Testing Guide to setup vTestBed & testing VLAN in SONiC

Aug 30, 2022

Revision History

Revision No.	Description	Editor	Date
1.0	Testing Guide to setup vTestBed & testing VLAN in SONiC	Humza Altaf	Aug 30, 2022
2.0	Testing Guide for VLAN in SONiC	Bushra Azmat Qureshi	March 23, 2023

Table of Contents

Introduction

This testing guide is to set up a testbed and then deploy and test the "VLAN" topology specifically for SONiC (Software for Open Networking in the Cloud) which is a free and open-source network operating system (OS) based on Linux that runs on switches from multiple vendors and ASICs and uses a key-value database (Redis). Initially developed by Microsoft and Open Compute Project and now the whole community is contributing to its development. SONiC decouples network software from the underlying hardware and is built on the SAI (Switch Abstraction Interface) switch-programming API.

With its incremental development through multiple vendors and other networking experts, all the files and resources are very widely dispersed in the repository and this is a proper guide to sift through it. This testing guide explains the step-by-step procedure to set up a testbed and then how to properly deploy topologies (VLAN topology - our main focus) and verify features by running necessary commands in SONiC CLI.

Testbed Setup

To deploy any topology, we will need a testbed that will set up the perfect environment where we can deploy our topologies. Now testbeds are of two types i.e., physical and virtual, depending on our availability of resources (switches, hosts, servers). If we have the required devices available for our topology, then we can go with a physical testbed otherwise we will opt for the virtual one.

SONiC Virtual Switch Testbed

To prepare the testbed, we need the following things:

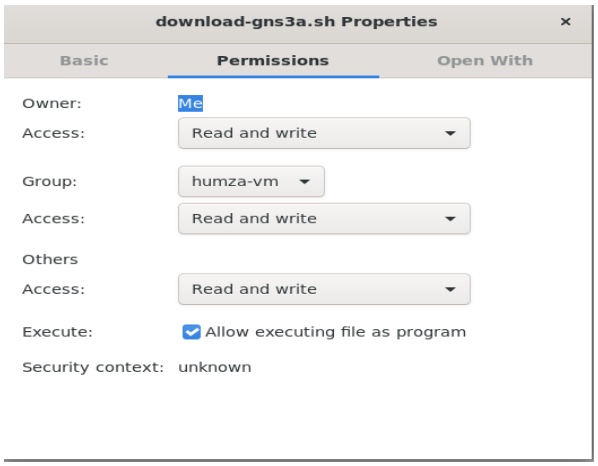
- GNS3
- Device image for GNS3
- SONiC image (.img file)
- The proper set of commands
- Only for SONiC versions>=201904

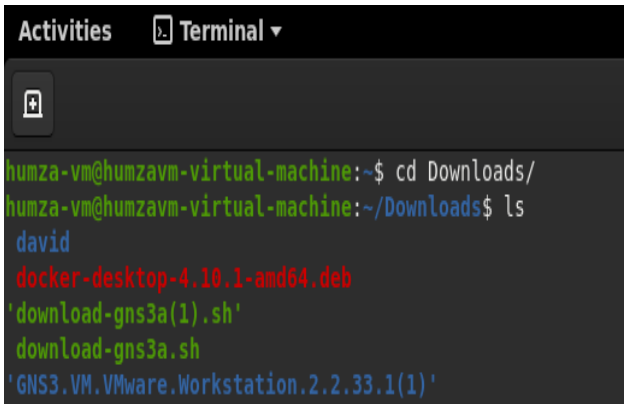
This document describes all steps one by one with necessary screenshots and links.

