features

cnMatrix DHCP Relay Parameters and Commands

Commands	Description	CLI Mode
`service dhcp-relay`	Enables the DHCP relay agent. DHCP relay agent relays DHCP messages between DHCP clients and DHCP server located in different subnets. The DHCP relay agent can be enabled only if the DHCP server is disabled.	Global Configuration
`no service dhcp-relay`	Disables the DHCP relay agent feature on the switch.	Global Configuration
`ip dhcp server <ip address>`	Configures the DHCP Server IP Address to which the DHCP packets will be relayed. 5 DHCP Server IP addresses can be configured.	Global Configuration
`ip dhcp relay information option`	Inserts the DHCP relay information option 82 in the DHCP request messages forwarded to a DHCP server from a DHCP client.	Global Configuration
`ip dhcp relay circuit-id option` Available options: • `recv-port` - Adds information related to physical interfaces or LAG ports in the circuit ID sub-option. • `router-index` - Adds information related to	Defines the type of information to be present in circuit ID sub-option that is used in the DHCP relay agent information option.	Global Configuration

cnMatrix Parameters and Commands

Commands	Description	CLI Mode
router interface indexes in the circuit ID sub-option. • Vlanid - Adds information related to VLAN IDs in the circuit ID sub-option.		
ip dhcp relay circuit-id <integer>	Configures the circuit ID value for an interface. The **circuit ID** uniquely identifies a circuit over which the incoming DHCP packet is received. In DHCP relay, it is used to identify the correct circuit over which the DHCP responses should be relayed. The **configured circuit ID** is used in the DHCP relay agent information option to inform the DHCP server about the interface from which DHCP packet is received. The circuit ID is unique for the interfaces and ranges from 1 to 2147483647. The minimum value depends upon the number of interfaces that can be created. For example, if a total of 160 interfaces are allowed to be created in the switch, then the circuit ID value range starts from 161 only. The interfaces include all physical interfaces, port channels and logical L3 interfaces.	Interface Configuration (VLAN / Router Ports)
ip dhcp relay remote-id <string>	Configures the remote ID value for an interface.	Interface Configuration (VLAN / Router Ports)

cnMatrix IP Routing Parameters and Commands

Commands	Description	CLI Mode
ip routing	Enables IP routing.	Global Configuration
ip route <prefix> <mask> {<next-hop> | Vlan <vlan-id/vfi-id> | Mgmt0} [<distance (1-255)>] **Starting with version 2.1:** ip route <prefix> <mask> {<next-hop> | Vlan <vlan-id/vfi-id> | <interface-type> <interface-id>} [<distance (1-255)>]	Adds a static route. The Route defines the IP address or interface through which the destination can be reached. Note: If the static route is configured without any metric value, then the route will be configured with metric value 1.	Global Configuration
ip address <ip-address> <subnet-mask>	Sets the IP address for an interface.	Interface Configuration
no switchport	Sets the port as router port. Only router port Related Command are made available for the interface, when the port is configured as router port.	Interface Configuration (Physical interface)
ip default-ttl <value (1-255)>	Sets the Time-To-Live (TTL) value. TTL is the time set for a unit of data (a packet) to remain in the network or computer before it could be discarded. This value ranges from 1 to 255 seconds.	Global Configuration
arp timeout <seconds (30-86400)>	Sets the ARP (Address Resolution Protocol) cache timeout. The arp timeout defines the time period an	Global Configuration

Commands	Description	CLI Mode
	arp entry remains in the cache. When a new timeout value is assigned, it only affects the new arp entries. All the older entries retain their old timeout values.	
`ip arp max-retries <value (2-10)>`	Sets the maximum number of ARP request retries. The maximum number of ARP requests that the switch generates before deleting an un-resolved ARP entry is defined.	Global Configuration
`clear ip arp`	Clears the dynamically learnt ARP entries.	Global Configuration
`ip proxy-arp`	Enables proxy ARP for the IPv4 interface.	Interface Configuration
`ip redirects`	Enables the router to send ICMP Redirect messages. The Redirect Message is an ICMP message which informs a host to update its routing information to send packets on an alternate route when a packet enters an IP interface and exits the same interface. The redirect message is sent to inform the host of the presence of alternative route.	Global Configuration
`ip unreachables`	Enables the router to send an ICMP unreachable message to the source if the router receives a packet that has an unrecognized protocol or no route to the destination address. ICMP provides a mechanism that enables a router or destination host to report an error in data traffic processing to the original source of the packet. This informs the source that the packet is dropped.	Global Configuration
`ip mask-reply`	Enables the router to send ICMP Mask Reply messages. The IP mask reply is an ICMP message sent by the router to the host informing the subnet mask of the network. This reply is in correspondence to a request sent by the host seeking the subnet mask of the network.	Global Configuration
`ip echo-reply`	Enables the router to send ICMP Echo Reply messages. The ip echo reply is a message sent by a device, in response to a request sent by another device. This message is used to check if device is able to communicate (send and receive data) with the destination device.	Global Configuration
`ip path mtu <dest ip> <tos(0-255)> <mtu(68-65535)>`	Sets the Maximum Transmission Unit (MTU) for usage in PMTU discovery. The transmission of packets from source to destination has many networks to pass through. Each network has its own Maximum transmission unit. The smallest MTU of all the links is the path MTU. This PMTU can be manually configured by the administrator.	Global Configuration
`ip path mtu discover`	Initiates path MTU (Maximum Transmission Unit) discovery.	Global Configuration
`show ip route [ { <ip-address> [<mask>] | connected | static | summary | details | failed} ]` Available options: • **`<ip-address>`** - Displays the IP routing table for the specified destination IP Address.	Displays the IP routing table.	Privileged EXEC

cnMatrix Parameters and Commands

Commands	Description	CLI Mode
• `details` - Displays the information about route status (Route in Hardware, Route Reachable, Best route) • `failed` - Displays the information about the routes that failed to be programmed in hardware. • `static` - Displays the Static Routes in the table. • `summary` - Displays the Summary of all routes. • `ospf` – Displays the ospf routes. • `rip` – Displays the rip routes.		
`show ip default-distance`	Displays the detailed information of the default administrative distance for static IPv4 routes.	Privileged EXEC
`show ip traffic [ interface { Vlan<vlan-id> | <interface-type> <interface-id>} ] [hc]`	Displays the IP protocol statistics.	Privileged EXEC
`show ip information`	Displays the IP configuration information.	Privileged EXEC
`show ip arp [ { Vlan <vlan-id> | <interface-type> <interface-id> | <ip-address> | <mac-address> | summary | information | statistics }]`	Displays the IP ARP table.	Privileged EXEC
`show ip proxy-arp`	Displays the status of the proxy ARP for all the created interfaces.	Privileged EXEC
`traceroute {<ip-address> | ipv6 <prefix>} [min-ttl <value (1-15)>] [max-ttl <value (1-99)>]`	Traces route to the destination IP.	Privileged EXEC

cnMatrix OSPF Parameters and Commands (Starting with version 2.1)

Commands	Description	CLI Mode
`router ospf`	Enables the OSPF routing process and enters into the OSPF Router Configuration Mode.	Global Configuration
`router-id <router ip address>`	Sets the router-id for the OSPF process.	OSPF Router Configuration
`area <area-id> stub [no-summary]` Available options: • `<area-id>` - Configures the identifier for the area (IP address format). • `no-summary` - Prevents an Area Border Router (ABR) from sending summary link advertisements.	Specifies an area as a stub area and other parameters related to that area.	OSPF Router Configuration

cnMatrix Parameters and Commands

Commands	Description	CLI Mode
`area <area-id> default-cost <cost> [tos <tos value(0-30)>]` Available options: • `<area-id>` - Configures the identifier for the area (IP address format). • `default-cost <cost>` - Configures the cost for the default summary route used for a stub or NSSA. • `tos <tos value(0-30)>` - Configures the Type of Service of the route being configured.	Specifies a cost for the default summary route sent into a stub or NSSA.	OSPF Router Configuration
`area <area-id> stability-interval <Interval-Value (0 - 0x7fffffff)>` Available options: • `<area-id>` - Configures the identifier for the area (IP address format). • `<Interval-Value (0 - 0x7fffffff)>` - Stability interval value in seconds.	Configures the Stability interval for NSSA.	OSPF Router Configuration
`area <area-id> nssa [{ no-summary | default-information-originate [metric <value (0-16777215)>] [metric-type <Type(1-3)>] [tos <tos value (0-30)>] [no-redistribution] }]` Available options: • `<area-id>` - Configures the identifier for the area (IP address format). • `no-summary` – Allows an area to be nssa, and not having summary routes inserted into it. • `Default-information-originate` - Configures an area as a NSSA area and other parameters related to that area.	Configures a particular area as not-so-stubby area (NSSA).	OSPF Router Configuration
`area <area-id> translation-role { always | candidate }` Available options: • `<area-id>` - Configures the identifier for the area (IP address format). • `translation-role` - Configures the NSSA Border router ability to perform NSSA Translation of Type-7 LSAs to Type-5 LSAs. - `always` - Sets translator role where the Type-7 LSAs are always translated into Type-5 LSAs. - `candidate` - Sets translator role where an NSSA border router participates in the translator election process.	Configures the translation role for the NSSA.	OSPF Router Configuration
`area <area-id> range <Network> <Mask> {summary | Type7} [{advertise | not-advertise}] [tag <value>]` Available options: • `<Network>` - Configures the IP address of the network indicated by the range. • `Summary` - Sets the LSA type as summary LSA. • `Type7` - Sets the LSA type as Type-7 LSA. • `advertise` - Sets the address range status to advertise and generates a Type 3 summary link-state advertisement (LSA).	Consolidates and summarizes routes at an area boundary which is used only with Area Border Routers (ABRs).	OSPF Router Configuration

Commands	Description	CLI Mode
• tag <tag-value> - Configures the Tag Type which describes whether Tags will be generated automatically or manually configured.		
compatible rfc1583	Sets the OSPF compatibility list compatible with RFC 1583.	OSPF Router Configuration
abr-type { standard | cisco | ibm } Available options: • standard - Configures the Standard ABR type as defined in RFC 2328. • cisco - Configures the CISCO ABR type as defined in RFC 3509. • ibm - Configures the IBM ABR type as defined in RFC 3509.	Sets the Alternative ABR Type.	OSPF Router Configuration
default-information originate always [metric <metric-value (0-16777215)>] [metric-type <type (1-2)>] Available options: • always - Advertises the default route whether the software has a default route or not. • metric <metric-value (0-16777215)> - Sets the Metric value applied to the route before it is advertised into the OSPF Domain Metric used for generating the default route. • metric-type <type (1-2)> - Sets the Metric Type applied to the route before it is advertised into the OSPF Domain External link type associated with the default route advertised into the OSPF routing domain.	Enables the generation of a default external route into an OSPF routing domain and other parameters related to that area.	OSPF Router Configuration
ASBR Router	Specifies this router as ASBR.	OSPF Router Configuration
summary-address <Network> <Mask> <area-id> [{allowAll | denyAll | advertise | not-advertise}] [Translation {enabled | disabled}][tag tag-value] Available options: • <Network> - Configures the IP address of the network indicated by the range. • <Mask> - Configures the subnet mask that pertains to the range.	Creates aggregate addresses for OSPF and helps in reducing the size of the routing table.	OSPF Router Configuration
redistribute {static | connected | rip | all} [metric <metric_value(0-16777214)>] [metric-type {1-2}] Available options: • static - Redistributes the statically configured route in the OSPF routing process. • connected – Redistributes the directly connected network routes in the OSPF routing process. • rip – Redistributes the routes learned by the RIP process in the OSPF routing process. • all - Imports all routes learned in the OSPF routing process.	Configures the protocol from which the routes have to be redistributed into OSPF and advertises the routes learned by other protocols.	OSPF Router Configuration

Commands	Description	CLI Mode
`distance <1-255>`	Configures the administrative distance to reach the destination	OSPF Router Configuration
`network <Network number> area <area-id>` Available options: • `<Network number>` - Configures the Network type for the interfaces. • `<area-id>` - Configures the identifier for the area (IP address format).	Defines the interfaces on which OSPF runs and the area ID for those interfaces.	OSPF Router Configuration
`passive-interface {vlan <vlan-id > <interface-type> <interface-id> | <IP-interface-type> <IP-interface-number>}` Available options: • `<vlan -id>` - Configures the specified VLAN ID as passive interface. • `<interface-type>` - Configures OSPF for the specified type of interface.	Suppresses routing updates on an interface and makes the interface passive.	OSPF Router Configuration
`passive-interface default`	Suppresses routing updates on all interfaces and makes the passive interface to default.	OSPF Router Configuration
`debug ip ospf { pkt { hp | ddp | lrq | lsu | lsa } | module { adj_formation | ism | nsm | config | interface | restarting-router | helper | redundancy } }` Available options: • `pkt` – Generates debug statements for Packet High Level Dump trace. • `module` - Generates debug statements for RTM Module traces.	Sets the OSPF debug level	Privileged EXEC Mode
`timers spf <spf-delay(0-65535)> <spf-holdtime(0-65535)>`	Configures the delay time and hold time in starting a SPF calculation after receiving a topology change.	OSPF Router Configuration
`ip ospf key <Key-ID (0-255)> start-accept <DD-MON-YEAR,HH:MM>` Available options: • `key <Key-ID (0-255)>` - Identifies the secret key used to create the message digest appended to the OSPF packet. • `start-accept <DD-MON-YEAR,HH:MM>` - Configures the time when the router will start accepting packets that have been created with this key.	Configures the time the router will start accepting packets that have been created with the specified key.	Interface Configuration (VLAN interface / Router port)
`ip ospf key <Key-ID (0-255)> start-generate <DD-MON-YEAR,HH:MM>`	Configures the time when the switch will start generating OSPF packets with the same key ID on the interface.	Interface Configuration (VLAN interface / Router port)

cnMatrix Parameters and Commands

Commands	Description	CLI Mode
`ip ospf key <Key-ID (0-255)> stop-generate <DD-MON-YEAR,HH:MM>`	Configures the time when the router will stop using configured key for packet generation.	Interface Configuration (VLAN interface / Router port)
`ip ospf key <Key-ID (0-255)> stop-accept <DD-MON-YEAR,HH:MM>`	Configures the time when the router will stop accepting OSPF packets created by using the configured key.	Interface Configuration (VLAN interface / Router port)
`show ip ospf`	Displays general information about the OSPF routing process.	Privileged EXEC
`show ip ospf interface [ { vlan <vlan-id> | <interface-type> <interface-id> | <IP-interface-type> <IP-interface-number>}]`	Displays general information about the OSPF routing processes for the specified interface.	Privileged EXEC
`show ip ospf neighbor [{ vlan <vlan-id > [ <interface-type> <interface-id> | <IP-interface-type> <IP-interface-number>}] [Neighbor ID] [detail]`	Displays the OSPF related neighbor information list and observes the neighbor data structure.	Privileged EXEC
`show ip ospf request-list [<neighbor-id>] [{ vlan <vlan-id > [ <interface-type> <interface-id> | <IP-interface-type> <IP-interface-number>}]`	Displays the OSPF Link state request list advertisements (LSAs) requested by a router and debugging OSPF routing operations.	Privileged EXEC
`show ip ospf retransmission-list [<neighbor-id>] [{ vlan <vlan-id > [ <interface-type> <interface-id> | <IP-interface-type> <IP-interface-number>}]`	Displays the OSPF Link state retransmission list information waiting to be resent.	Privileged EXEC
`show ip ospf border-routers`	Displays the OSPF Border and the Boundary Router Information.	Privileged EXEC
`show ip ospf area-range`	Displays the OSPF summary-address redistribution information.	Privileged EXEC
`show ip ospf route`	Display the routes learned by the OSPF process.	Privileged EXEC
`show ip ospf database database-summary`	Displays the OSPF LSA Database summary.	Privileged EXEC
`ip ospf retransmit-interval <seconds (1 - 3600)>`	Sets the interval value (in seconds) between LSA retransmissions.	Interface Configuration (VLAN interface / Router port)
`ip ospf transmit-delay <seconds (1 - 3600)>`	Sets the estimated time (in seconds) to transmit a link state update packet on the interface.	Interface Configuration (VLAN interface / Router port)
`ip ospf priority <value (0 - 255)>`	Sets the router priority.	Interface Configuration

