26 Understand the working of basic networking commands (Ping, Route Add/Delete/Print, ACL)

26.1 Theory

NetSim allows users to interact with the simulation at runtime via a socket or through a file. User Interactions make simulation more realistic by allowing command execution to view/modify certain device parameters during runtime.

26.1.1 Ping Command

- The ping command is one of the most often used networking utilities for troubleshooting network problems.
- You can use the ping command to test the availability of a networking device (usually a computer) on a network
- When you ping a device, you send that device a short message, which it then sends back (the echo)
- If you receive a reply then the device is in the Network, if you do not, then the device is faulty, disconnected, switched off, or incorrectly configured.

26.1.2 Route Commands

You can use the route commands to view, add and delete routes in IP routing tables.

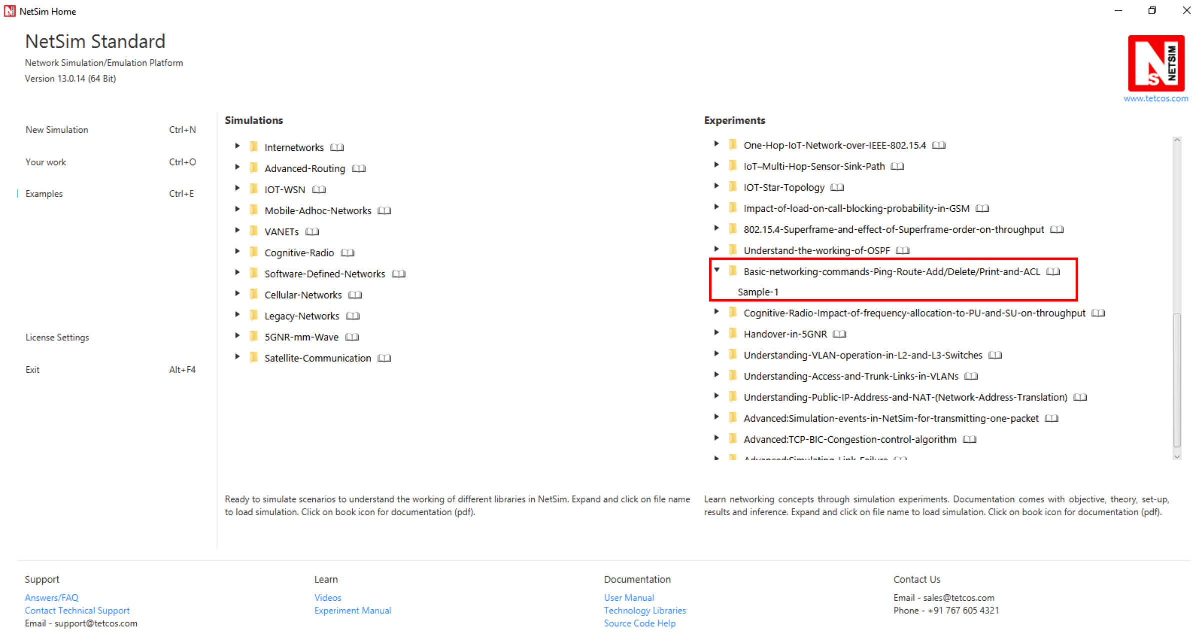
- **route print:** In order to view the entire contents of the IP routing table.
- **route delete:** In order to delete all routes in the IP routing table.
- **route add:** In order to add a static TCP/IP route to the IP routing table.

26.1.3 ACL Configuration

Routers provide basic traffic filtering capabilities, such as blocking the Internet traffic with access control lists (ACLs). An ACL is a sequential list of **Permit** or **Deny** statements that apply to addresses or upper-layer protocols. These lists tell the router what types of packets to: **PERMIT** or **DENY**. When using an access-list to filter traffic, a PERMIT statement is used to **"allow"** traffic, while a DENY statement is used to **"block"** traffic.

26.2 Network setup

Open NetSim and click **Examples > Experiments > Basic-networking-commands-Ping-Route-Add/Delete/Print-and-ACL > Sample-1** as shown below **Figure 26-1**.



NetSim Home

NetSim Standard

Network Simulation/Emulation Platform

Version 13.0.14 (64 Bit)

New Simulation Ctrl+N

Your work Ctrl+O

Examples Ctrl+E

License Settings

Exit Alt+F4

Simulations

- Internetworks
- Advanced-Routing
- IOT-WSN
- Mobile-Adhoc-Networks
- VANETs
- Cognitive-Radio
- Software-Defined-Networks
- Cellular-Networks
- Legacy-Networks
- 5GNR-mm-Wave
- Satellite-Communication

Ready to simulate scenarios to understand the working of different libraries in NetSim. Expand and click on file name to load simulation. Click on book icon for documentation (pdf).

Experiments

- One-Hop-IoT-Network-over-IEEE-802.15.4
- IoT–Multi-Hop-Sensor-Sink-Path
- IOT-Star-Topology
- Impact-of-load-on-call-blocking-probability-in-GSM
- 802.15.4-Superframe-and-effect-of-Superframe-order-on-throughput
- Understand-the-working-of-OSPF
- Basic-networking-commands-Ping-Route-Add/Delete/Print-and-ACL
  - Sample-1
- Cognitive-Radio-Impact-of-frequency-allocation-to-PU-and-SU-on-throughput
- Handover-in-5GNR
- Understanding-VLAN-operation-in-L2-and-L3-Switches
- Understanding-Access-and-Trunk-Links-in-VLANs
- Understanding-Public-IP-Address-and-NAT-(Network-Address-Translation)
- Advanced:Simulation-events-in-NetSim-for-transmitting-one-packet
- Advanced:TCP-BIC-Congestion-control-algorithm
- Advanced:Simulating-Link-Failure

Learn networking concepts through simulation experiments. Documentation comes with objective, theory, set-up, results and inference. Expand and click on file name to load simulation. Click on book icon for documentation (pdf).

Support

Answers/FAQ

Contact Technical Support

Email - support@tetcos.com

Learn

Videos

Experiment Manual

Documentation

User Manual

Technology Libraries

Source Code Help

Contact Us

Email - sales@tetcos.com

Phone - +91 767 605 4321

Figure 26-1: Experiments List

NetSim UI displays the configuration file corresponding to this experiment as shown below **Figure 26-2**.

