NetSim®

Accelerate Network R & D

Advanced Routing

A Network Simulation & Emulation Software

By

TETCOS LLP

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

Table of 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 (rules) that apply to IP packets originating or destined to 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 inbound or outbound categorized against the permit statements, the router forwards the packets to the next hop in the network.
- If the router finds packets inbound or outbound categorized against the deny statements, the router blocks and drops the packets at the router's 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 for a protocol, you must create two ACLs, one for each direction, one for inbound and one for outbound traffic.
- The precedence of the ACL commands is from top to bottom.

For example, If ACL is configured in 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

Then, the Permit statements will over-ride the deny statements. That is, Outbound TCP packets from Router through interface 3 will be permitted first, after that, the Inbound TCP packets to Router through interface 3 will be permitted. All other packets through the third interface of Router will be denied in both directions.

2 Virtual LAN (VLAN)

2.1 Introduction

VLAN is called as virtual local area network, used in Switches and it operates at layer2 and Layer3. A VLAN, is a group of hosts which communicate as if they were attached to the same broadcast domain, regardless of their physical location.

For example, all workstations and servers used by a particular workgroup team 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 just 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. VLANs are implemented by using the appropriate switch configuration commands to create the VLANs and assign specific switch interfaces to the desired VLAN.

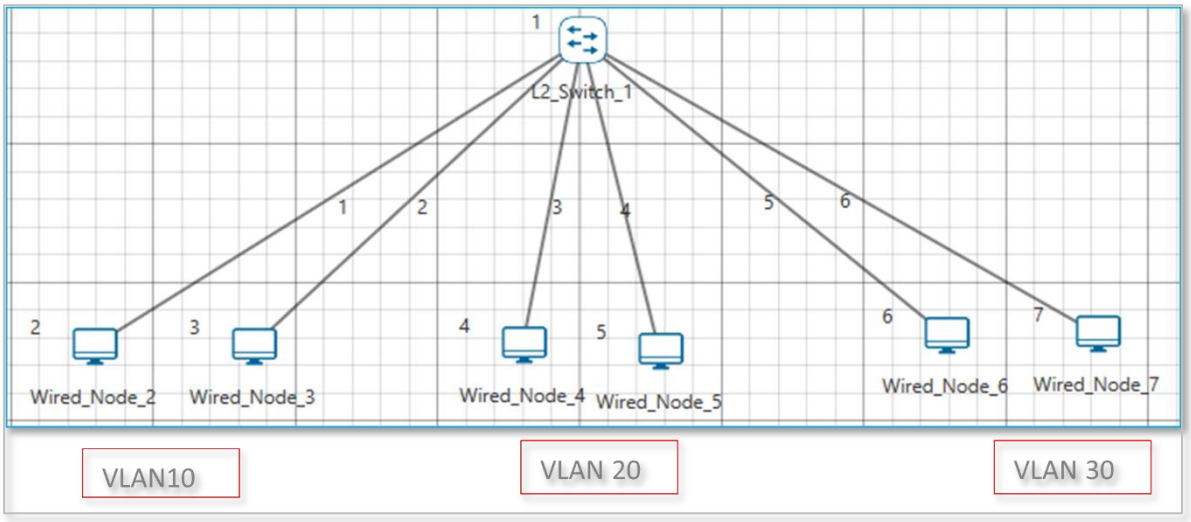

Figure 2-1: Virtual local area network (VLAN)

Switches implement VLANs by adding a VLAN tag to the Ethernet frames as they enter the switch. The VLAN tag contains the VLAN ID and other information, which is determined by the interface from which the frame enters the switch. The switch uses VLAN tags to ensure that each Ethernet frame is confined to the VLAN to which it belongs based on the VLAN ID contained in the VLAN tag. The VLAN tags are removed as the frames exit the switch on the way to their destination.

Any port can belong to a VLAN, and unicast, broadcast, and multicast packets are forwarded and flooded only to end stations in that VLAN. Each VLAN is considered a logical network.

Packets destined for stations that do not belong to the VLAN must be forwarded through a router. In the below screenshot, the stations in the development department are assigned to one VLAN, the stations in the marketing department are assigned to another VLAN, and the stations in the testing department are assigned to another VLAN.

