NetSim®

Accelerate Network R & D

Advanced Routing

A Network Simulation & Emulation Software

By

The information contained in this document represents the current view of TETCOS LLP on the issues discussed as of the date of publication. Because TETCOS LLP must respond to changing market conditions, it should not be interpreted to be a commitment on the part of TETCOS LLP, and TETCOS LLP cannot guarantee the accuracy of any information presented after the date of publication.

This manual is for informational purposes only.

The publisher has taken care in the preparation of this document but makes no expressed or implied warranty of any kind and assumes no responsibility for errors or omissions. No liability is assumed for incidental or consequential damages in connection with or arising out of the use of the information contained herein.

Warning! DO NOT COPY

Contact us at

TETCOS LLP
214, 39th A Cross, 7th Main, 5th Block Jayanagar,
Bangalore - 560 041, Karnataka, INDIA.
Phone: +91 80 26630624
E-Mail: sales@tetcos.com
Visit: www.tetcos.com

Contents

1 Access Control Lists (ACLs)

1.1 Introduction

Access Control Lists (ACLs) are filters that routers use to control which routing updates or packets are permitted or denied in or out of a network. An ACL contains a sequential list of permit or deny statements that apply to IP packets originating from or destined to specific hosts, IP addresses, and upper-layer IP protocols.

An ACL tells the router what types of packets to permit or deny. The router using the ACL does the following when it finds packets inbound to or outbound from a network:

- If the router finds packets categorized against the permit statements, the router forwards the packets to the next hop in the network.
- If the router finds packets categorized against the deny statements, the router blocks and drops the packets at the router interface. The packets cannot reach the intended destination host or IP address.
- ACLs control traffic in one direction at a time on an interface. To allow inbound and outbound traffic from a host, IP address, or protocol, two ACLs are required: one inbound and one outbound.
- The precedence of the ACL commands is from top to bottom.

For example, if an ACL is configured in a router as follows:

```
PERMIT OUTBOUND TCP ANY ANY 0 0 3
PERMIT INBOUND TCP ANY ANY 0 0 3
DENY BOTH ANY ANY ANY 0 0 3
```

The permit statements override the deny statements. Outbound TCP packets through interface 3 are permitted first, followed by inbound TCP packets through interface 3. All other packets through the third interface are denied in both directions.

2 Virtual LAN (VLAN)

2.1 Introduction

VLAN stands for Virtual Local Area Network. It is used in switches and operates at Layer 2 and Layer 3. A VLAN is a group of hosts that communicate as though they were attached to the same broadcast domain regardless of their physical location.

For example, all workstations and servers used by a particular workgroup can be connected to the same VLAN regardless of their physical connections to the network or the fact that they might be intermingled with other teams. VLANs have the same attributes as physical LANs, but you can group end stations even if they are not physically located on the same LAN segment.

A VLAN behaves like a LAN in all respects but with additional flexibility. By using VLAN technology, it is possible to subdivide a single physical switch into several logical switches.