Commands	Description	CLI Mode
		(VLAN interface / Router port)
`ip ospf hello-interval <seconds (1 - 65535)>` The smaller the hello interval, the faster the topological changes will be detected.	Sets the hello interval time on the interface.	Interface Configuration (VLAN interface / Router port)
`ip ospf dead-interval <seconds (1-65535)>`	Sets the interval (in seconds) at which hello packets must not be seen before neighbors declare the router down.	Interface Configuration (VLAN interface / Router port)
`ip ospf cost <cost (1-65535)>`	Specifies the cost of sending a packet on an interface.	Interface Configuration (VLAN interface / Router port)
`ip ospf network broadcast`	Configure the OSPF network type broadcast	Interface Configuration (VLAN interface / Router port)
`ip ospf authentication-key <password (8)>`	Specifies the password to be used by neighboring routers that are using the OSPF simple password authentication	Interface Configuration (VLAN interface / Router port)
`ip ospf message-digest-key <Key-ID (0-255)> [{ md5 | sha-1 | sha-224 | sha-256 | sha-384 | sha-512}] <Key (16)>` Available options: • `md5` - Sets the authentication type as Message Digest 5 (MD5) authentication. • `sha-1` - Sets the authentication type as Secure Hash Algorithm 1 (SHA1) authentication. • `sha-224`- Sets the authentication type as Secure Hash Algorithm 224 (SHA224) authentication. • `sha-256` - Sets the authentication type as Secure Hash Algorithm 256 (SHA256) authentication. • `sha-384` - Sets the authentication type as Secure Hash Algorithm 384 (SHA384) authentication. **Starting with version 2.1**, this parameter has been removed. • `sha-512` - Sets the authentication type as Secure Hash Algorithm 512 (SHA512) authentication. **Starting with version 2.1**, this parameter has been removed.	Enables the OSPF MD5 authentication.	Interface Configuration (VLAN interface / Router port)
`ip ospf authentication {message-digest | sha-1 | sha-224 | sha-256 | sha-384 | sha-512 | null | simple}`	Specifies the authentication type for an interface.	Interface Configuration (VLAN interface / Router port)
`redist-config <Network> <Mask> [metric-value <metric (1 - 16777215)>] [metric-type {asExttype1 | asExttype2}] [tag <tag-value>}` Available options:	Configures the information to be applied to routes learnt from RTM.	OSPF Router Configuration

Commands	Description	CLI Mode
• `<Network>` - Configures the IP Address of the Destination route. • `<Mask>` - Configures the Mask of the Destination route. • `metric-value <metric (1 - 16777215)>` - Configures the Metric value applied to the route before being advertised into the OSPF Domain. • `metric-type` - Configures the Metric Type applied to the route before being advertised into the OSPF Domain. `tag <tag-value>` - Configures the Tag Type describes whether Tags will be automatically generated or will be manually configured. **Starting with version 2.1**, the `redist-config` command has been removed.		
`show ip protocols`	Displays information about the active routing protocol process.	Privileged EXEC

cnMatrix RIP Parameters and Commands (Starting with version 2.1)

Commands	Description	CLI Mode
`router rip`	Enables the RIP feature and enters the router configuration mode.	Global Configuration
`ip rip security { minimum | maximum }` Available options: • `minimum` – RIPv1 packets will be accepted even if authentication is enabled. • `maximum` – RIPv1 packets will be ignored when authentication is enabled.	Configures the security level of the RIP feature in the system to accept or ignore RIPv1 packets when authentication is enabled.	RIP Router Configuration
`network <ip-address>` Available options: • `<ip-address>` - Configures the IP network address of the interface that is to be associated with RIP routing process.	Enables the RIP feature on an IP network for an unnumbered VLAN interface / router port.	RIP Router Configuration
`passive-interface {vlan <vlan-id/vfi-id> | <interface-type> <interface-id>}` Available options: • `vlan <vlan-id >` - Sets the specified VLAN interface as a passive interface on which RIP routing updates are suppressed. • `<interface-type>` - Sets the specified type of router interface as passive interface.	Suppresses the RIP routing updates on a specified VLAN interface in the default switch context or on a specified router port.	RIP Router Configuration

cnMatrix Parameters and Commands

Commands	Description	CLI Mode
• <interface-id> - Configures the specified interface identifier.		
redistribute { all | connected | ospf | static } Available options: • all - Specifies that all routes have to be imported from the RIP. • connected - Imports directly connected networks routes into RIP routing process. • ospf - Imports routes that are learnt by the OSPF process in the RIP routing process. • static - Imports routes configured statically in the RIP routing process.	Enables the RIP feature to participate in Route Redistribution.	RIP Router Configuration
default-metric [<value>]	Sets the default metric values to be used for redistributed routes for RIP.	RIP Router Configuration
distance <1-255>	Enables the administrative distance of the routing protocol and sets the administrative distance value.	RIP Router Configuration
auto-summary {enable | disable}	Enables or disables the auto summarization of routes in RIP and restores the default behavior of automatic summarization of subnet routes into network-level routes.	RIP Router Configuration
ip rip summary-address <ip-address> <mask>	Sets route aggregation over a VLAN interface / router port for all subnet routes that fall under the specified IP address and mask.	Interface Configuration
ip rip default route install	Installs the received route in the RIP database.	Interface Configuration
ip rip send version { [1] [2] }	Sets the IP RIP version number for transmitting advertisements.	Interface Configuration
ip rip receive version { [1] [2]}	Sets IP RIP version number for receiving advertisements.	Interface Configuration
ip rip authentication mode { text | md5 }	Configures the authentication mode to be used in RIP packets for VLAN interface / router port.	Interface Configuration
ip rip authentication key-chain <key-chain-name (16)>	Configures the interface RIP version 2 authentication string.	Interface Configuration
no ip rip authentication	Disables authentication.	Interface Configuration
debug ip rip { all | init | data | control | dump | os | mgmt | failure | buffer }	Sets the debug level for RIP module.	Privileged EXEC
show ip rip database [<ip-address> <ip-mask>] | statistics | authentication}	Displays the IP RIP protocol database, statistics or authentication related information.	Privileged EXEC
ip rip send version none	Stops the IP RIP transmitting advertisements to be sent on a VLAN interface / router port.	Interface Configuration
ip rip auth-type { md5 | sha-1 | sha-256 | sha-384 | sha-512 } Available options:	Configures the authentication type.	Interface Configuration

Commands	Description	CLI Mode
• `md5` - Configures the authentication type as keyed MD5 (Message Digest 5) authentication. • `sha-1` - Configures the authentication type as Secure Hash Algorithm 1 (SHA1) authentication. SHA1 generates Authentication digest of length 20 bytes. • `sha-256` - Configures the authentication type as Secure Hash Algorithm 256 (SHA256) authentication. SHA256 generates Authentication digest of length 32 bytes. • `simple` -		
`ip rip authentication key-id <integer (0-255)> key <string (16)>` Available options: • `<integer (0-255)>` - Configures the active authentication KeyID. • `key <string (16)>` - Configures the key used as the authentication key.	Configures the authentication key ID and the authentication key.	Interface Configuration
`ip rip key-id <integer (0-255)> start-accept <key>`	Configures the time when the router starts accepting RIP updates for a specific key ID.	Interface Configuration
`ip rip key-id <integer (0-255)> stop-accept <key>`	Configures the time when the router stops accepting RIP updates for a specific key ID.	Interface Configuration
`ip rip key-id <integer (0-255)> start-generate <key>`	Configures the time when the router starts generating RIP updates for a specific key ID.	Interface Configuration
`ip rip key-id <integer (0-255)> stop-generate <key>`	Configures the time when the router stops generating RIP updates for a specific key ID.	Interface Configuration
`timers basic <update-value (10-3600)> <routeage-value (30-500)> <garbage-value (120-180)>` Available options: • `update-interval (10-3600)> –` Configures the time interval (in seconds) at which the updates are sent. • `routeage-value(30-500)> –` Configures the time interval (in seconds) after which the route entry is put into garbage collect (that is, marked as invalid). • `garbage-value(120-180) –` Configures the time interval (in	Configures the update timers, route age and garbage collection timers for the VLAN interface / router port.	Interface Configuration

cnMatrix Parameters and Commands

Commands	Description	CLI Mode
seconds) after which the route entry marked as invalid is deleted. The advertisements of this entry is set to INFINITY while sending to others.		
`ip rip receive version {none|1|2}` Available options: • `1` - Version 1 of RIP update to be received. • `2` - Version 2 of RIP update to be received. • `None` - No RIP update to be received.	Configures the RIP version that is to be accepted.	Interface Configuration
`default-information originate`	Metric value to be used for the default route.	Interface Configuration
`ip split-horizon`	Sets the split horizon status.	Interface Configuration
`ip split-horizon poison`	Enables split horizon with poison reverse.	Interface Configuration

Management Features

cnMatrix DHCP Client Parameters and Commands

Commands	Description	CLI Mode
`debug ip dhcp client { all | bind | errors | events | packets }` Available options: • `all` - Generates debug statements for all kind of failure traces. • `bind` - Generated debug statements for trace bind messages. • `errors` - Generates debug statements for trace error code debug messages. • `event` - Generates debug statements for DHCP client events that provide DHCP client service status. • `packets` - Generates debug statements for packets related messages.	Enables the tracking of the DHCP client operations as per the configured debug levels.	Privileged EXEC
`release dhcp { mgmt0 | vlan <vlan-id (1-4066)> | <interface-type> <interface-id> }`	Releases the DHCP lease obtained for an IP address from a DHCP server and assigned to the specified interface.	Privileged EXEC

Commands	Description	CLI Mode
`renew dhcp { mgmt0 | vlan <vlan-id (1-4066)> | <interface-type> <interface-id> }`	Renews the DHCP lease for the interface specified.	Privileged EXEC
`show ip dhcp client stats`	Displays the DHCP client statistics information for interfaces that are configured to acquire IP address dynamically from the DHCP server.	Privileged EXEC
`ip dhcp client discovery timer <integer (1-300)>`	Configures the DHCP Client Discovery timer waiting time between discovery messages sent by the DHCP client.	Privileged EXEC
`no ip dhcp client discovery timer`	The no form of the command resets DHCP Client discovery timer with its default value.	Privileged EXEC
`ip dhcp client idle timer <integer (1-30)>`	Configures the DHCP Client idle timer, which specifies the time to wait after four unsuccessful DHCP client discovery messages.	Privileged EXEC
`no ip dhcp client idle timer`	The no form of the command resets the DHCP Client idle timer with the default value.	Privileged EXEC
`ip dhcp client arp-check timer <integer (1-20)>`	Configures DHCP client retransmission timeout between ARP messages.	Privileged EXEC
`no ip dhcp client arp-check timer`	The no form of the command resets DHCP Client arp timer with the default value.	Privileged EXEC
`[no] ip dhcp client fast-access`	Enables DHCP Fast access Mode. If fast access mode is enabled, time to wait between discovery messages i.e. discovery timeout and time to wait after four unsuccessful discovery will be user configurable and the default value for discovery timeout is 5 seconds and for the null state timeout is 1 second. The no form of the command disables DHCP Client fast access mode. If the mode is disabled, default value for discovery timeout and null state timeout will be 15 seconds and 180 seconds respectively. The timeout values cannot be changed under disable mode.	Privileged EXEC
`ip dhcp client client-id {<interface-type> <interface-id> | vlan <vlan-id (1-4094)> | ascii <string> }`	Sets the unique identifier to dhcp client identifier.	Interface Configuration
`ip dhcp client request { sip-server-info | option43 | option240}`	Sets the dhcp option type to request the server.	Interface Configuration
`ip dhcp client vendor-specific <vendor-info>`	Configures vendor specific information for the DHCP client.	Interface Configuration
`ip address dhcp`	Enables the DHCP client functionality on the selected interface.	Interface Configuration
`no ip address`	Disables DHCP client functionality on the selected interface.	Interface Configuration

cnMatrix Parameters and Commands

Commands	Description	CLI Mode
`show ip dhcp client fast-access`	Displays DHCP fast access information such as Fast Access Mode status, Dhcp Client Fast Access DiscoverTimeOut, Dhcp Client Fast Access NullStateTimeOut, Dhcp Client Fast Access Arp Check TimeOut values.	Privileged EXEC
`show ip dhcp client option`	Displays DHCP client options set by Server which provides the details like interface, interface type, length and value.	Privileged EXEC
`show ip dhcp client client-id`	Displays the unique identifier to DHCP client.	Privileged EXEC
`clear ip dhcp client statistics [interface {vlan <VlanId(1-4094)> |<interface-type> <interface-id>}]`	Clears the DHCP client statistics for all ports or for the specified interface created in the system.	Global Configuration

cnMatrix DHCP Server Parameters and Commands

Commands	Description	CLI Mode
`debug ip dhcp server { all | bind | errors | events | linkage | packets }` Available options: • `all` - Generates debug traces for all failures. • `bind` - Generated traces for bind messages. • `errors` - Generates traces for error code debug messages. • `event` - Generates traces for DHCP Server status events. • `packets` - Generates traces for Database linkage messages. • `packets` - Generates traces for DHCP protocol packets related messages.	Enables the tracking of the DHCP Server operations as per the configured debug levels.	Privileged EXEC
`[no] service dhcp-server`	Enables the DHCP Server service on the system. The 'no' form disables DHCP Server service.	Global Configuration
`ip dhcp pool <index (1-2147483647)> [<Pool Name>]`	This command creates a DHCP server address pool and enters in to the DHCP pool configuration mode in which the pool is customized. The address pool has a range of IP addresses that can be assigned to the DHCP client and also information about client configuration parameters such as domain name.	Global Configuration
`no ip dhcp pool <index (1-2147483647)>`	The 'no' form of the command deletes the existing DHCP server address pool.	Global Configuration
`ip dhcp { ping packets | server offer-reuse <timeout (1-120)> }` Available options:	Enables the ICMP echo mechanism or configures offer-reuse timeout for the DHCP server. These parameters are used to control the allocation of IP address to a DHCP client.	Global Configuration

