Secure VLAN Networks

Setup

In the realm of computer networks, network administrators often encounter complex scenarios that require innovative solutions. One such solution involves the use of Virtual Local Area Networks (VLANs) to enhance network segmentation and security. In this context, we will explore a setup using GNS3 and VMware® Workstation Pro to emulate a network environment, along with VLAN Access-Lists (VACLs) and Private VLANs (PVLANs) for improved control and isolation.

Resources

GNS3 2.2.19

VMware® Workstation 16 Pro. – GNS3 VM

Windows 10 Pro. - Host machine

Network

GNS3 with 2 Virtual Network Adapter.

- Custom (VMNET 1)
- Custom (VMNET 2)

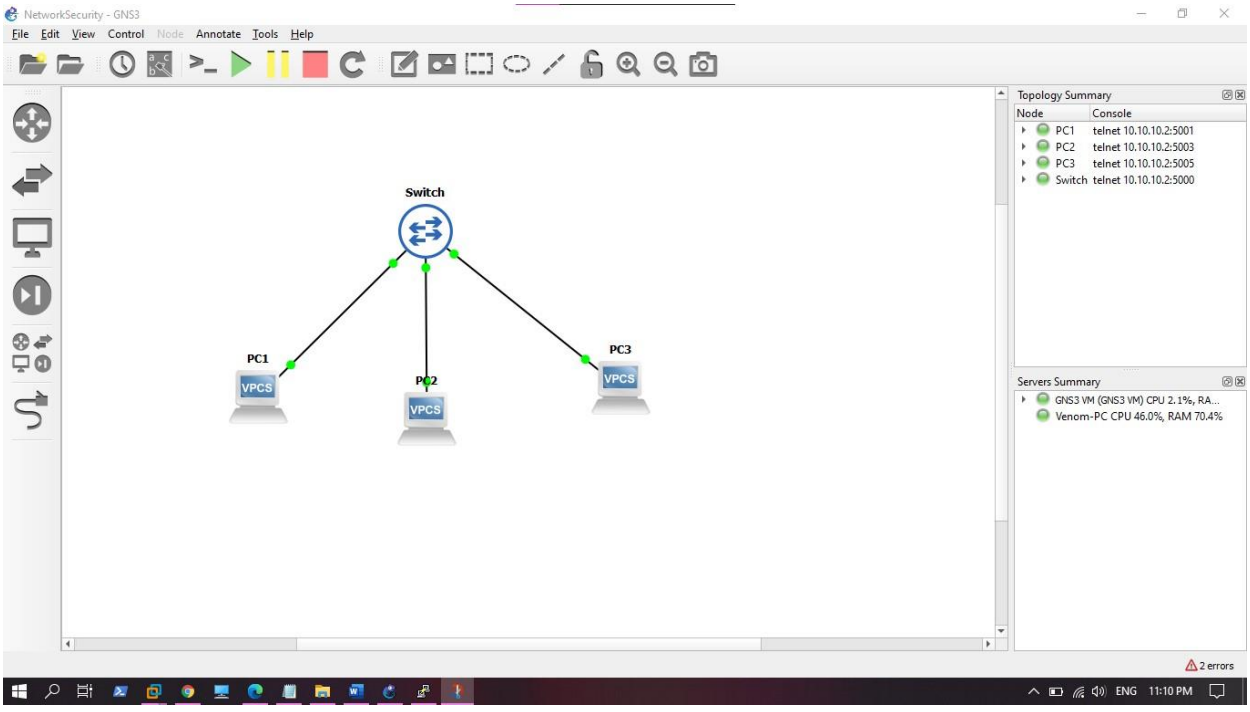
VLAN Access-List (VACL)

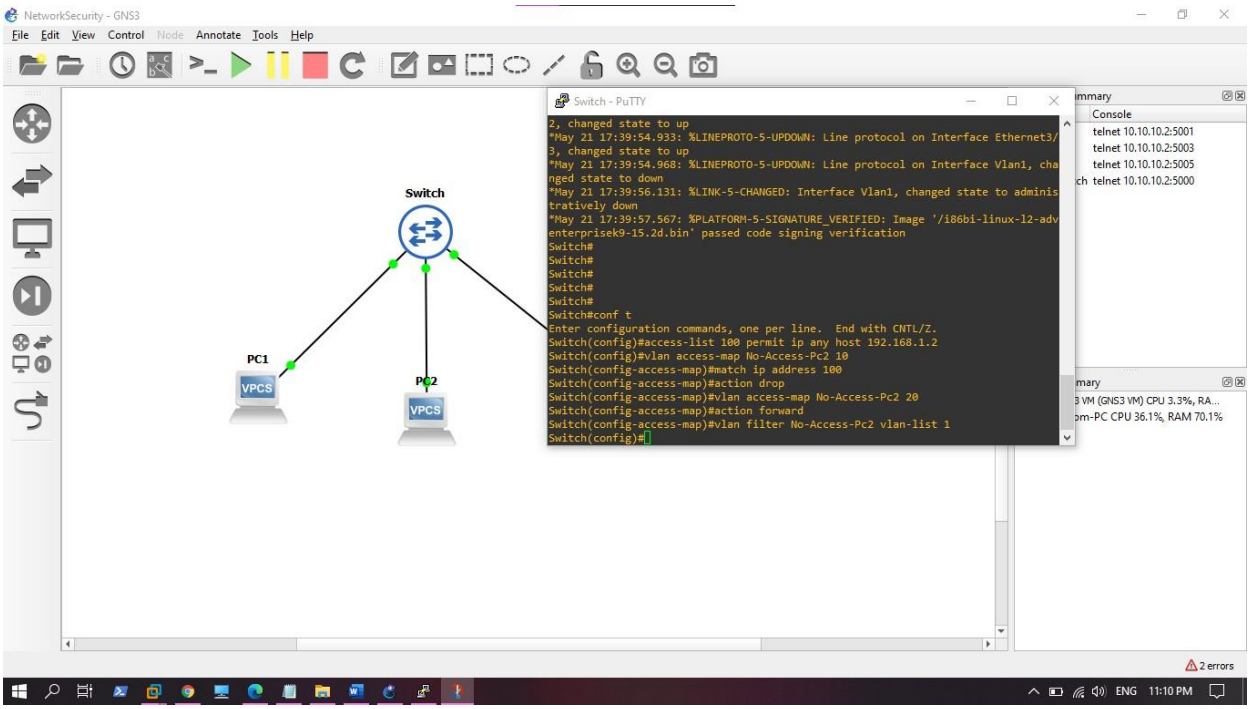
access-list 100 permit ip any host 192.168.1.2
vlan access-map No-Access-Pc2 10
match ip address 100
action drop
vlan access-map No-Access-Pc2 20
action forward
vlan filter No-Access-Pc2 vlan-list 1