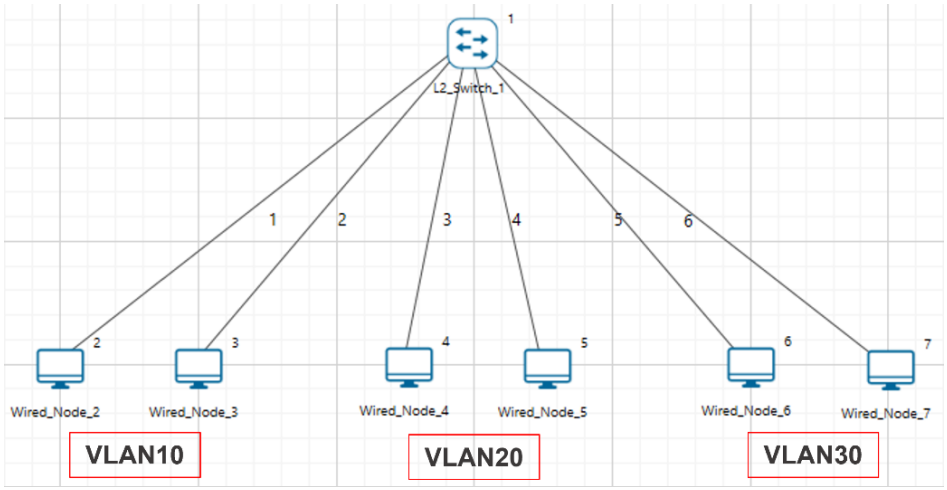

Figure 2-1: *Virtual local area network (VLAN)*

Switches implement VLANs by adding a VLAN tag to Ethernet frames as they enter the switch. The VLAN tag contains the VLAN ID and other information determined by the interface from which the frame enters the switch.

Packets destined for stations that do not belong to the VLAN must be forwarded through a router.

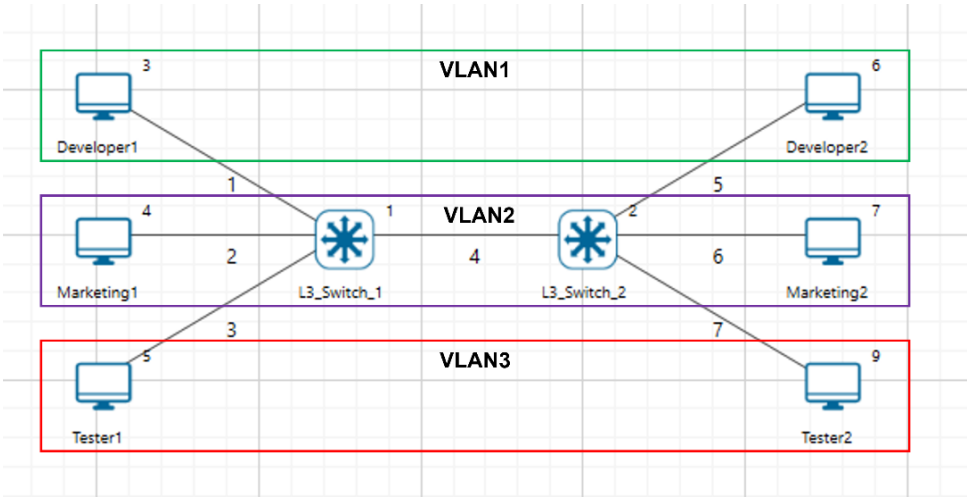

Figure 2-2: *Hosts in one VLAN need to communicate with hosts in another VLAN*

2.1.1 When do we need a VLAN?

You need to consider using VLANs in any of the following situations:

- You have more than 200 devices on your LAN.
- You have a lot of broadcast traffic on your LAN.
- Groups of users need more security or are being slowed down by too many broadcasts.
- Groups of users need to be on the same broadcast domain because they are running the same applications.

VLAN ID VLANs are identified by a VLAN ID, a number between 0 and 4095. Each port on a switch or router can be assigned to be a member of a VLAN.

On a switch, traffic sent to a port that is a member of VLAN 2 may be forwarded to any other VLAN 2 port on the switch, and it can also travel across a trunk port to another switch and be forwarded to all VLAN 2 ports on that switch.