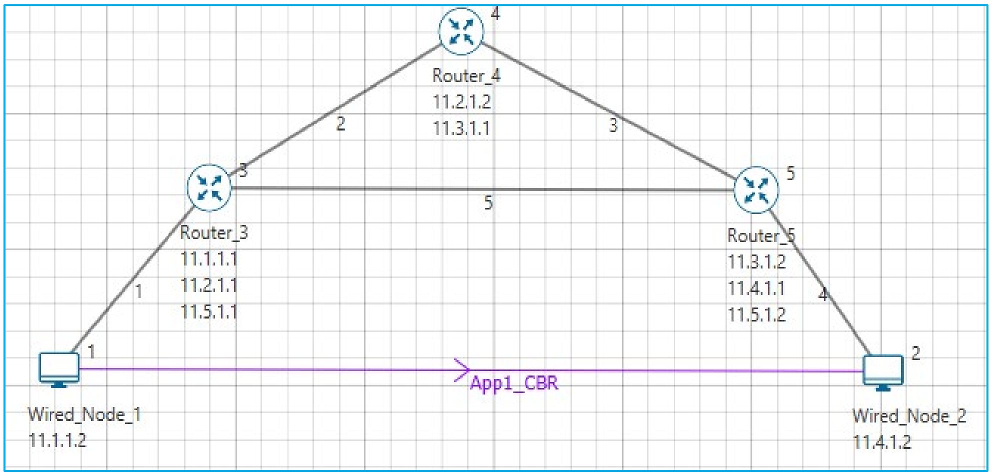


Figure 26-2: Network topology in the sample scenario

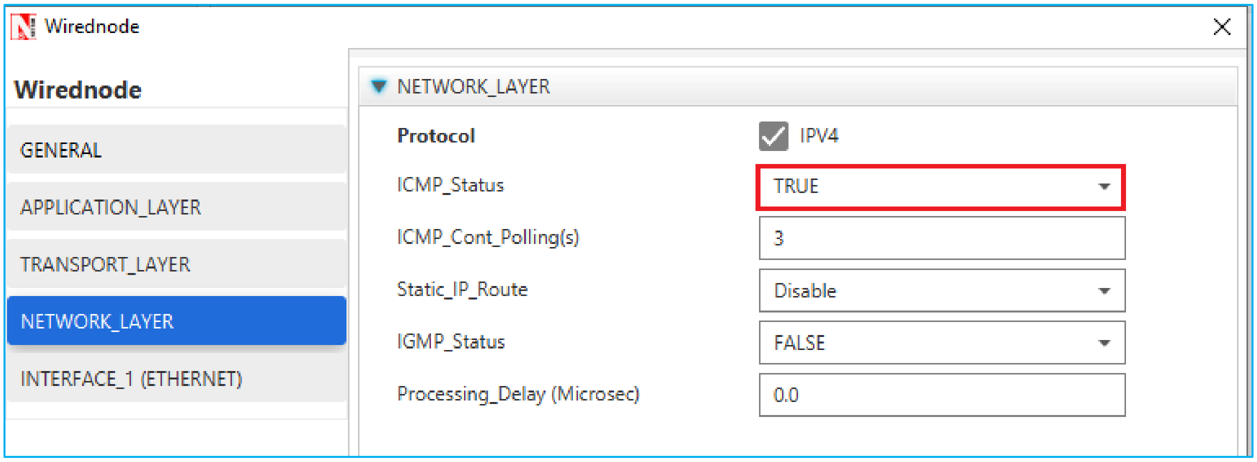
26.3 Procedure

The following set of procedures were done to generate this sample:

Step 1: A network scenario is designed in NetSim GUI comprising of 2 Wired Nodes and 3 Routers in the **"Internetworks"** Network Library.

Step 2: In the Network Layer properties of Wired Node 1, **"ICMP Status"** is set as TRUE.

Similarly, ICMP Status is set as TRUE for all the devices as shown **Figure 26-3**.



Wirednode

Wirednode

- GENERAL
- APPLICATION_LAYER
- TRANSPORT_LAYER
- NETWORK_LAYER
- INTERFACE_1 (ETHERNET)

NETWORK_LAYER

Protocol	☑ IPV4
ICMP_Status	TRUE
ICMP_Cont_Polling(s)	3
Static_IP_Route	Disable
IGMP_Status	FALSE
Processing_Delay (Microsec)	0.0

Figure 26-3: Network Layer properties of Wired Node 1

Step 3: In the General properties of Wired Node 1, **Wireshark Capture** is set as Online.

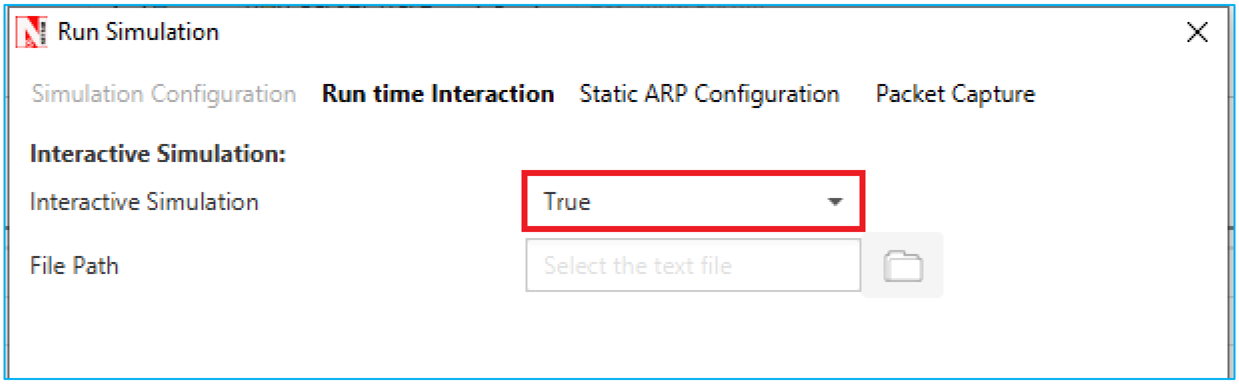
Step 4: Right click on the Application Flow **App1 CBR** and select Properties or click on the Application icon present in the top ribbon/toolbar.

A CBR Application is generated from Wired Node 1 i.e. Source to Wired Node 2 i.e. Destination with Packet Size remaining 1460Bytes and Inter Arrival Time remaining 233.6µs. Transport Protocol is set to **UDP**.

Additionally, the **"Start Time(s)"** parameter is set to 30, while configuring the application. This time is usually set to be greater than the time taken for OSPF Convergence (i.e., Exchange of OSPF information between all the routers), and it increases as the size of the network increases.

Step 5: Packet Trace is enabled in NetSim GUI. At the end of the simulation, a very large .csv file is containing all the packet information is available for the users to perform packet level analysis. Plots are enabled in NetSim GUI.

Step 6: Click on Run Simulation. Simulation Time is set to 300 Seconds and in the **Runtime Interaction** tab **Figure 26-4**, Interactive Simulation is set to True.



Interactive Simulation:

Interactive Simulation: True

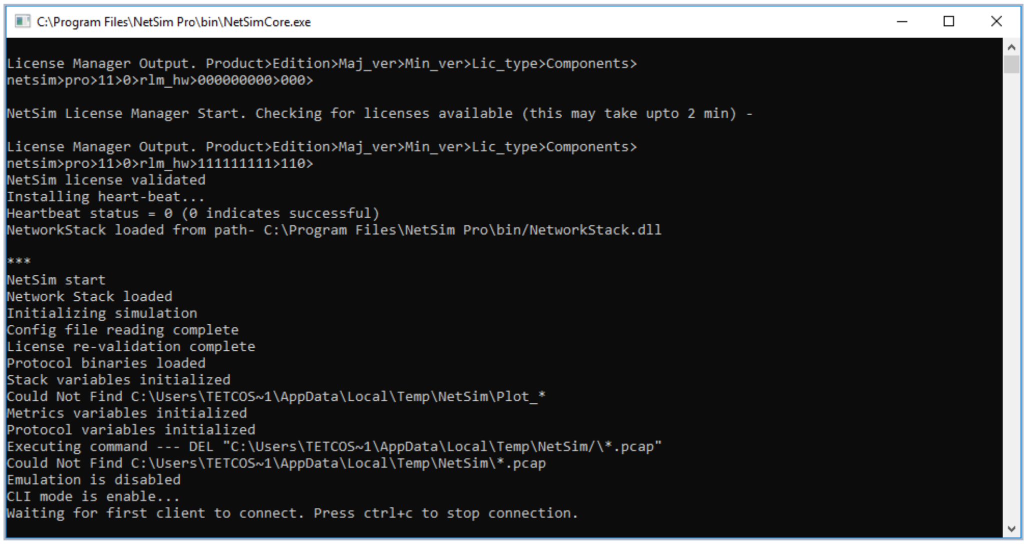
File Path: Select the text file

Figure 26-4: Runtime Interaction window

NOTE: ***It is recommended to specify a longer simulation time to ensure that there is sufficient time for the user to execute the various commands and see the effect of that before the Simulation ends.***

Click on **Accept** and then click on **OK**.