• `ping packets`- Enables / disables ICMP echo mechanism. This mechanism allows the DHCP server to verify the availability of an IP address before assigning it to a DHCP client. DHCP server sends ping packets to the IP address that is intended to be assigned for the DHCP client. If the ping operation fails, DHCP server assumes that the address is not in use and assigns the address to the requesting DHCP client. • `server offer-reuse` - Configures the amount of time (in seconds), the DHCP server entity should wait for the DHCP REQUEST from the DHCP client before reusing the lease offer for other DHCP client. This value ranges from 1 to 120 seconds.		
`no ip dhcp { ping packets | server offer-reuse | binding <ip address> }`	The no form of the command disables ICMP echo mechanism, resets server offer-reuse time to its default value or removes a bind entry from a server binding table.	Global Configuration
`ip dhcp option <code (1-2147483647)> { ascii <string> | ip <address> | hex <hexadecimal> }` Available options: • `code` - Configures the unique DHCP option code that represents a specific DHCP option used in a DHCP OFFER message in response to a DHCP DISCOVER message. • `ascii <string>` - Configures the ASCII value to be set for the corresponding option code that accepts ASCII string. • `Ip <address> -` Configures the unicast IP address to be set for the corresponding option code that accepts IP address. • `hex <hexadecimal>` - Configures the hexadecimal value to be set for the corresponding option code that accepts hexadecimal values.	Sets the DHCP Server options. This command globally configures the various available DHCP server options with the corresponding specific values. These values can be an ASCII string or an IP address. These global options are applicable for all DHCP server address pools.	Global Configuration
`no ip dhcp option <code (1-2147483647)>`	The no form of the command deletes the existing DHCP server option.	Global Configuration
`network <start- IP> [ { <mask> | / <prefix-length (1-31)> } ] [end ip]` Available options:	Creates a subnet pool that defines a network IP subnet address for the corresponding DHCP address pool and contains IP addresses to be assigned to the DHCP client.	DHCP Pool Configuration

• <start-IP> - Configures the IP subnet address for the DHCP pool. The addresses within the specified network subnet are assigned to the DHCP client. • <mask> - Configures the subnet mask for the network IP address • <prefix-length (1-31)> - Configures the number of high-order bits in the IP address. These bits are common among all hosts within a network. This value should be preceded by a slash (/) with space before and after the slash. • <end ip> - Configures the end IP address for the network IP subnet set for the DHCP address pool. This value restricts the IP addresses that can be assigned to the DHCP client. This value is used to manually set the end IP address.		
`no network`	The no form of the command deletes the created subnet pool.	DHCP Pool Configuration
`[no] excluded-address <low-address> <high-address>`	Creates an excluded pool that defines a range of IP addresses which needs to be excluded from the created subnet pool. That is, the IP addresses in this range including start and end IP address of the excluded pool are not assigned to any DHCP client. The no form of the command deletes the created excluded pool. The same start IP address and end IP address of the already created excluded pool should be provided while executing the no form of the command.	DHCP Pool Configuration
`[no] ip dhcp excluded-address <low-address> [<high-address>]`	Creates an excluded pool to prevent DHCP server from assigning certain addresses to DHCP clients. The no form of the command deletes the excluded pool.	Global Configuration

`domain-name <domain (63)>`
Starting with version 2.1:
`ip domain name`
	Configures the domain name option for the corresponding DHCP server address pool. A DHCP client uses this domain name while resolving host names through a domain name system. The DHCP option code is 15. This value is a string with maximum size of 63.	DHCP Pool Configuration

`no domain-name`	Deletes the domain name option configuration for the DHCP server address pool.	DHCP Pool Configuration
`dns-server <ip address> [<ip address>]`	Configures the IP address of a DNS server for the corresponding DHCP server address pool. The client correlates the DNS IP address with the host name. The DNS server is used to translate domain names and hostnames into corresponding IP addresses.	DHCP Pool Configuration
`no dns-server`	Deletes the DNS server IP address option configuration for the DHCP server address pool.	DHCP Pool Configuration

default-router <ip address>	Configures the IP address of a default router to be transmitted to a DHCP Client. The configured IP address of the default router should be on the same subnet of the DHCP client.	DHCP Pool Configuration
no default-router	Deletes the default router IP address configuration for the DHCP server address pool.	DHCP Pool Configuration
netbios-name-server <ip address>	Configures the IP address of a NetBIOS (Network Basic Input / Output System) and WINS (Windows Internet Naming Service) name server that is available to Microsoft DHCP clients, for the corresponding DHCP server address pool.	DHCP Pool Configuration
no netbios-name-server	Deletes the NetBIOS and WINS name server IP address configuration for the DHCP server address pool.	DHCP Pool Configuration
netbios-node-type { <0-FF> | b-node | h-node | m-node | p-node }	Configures the NetBIOS node type for Microsoft DHCP clients, for the corresponding DHCP server address pool. The node type denotes the method used to register and resolve NetBIOS names to IP addresses.	DHCP Pool Configuration
no netbios-node-type	Deletes the NetBIOS node type option configuration for the DHCP server address pool.	DHCP Pool Configuration
option <code (1-2147483647)> { ascii <string> | ip <address>}	Configures the various available DHCP server options with the corresponding specific values, for the corresponding DHCP server address pool These values can be an ASCII string or an IP address.	DHCP Pool Configuration
no option <code (1-2147483647)>	Deletes the DHCP server option for the DHCP server address pool.	DHCP Pool Configuration
lease { <days (0-365)> [<hours (0-23)> [<minutes (1-59)>]] | infinite }	Configures the DHCP lease period for an IP address that is assigned from a DHCP server to a DHCP client, for the corresponding DHCP server, The DHCP lease period represents the time interval (in seconds) until the DHCP client can use the assigned IP address.	DHCP Pool Configuration
no lease	Resets the DHCP lease period to its default value of 3600 seconds for the DHCP server address pool.	DHCP Pool Configuration
utilization threshold { <integer (0-100)> }	Configures the pool utilization threshold value (in percentage) for the corresponding DHCP server address pool.	DHCP Pool Configuration
no utilization threshold	Resets the pool utilization threshold to its default value - 75% - for the DHCP server address pool.	DHCP Pool Configuration
host hardware-type <type (1-255)> client-identifier <mac-address> { ip <address> | option <code (1-2147483647)> { ascii <string> | ip <address> | hex <hexadecimal> }}	Configures the host hardware type and its DHCP option with specific values for the corresponding DHCP server address pool. Hardware type of value 1 is associated with Ethernet type.	DHCP Pool Configuration
no host hardware-type <host-hardware-type (1-2147483647)>	The no form of the command deletes the hardware type and its DHCP option.	DHCP Pool Configuration
ip dhcp sip-server { {domain <string> [<string>] } | {ip <ip_addr> [<ip_addr>] } }	This command sets SIP Servers in the global DHCP server configuration parameters.	Global Configuration

no ip dhcp sip-server	Deletes the SIP Servers from the global DHCP server configuration parameters.	Global Configuration
ip dhcp ntp-server <ip address> [<ip address>]	Sets the NTP Servers in the global DHCP server configuration parameters.	Global Configuration
no ip dhcp ntp-server	Deletes the NTP Server from the global DHCP server configuration parameters.	Global Configuration
ip dhcp dns-server <ip address> [<ip address>]	Sets the DNS Servers in the global DHCP server configuration parameters	Global Configuration
no ip dhcp dns-server	Deletes the DNS Server from the global DHCP server configuration parameters.	Global Configuration
ntp-server <ip address> [<ip address>]	Sets the NTP Servers in the pool specific DHCP server configuration parameters.	DHCP Pool Configuration
no ntp-server	Deletes the NTP Server from the pool specific DHCP server configuration parameters.	DHCP Pool Configuration
sip-server { {domain <string> [<string>]} | {ip <ip_addr> [<ip_addr>]} }	Sets the SIP Servers in the pool specific DHCP server configuration parameters.	DHCP Pool Configuration
no sip-server	Deletes SIP Server from the pool specific DHCP server configuration parameters.	DHCP Pool Configuration
show ip dhcp server information	Displays the DHCP server configuration information. The information contains status of DHCP server, ICMP echo mechanism status, debug level, boot server IP address, boot file name and server offer reuse time.	Privileged EXEC
show ip dhcp server pools	Displays the global DHCP option configuration for all DHCP server address pools and configuration information such as utilization threshold, of address pools for which subnet pool is created or host options are configured.	Privileged EXEC
show ip dhcp server binding	Displays the DHCP server binding information. A DHCP binding is created when a DHCP server assigns an IP address to a DHCP client. The information contains the allocated IP address, host hardware type, host hardware address, binding state and expiry time of the allocated DHCP lease.	Privileged EXEC
show ip dhcp server statistics	Displays various DHCP server statistics related information such as number of DHCPDECLINE messages received, DHCPOFFER messages sent and so on.	Privileged EXEC
clear ip dhcp server statistics	Clears the DHCP server statistics	Privileged EXEC

cnMatrix OOB Parameters and Commands

Commands	Description	CLI Mode
show interface mgmt0	Displays interface status and configuration.	Privileged EXEC
show ip interface mgmt0	Displays IP interface status and configuration.	Privileged EXEC
shutdown	Disables a physical interface.	Interface Configuration

`no shutdown`	Enables a physical interface.	Interface Configuration
`ip address dhcp`	The IP Address negotiated via DHCP.	Interface Configuration
`no ip address`	Resets the IP address for this OOB Interface.	Interface Configuration
`ip address <IP address> <IP mask>`	Configures a static IP address on the OOB Interface.	Interface Configuration

cnMatrix Telnet Client Parameters and Commands

Commands	Description	Mode
`telnet <ipv4_addr/ipv6_addr> [-l <username>]` Available options: • `<ipv4_addr/ipv6_addr>` - Establishes telnet client session for the specified IP address. It supports both IPv4 and IPv6 addresses. • `-l <username>` - Specifies the user name.	Establishes the telnet client session with the specified IP address.	Privileged EXEC
`show telnet-client`	Displays the status of Telnet Client feature and the number of active client sessions.	Privileged EXEC

cnMatrix Telnet Server Parameters and Commands

Commands	Description	Mode

`feature telnet`
Starting with version 2.1:
`telnet-server [enable|disable]`
	Enables/Disables the telnet service.	Global Configuration

`show telnet-server`	Displays the telnet server status.	Privileged EXEC

cnMatrix System Resource Monitoring Parameters and Commands

Commands	Description	CLI Mode
`show env CPU`	Displays the threshold information of the CPU.	Privileged EXEC
`show env RAM`	Displays the threshold information of the RAM.	Privileged EXEC
`show env all`	Displays the threshold information of all resources, such as CPU, Flash, RAM and temperature.	Privileged EXEC

cnMatrix Parameters and Commands

show env fan	Displays the threshold information of the fan. Note: Only the EX2028-P model is equipped with fans.	Privileged EXEC
show env flash	Displays the threshold information of the Flash.	Privileged EXEC

cnMatrix SYSLOG Parameters and Commands

Commands	Description	CLI Mode
logging on	Enables the Syslog server. This command is also used to configure the Syslog server IP address, the log-level and other Syslog related parameters	Global Configuration
logging buffered (1-200)	Configures the Syslog server IP address, the log-level and other Syslog related parameters.	Global Configuration
show logging	Displays Logging status and configuration information	Privileged EXEC
logging-server {_short(128-191)> {ipv4 <ucast_addr> | ipv6 <ip6_addr> | <dns_host_name>} [port <integer(1-65535)>] }	Sets the priority of syslog messages.	Global Configuration
no logging-server <short(128-191)> {ipv4 <ucast_addr> |ipv6 <ip6_addr> | <dns_host_name>}	Removes the priority of syslog messages.	Global Configuration
logging severity {alerts | critical | debugging | emergencies | errors | informational | notification | warnings}	Configures the Syslog server IP address, the log-level and other Syslog related parameters.	Global Configuration
no logging-file <short(128-191)> <string(32)>	Removes the local logging files.	Global Configuration
show logging-file	Displays the syslog file table.	Privileged EXEC
show logging-server	Displays the syslog logging server table.	Privileged EXEC
show syslog information	Displays the syslog information.	Privileged EXEC
show syslog file-name	Displays the syslog local storage file name.	Privileged EXEC
show syslog localstorage	Displays the syslog local storage.	Privileged EXEC
syslog {{filename-one | filename-two | filename=three} <string(32)>}	Configures the file name to store the syslog messages.	Global Configuration
syslog localstorage	Configures the local storage related configuration.	Global Configuration

cnMatrix SNMP Parameters and Commands

Commands	Description	CLI Mode
enable snmpagent	Enables the SNMP agent feature.	Global Configuration
disable snmpagent	Disables the SNMP agent feature.	Global Configuration
snmp community index <CommunityIndex> name <CommunityName> security <SecurityName> [context <Name >] [{volatile | nonvolatile}] [transporttag <TransportTagIdentifier | none>] [contextengineid <ContextEngineID>]	Configures the SNMP community details.	Global Configuration
snmp group <GroupName> user <UserName> security-model {v1 | v2c | v3 } [{volatile | nonvolatile}]	Configures the SNMP group details.	Global Configuration
snmp access <GroupName> {v1 | v2c | v3 {auth | noauth | priv}} [read <ReadView | none>] [write <WriteView | none>] [notify <NotifyView | none>] [{volatile | nonvolatile}] [context <string(32)>]	Configures the SNMP group access details.	Global Configuration
snmp engineid <EngineIdentifier>	Configures the engine ID that is utilized as a unique identifier of a SNMPv3 engine.	Global Configuration
snmp view <ViewName> <OIDTree> [mask <OIDMask>] {included | excluded} [{volatile | nonvolatile}]	Configures the SNMP view.	Global Configuration
snmp targetaddr <TargetAddressName> param <ParamName> {<ucast_addr> | <IP6Address> | <dns_host_name>} [timeout <Seconds(1-1500)>] [retries <RetryCount(1-3)>] [taglist <TagIdentifier | none>] [{volatile | nonvolatile}] [port <integer (1-65535)>]no snmp targetaddr <TargetAddressName>	Configures the SNMP target address.	Global Configuration
snmp targetparams <ParamName> user <UserName> security-model {v1 | v2c | v3 {auth | noauth | priv}} message-processing {v1 | v2c | v3} [{volatile | nonvolatile}] [filterprofile-name <profilename> [filter-storagetype {volatile | nonvolatile}]]	Configures the SNMP target parameters.	Global Configuration
snmp user <UserName> [auth {md5 | sha} <passwd> [priv {{{DES | AES_CFB128} <passwd> } | None}]]	Configures the SNMP user details.	Global Configuration