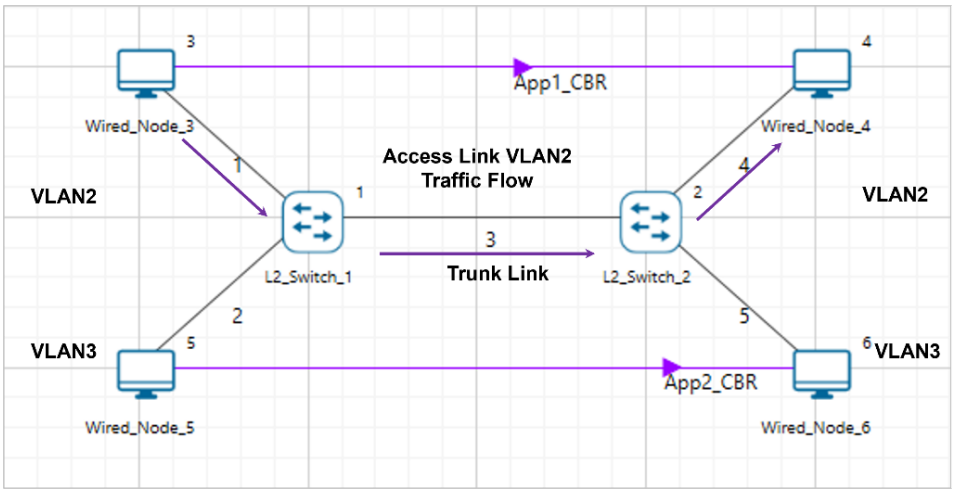

Figure 2-3: *Understanding access and trunk links*

2.1.2 Understanding Access and Trunk Links

The links connecting the end devices are called access links. These links usually carry the data VLAN information. The link between switches is called a trunk link. It carries packets from all the VLANs.

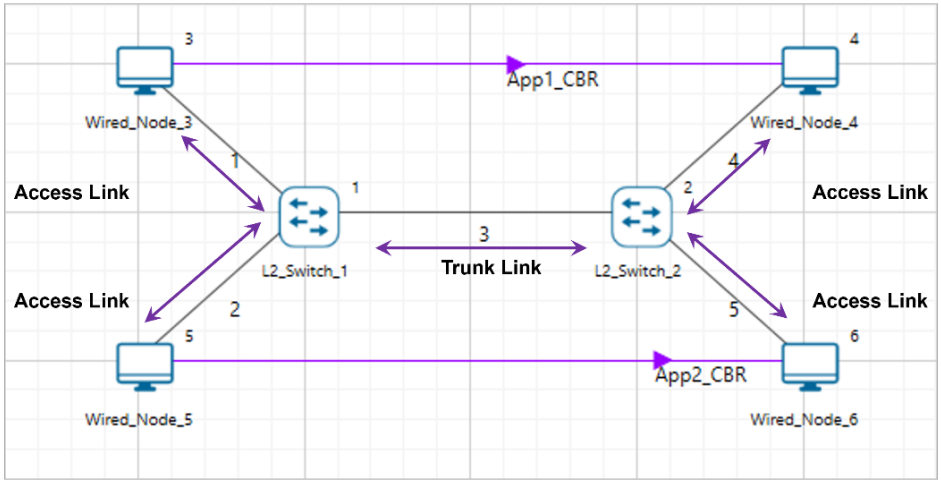

Figure 2-4: *Understanding access and trunk links*

Access Link Access link connection is the connection where a switch port is connected with a device that has a standardized Ethernet NIC. Access link connections can only be assigned to a single VLAN.

Trunk Link Trunk link connection is the connection where a switch port is connected with a device that can understand multiple VLANs. Usually, trunk link connection is used to connect

two switches.

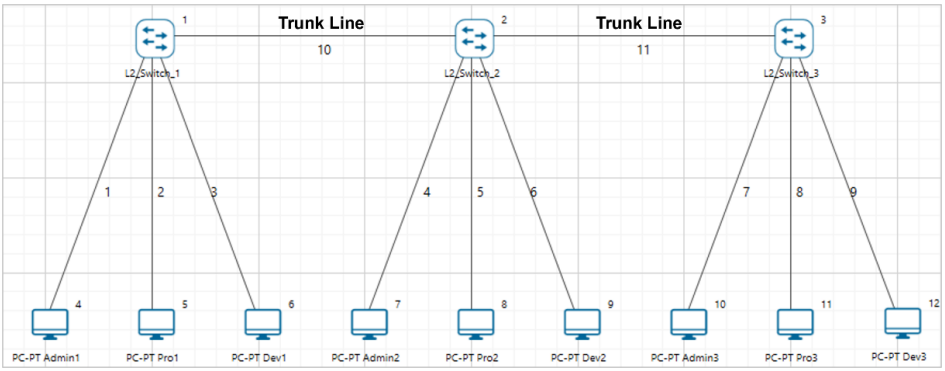

Figure 2-5: *Understand multiple VLANs*

3 Public IP Address & NAT (Network Address Translation)

3.1 Introduction

3.1.1 Public Address

A public IP address is assigned to every computer that connects to the Internet, where each IP is unique. This addressing scheme makes it possible for computers to find each other online and exchange information.