- Simulation (NetSimCore.exe) will start running and will display a message **"waiting for first client to connect"** as shown below **Figure 26-5**



```
License Manager Output. Product>Edition>Maj_ver>Min_ver>Lic_type>Components>
netsim>pro>11>0>rlm_hw>000000000>000>

NetSim License Manager Start. Checking for licenses available (this may take upto 2 min) -

License Manager Output. Product>Edition>Maj_ver>Min_ver>Lic_type>Components>
netsim>pro>11>0>rlm_hw>111111111>110>
NetSim license validated
Installing heart-beat...
Heartbeat status = 0 (0 indicates successful)
NetworkStack loaded from path- C:\Program Files\NetSim Pro\bin/NetworkStack.dll

***
NetSim start
Network Stack loaded
Initializing simulation
Config file reading complete
License re-validation complete
Protocol binaries loaded
Stack variables initialized
Could Not Find C:\Users\TETCOS~1\AppData\Local\Temp\NetSim\Plot_*
Metrics variables initialized
Protocol variables initialized
Executing command --- DEL "C:\Users\TETCOS~1\AppData\Local\Temp\NetSim/\*.pcap"
Could Not Find C:\Users\TETCOS~1\AppData\Local\Temp\NetSim\*.pcap
Emulation is disabled
CLI mode is enable...
Waiting for first client to connect. Press ctrl+c to stop connection.
```

Figure 26-5: Waiting for first client to connect

- Go back to the network scenario. Click on **"Display Settings"** in the top ribbon/toolbar and select the **"Device IP"** checkbox inorder to display the IP address of all the devices. Now, Right click on Router 3 or any other Router and select **"NetSim Console"** option as shown **Figure 26-6**.

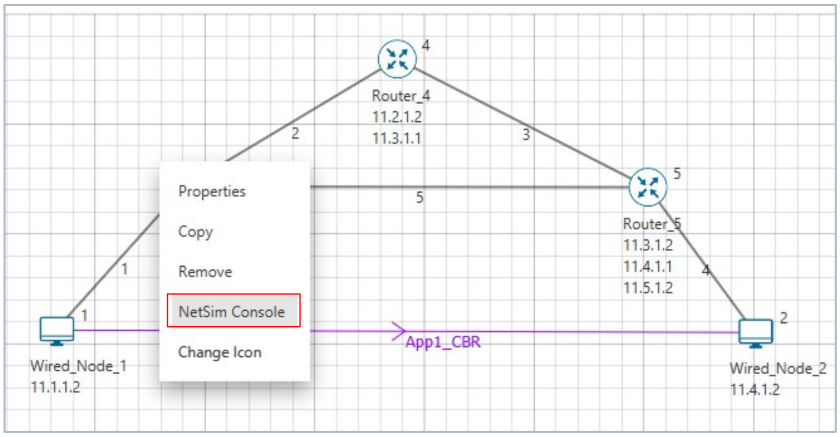
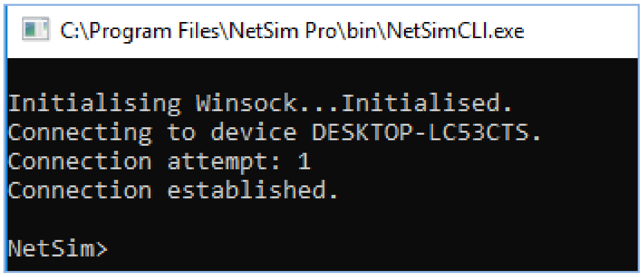


Figure 26-6: Select NetSim Console

- Now Client (NetSimCLI.exe) will start running and it will try to establish a connection with NetSimCore.exe. After the connection is established, the following will be displayed **Figure 26-7**.



C:\Program Files\NetSim Pro\bin\NetSimCLI.exe

```
Initialising Winsock...Initialised.
Connecting to device DESKTOP-LC53CTS.
Connection attempt: 1
Connection established.

NetSim>
```

Figure 26-7: Connection established

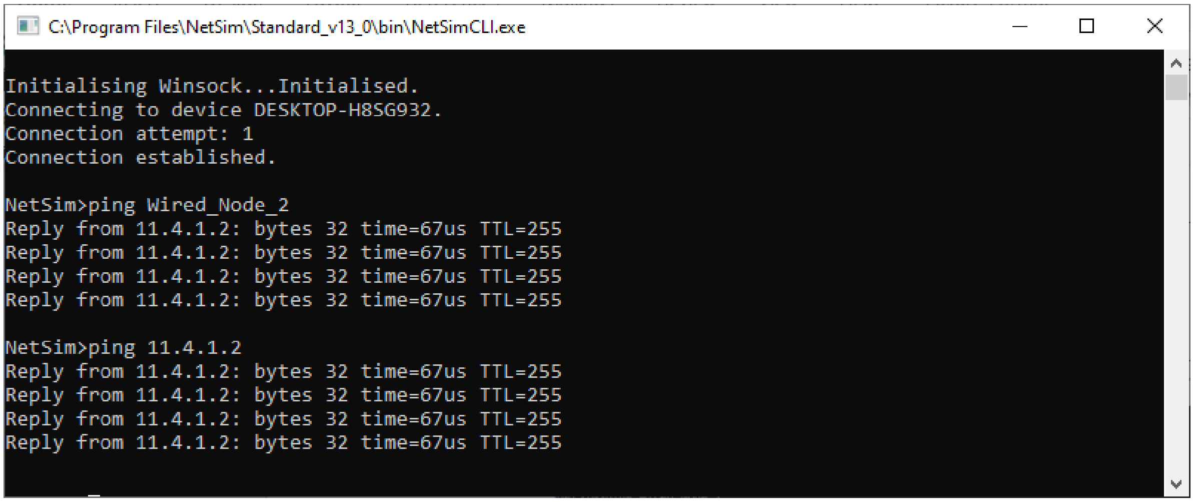
- After this the command line interface can be used to execute all the supported commands.

