Guide for VLAN in SONiC

HARDWARE NATION®

By: Humza Altaf
SONiC Network Engineer

Revision No.	Description	Editor	Date
1.0	Guide for VLAN in SONiC	Humza Altaf	Aug 26, 2023

Table of Contents

Introduction to VLAN

A VLAN, or Virtual Local Area Network, is a logical grouping of devices on a network. In a traditional network, all devices are part of the same physical LAN, meaning that they are all on the same broadcast domain and can communicate with each other freely. However, with VLANs, a single physical network can be divided into multiple virtual networks, each with its own unique VLAN ID.

Without VLANs, a broadcast sent from host A would reach all devices on the network. Each device will receive and process broadcast frames, increasing the CPU overhead on each device and reducing the overall security of the network.

Devices within the same VLAN can communicate with each other as if they were on the same physical LAN, but devices in different VLANs cannot communicate with each other unless specifically allowed by a router or switch. This can improve security by preventing unauthorized access to devices on the network and can also improve network performance by reducing broadcast traffic.

Network Topology

Suppose we have a network with two departments: Electrical, and Software. We want to create separate VLANs for each department to improve network security and performance.

To do this, we would need to configure our switches and hosts accordingly. Let's say we have two switches, S1 and S2, and four hosts, PC1 through PC4. Now draw network topology in GNS3 using community SONiC (version 202205) switches and hosts.

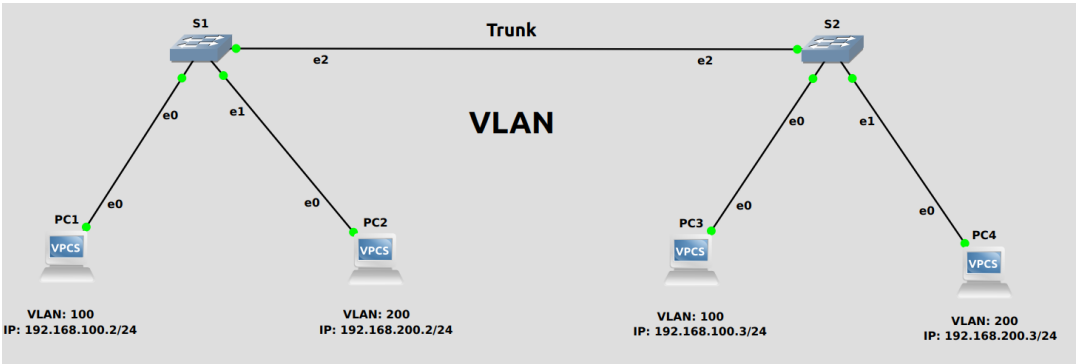

Fig: Network Topology

Port Mapping

GNS3	SONiC
Ethernet 0	Ethernet 0
Ethernet 1	Ethernet 4
Ethernet 2	Ethernet 8
Ethernet 3	Ethernet 12

Configurations

For the above topology, all hosts and switches are first configured before sending traffic. First, switch S1 is configured and the same steps are repeated for the switch S2. Command Reference guide is also available on GitHub for SONiC, whose link is given here.

Follow these steps to configure S1.

Step 1

Check the status of interfaces by using the command:

- `show interfaces status`

```
admin@sonic:~$ show interfaces status
  Interface            Lanes    Speed    MTU    FEC          Alias    Vlan    Oper    Admin    Type    Asym PFC
-----------  ---------------  -------  -----  -----  -------------  ------  ------  -------  ------  ----------
  Ethernet0      25,26,27,28       1G   9100    N/A    fortyGigE0/0  routed      up       up     N/A         N/A
  Ethernet4      29,30,31,32       1G   9100    N/A    fortyGigE0/4  routed      up       up     N/A         N/A
  Ethernet8      33,34,35,36       1G   9100    N/A    fortyGigE0/8  routed      up       up     N/A         N/A
 Ethernet12      37,38,39,40      40G   9100    N/A   fortyGigE0/12  routed    down       up     N/A         N/A
```

- The administrative port refers to the settings and configurations applied by a network administrator to a specific port on a switch, while the operational port status reflects the current operational state of that port. Suppose one wants to enable a port and sets Admin Status to "up," but there is no cable connected to the port. So, it can never reach Oper Status "up" and will stay in Oper Status "down."

Step 2

By default, all interfaces are routed (L3) and IP is assigned to them. To check the status of IP addresses, use the following command given below:

- `show ip interfaces`

```
admin@sonic:~$ show ip interfaces
Interface    Master    IPv4 address/mask    Admin/Oper    BGP Neighbor    Neighbor IP
-----------  --------  -------------------  ------------  --------------  -------------
Ethernet0              10.0.0.0/31          up/up         ARISTA01T2      10.0.0.1
Ethernet4              10.0.0.2/31          up/up         ARISTA02T2      10.0.0.3
Ethernet8              10.0.0.4/31          up/up         ARISTA03T2      10.0.0.5
Ethernet12             10.0.0.6/31          up/up         ARISTA04T2      10.0.0.7
Ethernet16             10.0.0.8/31          up/up         ARISTA05T2      10.0.0.9
```

Step 2 (Continued)

Remove the IP addresses to make that interface a switch port (L2). For this, command is given below:

- `sudo config interface ip remove/add <interface_name> <ip_addr>`

```
admin@sonic:~$ sudo config interface ip remove Ethernet0 10.0.0.0/31
admin@sonic:~$ sudo config interface ip remove Ethernet4 10.0.0.2/31
admin@sonic:~$ sudo config interface ip remove Ethernet8 10.0.0.4/31
```

Note: It is better practice to save configurations after executing two or three commands.

