COMMAND LINE INTERFACE GUIDE

QUICK CLI GUIDE

FOR QUANTUM SWITCH

Document ID: SW-CLI-001
Revision ID: 01 | Revision Date: 23-09-2024

Contents

How to Access the Quantum Switch Login Page for CLI 3

Steps to Configure IP, Gateway, DNS 5

Steps to Create Privilege Level User Profiles with CLI 7

Configure Switch Interfaces Using CLI 8

Main Switch Configuration for Stacking *9*

Backup or Slave Switch Configuration for Stacking *10*

Configure LACP by Using Below Steps 11

PIM Configuration Steps in Switch Using CLI 12

Configuring SPAN and RSPAN using CLI To Achieve Port Mirroring 13

Configuring SPAN *13*

Configuring RSPAN *13*

Configure Extended ACL 14

Configuring QoS in Quantum Switch 15

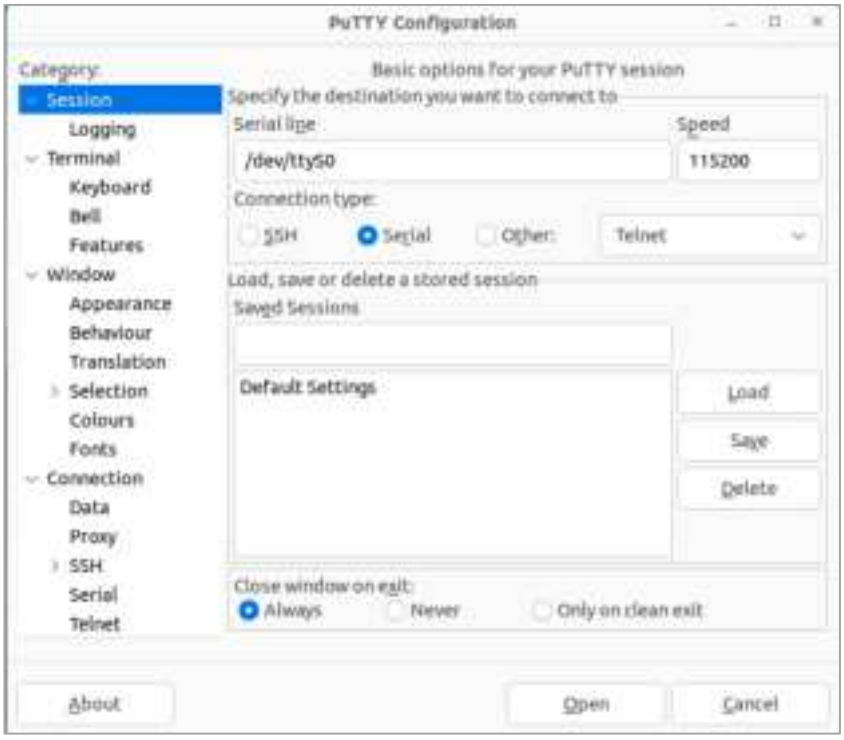
How to Access the Quantum Switch Login Page for CLI

Steps to access the quantum switch via OOB port

1. First, connect Laptop to OOB port in Quantum Switch through Lan cable
2. Assign the 192.168.254.x series IP on the laptop Lan adapter
3. Open putty application and enter OOB IP 192.168.254.254 with selecting SSH by default SSH is enable in Quantum switch.
4. After accessing the IP address, you'll be directed to the CLI page here need enter switch login credentials.