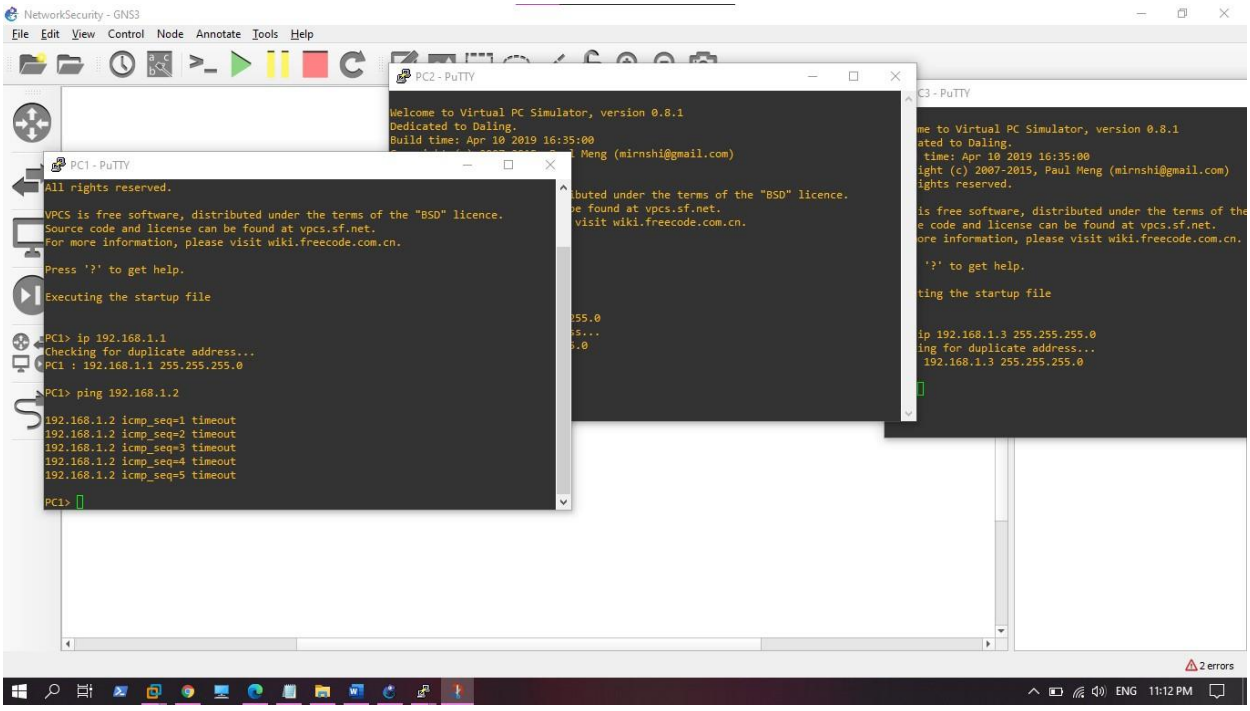
• Sequence number 10 will look for traffic that matches access-list 100. All traffic that is permitted in access-list 100 will match here. The action is to drop this traffic.