Step 3

Now create VLANs for topology. Before creating VLANs, check VLAN table by using the following command given below:

- `show vlan brief`

```
admin@sonic:~$ show vlan brief
+-----------+--------------+---------+----------------+-------------+-----------------------+
| VLAN ID   | IP Address   | Ports   | Port Tagging   | Proxy ARP   | DHCP Helper Address   |
+===========+==============+=========+================+=============+=======================+
+-----------+--------------+---------+----------------+-------------+-----------------------+
```

In the above table, no VLAN is created, so create VLANs by using the following command given below:

- `sudo config vlan (add | del) <vlan_id>`

```
admin@sonic:~$ sudo config vlan add 100
admin@sonic:~$ sudo config vlan add 200
```

Step 4

Assign VLANs to ports. In SONiC, a port can be tagged or un-tagged. Trunk ports are usually tagged while access ports are un-tagged.

- `sudo config vlan member add/del [-u|--untagged] <vlan_id> <member_portname>`

```
admin@sonic:~$ sudo config vlan member add -u 100 Ethernet0
admin@sonic:~$ sudo config vlan member add -u 200 Ethernet4
admin@sonic:~$ sudo config vlan member add 100 Ethernet8
admin@sonic:~$ sudo config vlan member add 200 Ethernet8
```

```
admin@sonic:~$ show vlan brief
+-----------+--------------+-----------+----------------+-------------+-----------------------+
|   VLAN ID | IP Address   | Ports     | Port Tagging   | Proxy ARP   | DHCP Helper Address   |
+===========+==============+===========+================+=============+=======================+
|       100 |              | Ethernet0 | untagged       | disabled    |                       |
|           |              | Ethernet8 | tagged         |             |                       |
+-----------+--------------+-----------+----------------+-------------+-----------------------+
|       200 |              | Ethernet4 | untagged       | disabled    |                       |
|           |              | Ethernet8 | tagged         |             |                       |
+-----------+--------------+-----------+----------------+-------------+-----------------------+
```

Step 5

Repeat steps 1-4 for the switch S2.

Step 6

Assign IP addresses to hosts PC1 to PC4 by using command given below:

- `ip <ip_addr> <subnet-mask>`

```
PC1> ip 192.168.100.2/24 255.255.255.0
Checking for duplicate address...
PC1 : 192.168.100.2 255.255.255.0
```

After assigning IP addresses, check the status of IP address using command given below:

- `show ip`

```
PC1> sh ip

NAME        : PC1[1]
IP/MASK     : 192.168.100.2/24
GATEWAY     : 255.255.255.0
DNS         :
MAC         : 00:50:79:66:68:00
LPORT       : 10010
RHOST:PORT  : 127.0.0.1:10011
MTU         : 1500
```

Result

PC1 to PC3

Once the switches and hosts are configured, communication becomes possible among hosts within the same VLAN. As is evident from the provided figure below, PC1 is receiving a response from PC3, as both of them belong to VLAN 100. However, PC1 cannot send data to PC4 since they are in different VLANs. Furthermore, the TTL (Time-to-Live) value stays at 64 and remains unchanged because it's a Layer 2 feature. Therefore, the VLAN has been successfully configured.

```
PC1> ping 192.168.100.3

84 bytes from 192.168.100.3 icmp_seq=1 ttl=64 time=4.837 ms
84 bytes from 192.168.100.3 icmp_seq=2 ttl=64 time=5.454 ms
84 bytes from 192.168.100.3 icmp_seq=3 ttl=64 time=5.471 ms
84 bytes from 192.168.100.3 icmp_seq=4 ttl=64 time=5.299 ms
84 bytes from 192.168.100.3 icmp_seq=5 ttl=64 time=5.455 ms

PC1> ping 192.168.200.3

host (255.255.255.0) not reachable
```

PC2 to PC4

```
PC2> ping 192.168.200.3

84 bytes from 192.168.200.3 icmp_seq=1 ttl=64 time=4.839 ms
84 bytes from 192.168.200.3 icmp_seq=2 ttl=64 time=5.383 ms
84 bytes from 192.168.200.3 icmp_seq=3 ttl=64 time=5.685 ms
84 bytes from 192.168.200.3 icmp_seq=4 ttl=64 time=5.044 ms
84 bytes from 192.168.200.3 icmp_seq=5 ttl=64 time=5.301 ms

PC2> ping 192.168.100.3

host (255.255.255.0) not reachable
```

References

https://study-ccna.com/what-is-a-vlan/
https://github.com/sonic-net/sonic-utilities/blob/master/doc/Command-Reference.md

We connect ideas, people, and technology.

HARDWARE NATION®