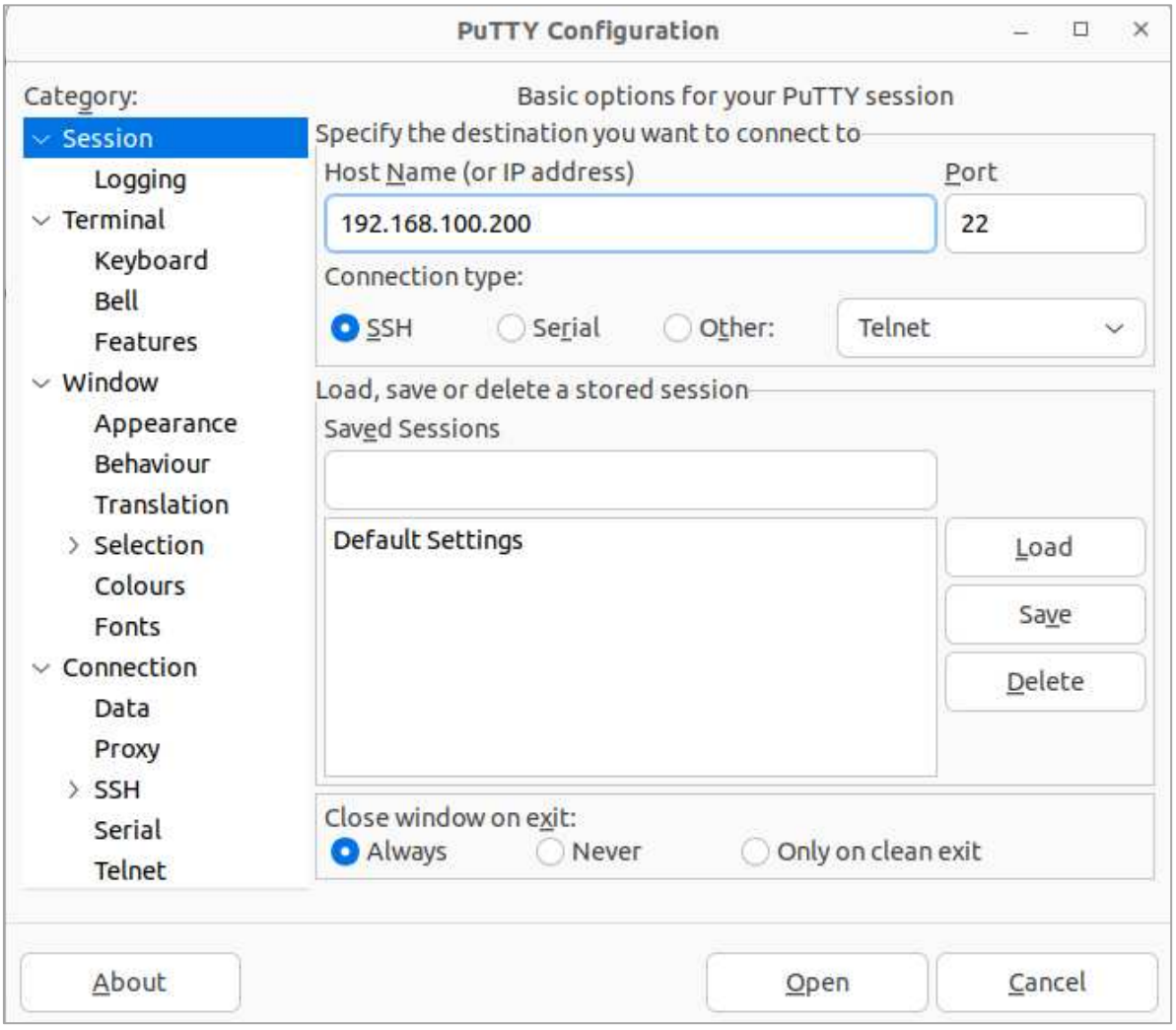
Steps to access the quantum switch via Console.

1. Connect RJ45 to the console port of the switch and other end to the PC.
2. Open putty application.
3. PuTTY Serial Settings (X is the number of the COM port, e.g. COM5)
4. Provide the Board Rate(speed) = 115200
5. Select Connection type = Serial
6. Click on Open. Enter switch username and password so you will get switch access.



Steps to access the quantum switch via SSH using Network IP.

1. Give Uplink on switch Port.
2. Connect laptop to any switch port through LAN cable
3. Find out the switch network IP using IP scanner.
4. Open Putty application and enter the Network Ip on Host Name = 192.168.100.200 (Ip address of Switch).
5. Select Connection type: SSH.
6. Click on Open. Enter switch username and password so you will get switch access.



Quick Setup using Failover IP

1. The default failover IP is 169.254.x.x, where 169.254 is constant & Last 2 Digits are based on MAC address of switch.
2. To Get the IP Address, first note the MAC address of the switch.
3. Convert the last 4 Hex digit of switch MAC address into Decimal using Hex to Decimal converter.

    - (Can use any Hex to Decimal converter like "https://www.rapidtables.com/convert/number/hex-to-binary.html").
    - For an example, the MAC address of switch is 58:61:63:00:C5:E1, where last four digits are "C5:E1". Now convert C5 and E1 to Decimal. C5 Decimal value will come as "197" and value of E1 will come as "225". As per this the switch fail over IP will come as 169.254.197.225.