Device Image for GNS3

To deploy a SONiC image in GNS3, we need a device image. To download that image, the link is given here

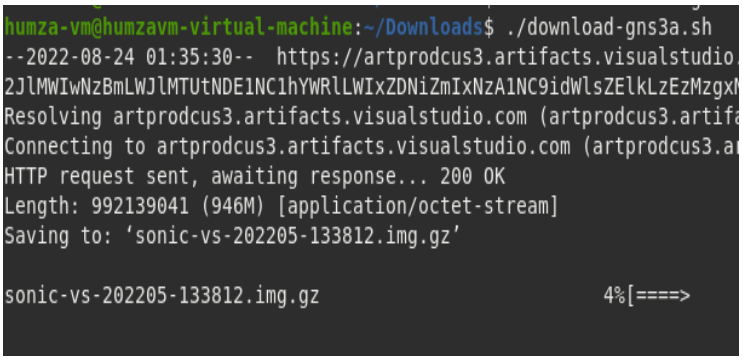
After downloading, some changings are required to make it compatible with GNS3. For Ubuntu, make it executable by following the path “right-click>properties>permissions>allow executing file as program”





After that make some changes to the file by using the command "sudo vi <filename>”. In our case, the command is “sudo vi download-gns3a.sh”. By using vim editor, press “i” to go to insert mode. SONiC image has different versions. In this testbed, version "202205" is used because it is the latest image. The figure, which is given below, explains where changes are made in the file.

- To run an executable file, write the following command "./download-gns3a.sh" in the terminal. Make sure that this command must be run in that directory in which "download-gns3a.sh" file is present.



After completing the above procedure, the device image as well as the zip file of SONiC (.img.gz file) will be installed. To obtain a SONiC image (.img file), extract the zip file.

SONiC image for GNS3

To download SONiC image (.img file) for GNS3, the procedure is given below:

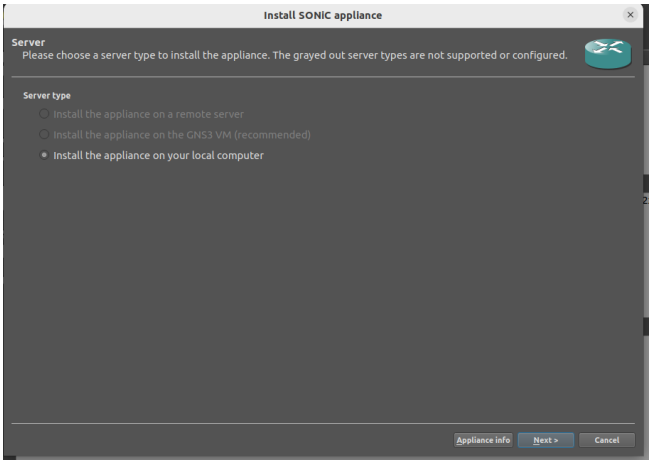
- By using the link which is given here, first zip file will be downloaded, and then extract the image file (.img)

There are many branches of SONiC at this site. In our case, “sonic-vs.img.gz” latest branch (202205) is used.

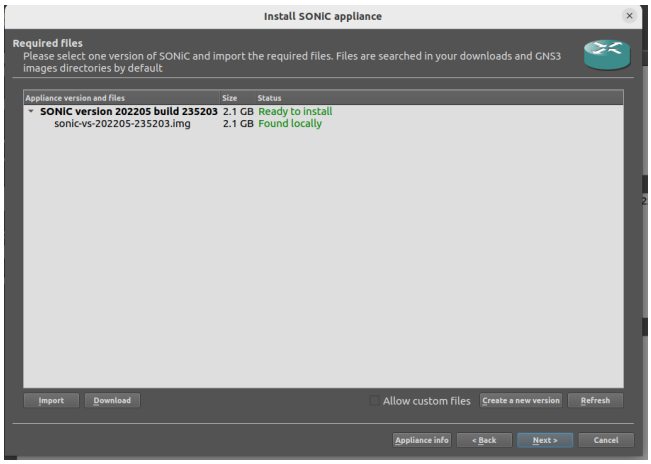
Importing device and SONiC image in GNS3

To import the device and SONiC image in GNS3 after creating a project, follow the path given below:

- file>import appliance
- After that, a pop-up menu is opened, Click on “Install the appliance on your local computer”.