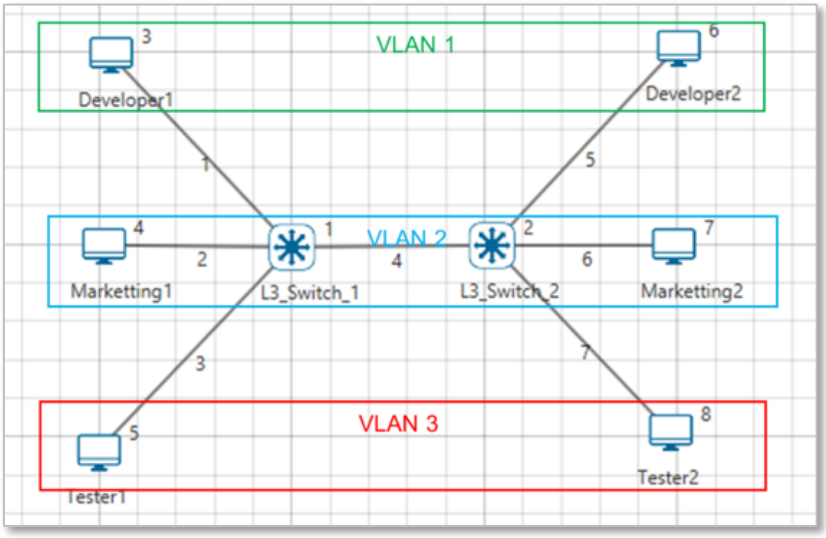

Figure 2-2: Hosts in one VLAN need to communicate with hosts in another VLAN

2.1.1 When do we need a VLAN?

You need to consider using VLAN's 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 are being slowed down by too many broadcasts.
- Groups of users need to be on the same broadcast domain because they are running same applications or just make a single switch into multiple virtual switches.

2.1.1.1 VLAN ID

VLANs are identified by a VLAN ID (a number between 0 – 4095), with the default VLAN on any network being VLAN 2. Each port on a switch or router can be assigned to be a member of a VLAN (i.e., to allow receiving and sending traffic on that VLAN).

For example: On a switch, traffic that is sent to a port that is a member of VLAN2, may be forwarded to any other VLAN2 port on the switch, and it can also travel across a trunk port (connections between switches) to another switch and forwarded to all VLAN2 ports on that switch. Traffic will not be forwarded to ports that are on a different VLAN ID.

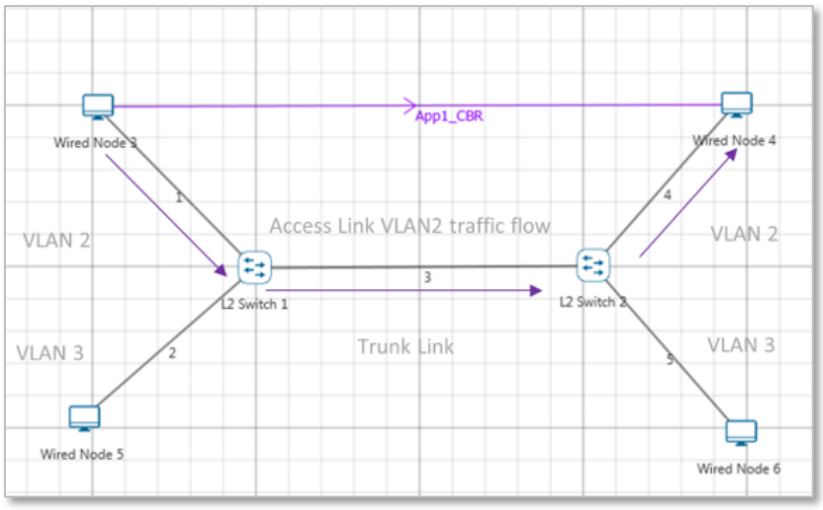

Figure 2-3: Understanding Access and Trunk Links

2.1.2 Understanding Access and Trunk Links

The links connecting the end devices are called access links. These are the links usually carrying the Data VLAN information

The link between the switches is called trunk link. It carries packets from all the VLANs.