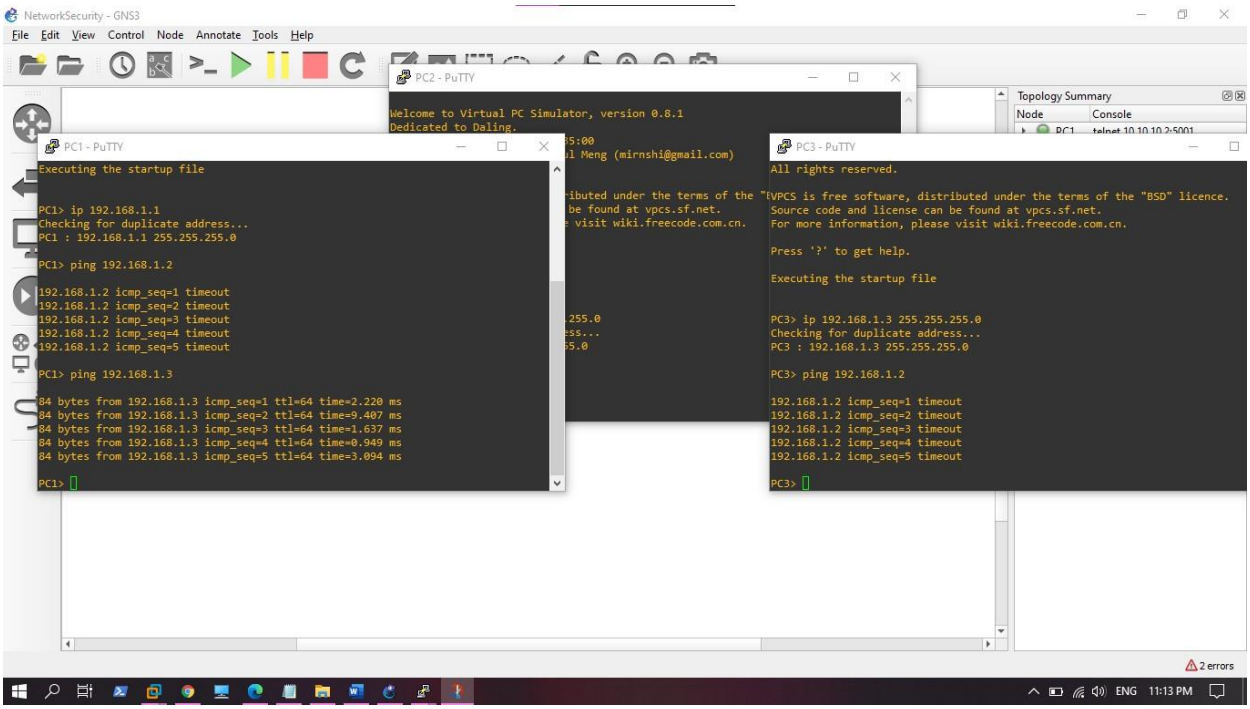
• Sequence number 20 doesn't have a match statement so everything will match, the action is to forward traffic.

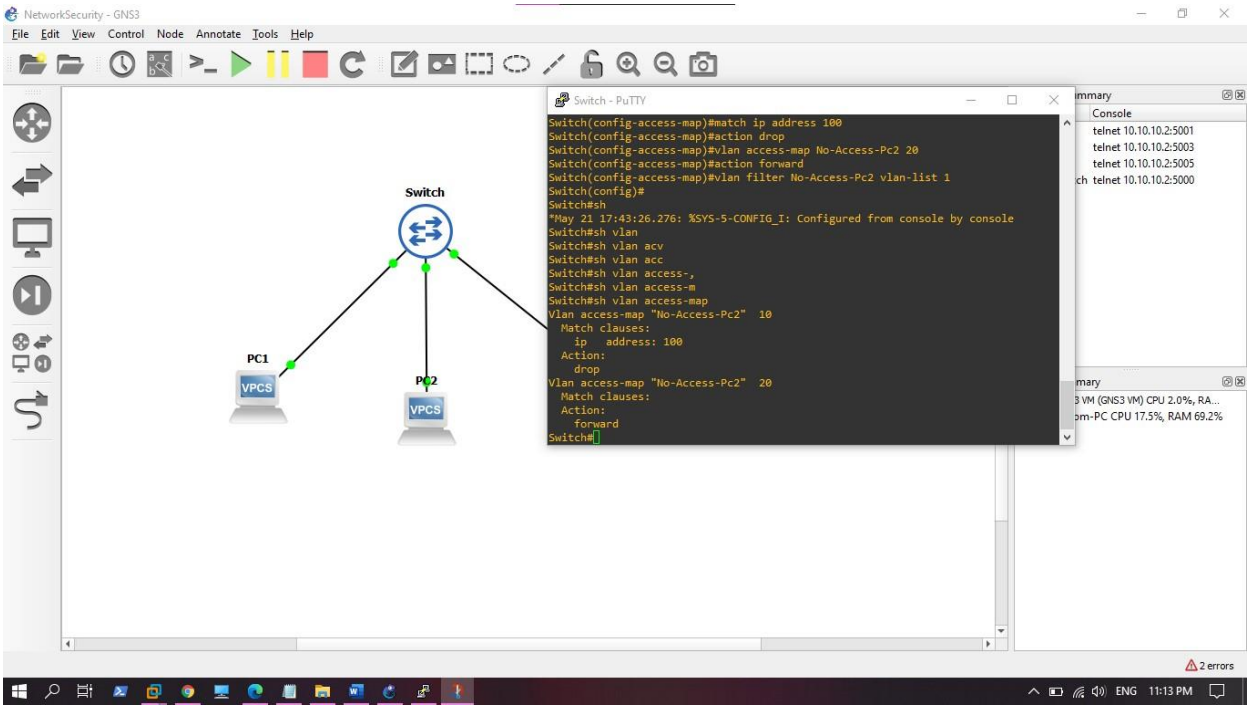
As a result, all traffic from any host to destination IP address 192.168.1.2 will be dropped, everything else will be forwarded.




NetworkSecurity - GNS3
File Edit View Control Node Annotate Tools Help
Switch - PuTTY
2, changed state to up
*May 21 17:39:54.933: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet3/
3, changed state to up
*May 21 17:39:54.968: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, cha
nged state to down
*May 21 17:39:56.131: %LINK-5-CHANGED: Interface Vlan1, changed state to adminis
tratively down
*May 21 17:39:57.567: %PLATFORM-5-SIGNATURE_VERIFIED: Image '/i86bi-linux-l2-adv
enterprisek9-15.2d.bin' passed code signing verification
Switch#
Switch#
Switch#
Switch#
Switch#
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#access-list 100 permit ip any host 192.168.1.2
Switch(config)#vlan access-map No-Access-Pc2 10
Switch(config-access-map)#match ip address 100
Switch(config-access-map)#action drop
Switch(config-access-map)#vlan access-map No-Access-Pc2 20
Switch(config-access-map)#action forward
Switch(config-access-map)#vlan filter No-Access-Pc2 vlan-list 1
Switch(config)#
Switch
PC1
VPCS
PC2
VPCS
Console
telnet 10.10.10.2:5001
telnet 10.10.10.2:5003
telnet 10.10.10.2:5005
telnet 10.10.10.2:5000
2 errors
ENG 11:10 PM