26.4 Network Commands

26.4.1 Ping Command

- You can use the ***ping*** command with an IP address or Device name.
- ICMP_Status should be set as True in all nodes for ping to work.

```
Ping <IP address> e.g. ping 11.4.1.2

Ping <Node Name> e.g. ping Wired_Node_2
```



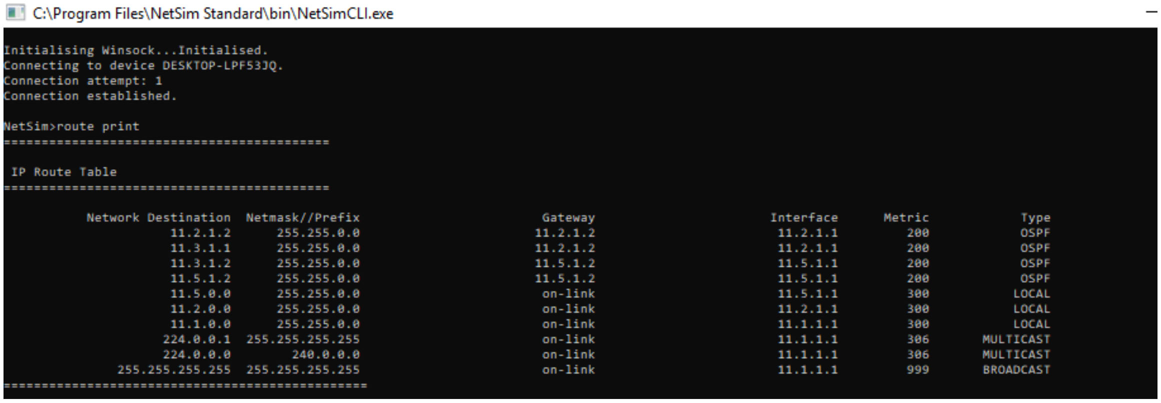
```
Initialising Winsock...Initialised.
Connecting to device DESKTOP-H8SG932.
Connection attempt: 1
Connection established.

NetSim>ping Wired_Node_2
Reply from 11.4.1.2: bytes 32 time=67us TTL=255
Reply from 11.4.1.2: bytes 32 time=67us TTL=255
Reply from 11.4.1.2: bytes 32 time=67us TTL=255
Reply from 11.4.1.2: bytes 32 time=67us TTL=255

NetSim>ping 11.4.1.2
Reply from 11.4.1.2: bytes 32 time=67us TTL=255
Reply from 11.4.1.2: bytes 32 time=67us TTL=255
Reply from 11.4.1.2: bytes 32 time=67us TTL=255
Reply from 11.4.1.2: bytes 32 time=67us TTL=255

_
```

Figure 26-8: Pinging Wired_Node_2

26.4.2 Route Commands

- In order to view the entire contents of the IP routing table, use following command **route print**

```
route print
```



```
Initialising Winsock...Initialised.
Connecting to device DESKTOP-LPF53JQ.
Connection attempt: 1
Connection established.

NetSim>route print
===========================================

 IP Route Table
===========================================

          Network Destination  Netmask//Prefix                  Gateway                  Interface      Metric          Type
                     11.2.1.2      255.255.0.0                 11.2.1.2                   11.2.1.1         200          OSPF
                     11.3.1.1      255.255.0.0                 11.2.1.2                   11.2.1.1         200          OSPF
                     11.3.1.2      255.255.0.0                 11.5.1.2                   11.5.1.1         200          OSPF
                     11.5.1.2      255.255.0.0                 11.5.1.2                   11.5.1.1         200          OSPF
                     11.5.0.0      255.255.0.0                  on-link                   11.5.1.1         300         LOCAL
                     11.2.0.0      255.255.0.0                  on-link                   11.2.1.1         300         LOCAL
                     11.1.0.0      255.255.0.0                  on-link                   11.1.1.1         300         LOCAL
                    224.0.0.1  255.255.255.255                  on-link                   11.1.1.1         306     MULTICAST
                    224.0.0.0        240.0.0.0                  on-link                   11.1.1.1         306     MULTICAST
              255.255.255.255  255.255.255.255                  on-link                   11.1.1.1         999     BROADCAST
================================================
```

Figure 26-9: IP routing table

- You'll see the routing table entries with network destinations and the gateways to which packets are forwarded, when they are headed to that destination. Unless you've already added static routes to the table, everything you see here is dynamically generated.
- In order to delete a route in the IP routing table you'll type a command using the following syntax

```
route delete destination_network
```

- So, to delete the route with destination network 11.5.1.2, all we'd have to do is type this command.

```
route delete 11.5.1.2
```

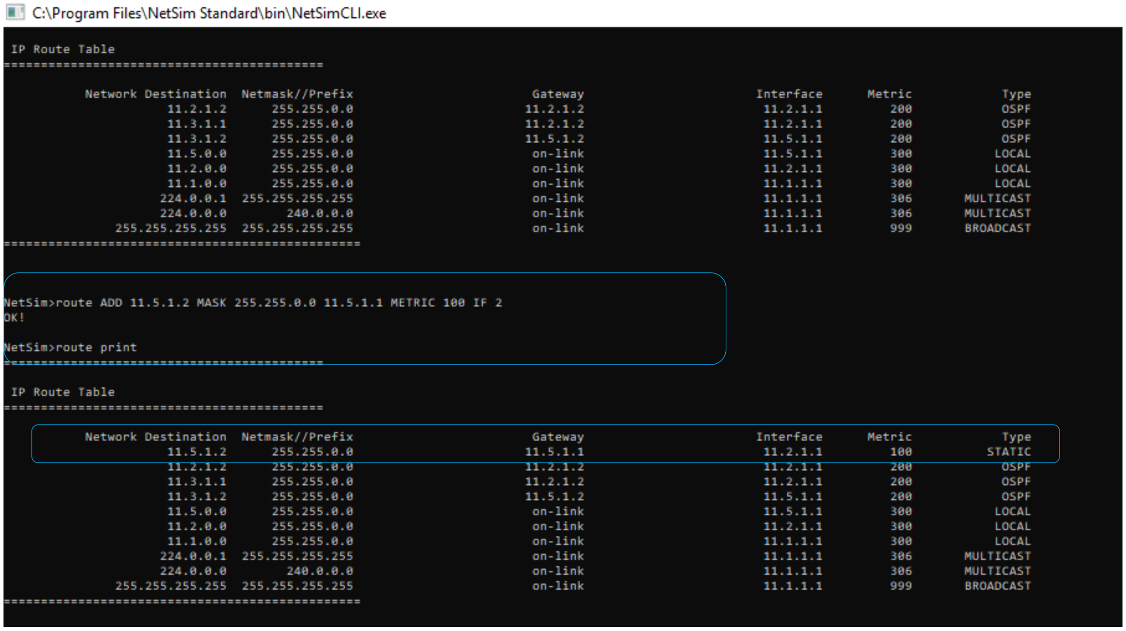
- To check whether route has been deleted or not check again using **route print** command.
- To add a static route to the table, you will type a command using the following syntax.

route ADD *destination_network* MASK *subnet_mask gateway_ip metric_cost interface*

- So, for example, if you wanted to add a route specifying that all traffic bound for the 11.5.1.2 subnet went to a gateway at 11.5.1.1

```
route ADD 11.5.1.2 MASK 255.255.0.0 11.5.1.1 METRIC 100 IF 2
```

- If you were to use the route print command to look at the table now, you'd see your new static route.