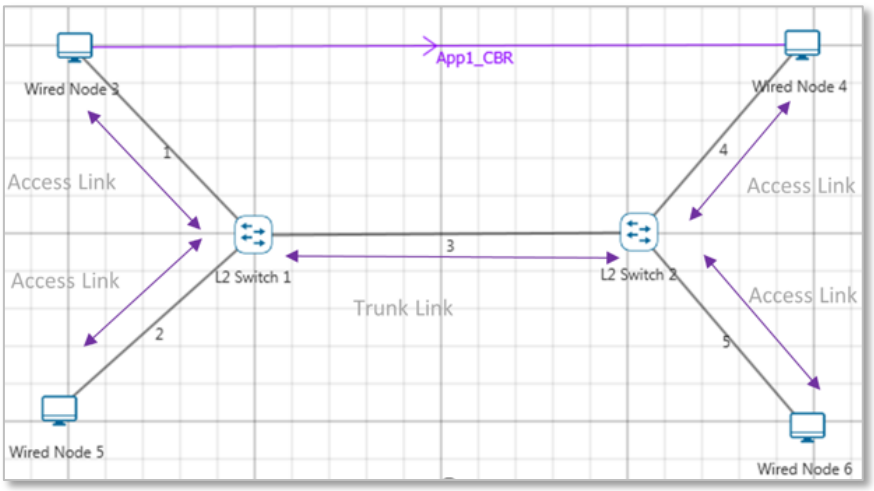

Figure 2-4: Understanding Access and Trunk Links

2.1.2.1 Access Link

Access link connection is the connection where switch port is connected with a device that has a standardized Ethernet NIC. Standard NIC only understand IEEE 802.3 or Ethernet II frames. Access link connection can only be assigned with single VLAN. That means all devices connected to this port will be in same broadcast domain.

For example, twenty users are connected to a hub, and we connect that hub with an access link port on switch, then all of these users belong to same VLAN. If we want to keep ten users in another VLAN, then we need to plug in those ten users to another hub and then connect it with another access link port on switch.

2.1.2.2 Trunk Link

Trunk link connection is the connection where switch port is connected with a device that is capable to understand multiple VLANs. Usually trunk link connection is used to connect two switches. Trunking allows us to send or receive VLAN information across the network. To support trunking, original Ethernet frame is modified to carry VLAN information.

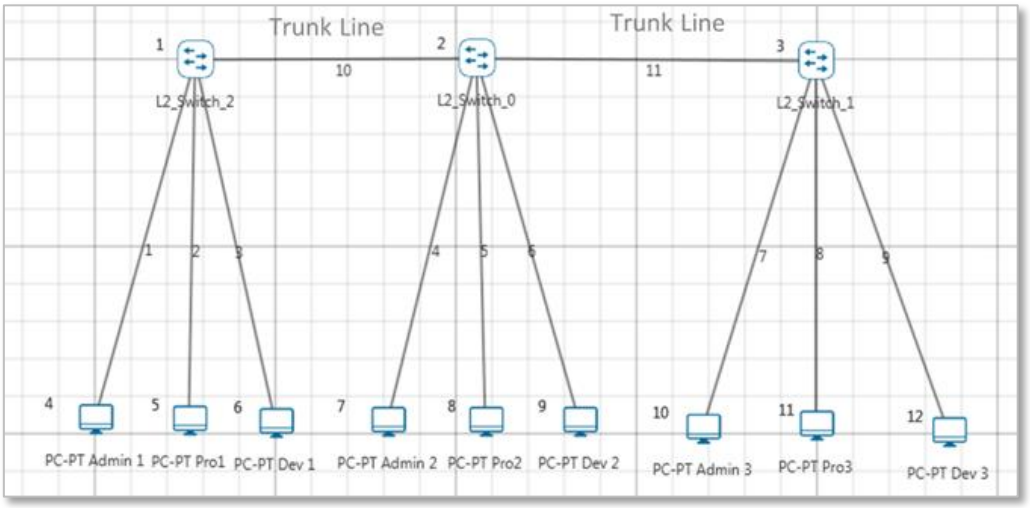

Figure 2-5: Understand multiple VLANs

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. Hence there cannot exist two computers with the same public IP address all over the Internet. This addressing scheme makes it possible for the computers to "find each other" online and exchange information. User has no control over the IP address (public) that is assigned to the computer. The public IP address is assigned to the computer by the Internet Service Provider as soon as the computer is connected to the Internet gateway.

3.1.2 Private Address

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

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

Table 3-1: Private IP address table

Private IP addresses are used for numbering the computers in a private network including home, school and business LANs in airports and hotels which makes it possible for the computers in the network to communicate with each other. For example, if a network A consists of 30 computers each of them can be given an IP starting from **192.168.0.1** to **192.168.0.30.**

Devices with private IP addresses cannot connect directly to the Internet. Likewise, computers outside the local network cannot connect directly to a device with a private IP. It is possible to interconnect two private networks with the help of a router or a similar device that supports Network Address Translation.