NetworkSecurity - GNS3
File Edit View Control Node Annotate Tools Help
PC1 - PuTTY
All rights reserved.
VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.
Press '?' to get help.
Executing the startup file
PC1> ip 192.168.1.1
Checking for duplicate address...
PC1 : 192.168.1.1 255.255.255.0
PC1> ping 192.168.1.2
192.168.1.2 icmp_seq=1 timeout
192.168.1.2 icmp_seq=2 timeout
192.168.1.2 icmp_seq=3 timeout
192.168.1.2 icmp_seq=4 timeout
192.168.1.2 icmp_seq=5 timeout
PC1>
PC2 - PuTTY
Welcome to Virtual PC Simulator, version 0.8.1
Dedicated to Daling.
Build time: Apr 10 2019 16:35:00
Meng (mirnshi@gmail.com)
visit wiki.freecode.com.cn.
2 errors
ENG 11:12 PM


NetworkSecurity - GNS3
File Edit View Control Node Annotate Tools Help
PC2 - PuTTY
Welcome to Virtual PC Simulator, version 0.8.1
Dedicated to Daling.
PC1 - PuTTY
Executing the startup file
PC1> ip 192.168.1.1
Checking for duplicate address...
PC1 : 192.168.1.1 255.255.255.0
PC1> ping 192.168.1.2
192.168.1.2 icmp_seq=1 timeout
192.168.1.2 icmp_seq=2 timeout
192.168.1.2 icmp_seq=3 timeout
192.168.1.2 icmp_seq=4 timeout
192.168.1.2 icmp_seq=5 timeout
PC1> ping 192.168.1.3
84 bytes from 192.168.1.3 icmp_seq=1 ttl=64 time=2.220 ms
84 bytes from 192.168.1.3 icmp_seq=2 ttl=64 time=9.407 ms
84 bytes from 192.168.1.3 icmp_seq=3 ttl=64 time=1.637 ms
84 bytes from 192.168.1.3 icmp_seq=4 ttl=64 time=0.949 ms
84 bytes from 192.168.1.3 icmp_seq=5 ttl=64 time=3.094 ms
PC1>
PC3 - PuTTY
All rights reserved.
VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.
Press '?' to get help.
Executing the startup file
PC3> ip 192.168.1.3 255.255.255.0
Checking for duplicate address...
PC3 : 192.168.1.3 255.255.255.0
PC3> ping 192.168.1.2
192.168.1.2 icmp_seq=1 timeout
192.168.1.2 icmp_seq=2 timeout
192.168.1.2 icmp_seq=3 timeout
192.168.1.2 icmp_seq=4 timeout
192.168.1.2 icmp_seq=5 timeout
PC3>
Topology Summary
Node
Console
2 errors
ENG 11:13 PM


NetworkSecurity - GNS3
File Edit View Control Node Annotate Tools Help
Switch - PuTTY
Switch(config-access-map)#match ip address 100
Switch(config-access-map)#action drop
Switch(config-access-map)#vlan access-map No-Access-Pc2 20
Switch(config-access-map)#action forward
Switch(config-access-map)#vlan filter No-Access-Pc2 vlan-list 1
Switch(config)#
Switch#sh
*May 21 17:43:26.276: %SYS-5-CONFIG_I: Configured from console by console
Switch#sh vlan
Switch#sh vlan acv
Switch#sh vlan acc
Switch#sh vlan access-,
Switch#sh vlan access-m
Switch#sh vlan access-map
Vlan access-map "No-Access-Pc2" 10
Match clauses:
ip address: 100
Action:
drop
Vlan access-map "No-Access-Pc2" 20
Match clauses:
Action:
forward
Switch#
Switch
PC1
VPCS
PC2
VPCS
Console
telnet 10.10.10.2:5001
telnet 10.10.10.2:5003
telnet 10.10.10.2:5005
telnet 10.10.10.2:5000
2 errors
ENG 11:13 PM

Private VLAN

Community VLAN: All ports within the community VLAN are able to communicate with each other and the promiscuous port.