cnMatrix Parameters and Commands

Commands	Description	CLI Mode
`[{volatile | nonvolatile}] [EngineId <EngineID>]`		
`snmp notify <NotifyName> tag <TagName> type {Trap | Inform} [{volatile | nonvolatile}]`	Configures the SNMP notification details.	Global Configuration
`snmp filterprofile <profile-name> <OIDTree> [mask <OIDMask>] {included | excluded} [{volatile | nonvolatile}]`	Creates Notify filter Profile entry.	Global Configuration
`snmp-server enable traps snmp authentication`	Enables the generation of authentication traps for SNMPv1 and SNMPv2c.	Global Configuration
`snmp-server trap udp-port <port>`	Configures the udp port over which agent sends the trap.	Global Configuration
`snmp agent port <port>`	Configures the agent port on which agent listens.	Global Configuration
`snmp-server enable traps coldstart`	Enables the generation of a coldstart trap. Note: A coldstart trap signifies that the SNMP entity, supporting a notification originator application, is reinitializing itself and that its configuration may have been altered.	Global Configuration
`show snmp`	Displays the status information of SNMP communications.	Privileged EXEC
`show snmp community`	Displays the configured SNMP community details.	Privileged EXEC
`show snmp group`	Displays the configured SNMP groups.	Privileged EXEC
`show snmp group access`	Displays the configured SNMP group access details.	Privileged EXEC
`show snmp engineID`	Displays the Engine Identifier.	Privileged EXEC
`show snmp viewtree`	Displays the configured SNMP Tree views.	Privileged EXEC
`show snmp targetaddr`	Displays the configured SNMP target Addresses.	Privileged EXEC
`show snmp targetparam`	Displays the configured SNMP Target Address Params.	Privileged EXEC
`show snmp user`	Displays the configured SNMP users.	Privileged EXEC

cnMatrix Parameters and Commands

Commands	Description	CLI Mode
`show snmp notif`	Displays the configured SNMP Notification types.	Privileged EXEC
`show snmp inform statistics`	Displays the inform message statistics.	Privileged EXEC
`show snmp-server traps`	Displays the set of traps that are currently enabled.	Privileged EXEC
`show snmp filter`	Displays the configured SNMP filters.	Privileged EXEC
`snmpset mib {name | oid} <name/oid> value <string> [short] [<datatype - i, o, x, s>]` Available options: • name <name> - Sets the mib object name. • oid <oid> - Sets the mib object identifier.	Sets the value of the mib (management information base) object through SNMP agent.	Global Configuration
`snmpget mib {name | oid} <value> [short]` Available options: • name <value> - Gets the mib object name. • oid <value> - Gets the mib object identifier.	Gets the value of the mib object through SNMP agent.	Global Configuration
`snmpgetnext mib {name | oid} <value> [short]` Available options: • name <value> - Gets the next mib object name. • oid <value> - Gets the next mib object identifier.	Gets the next mib object for the given object.	Global Configuration
`snmpwalk mib {name | oid} <value> [count <integer(1-100)>] [short]` Available options: • name <value> - Gets the next mib object name for the given mib object name. • oid <value> - Gets the next mib object identifier for the given mib object identifier.	Displays the mib objects of the given table.	Global Configuration
`snmp filter trap {name | oid} <name/oid>` Available options: • name <value> - Configures the mib object name. • oid <value> - Configures the mib object identifier.	Sets the traps to be filtered.	Global Configuration
`show mib oid <object name>`	Displays the OID (Object Identifier) of the corresponding mib object name.	Privileged EXEC

cnMatrix SSH Parameters and Commands

Commands	Description	CLI Mode
`ip ssh {version compatibility | cipher ([des-cbc] [3des-cbc] [aes128-cbc] [aes256-cbc]) | auth ([hmac-md5] [hmac-sha1]) }` Available options: • `version` – support for the SSH protocol version. • `cipher` - cipher-algorithm list. • `auth` – public key authentication for incoming SSH sessions. • `transport-max-allowed` – configures maximum of bytes allowed in an SSH transport connection.	Enables you to configure parameters associated with the SSH server.	Global Configuration
`ssh {enable | disable}`	Enables or disables SSH subsystem.	Global Configuration
`debug ssh ([all] [shut] [mgmt] [data] [ctrl] [dump] [resource] [buffer] [server])` Available options: • `all` – generates debug statement for all traces. • `shut` - generates debug statement for shutdown traces. • `mgmt` – generates debug statement for management place functionality traces. • `data` - generates debug statement for data path. • ctrl - generates debug statement for Control Pane functionality trace. • dump - generates debug statement for packets handling traces. • resource - generates debug statement for traces with respect to allocation expect buffers. • **buffer** - generates debug statement for buffer messages. • server - generates debug statement for server messages.	Enables the trace levels for SSH.	Privileged EXEC
`show ip ssh`	Displays the SSH server information such as version, cipher algorithm, authentication and trace level.	Privileged EXEC
`ip ssh transport-max-allowed bytes <integer(1-32768)>`	Configures the maximum number of bytes allowed in an SSH transport connection.	Global Configuration
`ip ssh pubkey-chain`	Configures the SSH clients public key, to be used for public key based authentication.	Global Configuration
`ssh server-address <ip-address> [port <integer(1-65535)>]`	Configures the SSH server listening IP address and the primary port number.	Global Configuration
`show ssh-configurations`	Displays the SSH server listening IP address and port information.	Privileged EXEC

cnMatrix Parameters and Commands

Commands	Description	CLI Mode
`ssh <ipv4_addr/ipv6_addr> [-1] [-2] [-4] [-6] [-A] [-a] [-C] [-N] [-s] [-V] [-v] [-l <username>] [-T] [-t] [<remote-command>]` Available options: • `<ipv4_addr/ipv6_addr>` - Establishes ssh client session for the specified IP address. It supports both IPv4 and IPv6 addresses. • `-1` - Forces ssh to try protocol version 1. • `-2` - Forces ssh to try protocol version 2. • `-4` - Forces ssh to use IPv4 addresses only • `-6` - Forces ssh to use IPv6 addresses only. • `-A` - Enables forwarding of the authentication agent connection. • `-a` - Disables forwarding of the authentication agent connection. • `-C` - Requests compression of all data. • `-N` - Does not execute a remote command. • `-s` - Specifies the subsystem as the remote command (SSH-2 only). • `-V` - Supports print version information and exit. • `-v` - Displays verbose messages. • `-l <username>` - Specifies the user name. • `-T` - Disables pseudo-tty allocation. • `-t` - Enables force pseudo-tty allocation. • `<remote-command>` - Specifies the remote command to be executed. If it is more than one argument use double quotes	This command establishes ssh client session with the specified IP address.	Privileged EXEC

cnMatrix IPv6 Management Parameters and Commands

Commands	Description	CLI Mode
`ipv6 enable`	Enables IPv6 processing on an interface that has not been configured with an explicit IPv6 address.	Interface Configuration
`no ipv6 unicast-routing`	Important notice: This command must be issued for IPv6 interface to function in IPv6 Host Mode. Router Advertisement (RA) packets will be processed only if this command is issued.	Global Configuration
`ipv6 address <prefix> <prefix Len> [{unicast | eui64 | link-local}]`	Configures an IPv6 address on an interface.	Interface Configuration

cnMatrix Parameters and Commands

`ipv6 address dhcp`	Enables the DHCPv6 client functionality on IPv6 interface.	Interface Configuration
`ipv6 neighbor <prefix> {vlan <vlan-id> | <interface-type> <interface-id>} <MAC ADDRESS (xx:xx:xx:xx:xx:xx)>`	Configures a static entry in the IPv6 neighbor cache table.	Global Configuration
`ipv6 nd dad attempts <no of attempts (1-10)>`	Sets the number of duplicate address detection (dad) attempts, where the maximum number of neighbor solicitations sent for the purpose of duplicate address detection on a tentative address. The value of the number of duplicate address detection attempt ranges between 1 and 10.	Interface Configuration
`ipv6 icmp error-interval <milliseconds(1-65535)> [<bucketsize(1-200)>]`	Configures the ICMPv6 (Internet Control Message Protocol) error rate limit for limiting the rate at which IPv6 ICMP error messages are sent out on the network. The maximum number of tokens allowed in the bucket can be specified, and for every error message to be sent, one token is removed from the bucket. If a series of error messages is generated, error messages can be sent until the bucket is empty. When the bucket is empty of tokens, IPv6 ICMP error messages are not sent until a new token is placed in the bucket.	Interface Configuration
`ipv6 icmp dest-unreachable { enable | disable }`	Enables or disables the ICMPv6 destination unreachable messages on the interface that has been previously configured.	Interface Configuration
`show ipv6 interface`	Displays IPv6 interface related information.	Privileged EXEC
`show ipv6 neighbors [summary]`	Displays IPv6 Neighbor Cache entries.	Privileged EXEC
`show ipv6 traffic`	Displays IPv6 ICMP and UDP statistics.	Privileged EXEC

In order for a switch to take an IPv6 address from a Router Advertisement sent by an IPv6 router the below steps are mandatory:

1. Disable IPv6 routing from global configuration mode using the following command: `no ipv6 unicast-routing`.
2. Enable IPv6 on VLAN interface mode using the following command: `ipv6 enable`.

cnMatrix Reload Parameters and Commands (Starting with version 2.1)

Commands	Description	CLI Mode
`show reload`	Displays the reload scheduled time and the reload reason.	Privileged EXEC
`reload cancel`	Terminates any scheduled reboot.	Privileged EXEC

cnMatrix Parameters and Commands

Commands	Description	CLI Mode
`reload [{default | partial-default}] [--yes] [reason <string>]`	Reboots the switch to the default or partial-default configurations.	Privileged EXEC
`reload in`	Specifies the remaining time until reboot.	Privileged EXEC
`reload at`	Specifies a fixed time / date to reboot.	Privileged EXEC
`reload {[--yes]}`	Soft reboots the switch	Privileged EXEC

cnMatrix USB Parameters and Commands (Starting with version 2.1)

Commands	Description	CLI Mode
`mount usb`	Performs USB mount.	Global Configuration
`unmount usb`	Performs USB unmount.	Global Configuration
`show usb files`	Displays the files that are currently available on the USB stick.	Privileged EXEC
`show usb tree`	Displays the files that are on the device in a tree structure.	Privileged EXEC
`show usb info`	Displays USB device and vendor information.	Privileged EXEC
`download agent usb:<agent_name>` Available options: • `<agent_name>`- The image name present on the USB device	Downloads the new agent. Note: While downloading the new agent, the CLI interface will be blocked.	Privileged EXEC
`copy startup-config usb:<config_file>` Available options: • `<config_file>` - Name of the file to which the startup config file will be copied	Enables you to copy a startup config file to the flash device.	Privileged EXEC
`copy usb:<config_file> startup-config` • `<config_file> - File on the USB device to be copied into configuration file`	Applies a startup config file from a flash device.	Privileged EXEC
`write usb:<filename>`	Specifies the destination path on the USB device to copy running config.	Privileged EXEC

Security Features

cnMatrix RADIUS Parameters and Commands

Commands	Description	CLI Mode
radius-server host {ipv4-address | ipv6-address | <dns_host_name>} [auth-port <integer(1-65535)>] [acct-port <integer(1-65535)>] [timeout <1-120>] [retransmit <1-254>] [key <secret-key-string>] [primary] Available options: • ipv4-address - Configures the IPv4 address of the RADIUS server host. • ipv6-address - Configures the IPv6 address of the RADIUS server host. • auth-port <integer(1-65535)> - Configures a specific UDP (**User Datagram Protocol**) destination port on this RADIUS server to be used solely for the authentication requests. • acct-port <integer(1-65535)> - Configures a specific UDP destination port on this RADIUS to be solely used for accounting requests. • retransmit <1-254> - Configures the maximum number of attempts to be tried by a client to get response from the server for a request. • timeout <1-120> - Configures the time period in seconds for which a client waits for a response from the server before retransmitting the request. • key <secret-key-string> - Configures the per-server encryption key which specifies the authentication and encryption key for all RADIUS communications between the authenticator and the RADIUS server. • primary - Sets the RADIUS server as the primary server.	Configures the RADIUS client with the parameters (host, timeout, key, retransmit).	Global Configuration
debug radius {all | errors | events | packets | responses | timers} Available options: • all - Generates traces for all the RADIUS server messages.	Enables the RADIUS debugging options.	Privileged EXEC

cnMatrix Parameters and Commands

Commands	Description	CLI Mode
- `errors` - Generates traces for error code messages. - `events` - Generates traces for events related messages. - `packets` – Generates packets related messages. - `responses` - Generates traces for responses sent from the server to authenticator. - `timers` - Generates traces for the different timers used in the session before the system is reboot.		
`show radius server [{<ucast_addr> | <ip6_addr> | <dns_host_name>}]`	Displays the RADIUS server Host information, which contains: Index, Server address, Shared secret, Radius Server status, Response Time, Maximum Retransmission, Authentication Port and Accounting Port.	Privileged EXEC
`show radius statistics`	Displays RADIUS Server Statistics for the data transfer between server and the client from the time of initiation.	Privileged EXEC

cnMatrix TACACS Parameters and Commands

Commands	Description	CLI Mode
`tacacs-server host {<ipv4-address> | <ipv6-address> | <dns_host_name>} } [single-connection] [port <tcp port (1-65535 )>] [timeout <time out in seconds(1-255)>] {key <secret key>}` Available options: - `<ipv4-address>` - Configures the IPv4 address of the host. - `<ipv6-address>` - Configures the IPv6 address of the host. - `single-connection` - Single TCP connection is established to communicate with TACACS Server. - `port<tcp port (1-65535 )>` - Configures the TCP port number in which the multiple sessions are established. - `timeout<time out in seconds(1-255)>` - Configures the timeout related information.	Configures the TACACS server with the parameters (host, timeout, key) and specifies the address of one or more TACACS and the names of the IP host or hosts maintaining a TACACS+ server.	Global Configuration

cnMatrix Parameters and Commands

Commands	Description	CLI Mode
• key<secret key> - Specifies the authentication and encryption key for all TACACS communications between the authenticator and the TACACS server.		
tacacs use-server address { <ipv4-address> | <ipv6-address> }	Configures the active server address and selects an active server from the list of servers available in the TACACS server table.	Global Configuration
tacacs-server retransmit < retries (1-5) >	Configures the retransmit value. It is the number of times the client searches the active server from the list of servers maintained in the TACACS client, when active server is not configured.	Global Configuration
debug tacacs { all | info | errors | dumptx | dumprx } Available options: • all - Generates debug messages for all possible traces (Dumptx, Dumprx, Error, Info). • info - Generates debug statements for server information messages such as TACACS session timed out, server unreachability, Session ID exceeded and so on. • errors - Generates debug statements for error debug messages such as failure caused during packet transmission and reception. • dumptx - Generates debug statements for handling traces. • dumprx - Generates debug statements for handling traces.	Sets the debug trace level for TACACS client module.	Privileged EXEC
show tacacs server	Displays server related information.	Privileged EXEC
show tacacs statistics	Displays TACACS statistics.	Privileged EXEC

cnMatrix IGMP Snooping Parameters and Commands

Commands	Description	CLI Mode
ip igmp snooping [vlan <vlanid >]	Enables IGMP snooping in the switch for a specific VLAN.	Global Configuration
ip igmp snooping report-suppression-interval <(1 - 25) seconds>	Sets the IGMP snooping report-suppression time interval.	Global Configuration
ip igmp snooping retry-count <1 - 5>	Sets the maximum number of group specific queries sent by the switch to check if there are any interested v2	Global Configuration

