NetSim®

Accelerate Network R & D

Internetworks

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

TETCOS LLP may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from TETCOS LLP, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, email address, logo, person, place, or event is intended or should be inferred.

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 Introduction

The Internetworks library in NetSim supports various protocols across all the layers of the TCP/IP network stack. These include Ethernet, Address Resolution Protocol (ARP), Wireless LAN – 802.11 a / b / g / n / ac and e (EDCA), Internet Protocol (IP), Transmission Control Protocol (TCP), Virtual LAN (VLAN), User Datagram Protocol (UDP), and routing protocols such as Routing Information Protocol (RIP), Open Shortest Path First (OSPF) and Internet Group Management Protocol (IGMP).

An internetwork is generally a collection of two or more networks (typically LANs and WLANs) which are interconnected to form a larger network. All networks in an Internetwork have a unique network address. Routers interconnect different networks.

Users can use the following devices to design Internetworks: wireless node, wired node, switch, router, and access point (AP). Wired nodes (term for computers, servers etc) connect via wired link to switches or routers, and wireless nodes connect via wireless links to Access Points (APs). Multiple links terminate at a switch/router, which enables connectivity between them. Many switches/routers are present in an internetwork to connect all the end-nodes. The end-nodes provide and consume useful information via applications like data, voice, video etc.

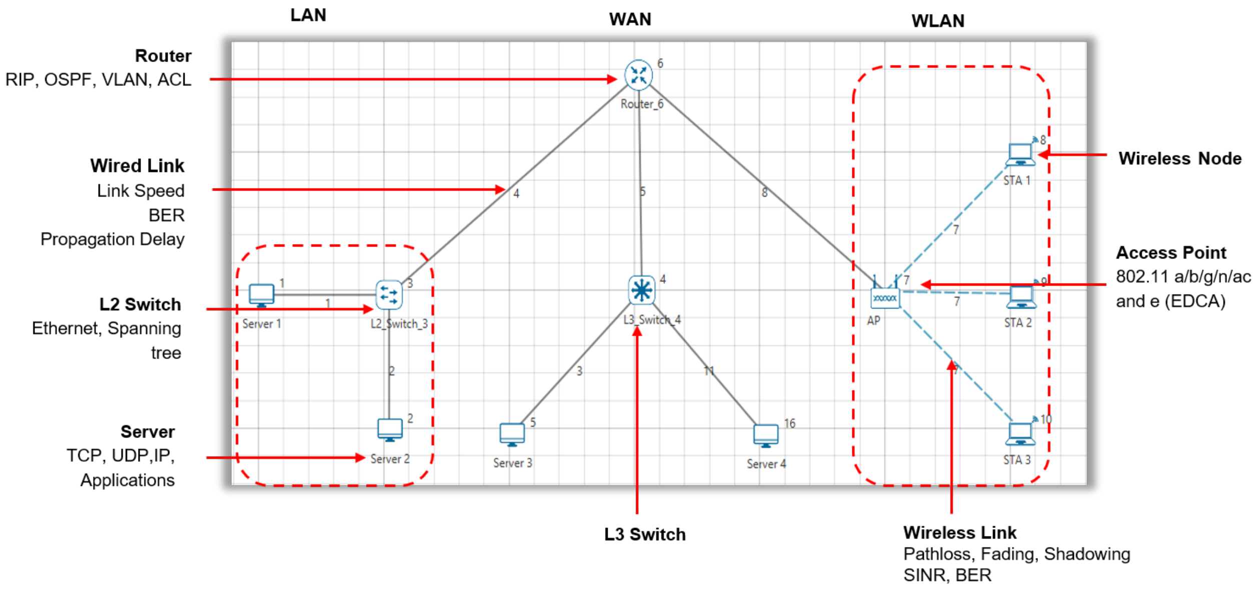
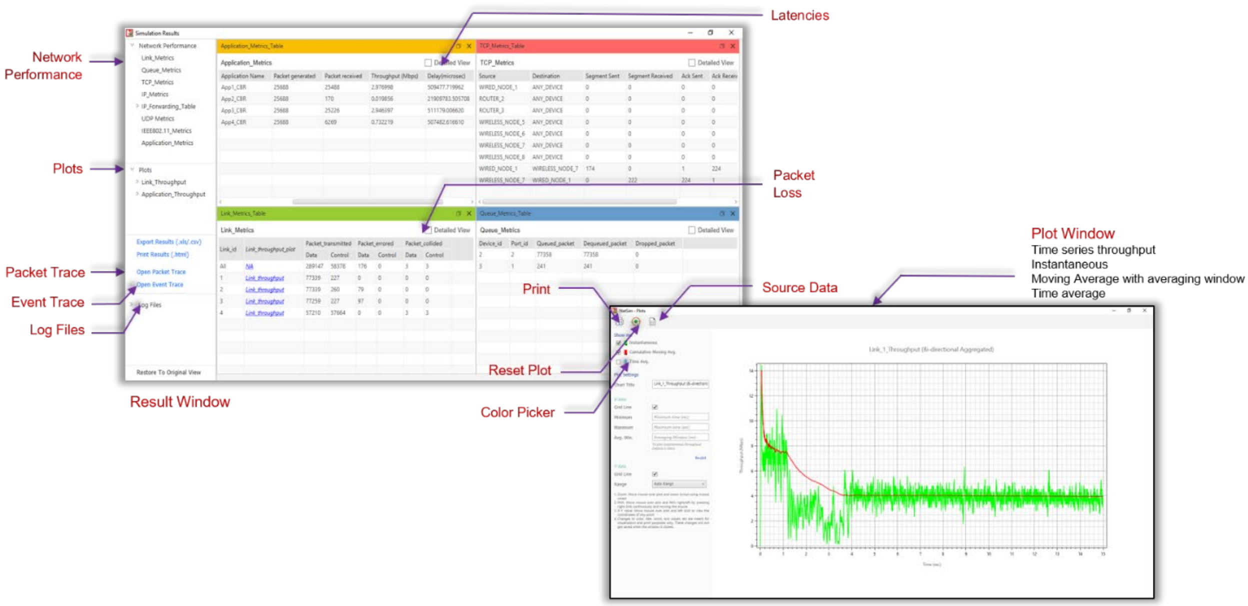


Figure 1-1: A typical Internetworks scenario in NetSim



Application_Metrics

Application Name	Packet generated	Packet received	Throughput (Mbps)	Delay(microsec)
App1_CBR	25688	25488	2.976998	509477.719962
App2_CBR	25688	170	0.019856	21909783.505708
App3_CBR	25688	25226	2.946397	511179.006620
App4_CBR	25688	6269	0.732219	507482.616610

TCP_Metrics

Source	Destination	Segment Sent	Segment Received	Ack Sent	Ack Receiv
WIRED_NODE_1	ANY_DEVICE	0	0	0	0
ROUTER_2	ANY_DEVICE	0	0	0	0
ROUTER_3	ANY_DEVICE	0	0	0	0
WIRELESS_NODE_5	ANY_DEVICE	0	0	0	0
WIRELESS_NODE_6	ANY_DEVICE	0	0	0	0
WIRELESS_NODE_7	ANY_DEVICE	0	0	0	0
WIRELESS_NODE_8	ANY_DEVICE	0	0	0	0
WIRED_NODE_1	WIRELESS_NODE_7	174	0	1	224
WIRELESS_NODE_7	WIRED_NODE_1	0	222	224	1

Link_Metrics

Link_id	Link_throughput_plot	Packet_transmitted		Packet_errored		Packet_collided	
		Data	Control	Data	Control	Data	Control
All	NA	289147	58378	176	0	3	3
1	Link_throughput	77339	227	0	0	0	0
2	Link_throughput	77339	260	79	0	0	0
3	Link_throughput	77259	227	97	0	0	0
4	Link_throughput	57210	57664	0	0	3	3