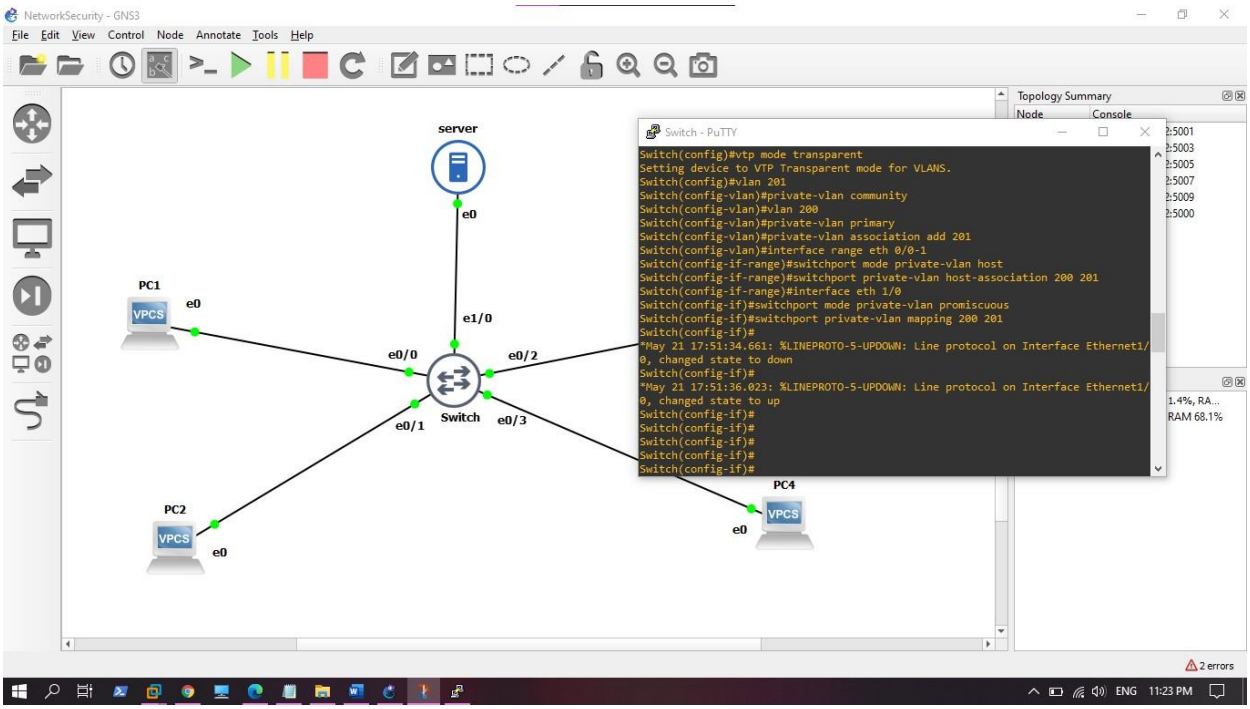
Isolated VLAN: All ports within the isolated VLAN are unable to communicate with each other but they can communicate with the promiscuous port.