If the private network is connected to the Internet (through an Internet connection via ISP) then each computer will have a private IP as well as a public IP. Private IP is used for communication within the network whereas the public IP is used for communication over the Internet.

3.1.3 Network address translation (NAT)

NAT (Network Address Translation or Network Address Translator) is the virtualization of Internet Protocol (IP) addresses. NAT helps to improve security and decrease the number of IP addresses an organization needs.

A device that is configured with NAT will have at least one interface to the inside network and one to the outside network. In a typical environment, NAT is configured at the exit device between a stub domain (inside network) and the backbone. When a packet leaves the domain, NAT translates the locally significant source address into a globally unique address. When a packet enters the domain, NAT translates the globally unique destination address into a local address. If more than one exit point exists, each NAT must have the same translation table. NAT can be configured to advertise to the outside world only one address for the entire network. This ability provides additional security by effectively hiding the entire internal network behind that one address. If NAT cannot allocate an address because it has run out of addresses, it drops the packet and sends an Internet Control Message Protocol (ICMP) host unreachable packet to the destination.

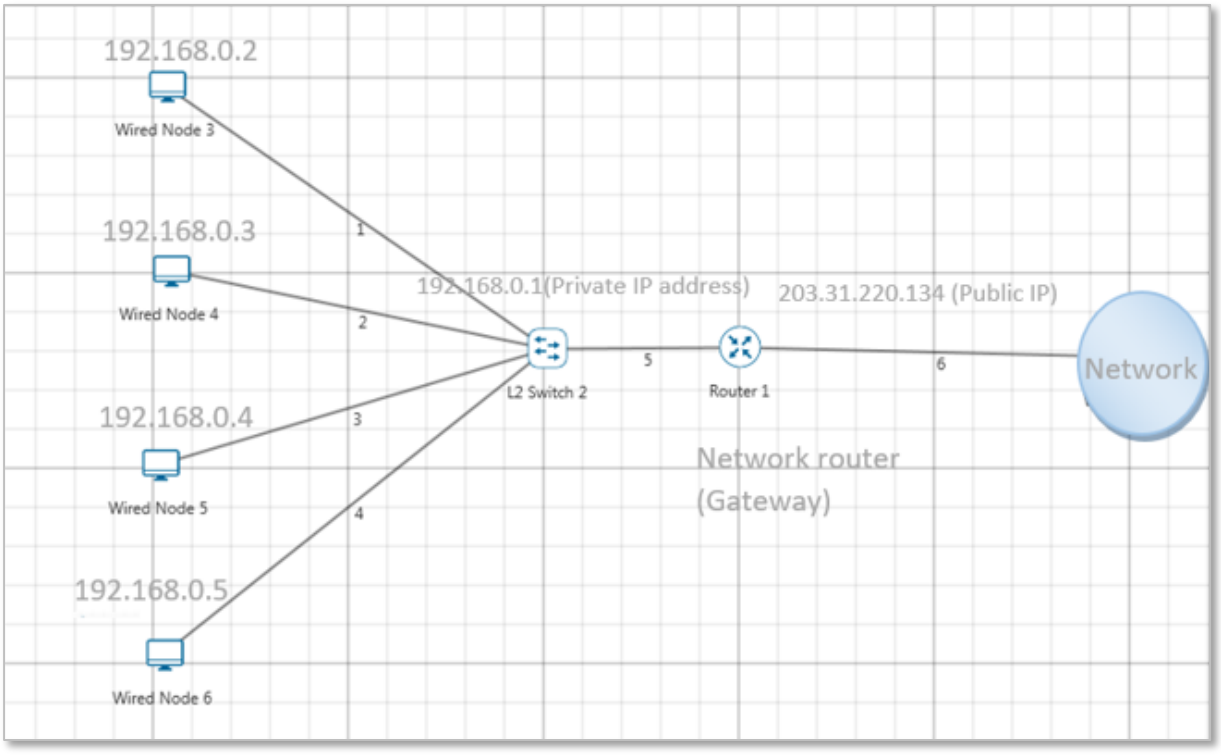

Figure 3-1: NAT implementation

NAT is secure since it hides network from the Internet. All communications from internal private network are handled by the NAT device, which will ensure all the appropriate translations are performed and provide a flawless connection between internal devices and the Internet.