C:\Program Files\NetSim Standard\bin\NetSimCLI.exe

```
 IP Route Table
===========================================

          Network Destination  Netmask//Prefix                              Gateway                      Interface      Metric            Type
                     11.2.1.2      255.255.0.0                             11.2.1.2                       11.2.1.1         200            OSPF
                     11.3.1.1      255.255.0.0                             11.2.1.2                       11.2.1.1         200            OSPF
                     11.3.1.2      255.255.0.0                             11.5.1.2                       11.5.1.1         200            OSPF
                     11.5.0.0      255.255.0.0                              on-link                       11.5.1.1         300           LOCAL
                     11.2.0.0      255.255.0.0                              on-link                       11.2.1.1         300           LOCAL
                     11.1.0.0      255.255.0.0                              on-link                       11.1.1.1         300           LOCAL
                    224.0.0.1  255.255.255.255                              on-link                       11.1.1.1         306       MULTICAST
                    224.0.0.0        240.0.0.0                              on-link                       11.1.1.1         306       MULTICAST
              255.255.255.255  255.255.255.255                              on-link                       11.1.1.1         999       BROADCAST
================================================


NetSim>route ADD 11.5.1.2 MASK 255.255.0.0 11.5.1.1 METRIC 100 IF 2
OK!

NetSim>route print
===========================================

 IP Route Table
===========================================

          Network Destination  Netmask//Prefix                              Gateway                      Interface      Metric            Type
                     11.5.1.2      255.255.0.0                             11.5.1.1                       11.2.1.1         100          STATIC
                     11.2.1.2      255.255.0.0                             11.2.1.2                       11.2.1.1         200            OSPF
                     11.3.1.1      255.255.0.0                             11.2.1.2                       11.2.1.1         200            OSPF
                     11.3.1.2      255.255.0.0                             11.5.1.2                       11.5.1.1         200            OSPF
                     11.5.0.0      255.255.0.0                              on-link                       11.5.1.1         300           LOCAL
                     11.2.0.0      255.255.0.0                              on-link                       11.2.1.1         300           LOCAL
                     11.1.0.0      255.255.0.0                              on-link                       11.1.1.1         300           LOCAL
                    224.0.0.1  255.255.255.255                              on-link                       11.1.1.1         306       MULTICAST
                    224.0.0.0        240.0.0.0                              on-link                       11.1.1.1         306       MULTICAST
              255.255.255.255  255.255.255.255                              on-link                       11.1.1.1         999       BROADCAST
================================================
```

Figure 26-10: Route delete/ Route add

***NOTE:* Entry added in IP table by routing protocol continuously gets updated. If a user tries to remove a route via route delete command, there is always a chance that routing protocol will re-enter this entry again. Users can use ACL / Static route to override the routing protocol entry if required.**

26.4.3 ACL Configuration

Commands to configure ACL

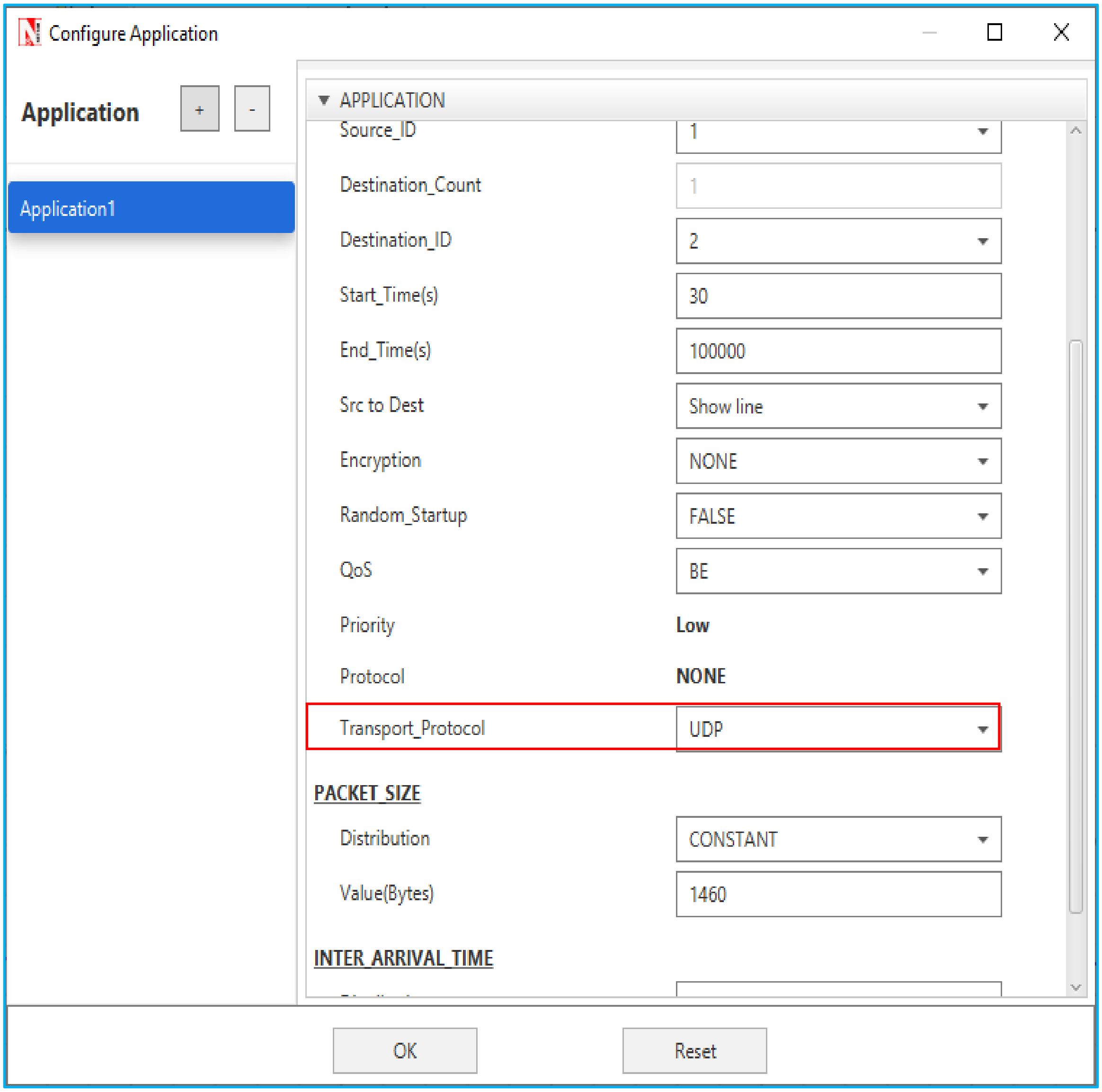
- To view ACL syntax: ***acl print***
- Before using ACL, we must first verify whether ACL option enabled. A common way to enable ACL is to use command: ***ACL Enable***
- Enter configuration mode of ACL: ***aclconfig***
- To view ACL Table: ***Print***
- To exit from ACL configuration: ***exit***
- To disable ACL: ***ACL Disable*** (use this command after **exit** from ACL Configuration)

To view ACL usage syntax use: **acl print**

```
[PERMIT, DENY] [INBOUND, OUTBOUND, BOTH] PROTO SRC DEST SPORT DPORT IFID
```

26.4.4 Step to Configure ACL

- To create a new rule in the ACL use command as shown below to block UDP packet in Interface 2 and Interface 3 of Router 3.
- Application properties → Transport Protocol → **UDP** as shown **Figure 26-11.**



Source_ID: 1
Destination_Count: 1
Destination_ID: 2
Start_Time(s): 30
End_Time(s): 100000
Src to Dest: Show line
Encryption: NONE
Random_Startup: FALSE
QoS: BE
Priority: Low
Protocol: NONE
Transport_Protocol: UDP

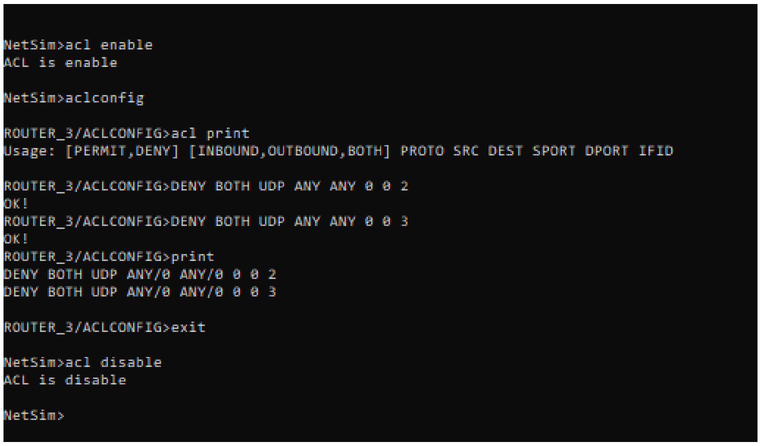
PACKET SIZE
Distribution: CONSTANT
Value(Bytes): 1460