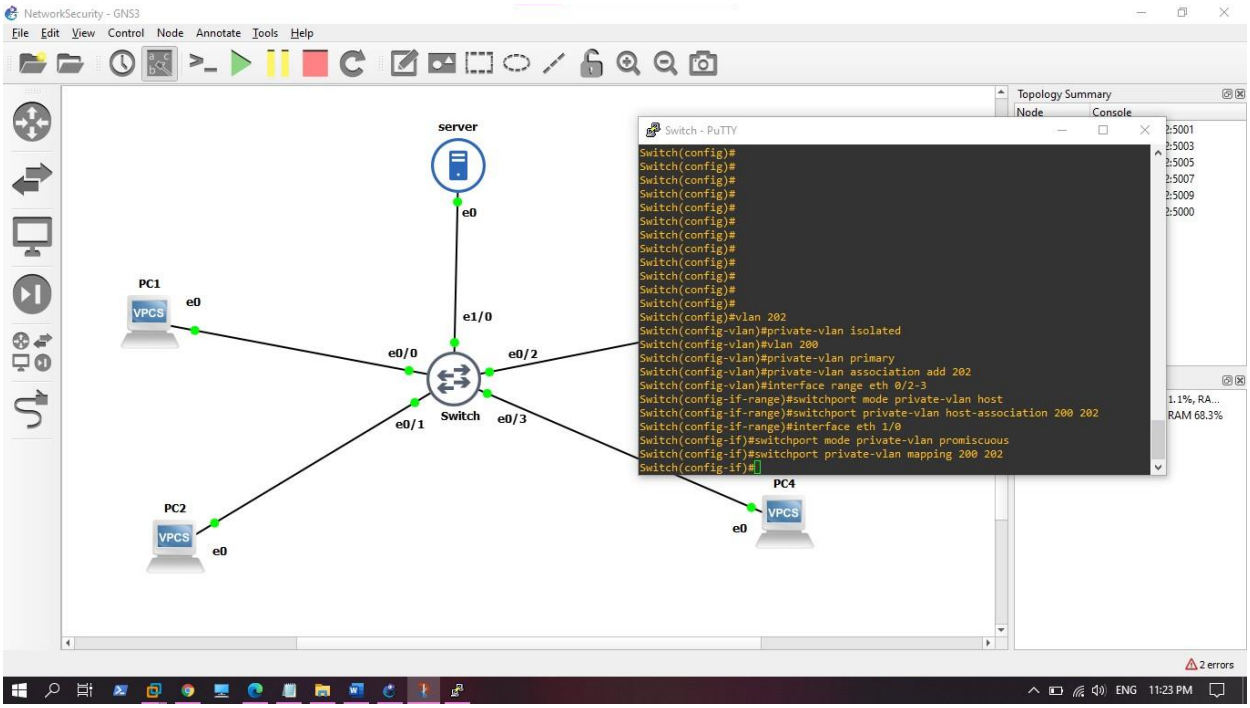
Community VLAN

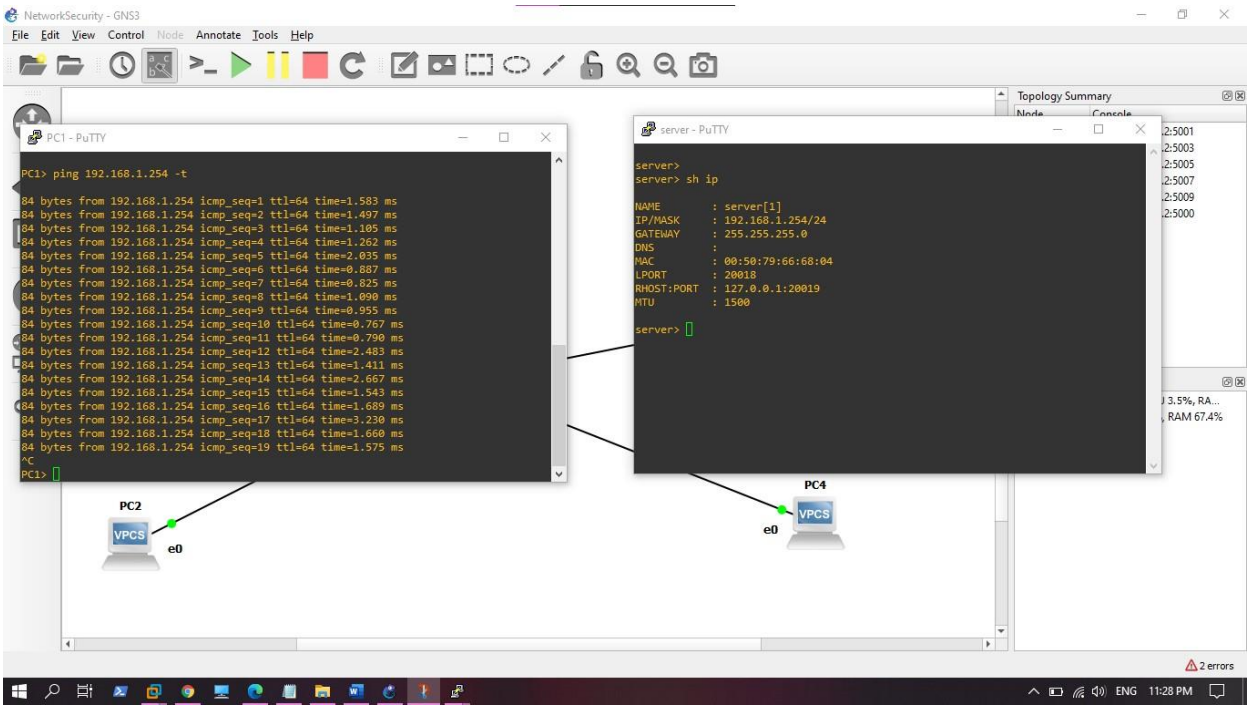
```
vtp mode transparent
vlan 201
private-vlan community
vlan 200
private-vlan primary
private-vlan association add 201
interface range eth 0/0-1
switchport mode private-vlan host
switchport private-vlan host-association 200 201
interface eth 1/0
switchport mode private-vlan promiscuous
switchport private-vlan mapping 200 201
```