In the above figure, a simple network of 4 hosts and one router that connects this network to the Internet. All hosts in the network have a private Class C IP Address, including the router's private interface (192.168.0.1), while the public interface that's connected to the Internet has a real IP Address (203.31.220.134). This is the IP address the Internet sees as all internal IP addresses are hidden.

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's interface.

The network modelled consists of:

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

NetSim uses the following directions for ACL simulations:

- The direction of the ACL is set to both. This means the ACL applies to both inbound and outbound traffic.
- The direction of ACL is set to Inbound. This means the ACL applies to inbound traffic only.
- The direction of ACL is set to Outbound. This means the ACL applies to outbound traffic only.

Open NetSim, Select **Examples->Advanced routing->ACL Configuration** then click on the tile in the middle panel to load the example as shown below in Figure 4-1.

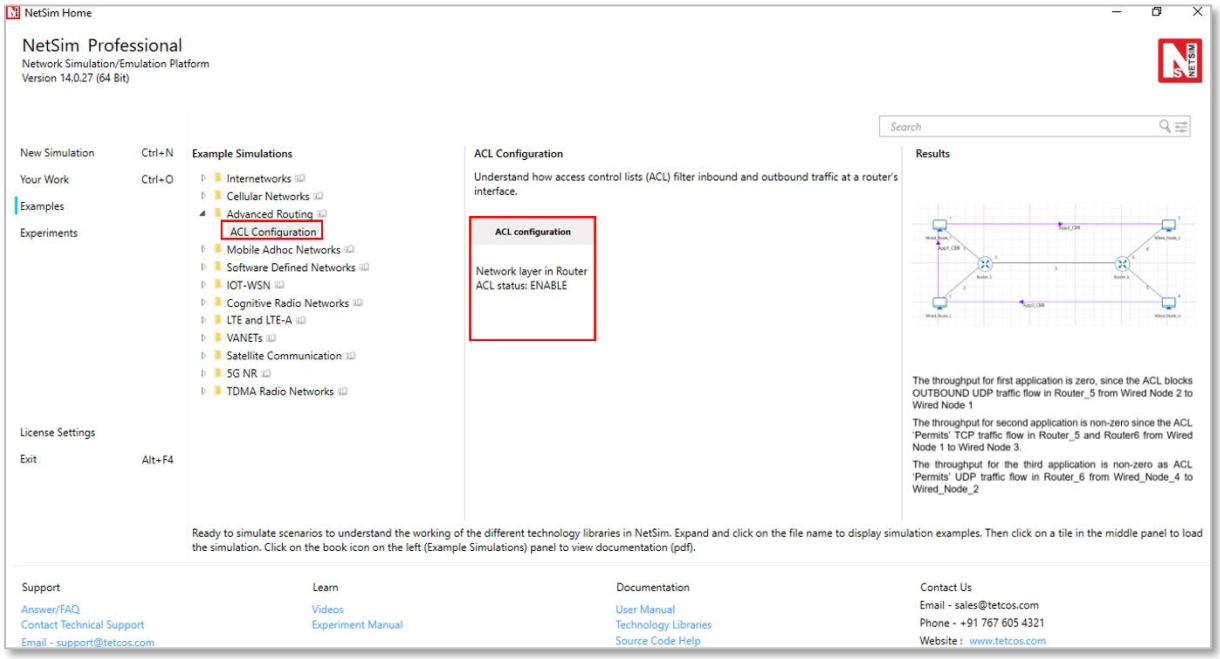

Figure 4-1: List of scenarios for the example of ACL Configuration

The following network diagram illustrates what the NetSim UI displays when you open the example configuration file for ACL as shown Figure 4-2.