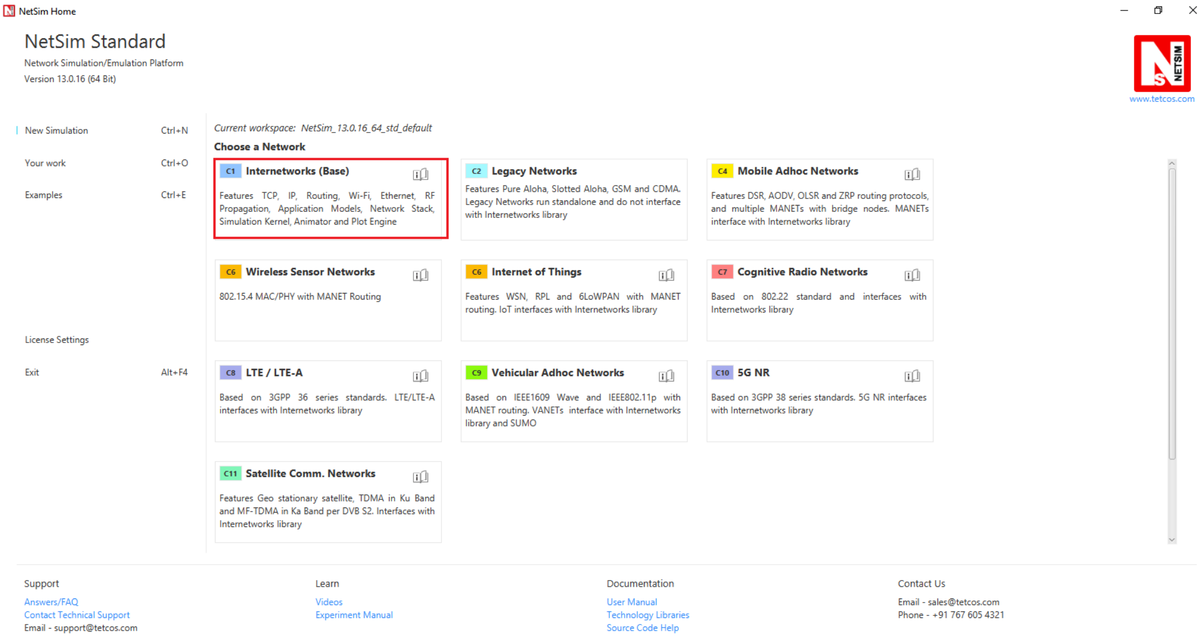
Queue_Metrics

Device_id	Port_id	Queued_packet	Dequeued_packet	Dropped_packet
2	2	77358	77358	0
3	1	241	241	0

Figure 1-2: The Result dashboard and Plot window shown in NetSim after completion of simulation

2 Simulation GUI

Open NetSim and click **New Simulation → Internetworks** as shown **Figure 2-1.**



Current workspace: NetSim_13.0.16_64_std_default

Choose a Network

C1 Internetworks (Base)
Features TCP, IP, Routing, Wi-Fi, Ethernet, RF Propagation, Application Models, Network Stack, Simulation Kernel, Animator and Plot Engine

C2 Legacy Networks
Features Pure Aloha, Slotted Aloha, GSM and CDMA. Legacy Networks run standalone and do not interface with Internetworks library

C4 Mobile Adhoc Networks
Features DSR, AODV, OLSR and ZRP routing protocols, and multiple MANETs with bridge nodes. MANETs interface with Internetworks library

C6 Wireless Sensor Networks
802.15.4 MAC/PHY with MANET Routing

C6 Internet of Things
Features WSN, RPL and 6LoWPAN with MANET routing. IoT interfaces with Internetworks library

C7 Cognitive Radio Networks
Based on 802.22 standard and interfaces with Internetworks library

C8 LTE / LTE-A
Based on 3GPP 36 series standards. LTE/LTE-A interfaces with Internetworks library

C9 Vehicular Adhoc Networks
Based on IEEE1609 Wave and IEEE802.11p with MANET routing. VANETs interface with Internetworks library and SUMO

C10 5G NR
Based on 3GPP 38 series standards. 5G NR interfaces with Internetworks library

C11 Satellite Comm. Networks
Features Geo stationary satellite, TDMA in Ku Band and MF-TDMA in Ka Band per DVB S2. Interfaces with Internetworks library

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 2-1: NetSim Home Screen

2.1 Create Scenario

Internetworks come with a palette of various devices like L2 Switch, L3 Switch, Router, Wired Node, Wireless Node, and AP (Access Point).

2.2 Devices specific to NetSim Internetworks Library

- **Wired node:** A Wired node can be an end-node or for a server. It is a 5-layer device that can be connected to a switch and router. It supports only 1 Ethernet interface and has its own IP and MAC Addresses.
- **Wireless Nodes:** A Wireless node can be an end-node or a server. It is a 5-layer wireless device that can be connected to an Access point. It supports only 1 Wireless interface and has its own IP and MAC Addresses.
- **L2 Switch:** Switch is a layer-2 device that uses the devices' MAC address to make forwarding decisions. It does not have an IP address.
- **Router:** Router is a layer-3 device and supports a maximum of 24 interfaces each of which has its own IP address.

- **Access point:** Access point (AP) is a layer-2 wireless device working per 802.11 Wi-Fi protocol. It can be connected to wireless nodes via wireless links and to a router or a switch via a wired link.

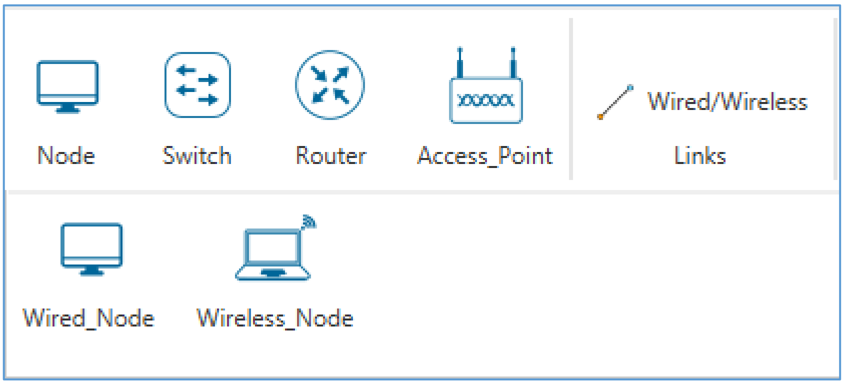


Figure 2-2: Internetworks Device Palette in GUI

2.2.1 Click and drop into environment

- **Add a Wired Node or Wireless Node:** In the toolbar, click the Node > Wired_Node icon (or) Node >Wireless_Node icon, and place the device in the grid.
- **Add a Router:** In the toolbar, click on the Router icon and place the Router in the grid.
- **Add a L2 Switch or L3 Switch:** In the toolbar, click on Switch > L2_Switch icon (or) Switch > L3_Switch icon and place the device in the grid.
- **Add an Access Point:** In the toolbar, click on the Access Point icon and place the Access Point in the grid
- Connect the devices by using Wired/Wireless Links present in the top ribbon/toolbar. Click on the first device and then click on the second device. A link will get formed between the two devices.
- Configure an application as follows:
  - Click the application icon on the top ribbon/toolbar.
  - Specify the source and destination devices.
  - Specify other application parameters per your model

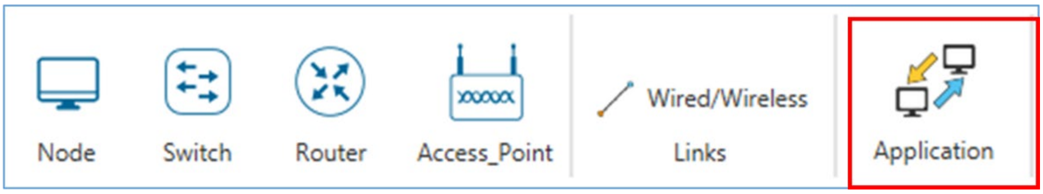


Figure 2-3: Top Ribbon/Toolbar

- Multiple applications can be generated by using add button in Application properties. Set the values and click on OK button. Detailed information on Application properties is available in **section 6** of NetSim User Manual.
- Right-click on any device (Router, Access_Point, L2_Switch, Wireless_Node, Wired_Node etc) and set the parameters.