- Now click on the “Next” button. It shows a SONiC image version downloaded previously. Now import the SONiC image by clicking on the "import" button, choose the required image, and then click on the "Next" button.



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.

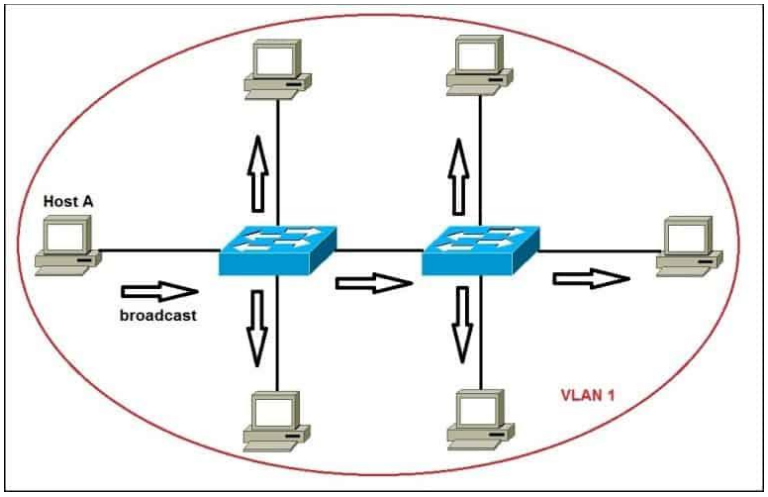


Fig: Topology with all hosts inside the same VLAN

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.

By placing interfaces on both switches into a separate VLAN, a broadcast from host A would reach only devices inside the same VLAN, since each VLAN is a separate broadcast domain. Hosts in other VLANs will not even be aware that the communication took place. This is shown in the picture below:

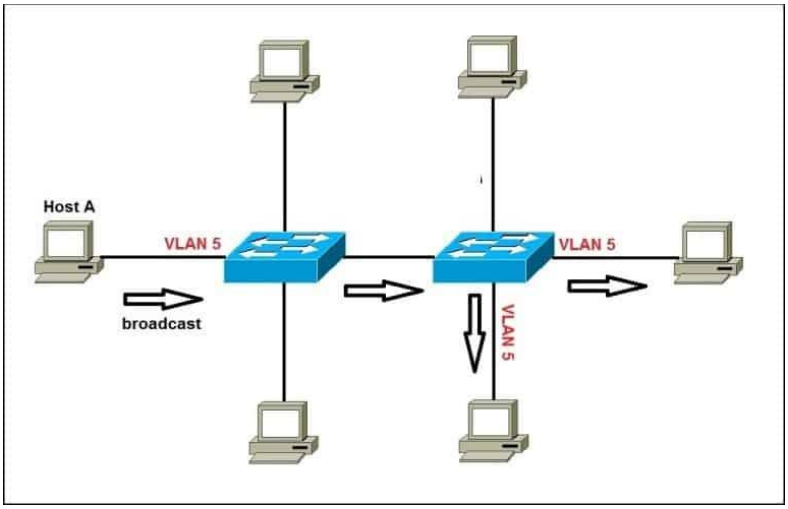


Fig: Topology hosts having different VLANs

NOTE: To reach hosts in a different VLAN, a router is needed.

Intra-Vlan

As the name suggests, “Intra” means “Inside”, Intra-VLAN communication refers to the ability of devices within the same VLAN to communicate with each other. Devices within the same VLAN are connected to the same broadcast domain, which means that they can communicate directly with each other without the need for routing.

To enable inter-VLAN communication, you will need to configure the devices with the appropriate IP addresses and subnet masks. The devices can then communicate with each other using these IP addresses.