4. Now, Assign 169.254.1.20 (or any IP address of 169.254.x.x series except Switch's failover IP) static IP address to the Desktop/Laptop device LAN port.
5. Open the browser and browse Switch's Failover IP.
6. You will be on the configuration page.

Steps to Configure IP, Gateway, DNS

Steps to configure IP, Gateway, DNS to Quantum Switch Interfaces and to check Basic network settings:

To assign Static IP address

Go to Global configuration mode:

Training # configure

To create VLAN 1 interface:

Training(config)# interface vlan 1

Assign IP to VLAN 1:

Training(config) #ip address 192.168.100.10 255.255.255.0

To verify: **Training(config)#do show ip interface**

To assign Dynamic IP address
Go to Global configuration mode:

Training # configure

To create VLAN 1 interface:

Training(config)# interface vlan 1

Assign IP to VLAN 1:

Training(config) #ip address dhcp

To verify: Training(config)#do show ip interface

To assign Gateway to switch interface

Training(config)# interface vlan 1

To assign gateway

Training(config)#ip default-gateway 192.168.100.1

To verify: **Training(config)#do show Ip route**

To assign DNS to switch

Training(config)#ip name-server 8.8.8.8 4.4.4.4

To verify: Training(config)#do show running-config

To create a VLAN in switch

Training(config)#vlan 10

To verify: Training(config)#do show vlan

To create multiple VLAN

Training(config)#vlan 20-30

To check the mac address learning in the switch

Training # show mac address

To check the ARP table running in switch - ARP table consists with IP address.

Training #show arp

To check interfaces created in your switch

Training # show IP interface

If we need to check Firmware in switch

Training(config)# do show version

Steps to Create Privilege Level User Profiles with CLI

To create the monitor profile username and password:

Training(config)# username abc password abc privilege 1

Exit from admin user and login to monitor user using your provided credentials

Try to enter global configuration mode:

Training>configure (You will get error like **unrecognized command)**

Check IP interfaces present in the switch

Training > show ip interface

Check switch port interfaces in switch

Training > show interface status

To shift monitor user to admin user

Training > enable

Configure Switch Interfaces Using CLI

Check switch port interfaces in switch:

Training(config)# do show interface status

Select the port which you want to do configuration changes in switch port

Training(config)# interface gigabitethernet1/0/4

To apply negotiation use:

Training(config)# negotiation

To disable the negotiation on switch port

Training(config-if) # no negotiation

If you want to shut down the switch port then use:

Training(config)#shutdown

To unshut the port:

Training(config)# no shutdown

Manually if you need to set speed to this port then:

Training(config)# speed 100

If you want to change switch port to full duplex to half duplex:

Training(config)# duplex half

To verify configuration changes on switch port you can use the command:

Training(config)# do show interface configuration

If you need to check POE power on all switch ports you can use:

Training(config)# do show power inline

To configure the port as access port and to assign VLAN 10 to that port

Training(config)# interface gigabitethernet1/0/4
Training(config-if)#switchport access vlan 10

To configure the port as Trunk port and to assign multiple VLANs to that port

```
Training(config)# interface gigabitethernet1/0/5
Training(config-if) # switchport mode trunk
```

Stack Configuration Steps in CLI

Main Switch Configuration for Stacking

We need to go global configuration mode so use this command

```
Training # configure
```

To enter the specified stack unit or all stack units, enter this stack unit command in configuration mode by entering this below command

```
Training(config)# stack unit 1
```

Here we are configuring primary switch as master switch, and we are giving unit-id 1 for master switch. This is the stack configuration command to configure the stack ports and unit.

```
Training(unit)# stack configuration links te1-2 unit-id 1
```

To exit back to global configuration mode use stack unit, use this below command

```
Training(unit)# exit
```

Now need to save configuration:

```
Training(config)# do write
```

Reboot the switch physically or in CLI:

```
Training(config)# do reload
```

Backup or Slave Switch Configuration for Stacking

We need to go global configuration mode so use this command

Training # configure

To enter the specified stack unit or all stack units, enter this stack unit command in configuration mode by entering this below command

Training(config)# stack unit 1

Here we are providing unit-id 2 to back up switch and this command is used to configure the stack ports and unit.