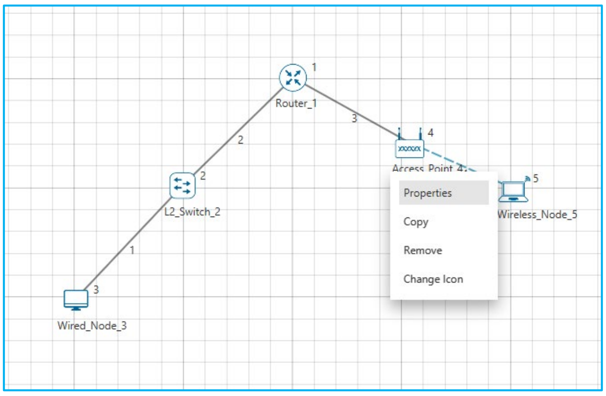
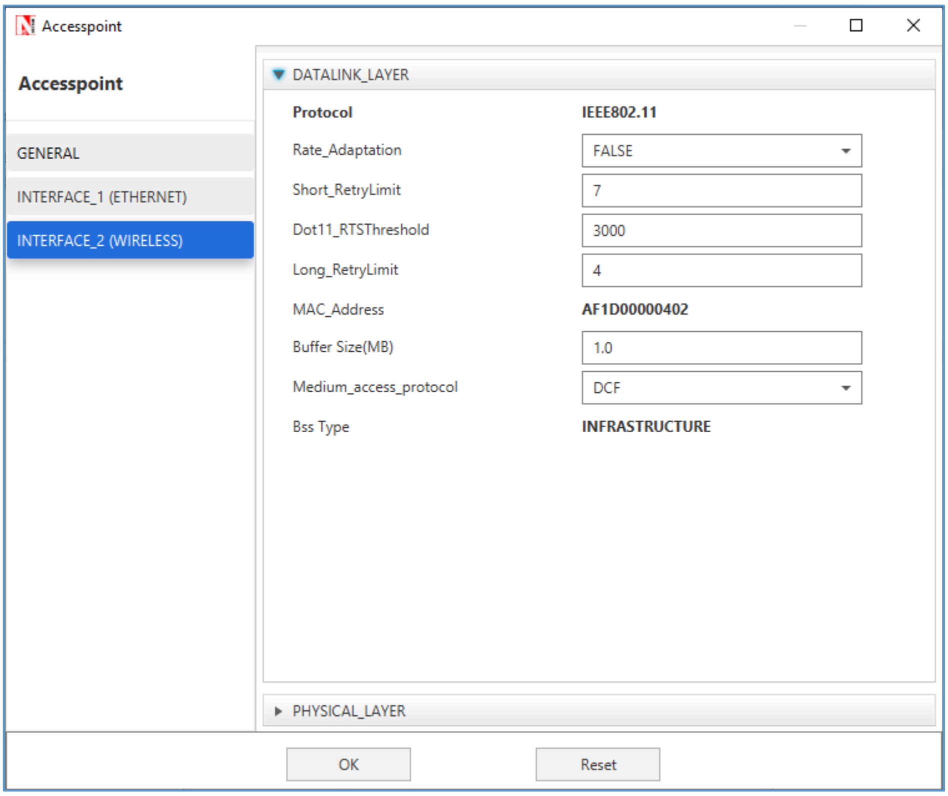


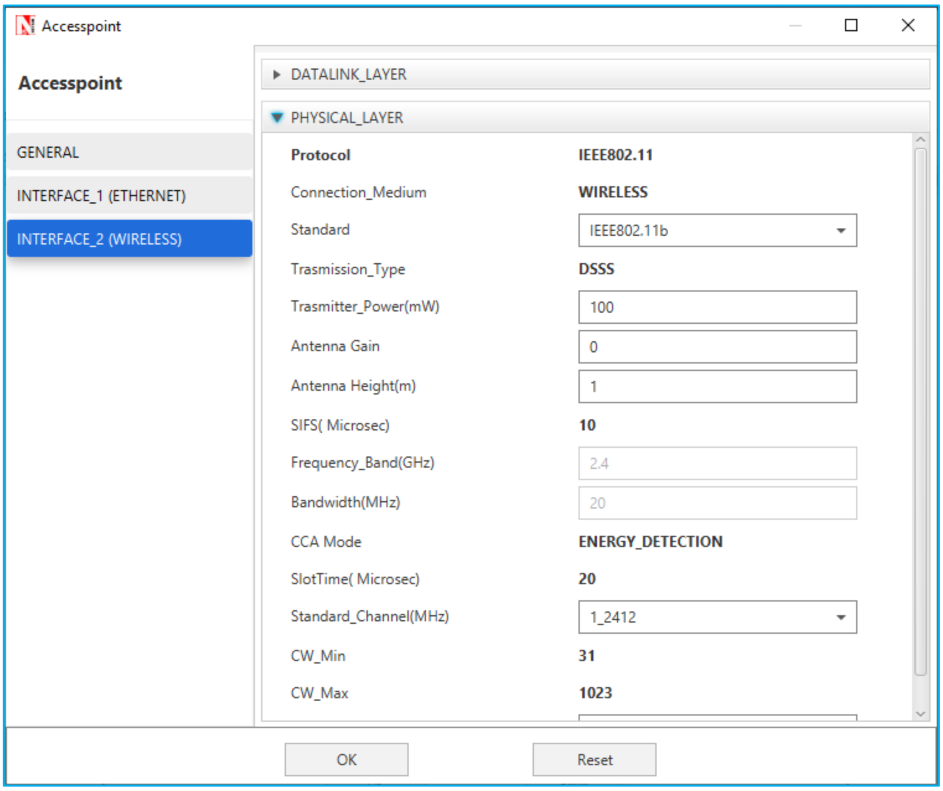
Figure 2-4: Device Properties

- The Interface_Wireless - Physical Layer and Interface_Wireless - DataLink Layer parameters are local. This means the parameter change does not propagate to the other devices. To set the same parameter value in all devices, ensure that you accordingly update the parameter values in all other devices (Access_Point or Wireless_Node) manually.



Protocol	IEEE802.11
Rate_Adaptation	FALSE
Short_RetryLimit	7
Dot11_RTSThreshold	3000
Long_RetryLimit	4
MAC_Address	AF1D00000402
Buffer Size(MB)	1.0
Medium_access_protocol	DCF
Bss Type	INFRASTRUCTURE

Figure 2-5: MAC properties of Access Point



Protocol	IEEE802.11
Connection_Medium	WIRELESS
Standard	IEEE802.11b
Trasmission_Type	DSSS
Trasmitter_Power(mW)	100
Antenna Gain	0
Antenna Height(m)	1
SIFS(Microsec)	10
Frequency_Band(GHz)	2.4
Bandwidth(MHz)	20
CCA Mode	ENERGY_DETECTION
SlotTime(Microsec)	20
Standard_Channel(MHz)	1_2412
CW_Min	31
CW_Max	1023

Figure 2-6: PHY Layer properties of Access Point

2.2.2 Link Properties

Right click on the link and click on properties to set link properties. Note that when simulating Internetworks if the link propagation delay is set too high then the applications may not see any throughput since it would take too long for OSPF to converge, and furthermore, TCP may also timeout (since max RTO is 3s).