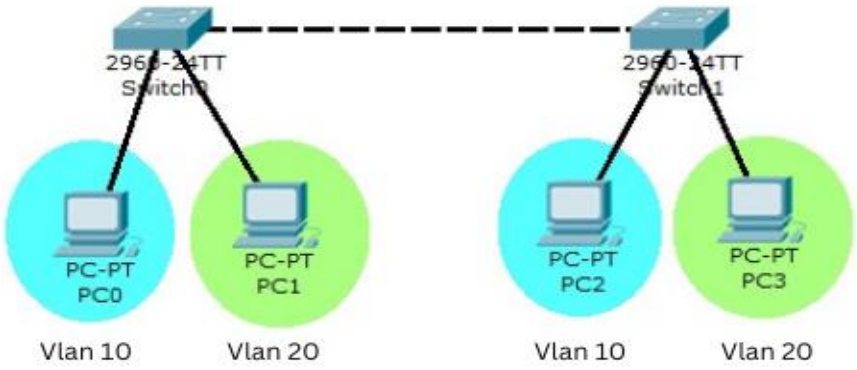


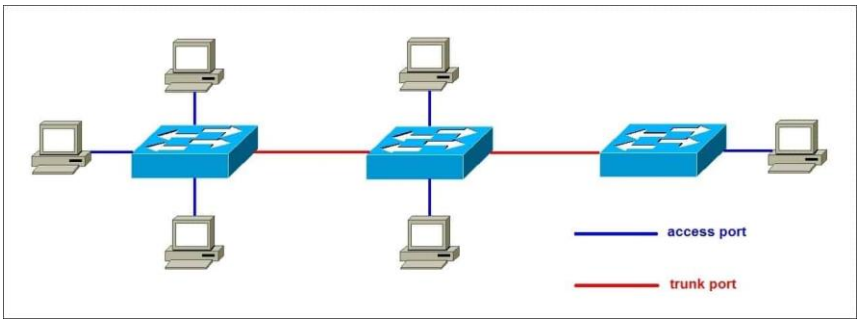
Fig: Intra-VLAN Topology using Multiple Switches

Trunk & Access Ports

If you intend to use VLANs in your network, you will need to configure some ports on a switch as access ports and as trunk ports. Here is a description of each port type:

Access port – a port that can be assigned to a single VLAN. This type of interface is configured on switch ports that are connected to end devices such as workstations, printers, or access points.

Trunk port – a port that is connected to another switch. This type of interface can carry traffic from multiple VLANs, thus enabling you to extend VLANs across your entire network. Frames are tagged by assigning a VLAN ID to each frame as they traverse between switches.



Network Topology

After importing images, consider this simple example. Suppose we have a network with two departments: marketing, and finance. 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, S-1 and S-2, and four hosts, PC1 through PC4. Now draw network topology in GNS3 using SONiC switches and hosts.

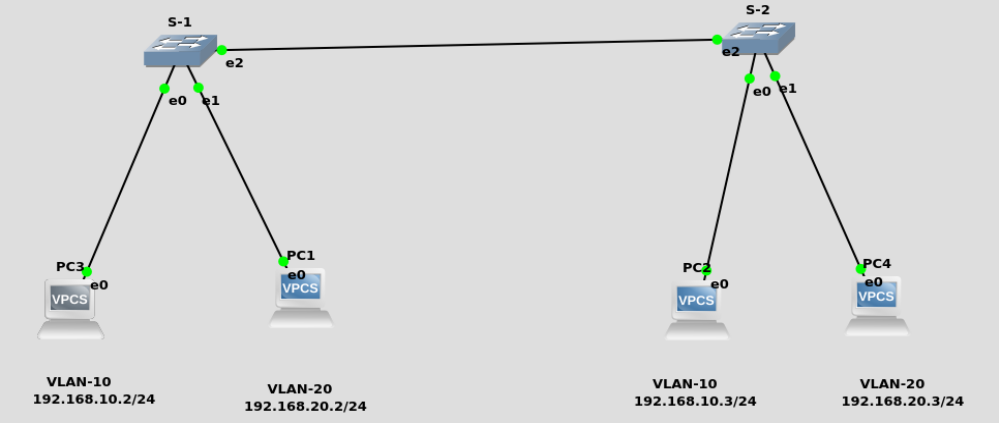


Fig: Network Topology

Note: Be patient while using SONiC CLI because it takes some time while showing results.