Training(unit)# stack configuration links te1-2 unit-id 2

Step 4: To exit back to global configuration mode use stack unit, use this below command

Training(unit)# exit

Step 5: Now need to save configuration:

Training(config)# do write

Step 6: Reboot the switch physically or in CLI:

Training(config)# do reload

Note1: Now you can check in master switch interface status it will show combined port details or interface details.

Training # show interface status

Note2: To verify the stack links in switch, use this below command

Training(config)#do show stack links details

Configure LACP by Using Below Steps

Go to global configuration mode:

Training> configure

Select the interface range which you need to bundle the links:

Training(config)# interface range gigabitethernet1/0/2-5

Select channel group and mode:

Training(config-if-range) # channel-group 1 mode on

To verify: **Training(config-if-range) # do show interface port-channel**

To remove particular port from bundling

Select the port which you need to remove from bundling:

Training(config)# interface gigabitethernet1/0/4

Use this command to remove the port:

Training(config-if) # no channel-group

To verify: **Training(config-if-range) # do show interface port-channel**

For Removing all ports from port bundling

Select the port range which you need to remove from the port bundling

Training(config)# interface gigabitethernet1/0/2-5

Use this command to remove the port:

Training(config-if) # no channel-group

To verify: **Training(config-if-range) # do show interface port-channel**

PIM Configuration Steps in Switch Using CLI

To enter global configuration mode:

Training # configure

If you want to enable PIM in the switch first, we need to enable multicast routing

Training(config)#Ip multicast-routing

Enable PIM on particular VLAN here need to select vlan interface

Training(config)#interface vlan 4

Now to enable PIM

Training(config-if)#ip pim

Select the port to enable PIM on respective port.

Training(config)#interface gigabitethernet1/0/5

Step 6: Now to enable PIM

Training(config-if) #ip pim

To verify PIM configuration: **Training(config)#do show ip pim interface**

Configuring SPAN and RSPAN using CLI To Achieve Port Mirroring

Configuring SPAN

To Configure SPAN command, Here First, we need to define source port from which port we need to copy the traffic.

Training(config)# monitor session 1 source interface gigabitethernet 1/0/4

Now the copied data we need to send to analyser connected port or any computer connected port that is destination port and use below command to configure.

Training(config)# monitor session 1 destination interface gigabitethernet 1/0/6

To verify: **Training(config)#do show monitor session**

Configuring RSPAN

First, we need to create VLAN then need to define this VLAN as a remote VLAN

Training(config)#interface VLAN 150

Training(config)#remote

Now need to define source as remote VLAN to monitor session 2

Training(config)#monitor session 2 source remote VLAN 150

we need to define destination port to copy the traffic from source remote vlan

Training(config)#monitor session 2 destination interface gigabitethernet2/0/6

To verify: **Training(config)#do show monitor session**

Configure Extended ACL

Go to Global Configuration Mode

Training> configure

To create the extended ACL name

Training(config)# Ip access-list extended Test

If you wish to permit (from subnet 0.0.255.255 source to destination 192.168.100.10)

Training(config)# permit ip 172.16.100.1 0.0.255.255 192.168.100.10 0.0.0.0

If you wish to deny (from subnet 0.0.255.255 source to destination 192.168.100.10)

Training(config)# deny ip 172.16.100.1 0.0.255.255 192.168.100.10 0.0.0.0

To verify: **do show access-lists**

Ingress (input): Binding the created extended ACL (test) to port 5 and applying inbound (input) rules.

Training(config)# interface gigabitethernet1/0/5
Training(config)# service-acl input Test