2.3 Enable Packet Trace, Event Trace & Plots (Optional)

Click Packet Trace / Event Trace icon in the tool bar and click on OK button. For detailed help, please refer **sections 8.4** and **8.5** of the User Manual. Select Plots icon for enabling Plots and click on OK button see **Figure 2-7**.

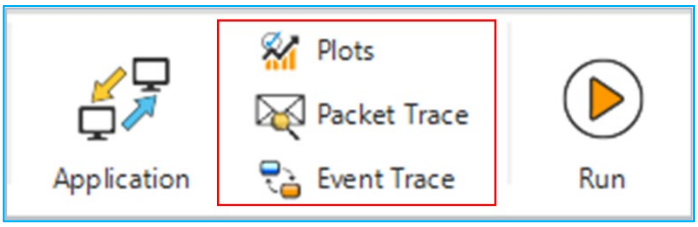


Figure 2-7: Packet Trace, Event Trace & Plots options on top ribbon

2.4 Run Simulation

Click on Run Simulation icon on the top ribbon/toolbar.

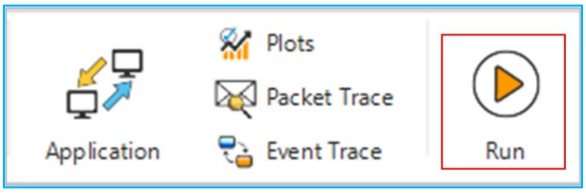
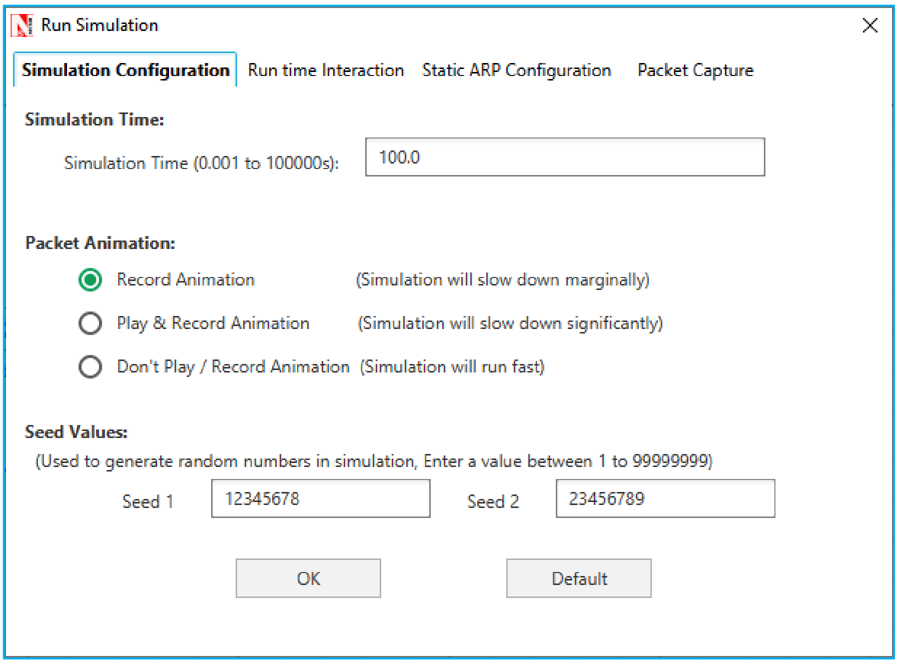


Figure 2-8: Run Simulation on top ribbon

Set the Simulation Time and click on OK button.


Run Simulation

Simulation Time:

Simulation Time (0.001 to 100000s): 100.0

Packet Animation:

● Record Animation (Simulation will slow down marginally)

○ Play & Record Animation (Simulation will slow down significantly)

○ Don't Play / Record Animation (Simulation will run fast)

Seed Values:

(Used to generate random numbers in simulation, Enter a value between 1 to 99999999)

Seed 1 12345678 Seed 2 23456789

Figure 2-9: Run Simulation window

3 Model Features

3.1 WLAN 802.11

The 802.11 models implement the 802.11 MAC and the 802.11 PHY abstracted at a packet-level.

The MAC Layer implements:

- Three kinds of nodes.
  - Wi-Fi AP (Internetworks).
  - Wireless Nodes (Internetworks) - In Internetworks APs and Wireless nodes are associated based on the connecting wireless link.
  - Standalone Wireless nodes (Mobile Adhoc networks).
- RTS/CTS/DATA/ACK transmissions.
- Packet queuing, aggregation, transmission, and retransmission.
- 802.11 EDCA.

The PHY layer implements:

- Propagation model (documented separately).
- Received power based on propagation model.
- Interference and signal to interference noise calculation.
- PHY Rate setting based on rate adaptation algorithms.
- BER calculation and packet error modelling.

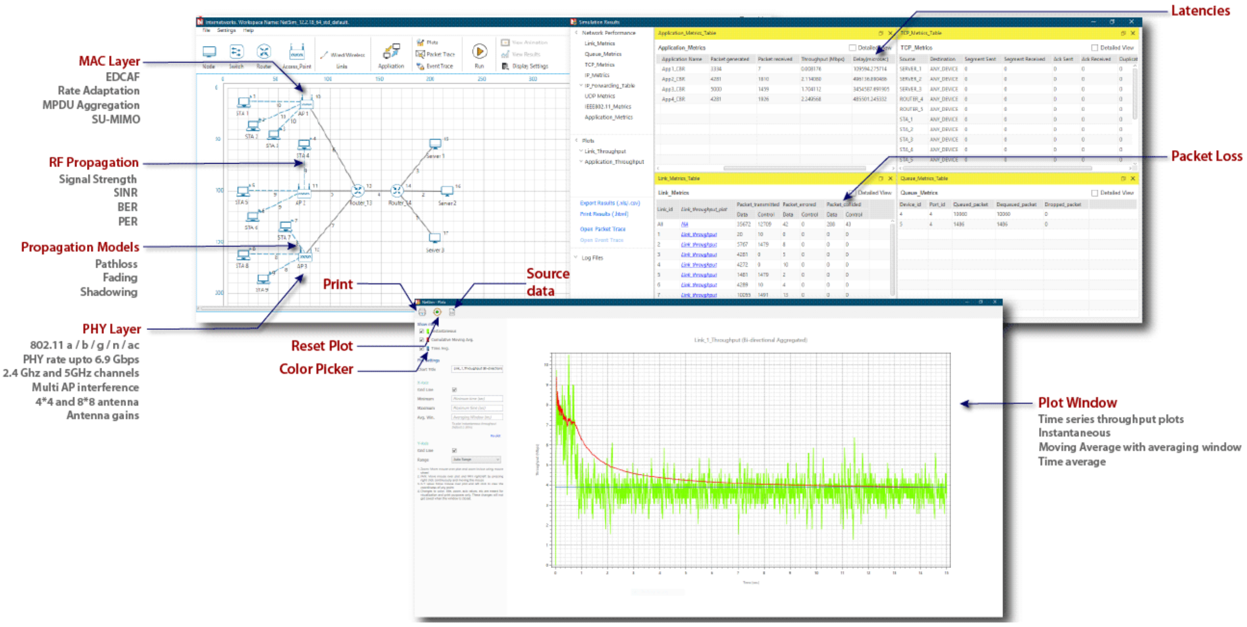


Figure 3-1: NetSim's Wifi design window, the results dashboard and the plots window

3.1.1 WLAN standards supported in NetSim

802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, 802.11e (EDCA) and 802.11p are the WLAN standards available in NetSim.