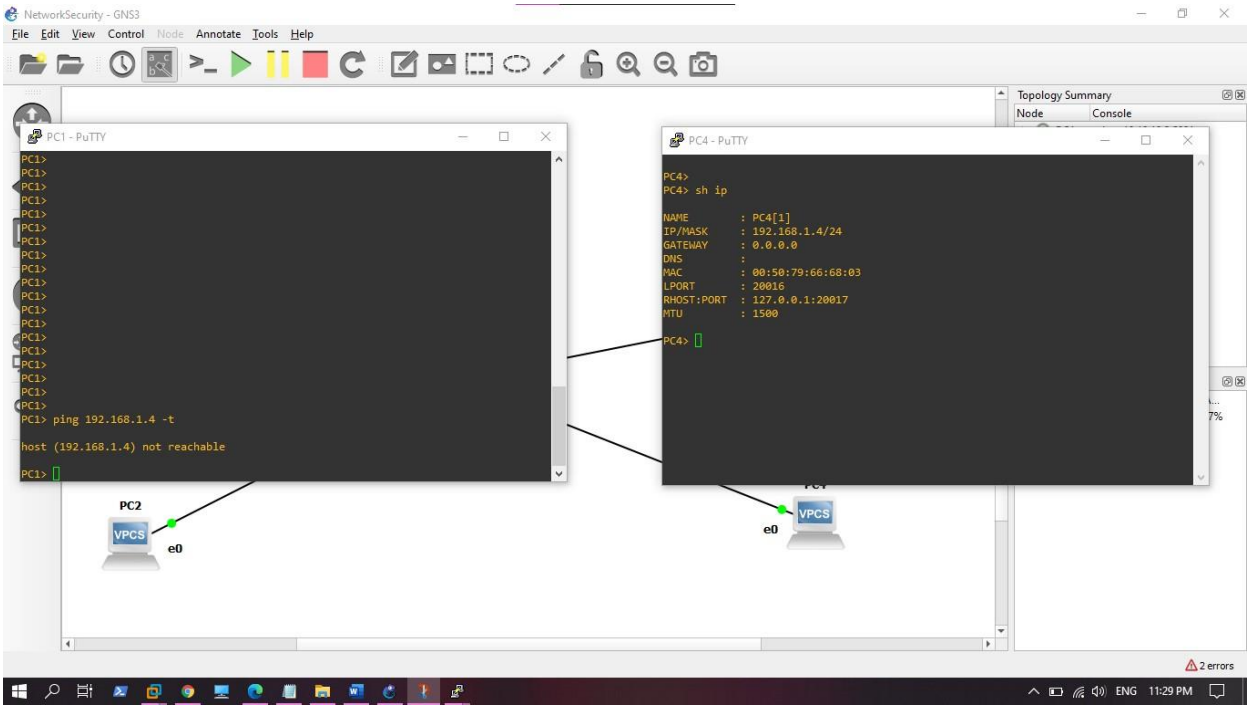
Isolated VLAN

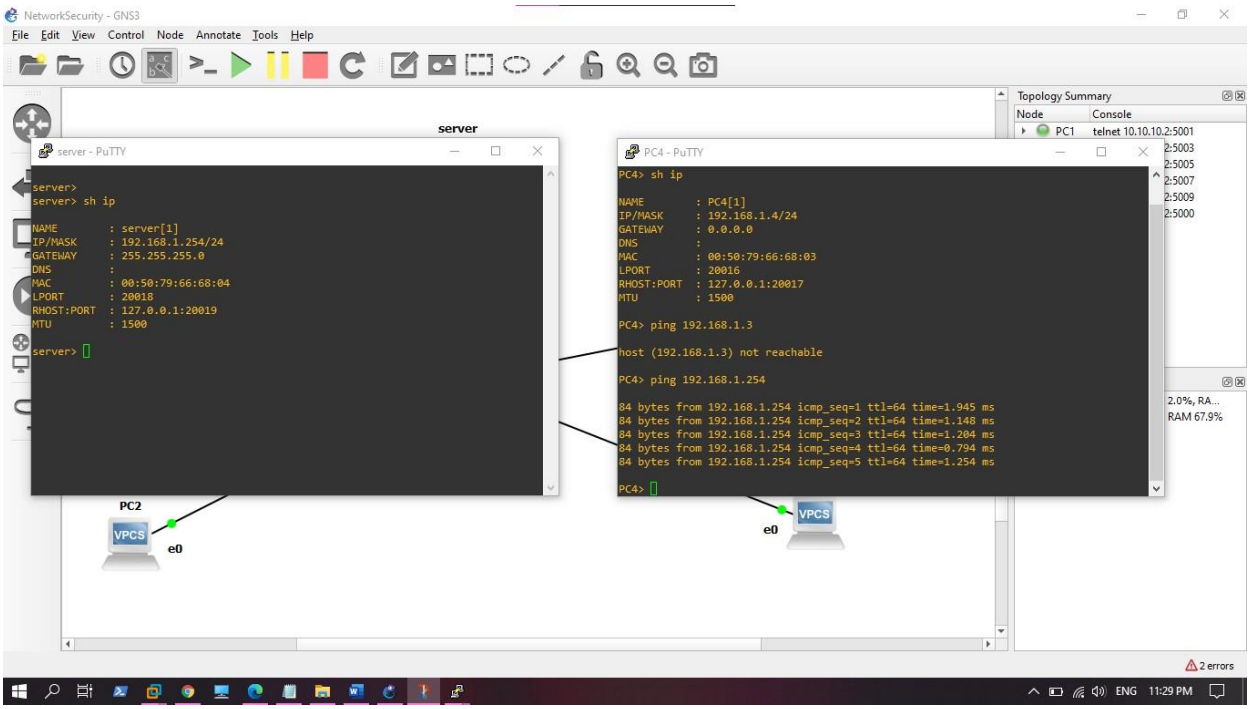
```
vlan 202
private-vlan isolated
vlan 200
private-vlan primary
private-vlan association add 202
interface range eth 0/2-3
switchport mode private-vlan host
switchport private-vlan host-association 200 202
interface eth 1/0
switchport mode private-vlan promiscuous
switchport private-vlan mapping 200 202
```