Port Breakout

In SONiC, all ports are integral of 4 like Ethernet0, Ethernet4, Ethernet8, and so on. In GNS3, when connections are made with a switch, a pop-up menu is opened and shows which port one wants to use. If Ethernet1 is selected in GNS3, it means that Ethernet4 will be used in SONiC CLI. Ethernet2 in GNS3 is mapped with Ethernet8 in SONiC CLI.

Configurations

For the above topology, all hosts and switches are first configured before sending traffic. First, switch (S-1) is configured and the same steps are repeated for the switch (S-2). Command Reference guide is also available on GitHub for SONiC, whose link is given here

Follow these steps to configure Switch-1.

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      40G   9100    N/A    fortyGigE0/0  routed    down       up     N/A         N/A
  Ethernet4      29,30,31,32      40G   9100    N/A    fortyGigE0/4  routed    down       up     N/A         N/A
  Ethernet8      33,34,35,36      40G   9100    N/A    fortyGigE0/8  routed    down       up     N/A         N/A
 Ethernet12      37,38,39,40      40G   9100    N/A   fortyGigE0/12  routed    down       up     N/A         N/A
 Ethernet16      45,46,47,48      40G   9100    N/A   fortyGigE0/16  routed    down       up     N/A         N/A
 Ethernet20      41,42,43,44      40G   9100    N/A   fortyGigE0/20  routed    down       up     N/A         N/A
 Ethernet24          1,2,3,4      40G   9100    N/A   fortyGigE0/24  routed    down       up     N/A         N/A
 Ethernet28          5,6,7,8      40G   9100    N/A   fortyGigE0/28  routed    down       up     N/A         N/A
 Ethernet32     13,14,15,16      40G   9100    N/A   fortyGigE0/32  routed    down       up     N/A         N/A
 Ethernet36      9,10,11,12      40G   9100    N/A   fortyGigE0/36  routed    down       up     N/A         N/A
 Ethernet40     17,18,19,20      40G   9100    N/A   fortyGigE0/40  routed    down       up     N/A         N/A
 Ethernet44     21,22,23,24      40G   9100    N/A   fortyGigE0/44  routed    down       up     N/A         N/A
 Ethernet48     53,54,55,56      40G   9100    N/A   fortyGigE0/48  routed    down       up     N/A         N/A
 Ethernet52     49,50,51,52      40G   9100    N/A   fortyGigE0/52  routed    down       up     N/A         N/A
 Ethernet56     57,58,59,60      40G   9100    N/A   fortyGigE0/56  routed    down       up     N/A         N/A
 Ethernet60     61,62,63,64      40G   9100    N/A   fortyGigE0/60  routed    down       up     N/A         N/A
 Ethernet64     69,70,71,72      40G   9100    N/A   fortyGigE0/64  routed    down       up     N/A         N/A
```

- Administrative ports (Admin) are used for device management and configuration, and allow administrators to remotely access and configure the device. Operational ports (Oper), on the other hand, are used for regular network traffic, such as passing data between devices on the network.
- In the above figure, all interfaces are operationally "down" but administratively "up". In most cases, operational status is usually down but sometimes it is "up" after running devices in GNS3.

Step-2

- There are two methods to change operational status, which are given below:

1st Method

To "up" the operational status of an interface, use the following command:

- sudo config interface startup <interface_name> (for 201904+ version)
- admin@sonic:~$ sudo config interface startup Ethernet64

2nd Method

In this method, interface status can be changed by configuring “config_db” and the path is /etc/sonic. To configure "config_db”, command is given below:

sudo vi config_db.json

Note: It is highly recommended that, first save all the configurations and then reload it using the “sudo config reload” command.

By following the above commands, make changes in "config_db” and then save it.

Note: Using the first method to change interface status is recommended. Sometimes interface status remains down after using 1st command. So, change the status by using config_db.

Step-3

By default, all interfaces are routed (L3) and IP is assigned to them. Remove the IP to make that interface a switch port (L2). For this, commands are given below:

- sudo config interface ip remove/add <interface_name> <ip_addr>
- admin@sonic:~$ sudo config interface ip remove Ethernet64 10.11.12.13/31

IP must be removed from all those interfaces, which are to be used in network topology.

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

Step-4

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

show vlan brief

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

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

- sudo config vlan (add | del) <vlan_id>
- admin@sonic:~$ sudo config vlan add 10