Commands	Description	CLI Mode
	receivers for the group when it receives a leave message.	
`ip igmp snooping group-query-interval <(2-5) seconds>`	Sets the time interval after which the switch sends a group specific query to find out if there are any interested receivers in the group when it receives a leave message.	Global Configuration
`ip igmp snooping version { v1 |v2 }` Available options: • `v1` - Configures the version as IGMP snooping Version 1. • `v2` - Configures the version IGMP snooping Version 2.	Configures the operating version of the IGMP snooping switch for a specific VLAN.	Config-VLAN
`ip igmp snooping querier [{address | <ucast_addr>}]`	Configures the IGMP snooping switch as a querier for a specific VLAN.	Config-VLAN
`ip igmp snooping query-interval <(60 - 600) seconds>`	Sets the time period with which the general queries are sent by the IGMP snooping switch when configured as querier on a VLAN.	Config-VLAN
`ip igmp snooping startup-query-interval <(15 - 150) seconds>`	Sets the time interval between the general query messages sent by the IGMP snooping switch, during startup of the querier election process.	Config-VLAN
`ip igmp snooping startup-query-count <2 - 5>`	Sets the maximum number of general query messages sent out on switch startup, when the switch is configured as a querier.	Config-VLAN
`ip igmp snooping other-querier-present-interval <value (120-1215) seconds>`	Sets the maximum time interval to decide that another querier is present in the network.	Config-VLAN
`ip igmp snooping mrouter <interface-type>`	Enables IGMP snooping and configures a list of multicast router ports for a specific VLAN, when IGMP snooping is globally enabled.	Config-VLAN
`snooping report-process config-level {non-router-ports | all-ports}` Available options: • `non-router-ports` - The incoming report messages are processed only in the non-router ports. • `all-ports` - The incoming report messages are processed in all the ports inclusive of router ports.	Sets the configuration-level for report processing as non-router ports or as all ports.	Global Configuration
`ip igmp snooping filter`	Enables the IGMP snooping filter.	Global Configuration
`ip igmp snooping proxy`	Enables proxy in the IGMP snooping switch.	Global Configuration

cnMatrix Parameters and Commands

Commands	Description	CLI Mode
`show ip igmp snooping mrouter [Vlan <vlan-id>] [detail]` Available options: - `vlan <vlan-id >` - Displays the router ports for the specified VLAN. - `detail` - Displays detailed information about the router ports.	Displays the router ports for all VLANs or a specific VLAN.	Privileged EXEC
`show ip igmp snooping globals`	Displays the IGMP snooping information for all VLANs or a specific VLAN.	Privileged EXEC
`show ip igmp snooping [Vlan <vlan-id>]`	Displays the IGMP snooping information for all VLANs or a specific VLAN.	Privileged EXEC
`show ip igmp snooping groups [Vlan <vlan-id> [Group <Address>]][{static | dynamic}]`	Displays the IGMP group information for all VLANs or a specific VLAN or specific VLAN and group address.	Privileged EXEC
`show ip igmp snooping statistics [Vlan <vlan-id >]`	Displays IGMP snooping statistics for all VLANs or a specific VLAN.	Privileged EXEC
`show ip igmp snooping blocked-router [Vlan <vlan-id>]`	Displays the blocked router ports for all VLANs or a specific VLAN.	Privileged EXEC
Starting with version 2.1:`show ip igmp snooping forwarding-database total`	Displays the total number of forwarding entries.	Privileged EXEC
Starting with version 2.1: `show ip igmp snooping groups total`	Displays the total number of groups.	Privileged EXEC
`debug ip igmp snooping trace ([data-path][ctrl-path][Rx][Tx][all])` Available options: - `data-path` - Generates debug statements for data path event traces.	Configures the debug and trace statements in the igmp snooping module.	Privileged EXEC

Commands	Description	CLI Mode
- ctrl-path - Generates debug statements for control path event traces. - Rx - Generates debug statements for RX Packet Dump traces. - Tx - Generates debug statements for TX Packet Dump traces. - all - Generates all types of trace messages.		
debug ip igmp snooping ([init][resources][tmr][src][grp][qry][redundancy] [pkt][fwd][vlan][entry][exit][mgmt][np][buffer][icch][all]) Available options: - init - Generates Init and Shutdown trace messages at the instances when the module is initiated or shutdown. The information is logged in a file. - resources - Generates System Resources management trace messages when there is a change in the resource status. The information is logged in a file. - tmr - Generates Timer trace messages at the instances where timers are involved. The information is logged ina file. - src - Generates trace messages when Source Information is involved. - grp - Generates trace messages when Group Information is involved. - qry - Generates trace messages when Query messages are sent or received. - pkt - Generates debug statements for packets handling traces. This trace is generated when there is an error condition in transmission or reception of packets. - fwd - Generates traces messages when forwarding Database is involved. - vlan - Generates trace messages when VLAN related Information is involved. - entry - Generates trace message to specify function entry points. - exit - Generates trace message to specify function exit points. - mgmt - Generates debug statements for management plane functionality traces. - np - Generates debug statements for Np calls traces.	Configures the various debug and trace statements to handle error and event management available in the igmp snooping module.	Privileged EXEC

Commands	Description	CLI Mode
• `all` - Generates all types of trace messages.		
`ip igmp snooping mrouter-port <iface_list> version {v1 | v2}`	Configures the operating version of the router port for a VLAN.	Config-VLAN
`ip igmp snooping mrouter-port <iface_list> time-out <short(60-600)>`	Configures the router port purge time-out interval.	
`ip igmp snooping max-response-code <(0 - 255)>`	Sets the max response code inserted in the general queries sent to host.	Config-VLAN
`ip igmp snooping blocked-router <interface-type> <0/a-b, 0/c, ...>`	Deletes the statically configured blocked router ports for a VLAN.	Config-VLAN
`ip igmp snooping send-query { enable | disable }`	Enables/Disables the feature of IGMP general query transmission upon topology change in the switch.	Global Configuration
`ip igmp sn robustness-variable (2-7)` (Starting with version 2.1)	Configures the robustness value for the specified VLAN.	Config-VLAN
`ip igmp snooping blocked-router`	Configures the blocked router port for a VLAN.	Config-VLAN
`ip igmp snooping sparse-mode`	Enables/Disables the snooping system sparse mode.	Config-VLAN
`ip igmp snooping leavemode {exp-hosttrack | fastLeave | normalleave}` Available options: • `exp-hosttrack` - Processes the leave messages using the explicit host tracking mechanism. • `fastLeave` - Processes the leave messages using the fast leave mechanism. • `Normalleave` - Sends a group or group specific query on the interface for every received leave message.	Configure the Port Leave mode for an interface.	Interface Configuration (Port)
`ip igmp profile <profile-id>`	Profile identifier for the multicast profile entry.	Global Configuration
`ip igmp filter < profile number >`	Profile identifier for multicast profile entry.	Interface Configuration (Port)
`ip igmp max-groups <integer32>`	Maximum number of multicast groups that can be learnt on the interface.	Interface Configuration (Port)
`ip igmp snooping ratelimit <(100 - 1000)>`	Configures the rate limit globally.	Global Configuration

cnMatrix Parameters and Commands

Commands	Description	CLI Mode
`ip igmp snooping clear counters [vlan_id]`	Clears the IGMP snooping statistics maintained for Vlan(s).	Privileged EXEC
`show ip igmp profile`	Displays the filters configured in the profile and the profile statistics.	Privileged EXEC
`show ip igmp snooping port-cfg [{interface <interface-type> <interface-id>`	Displays IGS Port configuration information for all VLANs or a specific VlanId.	Privileged EXEC
`show ip igmp snooping forwarding-database [Vlan <vlan-id/vfi-id>] [{static | dynamic}]` Available options: • `Dynamic` - Displays only dynamic multicast entries. • `Static` - Displays only static multicast entries. • `Vlan` - Protocol specific information for vlan.	Displays multicast forwarding entries for all VLANs or a specific VLAN.	Privileged EXEC
`copy running-config startup-config`	The running-configuration is copied to startup-configuration.	Privileged EXEC

cnMatrix DHCP Snooping Parameters and Commands

Commands	Description	CLI Mode
`ip dhcp snooping [ vlan < vlan-id (1-4094)>]`	Enables the layer 2 DHCP snooping in the switch or enables the snooping in the specific VLAN.	Global Configuration
`ip dhcp snooping verify mac-address`	Enables the DHCP MAC verification in the switch.	Global Configuration
`ip dhcp snooping`	Enables layer 2 DHCP snooping in the VLAN.	Config-VLAN
`show ip dhcp snooping globals`	Displays the global configuration of DHCP snooping.	Privileged EXEC
`show ip dhcp snooping [vlan <vlan-id (1-4094)>]` Available options: • vlan <vlan-id (1-4094)> - displays the DHCP snooping configuration and statistics for the specified VLAN ID..	Displays the DHCP snooping configuration and statistics of all VLANs in which the DHCP snooping feature is enabled.	Privileged EXEC
`debug ip dhcp snooping {[entry][exit][debug][fail] | all}` Available options: • entry - generates debug statements for function entry traces.	Enables the tracing of the DHCP snooping module as per the configured debug level.	Privileged EXEC

cnMatrix Parameters and Commands

• exit - generates debug statements for function exit traces. • debug - generates debug statements for debug traces. • fail - generates debug statements for all failure traces. • all - generates debug statements for all types of traces.		

cnMatrix ACL Feature Parameters and Commands

Commands	Description	CLI Mode
ip access-list {standard <access-list-number (1-1000)> | extended <access-list-number (1001-65535)> } Available options: • standard <access-list-number (1-1000)> - Configures a Standard access-list with the specified access list number. Standard access lists create filters based on IP address and network mask only (L3 filters only). This value ranges from 1 to 1000. • extended <access-list-number (1001-65535)> - Configures an Extended access-list with the specified access list number. Extended access lists enables specification of filters based on the type of protocol, range of TCP/UDP ports as well as the IP address and network mask (Layer 4 filters). This value ranges from 1001 to 65535.	Configures IP ACLs and enters into the standard or extended IP access-list configuration mode. Depending on the standard or extended option chosen by the user, this command returns a corresponding IP Access list configuration mode. ACLs on the system perform both access control and Layer 3 field classification.	Global Configuration
egress access-list mode {ip | mac} Available options: • ip - Configures the Egress access-list mode as IP which supports IP based PCL(Policy Control List) at egress. • mac - Configures the Egress access-list mode as MAC which supports MAC based PCL(Policy Control List) at egress . Existing access list configurations should be deleted before setting Egress Filter Mode as IP	Configures the default egress access-list mode as IP based or MAC based.	Global Configuration
permit {any | host <src-ip-address> | <network-src-ip> <mask>} [{ any | host <dest-ip-address> | <network-dest-ip> <mask>}] [redirect {interface <iftype> <ifnum>][priority <value (1-255)>] Available options: • any|host <src-ip-address>|<network-src-ip><mask> - Specifies the	Configures the packets to be forwarded depending on the associated parameters.	Standard IP ACL Configuration

source IP address. The source IP address can be : - any – Packets from any source are matched. - host <src-ip-address> - Packets from this IPv4 source address are matched. - <network-src-ip> <mask> - Packets are matched using this source IPv4 network and mask. • any|host <dest-ip-address>|<network-dest-ip><mask> - Specifies the destination IP address. The destination IP can be: - any - Packets to any destination are matched. - host <src-ip-address> - Packets for this IPv4 destination address are matched. • <network-src-ip> <mask> - Packets are matched using this destination IPv4 network and mask.redirect - Redirects the packets to the destination interface or set of interfaces. - <iftype>- Redirects the packets to the specified type of interface. - <ifnum>- Redirects the packets to the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface types gigabitethernet, fastethernet and extreme-ethernet. • priority <value(1-255)> - Configures the priority of the filter to decide which filter rule is applicable when the packet matches with more than one filter rules. Lower value of ‘filter priority’ implies a higher priority. This value ranges from 1 to 255.		
deny{ any | host <src-ip-address> | <network-src-ip> <mask> } [{ any | host <dest-ip-address> | <network-dest-ip> <mask> }] priority <value (1-255)> Available options:	Denies traffic if the conditions defined in the deny statement are matched.	Standard IP ACL Configuration

<table>
<tr><td></td><td></td><td></td></tr>
<tr><td>• any|host <src-ip-address>|<network-src-ip><mask> - Specifies the source IP address. The source IP can be:
- any – Packets from any source are matched.
- host <src-ip-address> - Packets from this IPv4 source address are matched.
- <network-src-ip> <mask> - Packets are matched using this source IPv4 network and mask.
• any|host <dest-ip-address>|<network-dest-ip><mask> - Specifies the source IP address. The source IP address can be :
- any - Packets to any destination are matched.
- host <src-ip-address> - Packets for this IPv4 destination address are matched.
- <network-src-ip> <mask> - Packets are matched using this destination IPv4 network and mask.
• priority <value(1-255)> - Configures the priority of the filter to decide which filter rule is applicable when the packet matches with more than one filter rules. Lower value implies a higher priority. This value ranges from 1 to 255.</td><td></td><td></td></tr>
<tr><td>permit { ip | ospf | pim | <protocol-type (1-255)>} { any | host <src-ip-address> | <src-ip-address> <mask>} { any | host <dest-ip-address> | <dest-ip-address> <mask> } [{tos{max-reliability | max-throughput | min-delay | normal |<value (0-7)>} | dscp <value (0-63)>}] [redirect {interface <iftype> <ifnum>] [priority <value (1-255)>]
Available options:
• ip| ospf |pim |<protocol-type (1-255)> - Specifies the type of protocol for the packet. It can also be a protocol number.</td><td>Configures traffic for a particular protocol packet if the conditions defined in the permit statement are matched.</td><td>Extended IP ACL Configuration</td></tr>
</table>