Figure 26-11: Application properties window

- Use the command as follows **Figure 26-12.**

```
NetSim>acl enable

ACL is enable

NetSim>aclconfig

ROUTER_3/ACLCONFIG>acl print

Usage: [PERMIT, DENY] [INBOUND, OUTBOUND, BOTH] PROTO SRC DEST SPORT
DPORT IFID
```

```
ROUTER_3/ACLCONFIG>DENY BOTH UDP ANY ANY 0 0 2

OK!

ROUTER_3/ACLCONFIG>DENY BOTH UDP ANY ANY 0 0 3

OK!

ROUTER_3/ACLCONFIG>print

DENY BOTH UDP ANY/0 ANY/0 0 0 2

DENY BOTH UDP ANY/0 ANY/0 0 0 3

ROUTER_3/ACLCONFIG>exit

NetSim>acl disable

ACL is disable

NetSim>
```



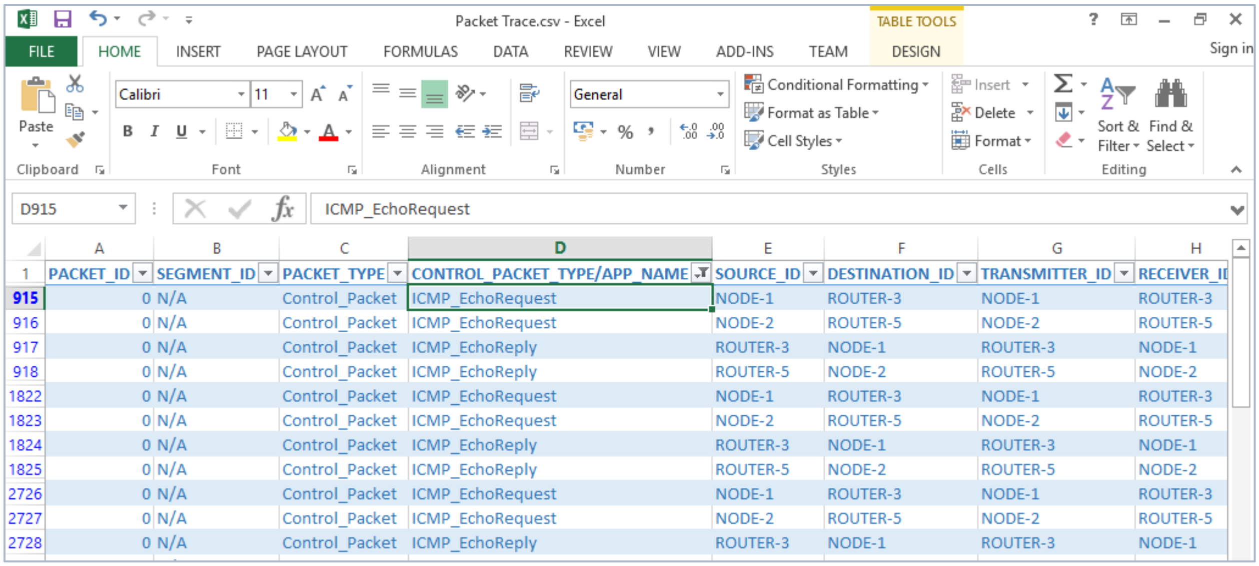
```
NetSim>acl enable
ACL is enable

NetSim>aclconfig

ROUTER_3/ACLCONFIG>acl print
Usage: [PERMIT,DENY] [INBOUND,OUTBOUND,BOTH] PROTO SRC DEST SPORT DPORT IFID

ROUTER_3/ACLCONFIG>DENY BOTH UDP ANY ANY 0 0 2
OK!
ROUTER_3/ACLCONFIG>DENY BOTH UDP ANY ANY 0 0 3
OK!
ROUTER_3/ACLCONFIG>print
DENY BOTH UDP ANY/0 ANY/0 0 0 2
DENY BOTH UDP ANY/0 ANY/0 0 0 3

ROUTER_3/ACLCONFIG>exit

NetSim>acl disable
ACL is disable

NetSim>
```

Figure 26-12: ACL Configuration command

26.4.5 Ping Command Results

Go to the Results Dashboard and click on **“Open Packet Trace”** option present in the Left-Hand-Side of the window and do the following:

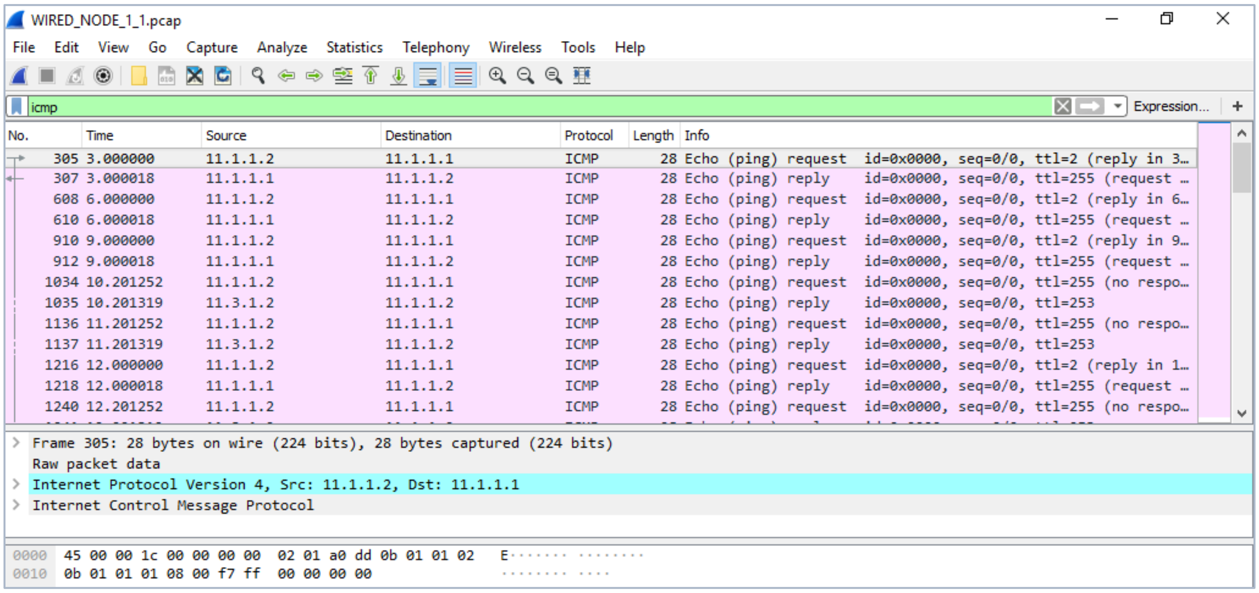
Filter Control Packet Type/App Name to **ICMP EchoRequest** and **ICMP EchoReply** as shown **Figure 26-13**.