3.1.2 Private Address

An IP address is considered private if the IP number falls within one of the address ranges reserved for private networks such as a Local Area Network. The Internet Assigned Numbers Authority (IANA) has reserved the following three blocks for private networks:

Table 3-1: *Private IP address table*

Class	Starting IP address	Ending IP address	No. of hosts
A	10.0.0.0	10.255.255.255	16,777,216
B	172.16.0.0	172.31.255.255	1,048,576
C	192.168.0.0	192.168.255.255	65,536

Private IP addresses are used for numbering computers in a private network. Devices with private IP addresses cannot connect directly to the Internet; connectivity is typically provided through a router or another device that supports Network Address Translation.

If the private network is connected to the Internet, then each computer may use a private IP within the local network while the gateway uses a public IP for communication over the Internet.

3.1.3 Network address translation (NAT)

NAT is the virtualization of Internet Protocol addresses. NAT helps improve security and decreases the number of IP addresses an organization needs.

A device configured with NAT will have at least one interface to the inside network and one to the outside network. When a packet leaves the domain, NAT translates the locally significant source address into a globally unique address.

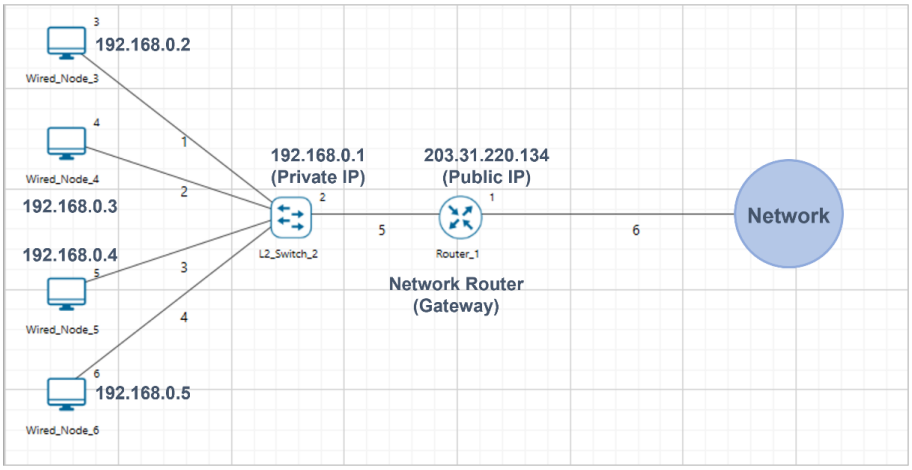

Figure 3-1: *NAT implementation*

NAT is secure because it hides the internal network from the Internet. In the simple example shown above, all hosts inside the network use private addresses while the public-facing interface uses a real Internet address.

4 Featured Examples

4.1 Access Control Lists (ACLs) Examples

4.1.1 ACL Example

This example models a network and simulates an ACL to understand how ACL filters inbound and outbound traffic at a router interface.

The network model consists of:

- Two subnets with 2 wired nodes, 1 router each, and 3 applications.
- ACLs with both permit and deny rules defined on the router interfaces.

NetSim uses the following directions for ACL simulations:

- The direction of the ACL is set to both, meaning the ACL applies to both inbound and outbound traffic.
- The direction of the ACL is set to inbound, meaning the ACL applies to inbound traffic only.
- The direction of the ACL is set to outbound, meaning the ACL applies to outbound traffic only.

Open NetSim, select Examples -> Advanced routing -> ACL Configuration, and click the tile in the middle panel to load the example as shown below.