<table>
<tr><td>Protocol type with the value 255 indicates that protocol can be anything and it will not be checked against the action to be performed.
• any|host <src-ip-address>|<network-src-ip><mask> - Specifies the source IP address. The source IP address can be :
- any – Packets from any source are matched.
- host <src-ip-address> - Packets from this IPv4 source address are matched.
- <network-src-ip> <mask> - Packets are matched using this source IPv4 network and mask.
- mask to use with the source IP address
• any|host <dest-ip-address>|<network-dest-ip><mask> - Specifies the destination IP address. The destination IP can be:
- any - Packets to any destination are matched
- host <src-ip-address> - Packets for this IPv4 destination address are matched
- <network-src-ip> <mask> - Packets are matched using this destination IPv4 network and mask.
• tos - Matches the protocol packets based on the following type of service configuration: The options are:
- max-reliability- Matches the protocol packets having TOS field set as high reliability.
- max-throughput - Matches the protocol packets having TOS field set as high throughput.
- min-delay- Matches the protocol packets having TOS field set as low delay.
- normal - Allows all protocol packets. Does not check for the TOS field in the packets.
- <value (0-7)>- Matches the protocol packets based on the TOS value set. This value ranges from 0 to 7.</td><td></td><td></td></tr>
</table>

cnMatrix Parameters and Commands

• dscp <value (0-63)> - Configures the Differentiated Services Code Point value to be checked against the packet, This value provides the quality of service control. This value ranges from 0 to 63. • redirect - Redirects the packets to the destination interface or set of interfaces. - <iftype>- Redirects the packets to the specified type of interface. - <ifnum>- Redirects the packets to the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface types gigabitethernet, fastethernet and extreme-ethernet. • priority <value(1-255)> - Configures the priority of the filter to decide which filter rule is applicable when the packet matches with more than one filter rules. Lower value implies a higher priority. This value ranges from 1 to 255.		
deny {ip | ospf | pim | <protocol-type (1-255)>} { any | host <src-ip-address> | <src-ip-address> <mask>} { any | host <dest-ip-address> | <dest-ip-address> <mask>} [tos{max-reliability | max-throughput | min-delay | normal |<value (0-7)>} | dscp <value (0-63)>}] [priority <value (1-255)>] Available options: • ip| ospf |pim |<protocol-type (1-255)> - Specifies the type of protocol for the packet. It can also be a protocol number. Protocol type with the value 255 indicates that protocol can be anything and it will not be checked against the action to be performed. • any|host <src-ip-address>|<network-src-ip><mask> - Specifies the source IP address. The source IP can be:	Denies traffic for a particular protocol packet if the conditions defined in the deny statement are matched.	Extended IP ACL Configuration

- any – Packets from any source are matched. - host <src-ip-address> - Packets from this IPv4 source address are matched. - <network-src-ip> <mask> - Packets are matched using this source IPv4 network and mask. • any|host <dest-ip-address>|<network-dest-ip><mask> - Specifies the source IP address. The source IP address can be : - any - Packets to any destination are matched - host <src-ip-address> - Packets for this IPv4 destination address are matched - <network-src-ip> <mask> - Packets are matched using this destination IPv4 network and mask. • tos - Matches the protocol packets based on the following type of service configuration: The options are: - max-reliability- Matches the protocol packets having TOS field set as high reliability. - max-throughput - Matches the protocol packets having TOS field set as high throughput. - min-delay- Matches the protocol packets having TOS field set as low delay. - normal - Allows all protocol packets. Does not check for the TOS field in the packets. - <value (0-7)>- Matches the protocol packets based on the TOS value set. This value ranges from 0 to 7. • dscp <value (0-63)> - Configures the Differentiated Services Code Point value to be checked against the packet, This value provides the quality of service control. This value ranges from 0 to 63. • priority <value(1-255)> - Configures the priority of the filter to decide which filter rule is applicable when the packet matches with more than one filter rules. Lower value		

<table>
<tr><td>implies a higher priority. This value ranges from 1 to 255.</td><td></td><td></td></tr>
<tr><td>permit tcp {any | host <src-ip-address> | <src-ip-address> <src-mask> }[{gt <port-number (1-65535)> | lt <port-number (1-65535)>|eq <port-number (1-65535)> |range <port-number (1-65535)> <port-number (1-65535)>}][{ any | host <dest-ip-address> | <dest-ip-address> <dest-mask> }[{gt <port-number (1-65535)> | lt <port-number (1-65535)> | eq <port-number (1-65535)> |range <port-number (1-65535)> <port-number (1-65535)>}][{ ack | rst }][{tos{max-reliability|max-throughput|min-delay|normal|<tos-value(0-7)>}|dscp <value (0-63)>}] [redirect {interface <ifXtype> <ifnum>] [priority <value(1-255)>]

Available options:
• any|host <src-ip-address>|<network-src-ip><mask> - Specifies the source IP address. The source IP can be:
- any – Packets from any source are matched.
- host <src-ip-address> - Packets from this IPv4 source address are matched.
- <network-src-ip> <mask> - Packets are matched using this source IPv4 network and mask.
• gt <port-number (1-65535)> - Matches the TCP packets having the TCP source port numbers greater than the specified port number. This value ranges from 1 to 65535.
• lt <port-number (1-65535)> - Matches the TCP packets having the TCP source port numbers less than the specified port number. This value ranges from 1 to 65535.
• eq <port-number (1-65535)> - Matches the TCP packets having the TCP source port numbers equal to specified port number. This value ranges from 1 to 65535.
• range <port-number (1-65535)> <port-number (1-65535)>- Matches the TCP packets having the TCP source port numbers within the specified range. This value ranges from 1 to 65535. This value specifies the minimum port number and the maximum port number values.</td><td>Configures the TCP packets to be forwarded based on the associated parameters.</td><td>Extended IP ACL Configuration</td></tr>
</table>

• any|host <dest-ip-address>|<network-dest-ip><mask> - Specifies the source IP address. The source IP address can be : - any - Packets to any destination are matched. - host <src-ip-address> - Packets for this IPv4 destination address are matched. - <network-src-ip> <mask> - Packets are matched using this destination IPv4 network and mask. • gt <port-number (1-65535)> - Matches the TCP packets having the TCP destination port numbers greater than the specified port number. This value ranges from 1 to 65535. • lt <port-number (1-65535)> - Matches the TCP packets having the TCP destination port numbers less than the specified port number. This value ranges from 1 to 65535. • eq <port-number (1-65535)> - Matches the TCP packets having the TCP destination port numbers equal to specified port number. This value ranges from 1 to 65535. • range <port-number (1-65535)> <port-number (1-65535)>- Matches the TCP packets having the TCP destination port numbers within the specified range. This value ranges from 1 to 65535. This value specifies the minimum port number and the maximum port number values. • ack – Matches TCP packets with the TCP ACK bit set. • rst – Matches TCP packets with the TCP RST bit set. • eq <port-number (1-65535)> - Matches the TCP control packets having the TCP source port numbers equal to specified port number. This value ranges from 1 to 65535. • tos - Matches the TCP packets based on the following type of service configuration: The options are: - max-reliability- Matches the TCP packets having TOS field set as high reliability. - max-throughput - Matches the TCP packets having TOS field set as high throughput.		

- min-delay- Matches the protocol TCP having TOS field set as low delay. - normal - Allows all TCP packets. Does not check for the TOS field in the packets. - <value (0-7)>- Matches the TCP packets based on the TOS value set. This value ranges from 0 to 7. • dscp <value (0-63)> - Configures the Differentiated Services Code Point value to be checked against the packet, This value provides the quality of service control. This value ranges from 0 to 63. • redirect - Redirects the packets to the destination interface or set of interfaces. - <iftype>- Redirects the packets to the specified type of interface. - <ifnum>- Redirects the packets to the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface types gigabitethernet, fastethernet and extreme-ethernet. - <iface_list>- Redirects the packets to the the list of interfaces • priority <value(1-255)> - Configures the priority of the filter to decide which filter rule is applicable when the packet matches with more than one filter rules. Lower value of ‘filter priority’ implies a higher priority. This value ranges from 1 to 255.		
deny tcp {any | host <src-ip-address> | <src-ip-address> <src-mask> }[{gt <port-number (1-65535)> | lt <port-number (1-65535)> |eq <port-number (1-65535)> | range <port-number (1-65535)> <port-number (1-65535)>}][{ any | host <dest-ip-address> | <dest-ip-address> <dest-mask> }[{gt <port-number (1-65535)> | lt <port-number (1-65535)> | eq <port-number (1-65535)> |range <port-number (1-65535)> <port-number (1-65535)>}][{ ack | rst }][{tos{max-reliability|max-throughput|min-delay|normal|<tos-	Configures the TCP packets to be rejected based on the associated parameters.	Extended IP ACL Configuration

value(0-7)>} | dscp <value (0-63)>}][priority <value(1-255)>] Available options: • any|host <src-ip-address>|<network-src-ip><mask> - Specifies the source IP address. The source IP can be: - any – Packets from any source are matched. - host <src-ip-address> - Packets from this IPv4 source address are matched. - <network-src-ip> <mask> - Packets are matched using this source IPv4 network and mask. • gt <port-number (1-65535)> - Matches the TCP packets having the TCP source port numbers greater than the specified port number. This value ranges from 1 to 65535. • lt <port-number (1-65535)> - Matches the TCP packets having the TCP source port numbers less than the specified port number. This value ranges from 1 to 65535. • eq <port-number (1-65535)> - Matches the TCP packets having the TCP source port numbers equal to specified port number. This value ranges from 1 to 65535. • range <port-number (1-65535)> <port-number (1-65535)>- Matches the TCP packets having the TCP source port numbers within the specified range. This value ranges from 1 to 65535. This value specifies the minimum port number and the maximum port number values. • any|host <dest-ip-address>|<network-dest-ip><mask> - Specifies the source IP address. The source IP address can be : - any - Packets to any destination are matched - host <src-ip-address> - Packets for this IPv4 destination address are matched - <network-src-ip> <mask> - Packets are matched using this destination IPv4 network and mask. • gt <port-number (1-65535)> - Matches the TCP packets having the TCP destination port numbers greater		

than the specified port number. This value ranges from 1 to 65535. • `lt <port-number (1-65535)> -` Matches the TCP packets having the TCP destination port numbers less than the specified port number. This value ranges from 1 to 65535. • `eq <port-number (1-65535)> -` Matches the TCP packets having the TCP destination port numbers equal to specified port number. This value ranges from 1 to 65535. • `range <port-number (1-65535)> <port-number (1-65535)>-` Matches the TCP packets having the TCP destination port numbers within the specified range. This value ranges from 1 to 65535. This value specifies the minimum port number and the maximum port number values. • `ack –` Matches TCP packets with the TCP ACK bit set. • `rst –` Matches TCP packets with the TCP RST bit set. • `tos` - Matches the TCP packets based on the following type of service configuration: The options are: - `max-reliability`- Matches the TCP packets having TOS field set as high reliability. - `max-throughput` - Matches the TCP packets having TOS field set as high throughput. - `min-delay`- Matches the protocol TCP having TOS field set as low delay. - `normal` - Allows all TCP packets. Does not check for the TOS field in the packets. - `<value (0-7)>`- Matches the TCP packets based on the TOS value set. This value ranges from 0 to 7. • `dscp <value (0-63)>` - Configures the Differentiated Services Code Point value to be checked against the packet, This value provides the quality of service control. This value ranges from 0 to 63. • `priority <value(1-255)>` - Configures the priority of the filter to decide which filter rule is applicable when the packet matches with more than one filter rules. Lower value of 'filter priority' implies a higher priority. This value ranges from 1 to 255		

permit udp { any | host <src-ip-address> |<src-ip-address> <src-mask>}[{gt <port-number (1-65535)> | lt <port-number (1-65535)>| eq <port-number (1-65535)> | range <port-number (1-65535)> <port-number (1-65535)>}]{ any | host <dest-ip-address> | <dest-ip-address> <dest-mask> }[{ gt <port-number (1-65535)> | lt <port-number (1-65535)>| eq <port-number (1-65535)>| range <port-number (1-65535)> <port-number (1-65535)>}][{tos{max-reliability|max-throughput|min-delay|normal|<tos-value(0-7)>} | dscp <value (0-63)>}][redirect {interface <iftype> <ifnum>][sub-action {none | modify-vlan<short (1-4094)> }] [priority <value(1-255)>] Available options: • any|host <src-ip-address>|<network-src-ip><mask> - Specifies the source IP address. The source IP can be: - any – Packets from any source are matched. - host <src-ip-address> - Packets from this IPv4 source address are matched. - <network-src-ip> <mask> - Packets are matched using this source IPv4 network and mask. • gt <port-number (1-65535)> - Matches the UDP packets having the UDP source port numbers greater than the specified port number. This value ranges from 1 to 65535. • lt <port-number (1-65535)> - Matches the UDP packets having the UDP source port numbers less than the specified port number. This value ranges from 1 to 65535. • eq <port-number (1-65535)> - Matches the UDP packets having the UDP source port numbers equal to specified port number. This value ranges from 1 to 65535. • range <port-number (1-65535)> <port-number (1-65535)>- Matches the UDP packets having the UDP source port numbers within the specified range. This value ranges from 1 to 65535. This value specifies the minimum port number and the maximum port number values. • any|host <dest-ip-address>|<network-	Specifies the UDP (User Datagram Protocol) packets to be forwarded based on the associated parameters.	Extende ACL Configu

dest-ip><mask> - Specifies the source IP address. The source IP address can be : - any - Packets to any destination are matched - host <src-ip-address> - Packets for this IPv4 destination address are matched - <network-src-ip> <mask> - Packets are matched using this destination IPv4 network and mask. • gt <port-number (1-65535)> - Matches the UDP packets having the UDP destination port numbers greater than the specified port number. This value ranges from 1 to 65535. • lt <port-number (1-65535)> - Matches the UDP packets having the UDP destination port numbers less than the specified port number. This value ranges from 1 to 65535. • eq <port-number (1-65535)> - Matches the UDP packets having the UDP destination port numbers equal to specified port number. This value ranges from 1 to 65535. • range <port-number (1-65535)> <port-number (1-65535)>- Matches the UDP packets having the UDP destination port numbers within the specified range. This value ranges from 1 to 65535. This value specifies the minimum port number and the maximum port number values. • tos - Matches the UDP packets based on the following type of service configuration: The options are: - max-reliability- Matches the UDP packets having TOS field set as high reliability. - max-throughput - Matches the UDP packets having TOS field set as high throughput. - min-delay- Matches the UDP packets having TOS field set as low delay. - normal - Allows all UDP packets. Does not check for the TOS field in the packets. - <value (0-7)>- Matches the UDP packets based on the TOS value set. This value ranges from 0 to 7. • dscp <value (0-63)> - Configures the Differentiated Services Code Point		

value to be checked against the packet, This value provides the quality of service control. This value ranges from 0 to 63. • redirect - Redirects the packets to the destination interface or set of interfaces. - <iftype>- Redirects the packets to the specified type of interface. - <ifnum>- Redirects the packets to the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface types gigabitethernet, fastethernet and extreme-ethernet. • sub-action - Configures the VLAN specific sub action to be performed on the packet. Options are: - none – Specifies that the actions related to the VLAN ID will not be considered. - modify-vlan <short (1-4094)> – Modifies the VLAN ID to which the packet gets classified. The packet could be an untagged or VLAN tagged packet. This value ranges from 1 to 4094. • priority <value(1-255)> - Configures the priority of the filter to decide which filter rule is applicable when the packet matches with more than one filter rules. Lower value of 'filter priority' implies a higher priority. This value ranges from 1 to 255.			
deny udp { any | host <src-ip-address> | <src-ip-address> <src-mask>}[{gt <port-number (1-65535)> | lt <port-number (1-65535)>| eq <port-number (1-65535)> | range <port-number (1-65535)> <port-number (1-65535)>}]{ any | host <dest-ip-address> | <dest-ip-address> <dest-mask> }[{ gt <port-number (1-65535)> | lt <port-number (1-65535)>| eq <port-number (1-65535)>| range <port-number (1-65535)> <port-number (1-65535)>}][{tos{max-reliability|max-throughput|min-	Configures the UDP packets to be rejected based on the associated parameters.	Extended IP ACL Configuration	

delay|normal|<tos-value(0-7)>} | dscp <value (0-63)>}] [priority <value(1-255)>] Available options: • any|host <src-ip-address>|<network-src-ip><mask> - Specifies the source IP address. The source IP can be: - any – Packets from any source are matched. - host <src-ip-address> - Packets from this IPv4 source address are matched. - <network-src-ip> <mask> - Packets are matched using this source IPv4 network and mask. • gt <port-number (1-65535)> - Matches the UDP packets having the UDP source port numbers greater than the specified port number. This value ranges from 1 to 65535. • lt <port-number (1-65535)> - Matches the UDP packets having the UDP source port numbers less than the specified port number. This value ranges from 1 to 65535. • eq <port-number (1-65535)> - Matches the UDP packets having the UDP source port numbers equal to specified port number. This value ranges from 1 to 65535. • range <port-number (1-65535)> <port-number (1-65535)>- Matches the UDP packets having the UDP source port numbers within the specified range. This value ranges from 1 to 65535. This value specifies the minimum port number and the maximum port number values. • any|host <dest-ip-address>|<network-dest-ip><mask> - Specifies the source IP address. The source IP address can be : - any - Packets to any destination are matched - host <src-ip-address> - Packets for this IPv4 destination address are matched - <network-src-ip> <mask> - Packets are matched using this destination IPv4 network and mask. • gt <port-number (1-65535)> - Matches the UDP packets having the		