WLAN standard	Frequency (GHz)	Bandwidth (MHz)
802.11 a	5	20
802.11 b	2.4	20
802.11 g	2.4	20
802.11 n	2.4, 5	20, 40
802.11 ac	5	20, 40, 80, 160

Table 3-1: WLAN standards supported in NetSim

802.11 p and WAVE are described in the VANET Technology library documentation.

3.1.2 2.4 GHz Wi-Fi Channels

The following channel numbers are well-defined for 2.4GHz standards:

Channel Number	Center Frequency (MHz)
1	2412
2	2417
3	2422
4	2427
5	2432
6	2437
7	2442
8	2447
9	2452
10	2457
11	2462
12	2467
13	2472
14	2477

Table 3-2: 2.4 GHz Wi-Fi Channels

Channel 1, when IEEE 802.11b is configured, corresponds to a channel width of 22MHz and a center frequency of 2412MHz.

3.1.3 5GHz Channels

The following channel numbers are well-defined for **5GHz** standards:

Channel Number	Center Frequency (MHz)
36	5180
38	5190
40	5200
42	5210
44	5220
46	5230
48	5240
52	5260
56	5280
60	5300
64	5320

Table 3-3: 5GHz Wi-Fi Channels

Channel 36, when IEEE 802.11n is configured at 5GHz, corresponds to a channel width of 20MHz and a center frequency of 5180MHz.

3.1.4 Channel Numbering

The standard method to denote 5 GHz channels has been to always use the 20 MHz center channel frequencies for both 20 MHz and 40 MHz wide channels.

Channel Width	Channel Numbers
20 MHz	36, 40, 44, 48, 52, 56, 60, 64
40 MHz	38, 46, 54, 62
80 MHz	42, 58
160 MHz	50

Table 3-4: Channel Numbering

The following are the channel numbers of the non-overlapping channels for 802.11ac in NetSim:

- 20MHz: 36, 40, 44, 48, 52, 56, 60, 64
- 40MHz: 36, 44, 52, 60
- 80MHz: 36, 52
- 160MHz: 36

3.1.5 WLAN PHY Rates in NetSim

WLAN Standard	Frequency (GHz)	Bandwidth (MHz)	MIMO streams	PHY rate (Mbps)
a	5	20	N/A	6, 9, 12, 18, 24, 36, 48, 54
b	2.4	22	N/A	1, 2, 5.5, 11
g	2.4	20	N/A	6, 9, 12, 18, 24, 36, 48, 54
n	2.4, 5	20	4	Up to 288.8
		40		Up to 600
ac	5	20	8	Up to 346.8
		40		Up to 800
		80		Up to 1733.2
		160		Up to 3466.8

Table 3-5: WLAN PHY Rates in NetSim

3.1.6 PHY Implementation

NetSim is a packet level simulator for simulating the performance of end-to-end applications over various packet transport technologies. NetSim can scale to simulating networks with 100s of end-systems, routers, switches, etc. NetSim provides estimates of the statistics of application-level performance metrics such as throughput, delay, packet-loss, and statistics of network-level processes such as buffer occupancy, collision probabilities, etc.

In order to achieve scalable, network simulation, that can execute in reasonable time on desktop level computers, in all networking technologies the details of the physical layer techniques have been abstracted up to the point that bit-error probabilities can be obtained from which packet error probabilities are obtained.

NetSim does not implement any of the digital communication functionalities of the PHY layer. For the purpose of PHY layer simulation, the particular modulation and coding scheme, along with the transmit power, path loss, noise, and interference, yields the bit rate and the bit error rate by using well-known formulas or tables for the particular PHY layer being used. User would need to use a PHY Layer/RF/Link Level simulator for simulating various digital communication and link level functionalities. Typically these simulators will simulate just one transmitter-receiver pair, rather than a network.

Generally, in NetSim, the PHY layer parameters available for the user to modify are Channel Bandwidth, Channel Centre Frequency, Transmit-power, Receiver-sensitivity, Antenna-gains, and the Modulation-and-Coding-Scheme. When simulating standard protocols, these parameters can only be chosen from a standard-defined set. NetSim also has standard models for radio pathloss; the parameters of these pathloss models can also be set.

3.1.7 PHY States

The PHY radio states implemented in NetSim 802.11 are RX_ON_IDLE, RX_ON_BUSY, TRX_ON_BUSY.

- RX_ON_IDLE: This is the default radio state
- RX_ON_BUSY: This state is set at receiver radio when the reception of data begins. Upon completion of reception it changes to RX_ON_IDLE
- TRX_ON_BUSY: This state is set at the transmitter radio at the start of frame transmission. Upon completion of transmission it changes to RX_ON_IDLE
- A node in back off slots can be considered as equivalent to CCA busy. In NetSim, the radio state continues to be in RX_ON_IDLE
- SLEEP state is not implemented since NetSim 802.11 does not currently implement power save mode.

3.1.8 802.11 implementation details

Packets arriving from the NETWORK Layer gets queued up in an access buffer from which they are sorted according to their priority per 802.11 EDCA. An event MAC_OUT with SubEvent CS (Carrier Sense – CSMA) is added to check if the medium is free

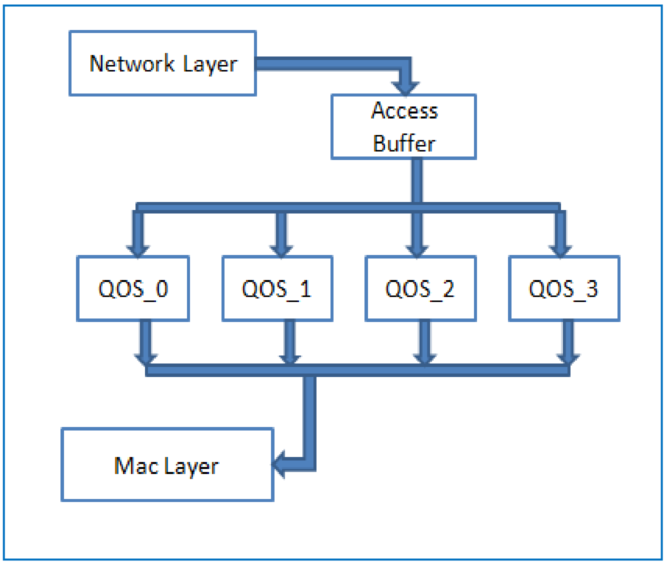


Figure 3-2: Packets transmission form Network layer to Mac Layer and how queued up in an access buffer

During CS, if the medium is free, then the NAV is checked. This occurs if the RTS/CTS mechanism is enabled which can be done so by adjusting the RTS Threshold. If the Present_Time > NAV, then an Event MAC_OUT with SubEvent DIFS End added at the time Present_Time + DIFS time.

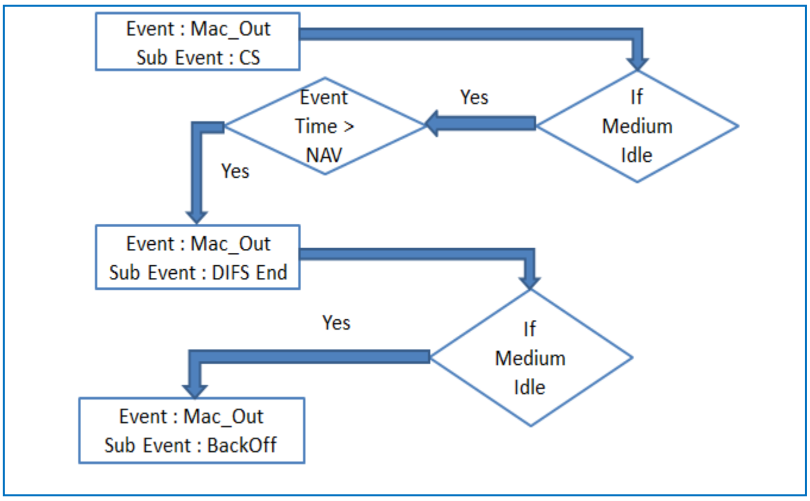


Figure 3-3: Event and SubEvent in Mac layer

The medium is checked at the end of DIFS time period and a random time BackOff is calculated based on the Contention Window (CW). An Event MAC_OUT with SubEvent BackOff is added at time Present_Time + BackOff Time.