	PACKET_ID	SEGMENT_ID	PACKET_TYPE	CONTROL_PACKET_TYPE/APP_NAME	SOURCE_ID	DESTINATION_ID	TRANSMITTER_ID	RECEIVER_ID
915	0	N/A	Control_Packet	ICMP_EchoRequest	NODE-1	ROUTER-3	NODE-1	ROUTER-3
916	0	N/A	Control_Packet	ICMP_EchoRequest	NODE-2	ROUTER-5	NODE-2	ROUTER-5
917	0	N/A	Control_Packet	ICMP_EchoReply	ROUTER-3	NODE-1	ROUTER-3	NODE-1
918	0	N/A	Control_Packet	ICMP_EchoReply	ROUTER-5	NODE-2	ROUTER-5	NODE-2
1822	0	N/A	Control_Packet	ICMP_EchoRequest	NODE-1	ROUTER-3	NODE-1	ROUTER-3
1823	0	N/A	Control_Packet	ICMP_EchoRequest	NODE-2	ROUTER-5	NODE-2	ROUTER-5
1824	0	N/A	Control_Packet	ICMP_EchoReply	ROUTER-3	NODE-1	ROUTER-3	NODE-1
1825	0	N/A	Control_Packet	ICMP_EchoReply	ROUTER-5	NODE-2	ROUTER-5	NODE-2
2726	0	N/A	Control_Packet	ICMP_EchoRequest	NODE-1	ROUTER-3	NODE-1	ROUTER-3
2727	0	N/A	Control_Packet	ICMP_EchoRequest	NODE-2	ROUTER-5	NODE-2	ROUTER-5
2728	0	N/A	Control_Packet	ICMP_EchoReply	ROUTER-3	NODE-1	ROUTER-3	NODE-1

Figure 26-13: Packet Trace - ICMP Control Packets

In Wireshark, apply filter as ICMP. we can see the ping request and reply packets in Wireshark as shown **Figure 26-14**.

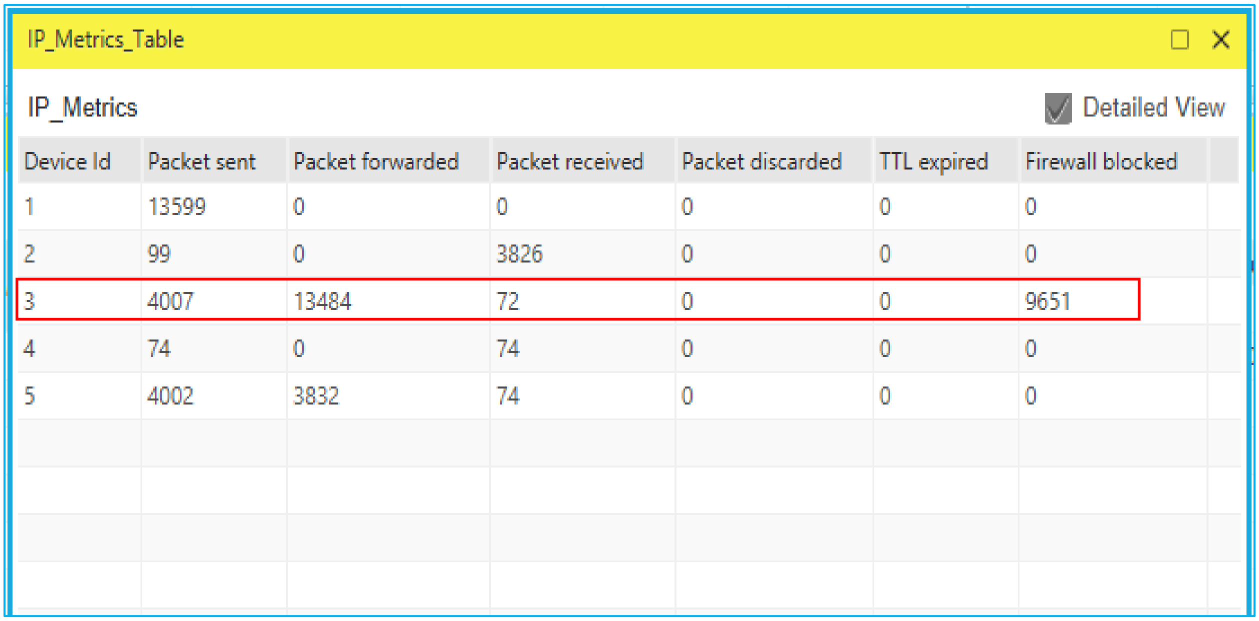


```
No.     Time       Source     Destination  Protocol  Length Info
    305 3.000000   11.1.1.2   11.1.1.1     ICMP          28 Echo (ping) request  id=0x0000, seq=0/0, ttl=2 (reply in 3…
    307 3.000018   11.1.1.1   11.1.1.2     ICMP          28 Echo (ping) reply    id=0x0000, seq=0/0, ttl=255 (request …
    608 6.000000   11.1.1.2   11.1.1.1     ICMP          28 Echo (ping) request  id=0x0000, seq=0/0, ttl=2 (reply in 6…
    610 6.000018   11.1.1.1   11.1.1.2     ICMP          28 Echo (ping) reply    id=0x0000, seq=0/0, ttl=255 (request …
    910 9.000000   11.1.1.2   11.1.1.1     ICMP          28 Echo (ping) request  id=0x0000, seq=0/0, ttl=2 (reply in 9…
    912 9.000018   11.1.1.1   11.1.1.2     ICMP          28 Echo (ping) reply    id=0x0000, seq=0/0, ttl=255 (request …
   1034 10.201252  11.1.1.2   11.1.1.1     ICMP          28 Echo (ping) request  id=0x0000, seq=0/0, ttl=255 (no respo…
   1035 10.201319  11.3.1.2   11.1.1.2     ICMP          28 Echo (ping) reply    id=0x0000, seq=0/0, ttl=253
   1136 11.201252  11.1.1.2   11.1.1.1     ICMP          28 Echo (ping) request  id=0x0000, seq=0/0, ttl=255 (no respo…
   1137 11.201319  11.3.1.2   11.1.1.2     ICMP          28 Echo (ping) reply    id=0x0000, seq=0/0, ttl=253
   1216 12.000000  11.1.1.2   11.1.1.1     ICMP          28 Echo (ping) request  id=0x0000, seq=0/0, ttl=2 (reply in 1…
   1218 12.000018  11.1.1.1   11.1.1.2     ICMP          28 Echo (ping) reply    id=0x0000, seq=0/0, ttl=255 (request …
   1240 12.201252  11.1.1.2   11.1.1.1     ICMP          28 Echo (ping) request  id=0x0000, seq=0/0, ttl=255 (no respo…

> Frame 305: 28 bytes on wire (224 bits), 28 bytes captured (224 bits)
  Raw packet data
> Internet Protocol Version 4, Src: 11.1.1.2, Dst: 11.1.1.1
> Internet Control Message Protocol

0000  45 00 00 1c 00 00 00 00  02 01 a0 dd 0b 01 01 02   E······· ········
0010  0b 01 01 01 08 00 f7 ff  00 00 00 00               ········ ····
```

Figure 26-14: ICMP Control packets in Wireshark

26.4.6 ACL Results

The impact of ACL rule applied over the simulation traffic can be observed in the IP Metrics Table in the simulation results window. In Router 3, the number of packets blocked by firewall has been shown below **Figure 26-15**.