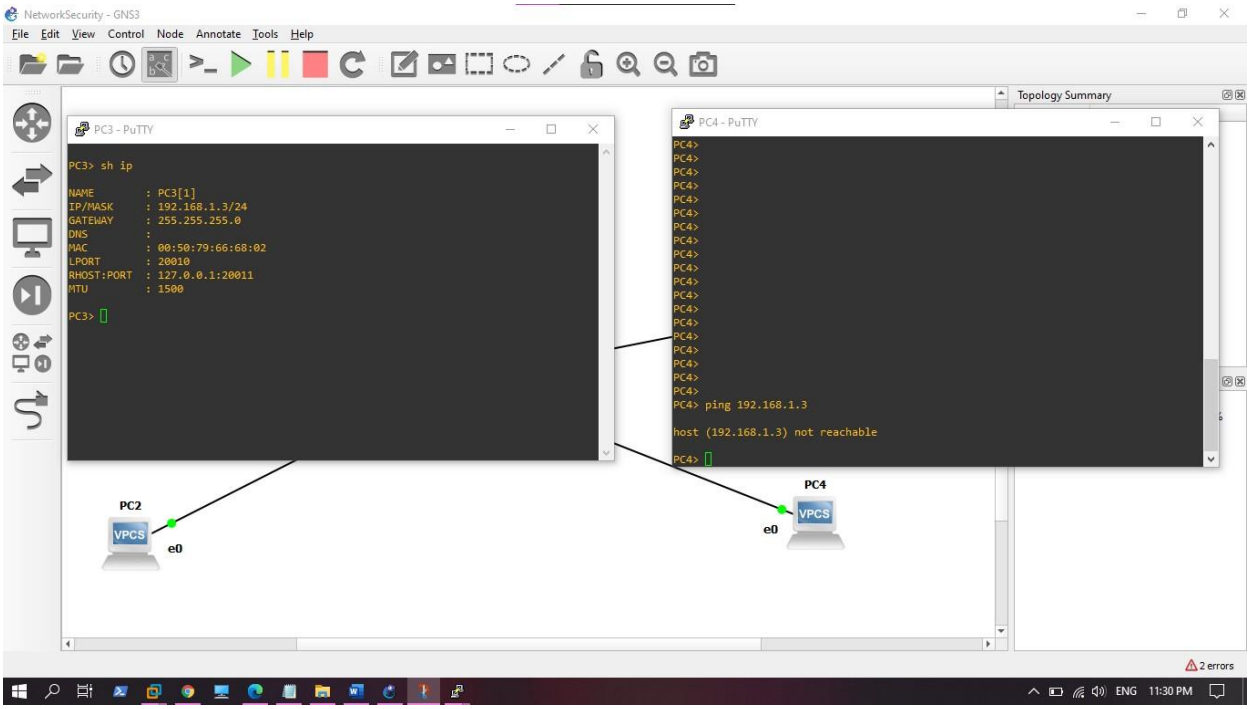

NetworkSecurity - GNS3
File Edit View Control Node Annotate Tools Help
Topology Summary
Node Console
server
e0
PC1
VPCS
e0
e1/0
e0/0
e0/2
Switch
e0/1
e0/3
PC2
VPCS
e0
PC4
VPCS
e0
Switch - PuTTY
Switch(config)#vtp mode transparent
Setting device to VTP Transparent mode for VLANS.
Switch(config)#vlan 201
Switch(config-vlan)#private-vlan community
Switch(config-vlan)#vlan 200
Switch(config-vlan)#private-vlan primary
Switch(config-vlan)#private-vlan association add 201
Switch(config-vlan)#interface range eth 0/0-1
Switch(config-if-range)#switchport mode private-vlan host
Switch(config-if-range)#switchport private-vlan host-association 200 201
Switch(config-if-range)#interface eth 1/0
Switch(config-if)#switchport mode private-vlan promiscuous
Switch(config-if)#switchport private-vlan mapping 200 201
Switch(config-if)#
*May 21 17:51:34.661: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/
0, changed state to down
Switch(config-if)#
*May 21 17:51:36.023: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/
0, changed state to up
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#
2 errors
ENG 11:23 PM


NetworkSecurity - GNS3
File Edit View Control Node Annotate Tools Help
Topology Summary
Node Console
server
e0
PC1
VPCS
e0
e1/0
e0/0
e0/2
Switch
e0/1
e0/3
PC2
VPCS
e0
PC4
VPCS
e0
Switch - PuTTY
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#vlan 202
Switch(config-vlan)#private-vlan isolated
Switch(config-vlan)#vlan 200
Switch(config-vlan)#private-vlan primary
Switch(config-vlan)#private-vlan association add 202
Switch(config-vlan)#interface range eth 0/2-3
Switch(config-if-range)#switchport mode private-vlan host
Switch(config-if-range)#switchport private-vlan host-association 200 202
Switch(config-if-range)#interface eth 1/0
Switch(config-if)#switchport mode private-vlan promiscuous
Switch(config-if)#switchport private-vlan mapping 200 202
Switch(config-if)#
2 errors
ENG 11:23 PM


NetworkSecurity - GNS3
File Edit View Control Node Annotate Tools Help
PC1 - PuTTY
PC1> ping 192.168.1.254 -t
84 bytes from 192.168.1.254 icmp_seq=1 ttl=64 time=1.583 ms
84 bytes from 192.168.1.254 icmp_seq=2 ttl=64 time=1.497 ms
84 bytes from 192.168.1.254 icmp_seq=3 ttl=64 time=1.105 ms
84 bytes from 192.168.1.254 icmp_seq=4 ttl=64 time=1.262 ms
84 bytes from 192.168.1.254 icmp_seq=5 ttl=64 time=2.035 ms
84 bytes from 192.168.1.254 icmp_seq=6 ttl=64 time=0.887 ms
84 bytes from 192.168.1.254 icmp_seq=7 ttl=64 time=0.825 ms
84 bytes from 192.168.1.254 icmp_seq=8 ttl=64 time=1.090 ms
84 bytes from 192.168.1.254 icmp_seq=9 ttl=64 time=0.955 ms
84 bytes from 192.168.1.254 icmp_seq=10 ttl=64 time=0.767 ms
84 bytes from 192.168.1.254 icmp_seq=11 ttl=64 time=0.790 ms
84 bytes from 192.168.1.254 icmp_seq=12 ttl=64 time=2.483 ms
84 bytes from 192.168.1.254 icmp_seq=13 ttl=64 time=1.411 ms
84 bytes from 192.168.1.254 icmp_seq=14 ttl=64 time=2.667 ms
84 bytes from 192.168.1.254 icmp_seq=15 ttl=64 time=1.543 ms
84 bytes from 192.168.1.254 icmp_seq=16 ttl=64 time=1.689 ms
84 bytes from 192.168.1.254 icmp_seq=17 ttl=64 time=3.230 ms
84 bytes from 192.168.1.254 icmp_seq=18 ttl=64 time=1.660 ms
84 bytes from 192.168.1.254 icmp_seq=19 ttl=64 time=1.575 ms
^C
PC1>
server - PuTTY
server>
server> sh ip
NAME : server[1]
IP/MASK : 192.168.1.254/24
GATEWAY : 255.255.255.0
DNS :
MAC : 00:50:79:66:68:04
LPORT : 20018
RHOST:PORT : 127.0.0.1:20019
MTU : 1500
server>
Topology Summary
Node Console
PC2
VPCS
e0
PC4
VPCS
e0
2 errors
ENG 11:28 PM


NetworkSecurity - GNS3
File Edit View Control Node Annotate Tools Help
PC1 - PuTTY
PC1> ping 192.168.1.4 -t
host (192.168.1.4) not reachable
PC1>
PC4 - PuTTY
PC4>
PC4> sh ip
NAME : PC4[1]
IP/MASK : 192.168.1.4/24
GATEWAY : 0.0.0.0
DNS :
MAC : 00:50:79:66:68:03
LPORT : 20016
RHOST:PORT : 127.0.0.1:20017
MTU : 1500
PC4>
Topology Summary
Node Console
PC2
VPCS
e0
VPCS
e0
2 errors
ENG 11:29 PM





In summary, this network setup showcases the effective utilization of VLANs, VACLs, and PVLANs to achieve enhanced network segmentation, security, and traffic control. This configuration allows network administrators to design and manage intricate network.