Once BackOff is successful, NetSim starts the transmission process wherein it gets the aggregated frames from the QOS buffer and stores it in the Retransmit buffer. If the A-MPDU size is > RTS Threshold, then it enables RTS/CTS mechanism which is an optional feature.

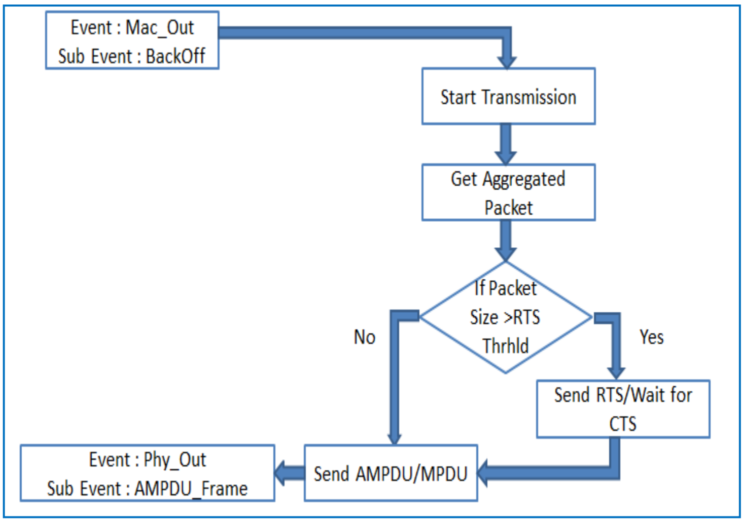


Figure 3-4: Event and SubEvent in Mac layer and Phy layer

NetSim sends the packet by calling the PHY_OUT Event with SubEvent AMPDU_Frame. Note that the implementation of A-MPDU is in the form of a linked list.

Whenever a packet is transmitted, the medium is made busy and a Timer Event with SubEvent Update Device Status is added at the transmission end time to set the medium again as idle.

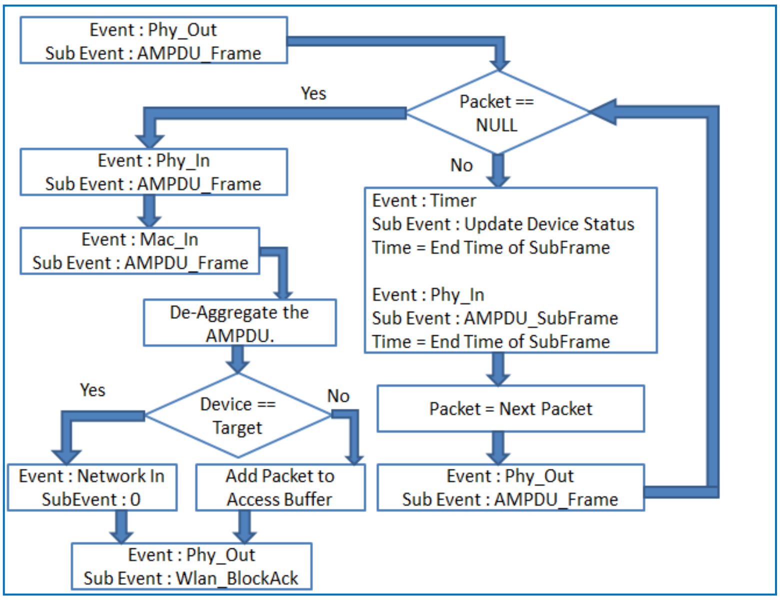


Figure 3-5: Event and SubEvent in Phy layer

Events PHY_OUT SubEvent AMPDU_SubFrame, Timer Event SubEvent Update Device Status and Event PHY_IN SubEvent AMPDU_SubFrame are added in succession for each MPDU (Subframe of the aggregated frame). This is done for collision calculations. If two stations start transmission simultaneously, then some of the SubFrames may collide. Only those collided SubFrames will be retransmitted again. The same logic is followed for an Errored packet. However, if the PHY header (the first packet) is errored or collided, the entire A-MPDU is resent.

At the receiver, the device de-aggregates the frame in the MAC Layer and generates a block ACK which is sent to the transmitter. If the receiver is an intermediate node, the de-aggregated frames are added to the access buffer of the receiver in addition to the packets which arrive from Network layer. If the receiver is the destination, then the received packets are sent to the Network layer. At the transmitter side, when the device receives the block acknowledgement, it retransmits only those packets which are errored. The rest of the packets are deleted from the retransmit buffer. This is done till all packets are transmitted successfully or a retransmit limit is reached after which next set of frames are aggregated to be sent.

3.1.9 802.11ac MAC and PHY Layer Implementation

Improvements in 802.11ac compared to 802.11n

Feature	802.11n	802.11ac
Spatial Streams	Up to 4 streams	Up to 8 streams
MIMO	Single User MIMO	Multi-User MIMO
Channel Bandwidth	20 and 40 MHz	20, 40, 80 and 160 MHz (optional)
Modulation	BPSK, QPSK, 16QAM and 64QAM	BPSK, QPSK, 16QAM, 64QAM and 256QAM (optional)
Max Aggregated Packet Size	65536 octets	1048576 octets

Table 3-6: Feature Comparison between 802.11ac to 802.11n

MAC layer improvements include only the increment of number of aggregated frames from 1 to 64. The MCS index for different modulation and coding rates are as follows:

1	Modulation	Code Rate
0	BPSK	1/2
1	QPSK	1/2
2	QPSK	3/4
3	16QAM	1/2
4	16QAM	3/4
5	64QAM	2/3
6	64QAM	3/4
7	64QAM	5/6
8	256QAM	3/4
9	256QAM	5/6

Table 3-7: Different Modulation scheme vs. Code Rates

Receiver sensitivity for different modulation schemes in 802.11ac (for a 20MHz Channel bandwidth) are as follows.

MCS Index	Receiver Sensitivity (in dBm)
0	-82
1	-79
2	-77
3	-74
4	-70
5	-66
6	-65
7	-64
8	-59
9	-57

Table 3-8: MCS index vs. Receiver Sensitivity (Rx-sensitivity)

The Rx-sensitivity is then set per the above table in conjunction with Max Packet Error Rate (PER) as defined in the standard.

If users wish to apply just the Rx-sensitivity (also termed as rate dependent input level), then the calculate_rxpower_by_per() function call in the function fn_NetSim_IEEE802_11_HTPhy_UpdateParameter() in the file IEEE802_11_HT_PHY.c can be commented.