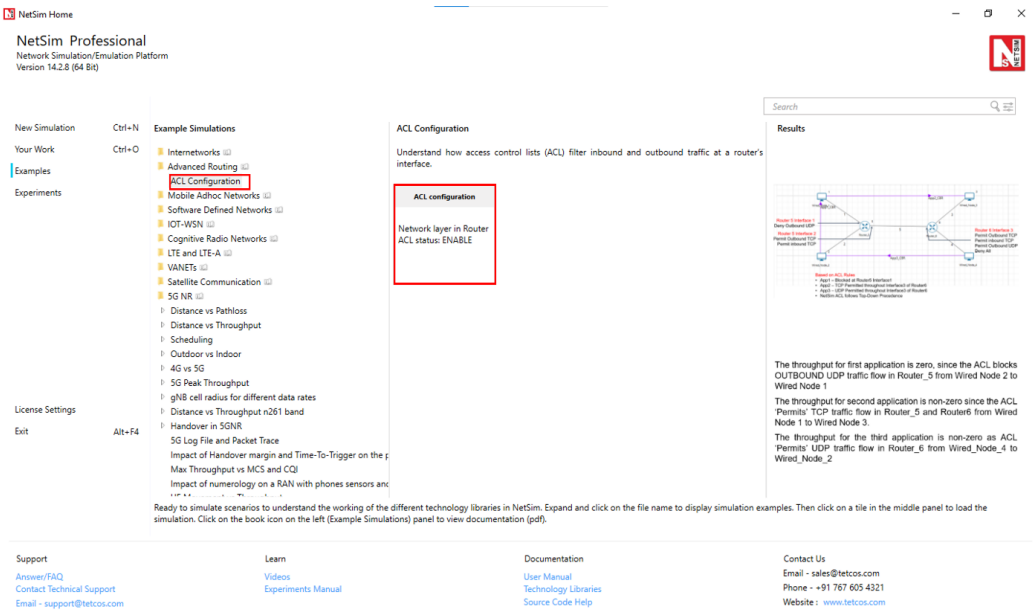

Figure 4-1: *List of scenarios for the example of ACL configuration*

The following network diagram illustrates what the NetSim UI displays when you open the example configuration file for ACL.