To verify: **Training(config)# do show running-config**

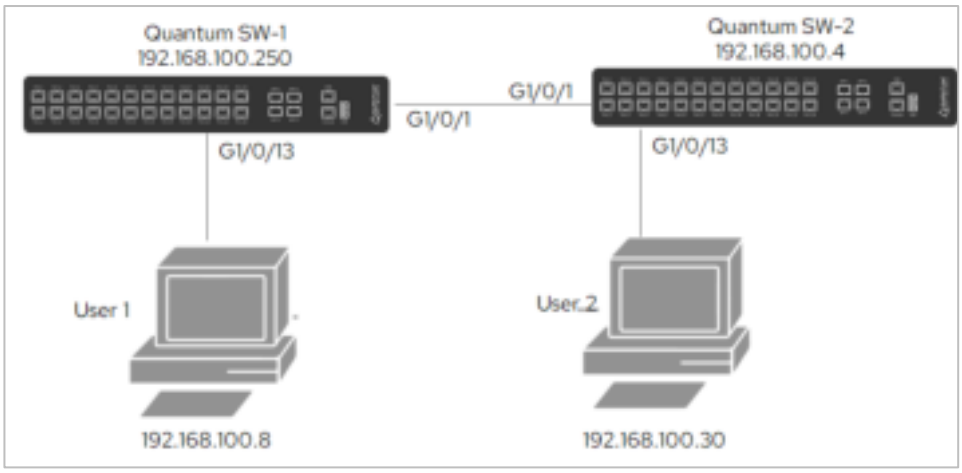
Egress (output): Binding the created extended ACL (test) to port 6 and applying outbound(output) rules.

Training(config)# interface gigabitethernet1/0/6
Training(config)# service-acl output Test

To verify: Training(config)# do show running-config

Configuring QoS in Quantum Switch

Priority tagging by COS:



You can observe this network there are two switches are connected user-1 is connected to SW-1 and user-2 is connected to SW-2.

For Example, we want to prioritize the ICMP and TCP (video or voice traffic) traffic moving from user-1 to user-2 using cos method. To achieve this configure the QOS parameters in SW-2 as shown below.

- **Note:** For L2 switch we configure COS (Class Of Service).
- For L3 switch we configure DSCP (Differentiated Service Code Point).

For L2 Switch –First we need to enable QOS advanced mode in the switch

Enable Quality of service for our traffic

```
Switch(config)#qos advanced
```

(Define the Quality of service means which mode you are going to use like we configure COS for L2 Switch)

```
Switch(config)#qos advanced-mode trust cos
```

Then we need to configure ACL to identify the traffic user 1 is initiating the traffic from 192.168.100.8 to switch 2(192.168.100.4) this traffic need to prioritize.
(First, we need to create the Access list for our traffic to be permit or deny like we have created Test Access list)

Switch(config)#ip access-list extended Test

(Under the Test access list, we are going to permit icmp traffic between Source (192.168.100.8 0.0.0.0) to Destination (192.168.100.4 0.0.0.0))

Switch(config-if-al)#permit icmp 192.168.100.8 0.0.0.0 192.168.100.4 0.0.0.0 any any

(Under the Test access list, we are going to permit tcp traffic between Source (192.168.100.8 0.0.0.0) to Destination (192.168.100.4 0.0.0.0))

Switch(config-if-al)#permit tcp 192.168.100.8 0.0.0.0 any 192.168.100.4 0.0.0.0 any

(here you can permit all protocol traffic like telnet, ssh, www, ftp and so on for all)

Switch(config-if-al)# permit ip any any

(After created the Test Access list, we need to map it in the class-map)

Switch(config)#class-map test match-any

(here we are going to map the Test Access list in Class-map by using above command)

Switch(config-cmap) #match access-group test

(After mapping Test Access list in Class-map, we need to map this class-map in the policy-map)

switch(config)#policy-map admin

(here we are going to map the class-map in policy-map)

switch(config-pmap)#class test

Now tagging the traffic if your marking layer 2 traffic then use cos 0 to 7 so I am selecting set cos 4 or if you want to mark layer 3 traffic then use dscp 0 to 63

(this is important part, here we are going to set the prior means what traffic we need pass like 4, please follow the below table according to different traffic)

switch(config-pmap-c)#set cos 4

QOS Classes	Example
Class 0 - Best Effort	Traffic is handled on a first-come, first-served basis with no prioritization.
Class 1 - Real-Time Interactive	voice and video conferencing
Class 2 - Interactive and Transactional Data	online gaming or interactive web browsing
Class 3 - Multimedia Conferencing	video streaming or video conferencing
Class 4 - Broadcast Video	streaming video or IPTV services
Class 5 - Call Signaling:	VoIP or other real-time communication systems.
Class 6 - Network Control:	routing updates or management protocols
Class 7 - Network Management:	SNMP or syslog messages

Now whatever traffic you marked need to send out through the switch interface so need to define switch port

Switch(config-pmap-c)#exit

(here we are going to implement this Class of service in the interface)

switch(config-pmap)#interface gigabitethernet1/0/1

(here we are going to map this policy-map with the interface)

switch(config-if)#service-policy input admin