Number of subcarriers for different channel bandwidths

PHY Standard	Subcarriers	Capacity relative to 20MHz in 802.11ac
802.11n/802.11ac 20MHz	Total 56, 52 Usable (4 pilot)	x1.0
802.11n/802.11ac 40MHz	Total 114, 108 Usable (6 pilot)	x2.1
802.11ac 80MHz	Total 242, 234 Usable (8 pilot)	x4.5
802.11ac 160MHz	Total 484, 468 Usable (16 pilot)	x9.0

Table 3-9: Number of subcarriers for different channel bandwidths

With the knowledge of MCS index and bandwidth of the channel data rate is set in the following manner

1. Get the number subcarriers that are usable for the given bandwidth of the medium.
2. Get the Number of Bits per Sub Carrier (NBPSC) from selected MCS
3. Number of Coded Bits Per Symbol (NCBPS) = NBPSC*Number of Subcarriers
4. Number of Data Bits Per Symbol (NDBPS) = NCBPS*Coding Rate
5. Physical level Data Rate = NDBPS/Symbol Time (4micro sec for long GI and 3.6 micro sec for short GI).

3.1.10 MAC Aggregation in NetSim

NetSim supports A-MPDU aggregation and does not support A-MSDU aggregation. MAC Aggregation is independent of PHY Rate or BER. It is the PHY Rate that adapts to BER via Rate Adaptation algorithms.

In the aggregation scheme shown in Figure 3-6, several MPDU's (MAC Protocol Data Units) are aggregated into a single A-MPDU (Aggregated MPDU). The A-MPDUs are created before transfer to the PHY. The MAC does not wait for MPDUs to aggregate. It aggregates the frames already queued to form an A-MPDU. The maximum size of an A-MPDU is 65,535 bytes.

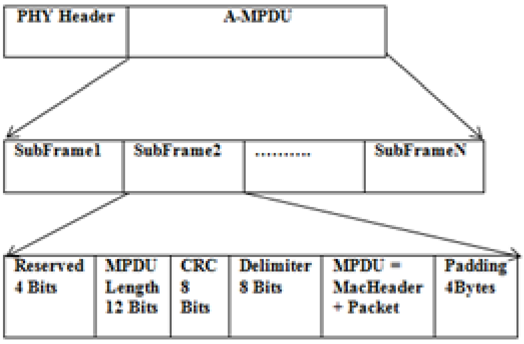
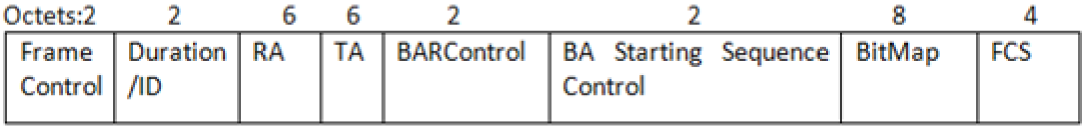


Figure 3-6: Aggregation scheme

In 802.11n, a single block acknowledgement is sent for the entire A-MPDU. The block ack acknowledges each packet that is received. It consists of a bitmap (compressed bitmap) of 64bits or 8 bytes. This bitmap can acknowledge up to 64 packets, 1bit for each packet.

The value of a bitmap field is 1, if respective packet is received without error else it is 0. Only the error packets are resent until a retry limit is reached. The number of packets in an A-MPDU is restricted to 64 since the size of block ack bitmap is 64bits.



Octets:2	2	6	6	2	2	8	4
Frame Control	Duration /ID	RA	TA	BARControl	BA Starting Sequence Control	BitMap	FCS

Figure 3-7: Block Ack Control Packet

- NetSim uses the parameter, Number of frames to aggregate, while the standard uses the parameter A-MPDU Length Exponent. Per standard the A-MPDU length in defned by two parameters: Max AMPDU length exponent and BLOCK ACK Bitmap. The AMPDU length in bytes is $2^{(13+MaximumAMPDULengthExponent)} - 1$.
- Since NetSim doesn't model A-MSDU, a design decision was made to model A-MPDU based on Block ACK bitmap size (to indicate the received status of up to 64 frames) and therefore the parameter - Number of frames to aggregate - in the GUI
- When EDCA is enabled, packet aggregation is done separately for each QoS class

- NetSim ignores the padding bytes added to the MPDU
- The MAC aggregates packets destined to the same receiver, irrespective of the end destination. Receiver is to be understood as the next hop in a wireless transmission.
- RTS threshold is compared against the total A-MPDU size.
- Aggregation functionality may be incorrectly executed if $NumberOfFramesToAggregate \times PacketSize\ (B) > 65{,}535\ (B)$

3.1.11 Signal to interference and noise calculation

At each receiver, in the beginning when the first packet is transmitted and every time the transmitter or receiver moves, NetSim calculates the received signal level from transmitter. The received signal level would be equal to transmit power less propagation losses. Next, NetSim calculates the interference received at the same receiver, from all the interfering transmission. Only co-channel interference is accounted, and adjacent channel interference is not calculated. Finally, NetSim takes the ratio (SINR) of the signal level to the sum of the total interference from other transmissions and the downlink noise.

Once the SINR is calculated the BER is got from the SNR-BER tables for the applicable modulation scheme. This BER is then converted to Packet-Error-Rate and packet error (Yes/No) is determined stochastically.

The same is explained diagrammatically below.

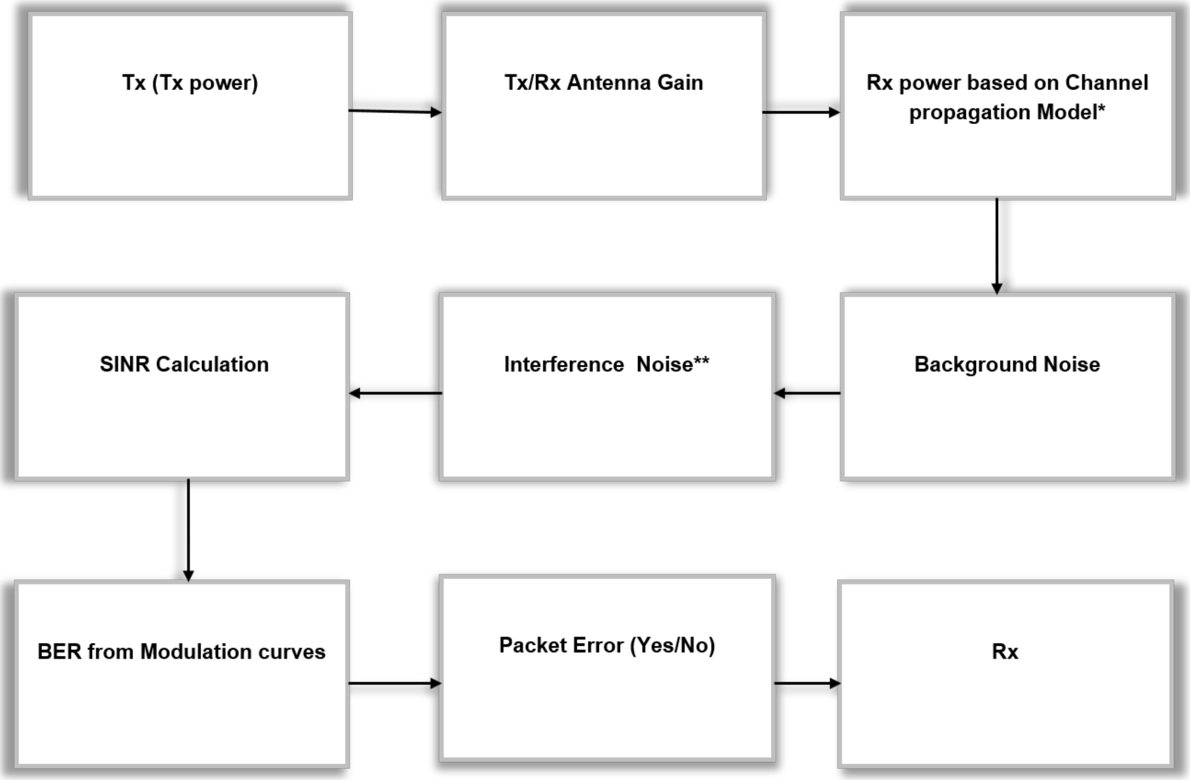


Figure 3-8: Radio Tx-Rx for one transmission

* Propagation model covers path loss, fading and shadowing. The models are documented in a separate document named Propagation-Models.pdf
** Interference noise due to other transmissions within the network

3.1.12 Transmit Power

The user can set a fixed transmit power via the GUI. Transmit power is a local variable; each STA and AP can be set to have different transmit powers. The transmit power can be dynamically varied by modifying the underlying 802.11 source C code.