UDP destination port numbers greater than the specified port number. This value ranges from 1 to 65535. • `lt <port-number (1-65535)>` - Matches the UDP packets having the UDP destination port numbers less than the specified port number. This value ranges from 1 to 65535. • `eq <port-number (1-65535)>` - Matches the UDP packets having the UDP destination port numbers equal to specified port number. This value ranges from 1 to 65535. • `range <port-number (1-65535)> <port-number (1-65535)>`- Matches the UDP packets having the UDP destination port numbers within the specified range. This value ranges from 1 to 65535. This value specifies the minimum port number and the maximum port number values. • `tos` - Matches the UDP packets based on the following type of service configuration: The options are: - `max-reliability`- Matches the UDP packets having TOS field set as high reliability. - `max-throughput` - Matches the UDP packets having TOS field set as high throughput. - `min-delay`- Matches the UDP packets having TOS field set as low delay. - `normal` - Allows all UDP packets. Does not check for the TOS field in the packets. - `<value (0-7)>`- Matches the UDP packets based on the TOS value set. This value ranges from 0 to 7. • `dscp <value (0-63)>` - Configures the Differentiated Services Code Point value to be checked against the packet, This value provides the quality of service control. This value ranges from 0 to 63. • `priority <value(1-255)>` - Configures the priority of the filter to decide which filter rule is applicable when the packet matches with more than one filter rules. Lower value of 'filter priority' implies a higher priority. This value ranges from 1 to 255.		
`permit icmp {any |host <src-ip-address>|<src-ip-address> <mask>}{any | host <dest-ip-address>`	Configures the ICMP (Internet Control Message Protocol) packets to be forwarded	Extended IP ACL Configuration

| <dest-ip-address> <mask> [message-type <short (0-255)>] [message-code <short (0-255)>] [redirect {interface <iftype> <ifnum}] [sub-action {none | modify-vlan<short (1-4094}] [priority <value(1-255)>] Available options: • any|host <src-ip-address>|<network-src-ip><mask> - Specifies the source IP address. The source IP can be: - any – Packets from any source are matched. - host <src-ip-address> - Packets from this IPv4 source address are matched. - <network-src-ip> <mask> - Packets are matched using this source IPv4 network and mask. • any|host <dest-ip-address>|<network-dest-ip><mask> - Specifies the source IP address. The source IP address can be : - any - Packets to any destination are matched - host <src-ip-address> - Packets for this IPv4 destination address are matched - <network-src-ip> <mask> - Packets are matched using this destination IPv4 network and mask. • message-type <short (0-255)> - Configures the ICMP Message type to be checked against the packet. The packet is allowed if it matches with the message type. This value ranges from 0 to 255. Some of the ICMP message types are: - 0 Echo reply - 3 Destination unreachable - 4 Source quench - 5 Redirect - 8 Echo request - 11 Time exceeded - 12 Parameter problem - 13 Timestamp request - 14 Timestamp reply - 15 Information request - 16 Information reply - 17 Address mask request - 18 Address mask reply - 255 No ICMP type	based on the IP address and the associated parameters.	

• message-code <short (0-255)> - Configures the ICMP Message code to be checked against the packet. The packet is allowed if it matches with the message code. This value ranges from 0 to 255. Some of the ICMP message Codes are: - 0 Network unreachable - 1 Host unreachable - 2 Protocol unreachable - 3 Port unreachable - 4 Fragment need - 5 Source route fail - 6 Destination network unknown - 7 Destination host unknown - 8 Source host isolated - 9 Destination network administratively prohibited - 10 Destination host administratively prohibited - 11 Network unreachable TOS - 12 Host unreachable TOS - 255 No ICMP code • redirect - Redirects the packets to the destination interface or set of interfaces. - <iftype>- Redirects the packets to the specified type of interface. - <ifnum>- Redirects the packets to the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface types gigabitethernet, fastethernet and extreme-ethernet. • sub-action - Configures the VLAN specific sub action to be performed on the packet. Options are: - none - Specifies that the actions related to the VLAN ID will not be considered. - modify-vlan <short (1-4094)> - Modifies the VLAN ID to which the packet gets classified. The packet could be an untagged or VLAN tagged packet. This value ranges from 1 to 4094. • priority <value(1-255)> - Configures the priority of the filter to		

decide which filter rule is applicable when the packet matches with more than one filter rules. Lower value of 'filter priority' implies a higher priority. This value ranges from 1 to 255.		
`deny icmp {any |host <src-ip-address>|<src-ip-address> <mask>}{any | host <dest-ip-address> | <dest-ip-address> <mask> }[ message-type <short (0-255)>] [message-code <short (0-255)>] [priority <value(1-255)>]` Available options: • `any|host <src-ip-address>|<network-src-ip><mask>` - Specifies the source IP address. The source IP can be: - `any` – Packets from any source are matched. - `host <src-ip-address>` - Packets from this IPv4 source address are matched. - `<network-src-ip> <mask>` - Packets are matched using this source IPv4 network and mask. • `any|host <dest-ip-address>|<network-dest-ip><mask>` - Specifies the source IP address. The source IP address can be : - `any` - Packets to any destination are matched - `host <src-ip-address>` - Packets for this IPv4 destination address are matched - `<network-src-ip> <mask>` - Packets are matched using this destination IPv4 network and mask. • `message-type <short (0-255)>` - Configures the ICMP Message type to be checked against the packet. The packet is allowed if it matches with the message type. This value ranges from 0 to 255. Some of the ICMP message types are: - 0 Echo reply - 3 Destination unreachable - 4 Source quench - 5 Redirect - 8 Echo request - 11 Time exceeded - 12 Parameter problem		Extended IP ACL Configuration

<table>
<tr>
<td>- 13 Timestamp request
- 14 Timestamp reply
- 15 Information request
- 16 Information reply
- 17 Address mask request
- 18 Address mask reply
- 255 No ICMP type
• message-code <short (0-255)> - Configures the ICMP Message code to be checked against the packet. The packet is allowed if it matches with the message code. This value ranges from 0 to 255. Some of the ICMP message Codes are:
- 0 Network unreachable
- 1 Host unreachable
- 2 Protocol unreachable
- 3 Port unreachable
- 4 Fragment need
- 5 Source route fail
- 6 Destination network unknown
- 7 Destination host unknown
- 8 Source host isolated
- 9 Destination network administratively prohibited
- 10 Destination host administratively prohibited
- 11 Network unreachable TOS
- 12 Host unreachable TOS
- 255 No ICMP code
• priority <value(1-255)> - Configures the priority of the filter to decide which filter rule is applicable when the packet matches with more than one filter rules. Lower value of ‘filter priority’ implies a higher priority. This value ranges from 1 to 255.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>permit ipv6 { flow-label <integer(1-65535)> | {any | host <ip6_addr> <integer(0-128)> } { any | host <ip6_addr> <integer(0-128)> }} [redirect {interface <iftype> <ifnum> }][sub-action {none | modify-vlan<short (1-4094}] [priority <value(1-255)>]
Available options:
• flow-label - Configures the Flow identifier in the IPv6 header. This value ranges from 1 to 65535.
• any | host <ip6_addr> <integer (0-128)> - Specifies the source IPv6 address.
o any – Packets from any source are matched.
o host <ip6_addr> <integer (0-128)> -</td>
<td>Configures IPv6 packets to be forwarded based on protocol and associated parameters.</td>
<td>Extended IP ACL Configuration</td>
</tr>
</table>

Packets from this IPv4 source address and prefix length are matched. • any | host <ip6_addr> <integer (0-128)> - Specifies the source IP address. The source IP address can be : o any - Packets to any destination are matched o host <ip6_addr> <integer (0-128)> - Packets for this IPv6 destination address and prefix length are matched • redirect - Redirects the packets to the destination interface or set of interfaces. o <iftype>- Redirects the packets to the specified type of interface. o <ifnum>- Redirects the packets to the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface types gigabitethernet, fastethernet and extreme-ethernet. • sub-action - Configures the VLAN specific sub action to be performed on the packet. Options are: o none - Specifies that the actions related to the VLAN ID will not be considered. o modify-vlan <short (1-4094)> - Modifies the VLAN ID to which the packet gets classified. The packet could be an untagged or VLAN tagged packet. This value ranges from 1 to 4094. • priority <value(1-255)> - Configures the priority of the filter to decide which filter rule is applicable when the packet matches with more than one filter rules. Lower value of ‘filter priority’ implies a higher priority. This value ranges from 1 to 255.		
deny ipv6 { flow-label <integer(1-65535)> | {any | host <ip6_addr> <integer(0-128)> } { any | host <ip6_addr> <integer(0-128)> }} [priority <value(1-255)>] Available options:	Specifies the IPv6 packets to be rejected based on associated parameters.	

• `flow-label` - Configures the Flow identifier in the IPv6 header. This value ranges from 1 to 65535. • `any | host <ip6_addr> <integer (0-128)>` - Specifies the source IPv6 address. o `any` – Packets from any source are matched. o `host <ip6_addr> <integer (0-128)>` - Packets from this IPv4 source address and prefix length are matched. • `any | host <ip6_addr> <integer (0-128)>` - Specifies the source IP address. The source IP address can be : o `any` - Packets to any destination are matched o `host <ip6_addr> <integer (0-128)>` - Packets for this IPv6 destination address and prefix length are matched • `priority <value(1-255)>` - Configures the priority of the filter to decide which filter rule is applicable when the packet matches with more than one filter rules. Lower value of 'filter priority' implies a higher priority. This value ranges from 1 to 255.		
`permit { any | host <src-mac-address>}{ any | host <dest-mac-address> } [ vlan <vlan-id (1-4094)>] [ vlan-priority <value (0-7)>] [redirect {interface <iftype> <ifnum> }] [sub-action {none | modify-vlan<short (1-4094)> }] [priority <value(1-255)>]` Available options: • `any | host <src-mac-address>`- Specifies the source MAC address. The source mac address can be: o `any` - Allows all packets. Does not check for the source MAC address in the packets. o `host <src-mac-address>` - Allows only the packets having the specified source MAC address. • `any | host <dest-mac-address>`- Specifies the destination MAC address. The destination mac address can be:	Configures the packets to be forwarded based on the MAC address and the associated parameters, that is, this command allows non-IP traffic to be forwarded if the conditions are matched.	Extended IP ACL Configuration

○ any - Allows all packets. Does not check for the source MAC address in the packets. ○ host <src-mac-address> - Allows only the packets having the specified destination MAC address. • vlan <vlan-id (1-4094)> - Specifies the vlan id to be filtered. This value ranges from 1 to 4094. • vlan-priority <value (0-7)>- Configures VLAN priority value to match against incoming packets. This value ranges from 0 to 7. • redirect - Redirects the packets to the destination interface or set of interfaces. ○ <iftype>- Redirects the packets to the specified type of interface. ○ <ifnum>- Redirects the packets to the specified interface identifier. This is a unique value that represents the specific interface. This value is a combination of slot number and port number separated by a slash, for interface types gigabitethernet, fastethernet and extreme-ethernet. • sub-action - Configures the VLAN specific sub action to be performed on the packet. Options are: ○ none - Specifies that the actions related to the VLAN ID will not be considered. ○ modify-vlan <short (1-4094)> - Modifies the VLAN ID to which the packet gets classified. The packet could be an untagged or VLAN tagged packet. This value ranges from 1 to 4094. • priority <value(1-255)> - Configures the priority of the filter to decide which filter rule is applicable when the packet matches with more than one filter rules. Lower value of 'filter priority' implies a higher priority. This value ranges from 1 to 255.		
deny { any | host <src-mac-address>}{ any | host <dest-mac-address> } <short (0-65535) }] [encaptype <integer (1-65535)>] [	Configures the packets to be rejected based on the MAC address and the associated parameters.	Extended IP ACL Configuration

vlan <vlan-id (1-4094)>] [vlan-priority <priority (0-7)>] [priority <value(1-255)>] Available options: • any | host <src-mac-address>- Specifies the source MAC address. The source mac address can be: ○ any - Allows all packets. Does not check for the source MAC address in the packets. ○ host <src-mac-address> - Allows only the packets having the specified source MAC address. • any | host <dest-mac-address>- Specifies the destination MAC address. The destination mac address can be: ○ any - Allows all packets. Does not check for the source MAC address in the packets. ○ host <src-mac-address> - Allows only the packets having the specified destination MAC address. • vlan <vlan-id (1-4094)> - Specifies the vlan id to be filtered. This value ranges from 1 to 4094. • vlan-priority <value (0-7)>- Configures VLAN priority value to match against incoming packets. This value ranges from 0 to 7. • priority <value(1-255)> - Configures the priority of the filter to decide which filter rule is applicable when the packet matches with more than one filter rules. Lower value of 'filter priority' implies a higher priority. This value ranges from 1 to 255.		
ip access-group <access-list-number (1-65535)> {in | out} Available options: • <access-list-number(1-65535)> - Specifies the IP access control list number which is to be enabled on the interface. This value ranges from 1 to 65535. • in - Applies the ACL on the ingress of the port. • out - Applies the ACL on the egress of the port. Redirect action is not applicable when applying the ACL on the egress of a port.	Applies the specified IP ACL on the port. The no form of this command removes all access groups or the specified access group from the port.	Interface Configuration

cnMatrix Parameters and Commands

`mac access-group <access-list-number (1-65535)> {in | out}` Available options: • `<access-list-number(1-65535)>` - Specifies the MAC access control list number which is to be enabled on the interface. This value ranges from 1 to 65535. • `in` - Apply the ACL on the ingress of the port. • `out` - Applies the ACL on the egress of the port. Redirect action is not applicable when applying the ACL on the egress of a port.	Applies the specified MAC ACL on the port. The no form of this command removes all access groups or the specified access group from the port.	Interface Configuration
`show access-lists [{ip <access-list-number (1-65535)> | mac <access-list-number (1-65535)> | <access-list-number (1-65535)> }]` Available options: • `ip <access-list-number (1-65535)>` - Displays the configurations for the specified IP access-list. This value ranges from 1 to 65535. • `mac <access-list-number (1-65535)>` - Displays the configurations for the specified mac access-list. This value ranges from 1 to 65535. • `<access-list-number (1-65535)>` - Displays the configurations for the specified access-list. This value ranges from 1 to 65535.	Displays the access lists configuration.	Privileged EXEC
`show egress access-list mode`	Displays the egress filter mode configuration.	Privileged EXEC

cnMatrix Static MAC Parameters and Commands

Commands	Description	CLI Mode
`mac-address-table static unicast <aa:aa:aa:aa:aa:aa> vlan <vlan-id> [{recv-port <interface-type> <ifnum>}] [interface ([<interface-type> <0/a-b, 0/c, ...>] [<interface-type> <0/a-b, 0/c, ...>] [port-channel <a,b,c-d>][status { permanent | deleteOnReset | deleteOnTimeout }]` Available options: • `<aa:aa:aa:aa:aa:aa>` - Configures the static unicast destination MAC address.	Configures a static unicast MAC address in the forwarding database.	Global Configuration