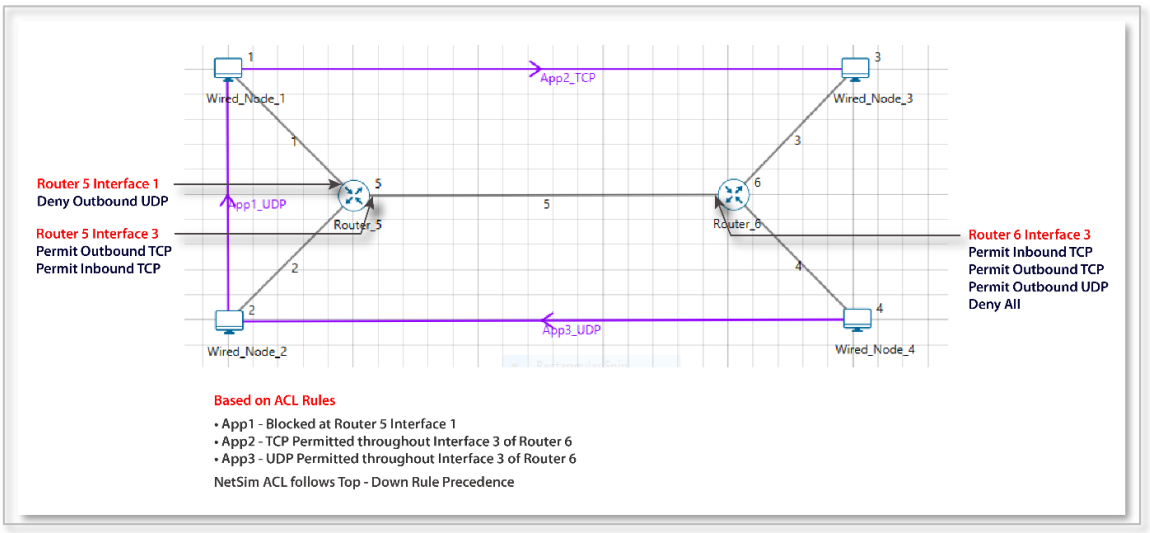

Figure 4-2: Network set up for studying the ACL Configuration

1. ACL enabled in Network Layer of Router_5 and were configured as follows as shown Figure 4-3.

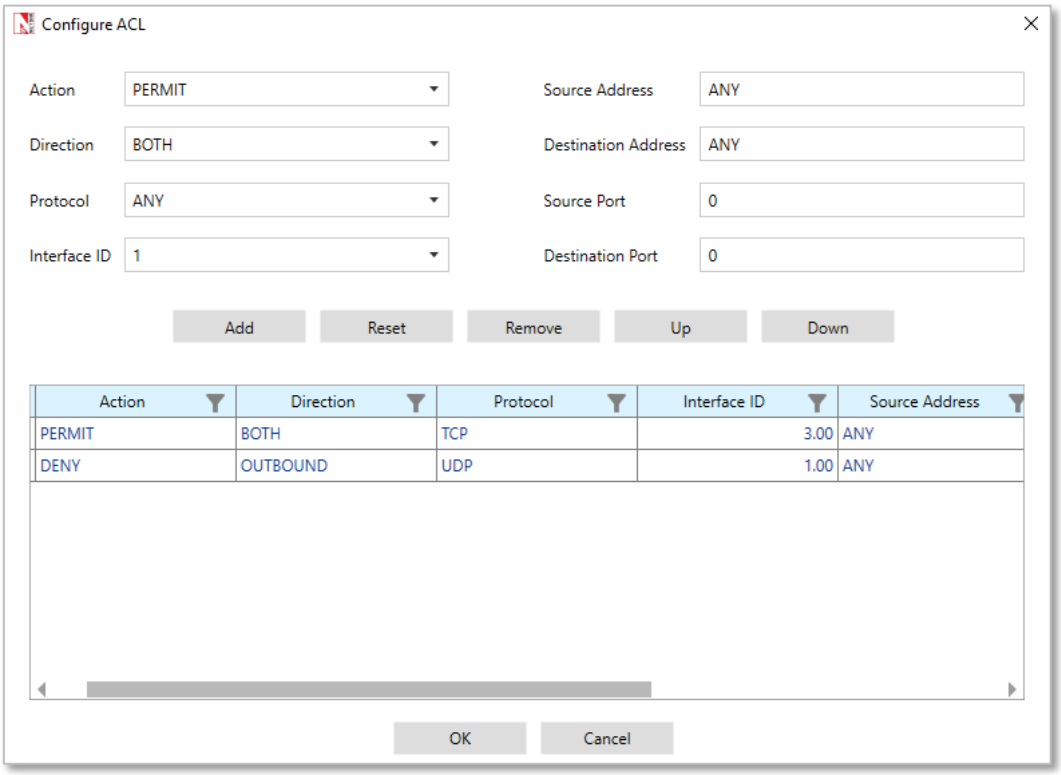

Figure 4-3: ACL Configuration for Router 5

2. ACL enabled in Network Layer of Router_6 and were configured as follows as Figure 4-4.

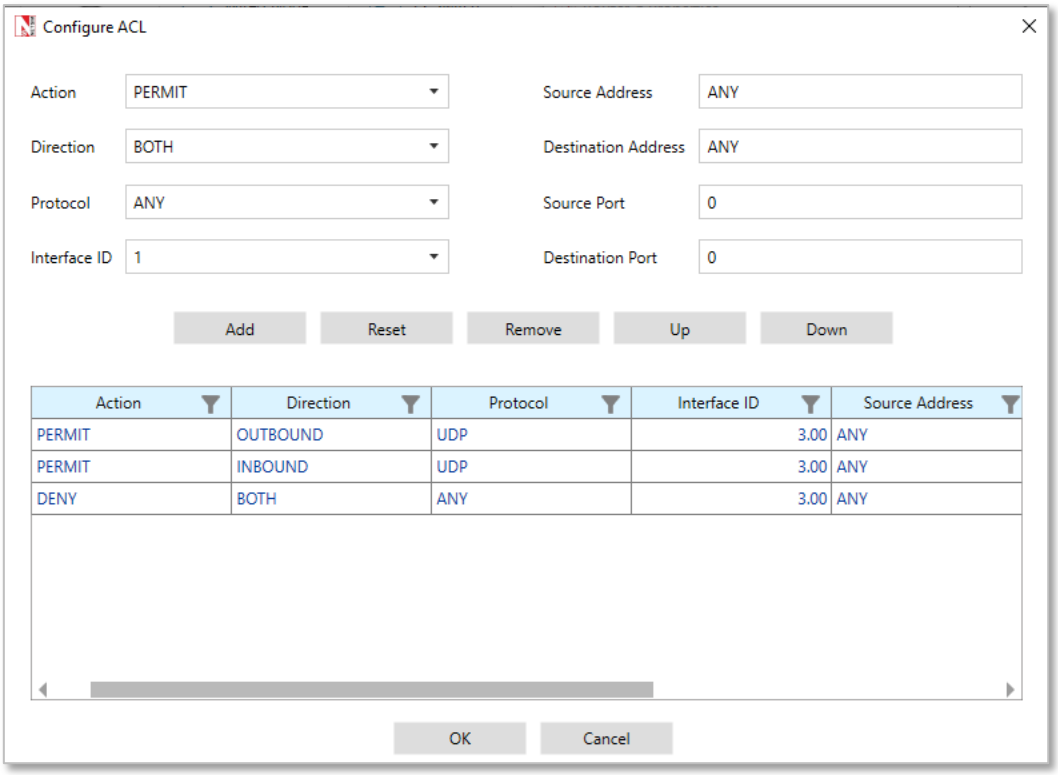

Figure 4-4: ACL Configuration for Router 6

3. Transport protocol set as UDP for APP_1_CBR and APP_3_CBR.
4. Transport protocol set as TCP for APP_2_CBR.
5. Enable the plots and run Simulation for 10 seconds and observe the throughput obtained for the three applications.

4.1.2 Result and Observations

Application_Metrics_Table

Application_Metrics

Application ID	*Throughput Plot*	Application Name	Packets Generated	Packets Received	Throughput (Mbps)	Delay (microsecond)	Jitter (microsecond)
1	*Application_Throughput_plot*	App1_CBR	500	0	0.000000	0.000000	0.000000
2	*Application_Throughput_plot*	App2_CBR	500	478	0.558304	27864.343602	4196.450082
3	*Application_Throughput_plot*	App3_CBR	500	499	0.582832	376.281924	0.001928

Figure 4-5: Application Metrics Table in result window

The throughput for 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 second application is non-zero, since the ACL ‘Permits’ TCP traffic flow in Router_5 and Router6 from Wired Node 1 to Wired Node 3.

The throughput for the third application is non-zero as 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. Experiments are designed to help the user (usually students) learn networking concepts through simulation. The experiments contain objective, theory, set-up, results, and inference. The following experiments are available in the Experiments manual (pdf file).

1. Understanding VLAN operation in L2 and L3 Switches
2. Understanding Access and Trunk Links in VLANs
3. Understanding Public IP Address & NAT (Network Address Translation)
4. Understand the working of basic networking commands (Ping, Route Add/Delete/Print, ACL)

6 Reference Documents

1. IEEE802.1Q 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 Advance Routing library is available at

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