IP_Metrics_Table

IP_Metrics ☑ Detailed View

Device Id	Packet sent	Packet forwarded	Packet received	Packet discarded	TTL expired	Firewall blocked
1	13599	0	0	0	0	0
2	99	0	3826	0	0	0
3	4007	13484	72	0	0	9651
4	74	0	74	0	0	0
5	4002	3832	74	0	0	0

Figure 26-15: IP Metrics Table in result window

NOTE: ***Number of packets blocked may vary based on the time at which ACL is configured.***

Users can also observe this in Packet Animation before and after the Packets are blocked as shown below **Figure 26-16**/**Figure 26-17**.

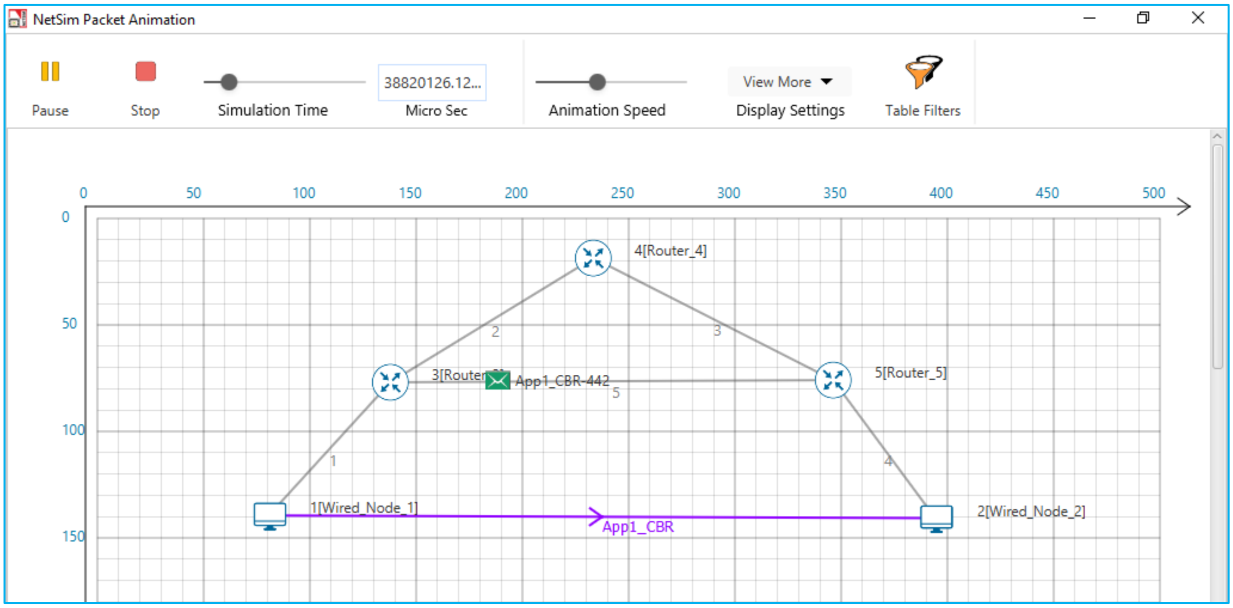
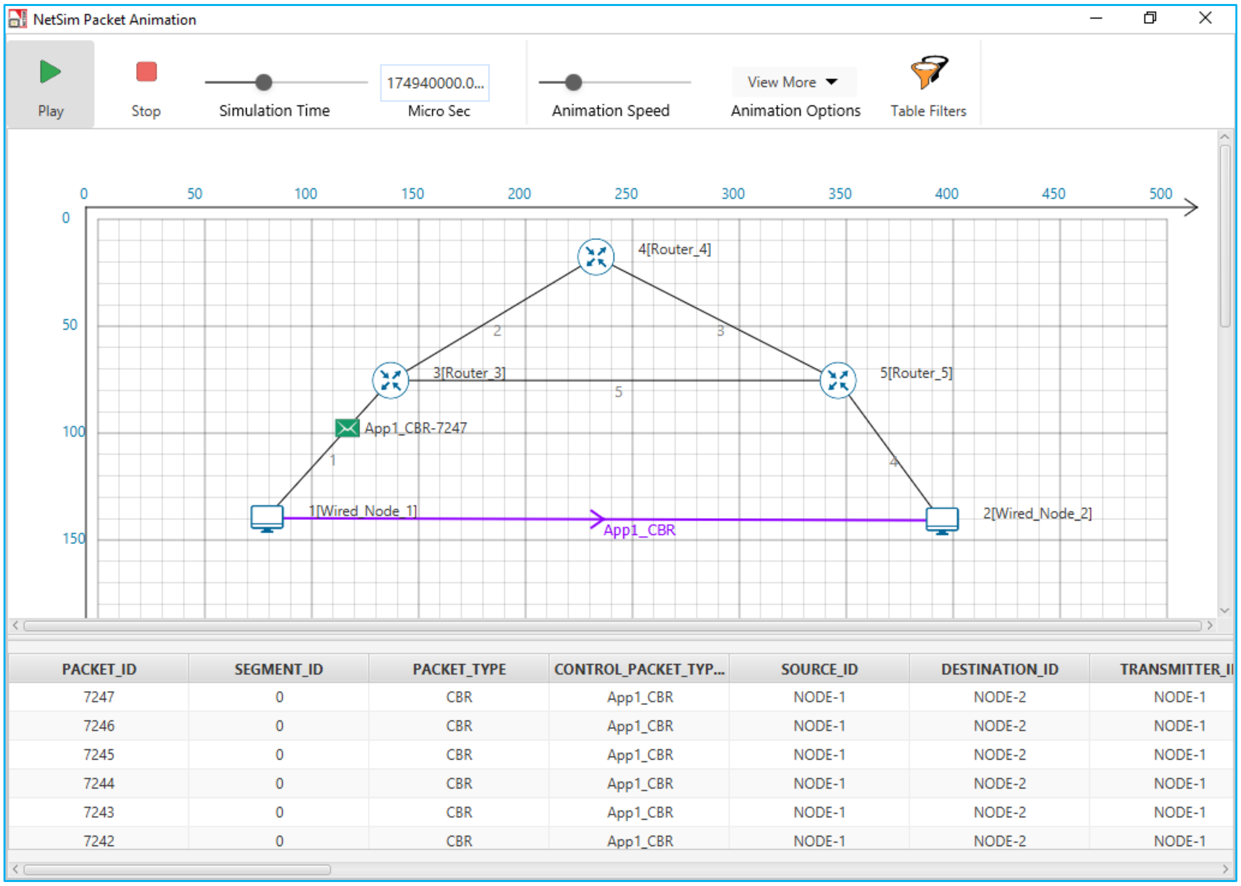


Figure 26-16: In Animation Window before applying ACL rules see the packet flow



PACKET_ID	SEGMENT_ID	PACKET_TYPE	CONTROL_PACKET_TYP...	SOURCE_ID	DESTINATION_ID	TRANSMITTER_I
7247	0	CBR	App1_CBR	NODE-1	NODE-2	NODE-1
7246	0	CBR	App1_CBR	NODE-1	NODE-2	NODE-1
7245	0	CBR	App1_CBR	NODE-1	NODE-2	NODE-1
7244	0	CBR	App1_CBR	NODE-1	NODE-2	NODE-1
7243	0	CBR	App1_CBR	NODE-1	NODE-2	NODE-1
7242	0	CBR	App1_CBR	NODE-1	NODE-2	NODE-1

Figure 26-17: In Animation Window after applying ACL rules see the packet flow

- Check Packet animation window whether packets has been blocked in Router_3 or not after entering ACL command to deny UDP traffic.
- Before applying ACL rule there is packet flow from Wired_Node_1 to Wired_Node_2
- After applying ACL rule Packet flows up to Router_3 only.