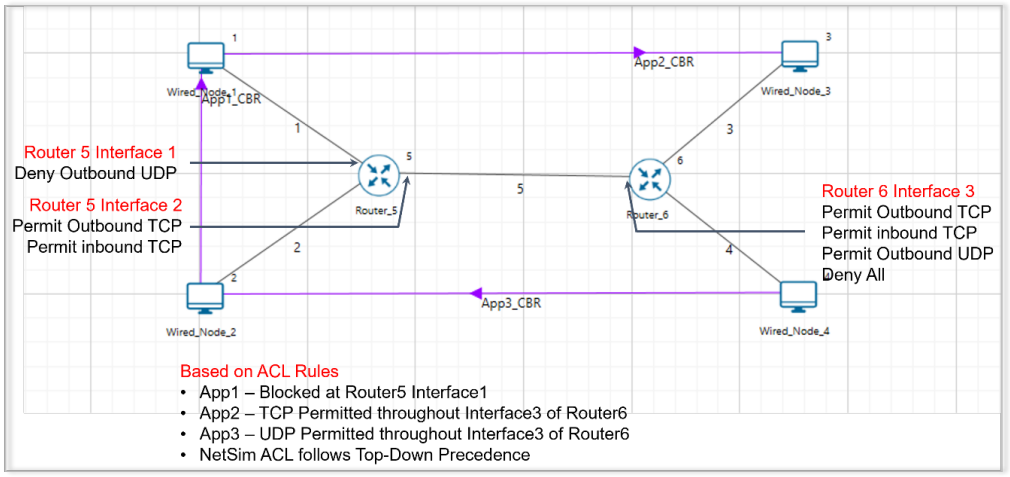

Figure 4-2: *Network setup for studying the ACL configuration*

1. ACL is enabled in the network layer of Router 5 and configured as shown below.

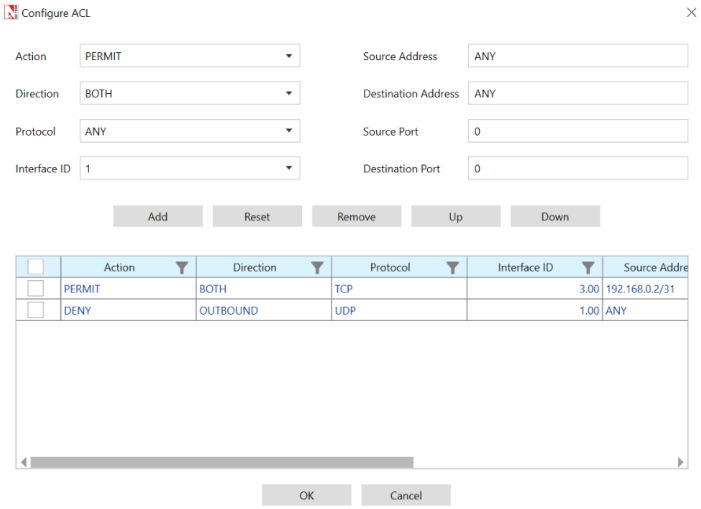

Figure 4-3: *ACL configuration for Router 5*

2. ACL is enabled in the network layer of Router 6 and configured as shown below.

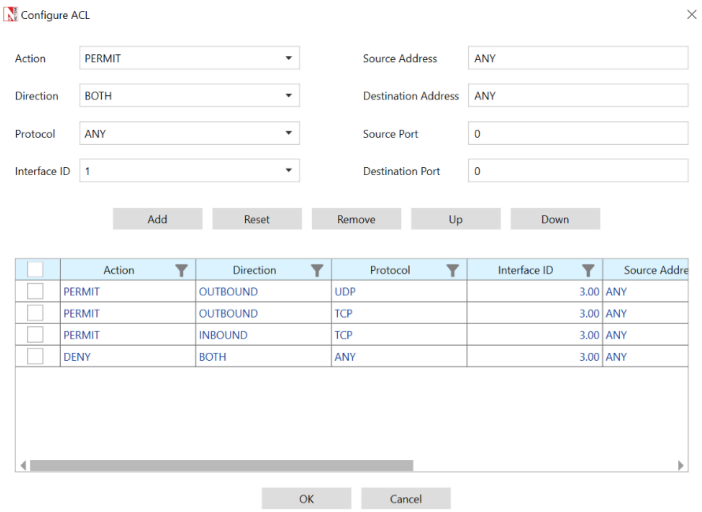

Figure 4-4: *ACL configuration for Router 6*

3. Set the transport protocol as UDP for APP_1_CBR and APP_3_CBR.
4. Set the transport protocol as TCP for APP_2_CBR.
5. Run the simulation for 10 seconds and observe the throughput obtained for the three applications.

4.1.2 Result and Observations

Application Metrics

End-to-end performance of applications running across the network.

Application ID	Application N	Source ID	Destination ID	Throughput (M	Delay (µs)	Jitter (µs)	Packets Gener	Packets Receiv
1	App1_CBR	2	1	0.000000	0.000000	0.000000	500	0
2	App2_CBR	1	3	0.558304	26817.456362	4114.302997	500	478
3	App3_CBR	4	2	0.582832	376.281924	0.001928	500	499

Figure 4-5: *Application metrics table in the result window*

The throughput for the first application is zero, since the ACL blocks outbound UDP traffic flow in Router 5 from Wired Node 2 to Wired Node 1.

The throughput for the second application is non-zero, since the ACL permits TCP traffic flow in Router 5 and Router 6 from Wired Node 1 to Wired Node 3.

The throughput for the third application is non-zero, since the ACL permits UDP traffic flow in Router 6 from Wired Node 4 to Wired Node 2.

5 Advanced Routing Experiments in NetSim

Apart from examples, in-built experiments are also available in NetSim. Examples help the user understand the working of features in NetSim, while experiments are designed to help users learn networking concepts through simulation.

1. Understanding VLAN operation in L2 and L3 switches
2. Understanding access and trunk links in VLANs
3. Understanding Public IP Address and NAT (Network Address Translation)
4. Understanding the working of basic networking commands such as Ping, Route Add/Delete/Print, and ACL

6 Reference Documents

1. IEEE 802.1Q for Virtual LAN
2. IETF 7761 for Protocol Independent Multicast – Sparse Mode (PIM-SM)
3. RFC 2236 for Internet Group Management Protocol, Version 2

7 Latest FAQs

Up-to-date FAQs on NetSim's Advanced Routing library are available at:

https://tetcos.freshdesk.com/support/solutions/folders/14000113123