```
+---------+--------------+---------+----------------+
| VLAN ID | IP Address   | Ports   | Port Tagging   |
+=========+==============+=========+================+
|      10 |              |         |                |
+---------+--------------+---------+----------------+
|      20 |              |         |                |
```

Step-5

Assign VLANs to interfaces. In SONiC, an interface can be tagged or un-tagged. Trunk ports should be 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 30 Ethernet8
  This command will add Ethernet8 as a member of vlan 30 and it is tagged.

- admin@sonic:~$ sudo config vlan member add -u 10 Ethernet0

This command will add Ethernet0 as a member of vlan 10 and it is un-tagged.

```
+---------+-------------+----------+---------------+---------+
| VLAN ID | IP Address  | Ports    | Port Tagging  | Proxy ARP |
+=========+=============+==========+===============+=========+
|      10 |             | Ethernet0 | untagged      | disabled |
|         |             | Ethernet8 | tagged        |          |
+---------+-------------+----------+---------------+---------+
|      20 |             | Ethernet4 | untagged      | disabled |
|         |             | Ethernet8 | tagged        |          |
+---------+-------------+----------+---------------+---------+
```

Step-6

Repeat steps 1-5 for the switch (s-2).

Step-7

Assign IP addresses to hosts given in network topology.

```
Checking for duplicate address...
PC1 : 192.168.10.2 255.255.255.0 gateway 192.168.10.1

PC1> ip 192.168.10.2/24 192.168.10.1
Checking for duplicate address...
PC1 : 192.168.10.2 255.255.255.0 gateway 192.168.10.1

PC1> save
Saving startup configuration to startup.vpc
.  done

PC1> write
Saving startup configuration to startup.vpc
.  done

PC1>
```

Note: It is highly recommended to save configurations in the host using the save command.

Result

After configuring the switches and hosts, hosts in the same VLAN can send traffic. In the figure below, it is clearly seen that PC1 can send traffic to PC4 because both are in the same VLAN i.e VLAN20, while it can not send traffic to PC3 due to a different VLAN. So, VLAN is successfully configured in the topology.

```
PC1> ping 192.168.20.3

84 bytes from 192.168.20.3 icmp_seq=1 ttl=64 time=9.538 ms
84 bytes from 192.168.20.3 icmp_seq=2 ttl=64 time=8.827 ms
84 bytes from 192.168.20.3 icmp_seq=3 ttl=64 time=9.021 ms
84 bytes from 192.168.20.3 icmp_seq=4 ttl=64 time=8.555 ms
84 bytes from 192.168.20.3 icmp_seq=5 ttl=64 time=8.631 ms

PC1> ping 192.168.10.3

host (255.255.255.0) not reachable

PC1>
```

References

- https://study-ccna.com/what-is-a-vlan/
- https://support.huawei.com/enterprise/en/doc/EDOC1000142081/9c0373e/intra-vlan-communication
- https://study-ccna.com/access-and-trunk-ports/