• `vlan <vlan-id >` - Configures the static unicast destination MAC address for the specified VLAN • `recv-port` - Configures the receive ports details. • `interface` - Configures the member ports interface type and ID. • `status` - Specifies the status of the Static unicast entry.		
`show mac-address-table static unicast [vlan <vlan-range>] [address <aa:aa:aa:aa:aa:aa>] [{interface <interface-type> <interface-id>}]` Available options: • `vlan <vlan-range>` - Displays all static unicast MAC address entries created in the FDB table for the specified VLANs alone. • `address <aa:aa:aa:aa:aa:aa>` - Displays all static unicast MAC address entries created in the FDB table for the specified unicast MAC address. • `interface` - Displays all static unicast MAC address entries for the specified interface	Displays all static unicast MAC address entries created in the FDB table.	Privileged EXEC

cnMatrix Local Management User Name Password Parameters and Commands

Commands	**Description**	**Mode**
`password max-life-time [<days (0-366)>]`	Configures the time after which the user password has to be expired in days.	Global Configuration
`show privilege`	Displays the current user privilege level.	Privileged EXEC
`enable password <password>`	Enables the specified password.	Global Configuration
`enableuser <username>`	Releases the unblocked user specified by the username string.	Global Configuration
`set minimum password length <8-20>`	Configures minimum password length.	Global Configuration
`password validate char [lowercase] [uppercase] [numbers] [symbols]` Available options: • `lowercase` - Sets lowercase flag for password validation. • `uppercase` - Sets uppercase flag for password validation. • `numbers` - Sets numbers flag for password validation. • `symbols` - Sets symbols flag for password validation.	Configure the type of characters to be considered for password validation rules and takes values as bit mask.	Global Configuration
`password validate uppercase [<count(0-20)>]`	Configures the minimum number of upper case characters that are to be present in the password.	Global Configuration

cnMatrix Parameters and Commands

Commands	Description	Mode
`password validate lowercase [<count(0-20)>]`	Configures the minimum number of lower case characters that are to be present in the password.	Global Configuration
`password validate numbers [<count(0-20)>]`	Configures the minimum numerical characters to be present in the password.	Global Configuration
`password validate symbols [<count(0-20)>]`	Configures the minimum special character to be present in the password.	Global Configuration
`show password validate rules`	Displays the password validation rules.	Privileged EXEC
`show minimum password length`	Displays minimum password length.	Privileged EXEC
`username <username> [password <passwd>] [privilege <1-15>]` Available options: • `username` - Specifies the login user name to be created. • `password` - Specifies the password to be entered by the user to login to the system. The size password entered must be a minimum of 8 and maximum of 20 characters containing at least one uppercase, one lowercase, one number and one special character. • `privilege` - Applies restriction to the user for accessing the CLI commands. This values ranges between 1 and 15. For Example, a user ID configured with privilege level as 4 can access only the commands having privilege ID lesser than or equal to 4. flag for password validation. The default **admin** user has privilege value 15, which is the highest privilege value. This enables the user to access all commands.	This command creates a user and sets the password and the privilege level for the user.	Global Configuration
`no username <username>`	Deletes the specified user.	Global Configuration
`listuser`	This command lists all the default and newly created users, along with their privilege values.	Privileged EXEC

cnMatrix HTTPS Parameters and Commands

cnMatrix Parameters and Commands

Commands	Description	CLI Mode
`ip http secure { server | ciphersuite [rsa-null-md5] [rsa-null-sha] [rsa-des-sha] [rsa-3des-sha] [dh-rsa-des-sha][dh-rsa-3des-sha][rsa-exp1024-des-sha] [rsa-with-aes-128-cbc-sha] [rsa-with-aes-256-cbc-sha] [dhe-rsa-with-aes-128-cbc-sha] [dhe-rsa-with-aes-256-cbc-sha] | crypto key rsa [usage-keys (512|1024)]}` Available options: • `server` - Configures the server status to be enabled. • `ciphersuite` - Configures the ciphersuite for providing the input. • `crypto` - Configures the usage key (512 or 1024). **Starting with version 2.1** , the crypto parameter configures the usage key (512, 1024 or 2048).	Enables the SSL server on the device and also configures ciphersuites and crypto keys.	Global Configuration
`ssl gen cert-req algo rsa sn <SubjectName>`	Creates a request to generate a certificate to the certificate authority.	Privileged EXEC
`ssl server-cert`	Configures the server-certificate input in PEM format.	Privileged EXEC
`debug ssl ([all] [shut] [mgmt] [data] [ctrl] [dump] [resource] [buffer])` Available options: • `all` - Generates debug statements for all traces. • `shut` - Generates debug statements for shutdown traces. • `mgmt` - Generates debug statements for management plane functionality traces. • `data` - Generates debug statements for datapath. • `ctrl` - Generates debug statements for Control Plane functionality traces. • `dump` - Generates debug statements for packets handling traces. • `resource` - Generates debug statements for Traces with respect to allocation and freeing of all resource except the buffers. • `buffer` - Generates debug statements for traces with respect to allocation and freeing of buffer.	Configures the debug trace messages levels for SSL.	Privileged EXEC

cnMatrix Parameters and Commands

Commands	Description	CLI Mode
`show ssl server-cert`	Displays SSL server certificate information such as Certificate, Data, version, serial number, Signature algorithm.	Privileged EXEC
`show ip http secure server status`	Displays the SSL status and configuration.	Privileged EXEC
`version {all | ssl3 | tls1}` Available options: • `all` - Allows configuration to both SSL3 and TLS1 SSL protocols. • `ssl3` - Configures SSL version 3 protocol. • `tls1` - Configures Transport Layer Security version 1 protocol. **Starting with version 2.1,** the following parameters have been added: • **`tls1_1`** - Configures Transport Layer Security version 1.1 protocol. • **`tls1_2`** - Configures Transport Layer Security version 1.2 protocol.	Configures the SSL version.	Global Configuration

`secure { crypto key rsa [usage-keys (512|1024)]}`
Starting with version 2.1:
`secure { crypto key rsa [usage-keys (512|1024|2048)]}`
	Sets the RSA key length for the secure crypto operations.	Global Configuration

cnMatrix HTTP/HTTPS Parameters and Commands

Commands	Description	CLI Mode

`set ip http {enable | disable}`
Starting with version 2.1:
`ip http {enable | disable}`
	Enables/Disables the HTTP Server.	Global Configuration

`ip http port <port(1-65535)>`	Sets the HTTP port.	Global Configuration
`show http server status`	Displays the HTTP server status and HTTP port.	Privileged EXEC
`ip http secure { server | ciphersuite [rsa-null-md5] [rsa-null-sha] [rsa-des-sha] [rsa-3des-sha] [dh-rsa-des-sha][dh-rsa-3des-sha][rsa-exp1024-des-sha] [rsa-with-aes-128-cbc-sha] [rsa-with-aes-256-cbc-sha] [dhe-rsa-with-aes-128-cbc-sha] [dhe-rsa-with-aes-256-cbc-sha] | crypto key rsa [usage-keys (512|1024)]}`	Enables TLS server on the device and also configures ciphersuites and crypto keys.	Global Configuration

cnMatrix Parameters and Commands

Available options: • server – Enables the TLS Server. • ciphersuite - Configures the ciphersuite to be used by the TLS Server. • crypto key rsa - Configures the usage key (512 or 1024).		
`set http authentication-scheme {default | basic | digest}` Available options: • `default` - Sets the configurable HTTP authentication scheme to default. • `basic` - Sets the configurable HTTP authentication scheme to basic. • `digest` - Sets the configurable HTTP authentication scheme to digest.	Configures the Configurable HTTP authentication scheme.	Global Configuration
`show http authentication-scheme`	Displays the operational and configurable authentication scheme values.	Privileged EXEC

cnMatrix 802.1X Authentication Parameters and Commands

Commands	Description	CLI Mode
`aaa authentication dot1x default group { radius | local}`	Enables the dot1x local authentication or RADIUS server based remote authentication method for all ports. The actual authentication of the supplicant happens at the authentication server.	Global Configuration
`dot1x local-database <username> password <password> permission {allow | deny} [<auth-timeout (value(1-7200))>] [interface <interface-type> <interface-list>]`	Configures dot1x authentication server local database with user name and password.	Global Configuration
`set nas-id <identifier>`	Sets the dot1x network access server id. Network Access Server Identifier is set in the RADIUS packets sent to the Remote Authentication Server Maximum length of the string is 16.	Global Configuration
`dot1x system-auth-control`	Enables dot1x in the switch. The dot1x is an authentication mechanism. It acts as mediator between the authentication server and the supplicant (client). If the client accesses the protected resources, it contacts the authenticator with EAPOL frames.	Global Configuration
`dot1x init-session <supp addr - aa:aa:aa:aa:aa:aa>`	Initiates dot1x authentication session for the given MAC address of the supplicant. The supplicant requests for access to the protected network. It sends EAPOL (Extensible Authentication Protocol) frames to the authenticator. When the supplicant is	Global Configuration

cnMatrix Parameters and Commands

Commands	Description	CLI Mode
	authorized by the remote server, the session is initiated.	
dot1x init session-reauth <supp addr - aa:aa:aa:aa:aa:aa >	Initiates dot1x re-authentication session for the specified MAC address. When the supplicant has exceeded the time limit for accessing the protected network, the supplicant is forced for re-authentication. This is to ensure that the supplicant is the same entity that was initially authenticated.	Global Configuration
dot1x default	Configures dot1x with default values for this port. The previous configurations on this port are reset to the default values. These details are not displayed but are the basic settings for a port.	Interface Configuration (Physical interface)
dot1x max-req <count(1-10)>	Sets the maximum number of EAP (Extensible Authentication Protocol) retries to the client by the authenticator before restarting authentication process. The count value ranges between 1 and 10.	Interface Configuration (Physical interface)
dot1x max-start <count(1-65535)>	This command sets the maximum number of EAPOL retries to the authenticator. The value range is 1 to 65535.	Interface Configuration (Physical interface)
dot1x reauthentication	Enables periodic re-authentication from authenticator to client. The periodic re-authentication is requested to ensure if the same supplicant is accessing the protected resources. The amount of time between periodic re-authentication attempts can be configured manually.	Interface Configuration (Physical interface)
dot1x timeout {quiet-period <value (0-65535)> | {reauth-period | server-timeout | supp-timeout | tx-period | start-period | held-period | auth-period }<value (1-65535)>}	Sets the dot1x timers. The timer module manages timers, creates memory pool for timers, creates timer list, starts and stops timer. It provides handlers to respective expired timers.	Interface Configuration (Physical interface)
dot1x port-control {auto|force-authorized|force-unauthorized}	Configures the authenticator port control parameter. The dot1x exercises port based authentication to increase the security of the network. The different Modes employed to the ports offer varied access levels. The 802.1x protocol is supported on both Layer 2 static-access ports and Layer 3 routed ports	Interface Configuration (Physical interface)
dot1x access-control {active | inactive}	Configures the supplicant access control. This setting is for the application of the Supplicant authorization state when the port is operating as both Supplicant and Authenticator.	Interface Configuration (Physical interface)
dot1x control-direction {in | both}	Configures port control direction.. The switch port authenticates incoming packets and outgoing packets. The direction can be configured manually by selecting either in or both. By default the value is both.	Interface Configuration (Physical interface)

cnMatrix Parameters and Commands

Commands	Description	CLI Mode
dot1x host-Mode {multi-host | single-host}	Configures the port authentication Mode of a port as either multi-host (which is also known as port-based) or single-host (which is also known as mac-based). Multi host authentication has different Modes of authentication. Single host authentication allows secured mac addresses to pass through the port. Non secure mac addresses are dropped.	Interface Configuration (Physical interface)
dot1x re-authenticate [interface <interface-type><interface-id>]	Initiates re-authentication of all dot1x-enabled ports or the specified dot1x-enabled port. This initializes the state machines and sets up the environment for fresh authentication. Re-authentication is manually configured if periodic re-authentication is not enabled. Re-authentication is requested by the authentication server to the supplicant to furnish the identity without waiting for the configured number of seconds (re-auth period). If no interface is specified, re-authentication is initiated on all dot1x ports	Privileged EXEC
dot1x initialize [interface <interface-type> <interface-id>]	Initializes the state machines and sets up the environment for fresh authentication. This initiates re-authentication of all dot1x-enabled ports or the specified dot1x-enabled port. Re-authentication is manually configured if periodic re-authentication is not enabled. Re-authentication is requested by the authentication server to the supplicant to furnish the identity without waiting for the configured number of seconds (re-auth period). If no interface is specified, re-authentication is initiated on all dot1x ports	Privileged EXEC
debug dot1x {all | errors | events | packets | state-machine | redundancy | registry }	This command enables debugging of dot1x module. The failure messages and error information are captured by the debug traces. Different traces are enabled to capture particular performance failures. Only one trace can be enabled at a time.	Privileged EXEC
show dot1x [{ interface <interface-type> <interface-id> | statistics interface <interface-type> <interface-id> | supplicant-statistics interface <interface-type> <interface-id>|local-database | mac-info [address <aa.aa.aa.aa.aa.aa>] | mac-statistics [address <aa.aa.aa.aa.aa.aa>] | all }]	Displays dot1x information. The configured information can be viewed by running this show command. When there is any change in the configuration to ensure that the port is configured as desired, the show command is used.	Privileged EXEC
dot1x clear statistics [{interface <iftype> <ifnum>}][{mac-statistics address <mac_addr>}]	Clears dot1x statistics information.	Privileged EXEC