3.1.13 Carrier Sense

Transmit power less propagation losses is the received power. The propagation loss is the sum (in dB scale) of pathloss, shadowing loss and fading loss. Various propagation models are available and are detailed in the Propagation model manual. Pathloss, Fading, and Shadowing can be turned on/off in GUI.

If $ReceiverSensitivity(Lowest\ MCS) \geq\ Receiver - Power \geq ED - Threshold$ the medium is set to busy. Note that CSMA/CA algorithm operates according to the medium state (busy/idle).

If $Received - Power > Reciver - Sensitivity\ (LowestMCS)$ then MCS is set depending by comparing Received-power against Receiver-sensitivity per standard tables, and signal is decoded. Packet error is decided by looking up the SINR-BER table for the given MCS.

These variables can also be dynamically by modifying the underlying 802.11 source C code.

3.1.14 Carrier Sense Range

Consider two 802.11 STAs, each at their decode distance (for a given MCS) on opposite sides of an AP. They should be able to sense each other for good operation of DCF even within a single AP network. Therefore, in NetSim we have taken a conservative approach whereby the CarrierSenseRange would approximately be twice the largest DecodeRange.

This is implemented using the variable CSRANGEDIFF which is set to -10dB. This implies a 10dB differential between Rx-sensitivity (which determines DecodeRange) and EDThreshold (which determines CarrierSenseRange). The value of CSRANGEDIFF can be modified by the user in NetSim Standard or Pro versions, which ship with source code.

3.1.15 Transmitter’s choice of MCS

If the rate adaptation algorithm is turned off, then the transmitter chooses MCS by comparing the RSSI (calculated at the receiver) against the Receiver-sensitivity tables for different MCS.

If rate adaptation is turned on, then for the very first packet alone, the MCS is chosen like when the adaptation algorithm is off. Subsequently, the adaptation algorithm takes over. To give an example, in one algorithm, the rate (MCS) goes up 1-step for every 20 continuous successful packet transmissions and goes down 1-step for every 3 continuous packet transmission failures.

3.1.16 IEEE 802.11 e QoS and EDCA

Quality of Service (QoS) provides you with the ability to specify parameters on multiple queues for increased throughput and better performance of differentiated wireless traffic like Voice-over-IP (VoIP), other types of audio, video, and streaming media, as well as traditional IP data over the Access Point.

QoS was introduced in 802.11e and is achieved using enhanced distributed channel access functions (EDCAFs). EDCA provides differentiated priorities to transmitted traffic, using four different access categories (ACs). With EDCA, high-priority traffic has a higher chance of being sent than low-priority traffic: a station with high priority traffic waits a little less before it sends its packet, on average, than a station with low priority traffic. This differentiation is achieved through varying the amount of time a station would sense the channel to be idle, and the length of the contention window for a backoff.

In addition, EDCA provides contention-free access to the channel for a period called a Transmit Opportunity (TXOP). A TXOP is a bounded time interval during which a station can send as many frames as possible (as long as the duration of the transmissions does not extend beyond the maximum duration of the TXOP). If a frame is too large to be transmitted in a single TXOP, it should be fragmented into smaller frames. The use of TXOPs reduces the problem of low rate stations gaining an inordinate amount of channel time in the legacy 802.11 DCF MAC. A TXOP time interval of 0 means it is limited to a single MPDU.

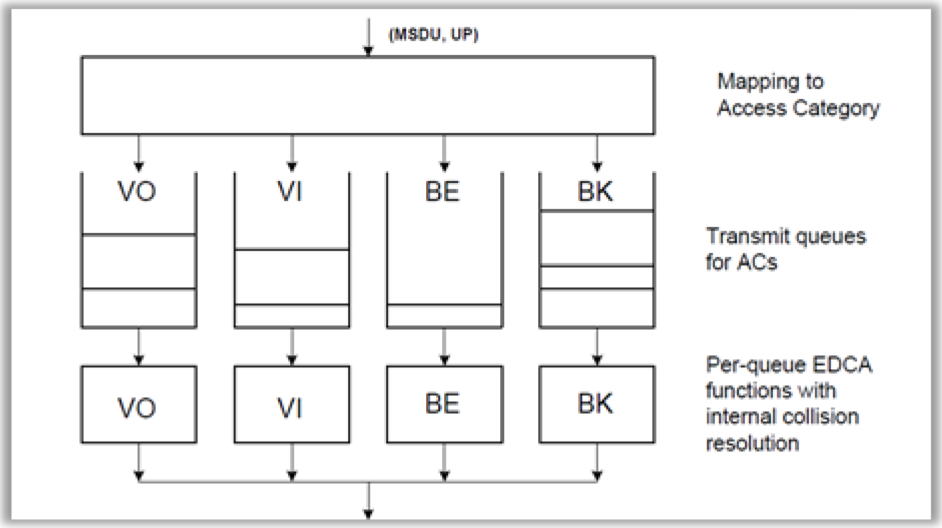

(MSDU, UP)
Mapping to Access Category
VO
VI
BE
BK
Transmit queues for ACs
VO
VI
BE
BK
Per-queue EDCA functions with internal collision resolution

Figure 3-9: Enhanced Distributed Channel Access (EDCA) in 802.11

NetSim categorizes application packets based on QoS class set in application properties as follows

- VO: UGS and RTPS
- VI: NRTPS and ERTPS
- BE: BE and all control packets suck as TCP ACKs
- BK: Everything else

3.1.16.1 Default EDCA Parameters

The following tables shows the default EDCA parameters. This default parameter set is per page 899, IEEE Std 802.11-2016

Access Category	CWmin	CWmax	AIFSN	Max TXOP (μs)
Background (AC_BK)	31	1023	7	3264
Best Effort (AC_BE)	31	1023	3	3264
Video (AC_VI)	15	31	2	6016
Voice (AC_VO)	7	15	2	3264

Table 3-10: Default EDCA access parameters for 802.11 b for both AP and STA

Access Category	CWmin	CWmax	AIFSN	Max TXOP (μs)
Background (AC_BK)	15	1023	7	2528
Best Effort (AC_BE)	15	1023	3	2528

Video (AC_VI)	7	15	2	4096
Voice (AC_VO)	3	7	2	2080

Table 3-11: Default EDCA access parameters for 802.11 a / g / n / ac for both AP and STA

Access Category	CWmin	CWmax	AIFSN	Max TXOP (μs)
Background (AC_BK)	15	1023	9	0
Best Effort (AC_BE)	15	1023	6	0
Video (AC_VI)	7	15	3	0
Voice (AC_VO)	3	7	2	0

Table 3-12: Default EDCA access parameters for 802.11 p (dot11OCBActivated is true)

Note: The EDCA parameters can be configured by changing the Physical type parameter according to the different standard, IEEE802.11b (Medium Access Protocol → DSSS), IEEE802.11n (Medium Access Protocol → HT), IEEE802.11ac (Medium Access Protocol → VHT), IEEE802.11a and g (Medium Access Protocol → OFDMA and OCBA →FALSE), IEEE802.11p (Medium Access Protocol → OFDMA and OCBA →TRUE).

3.1.17 Rate Adaptation

Three rate adaptation settings are available in NetSim.

1. FALSE: This is similar to Receiver Based Auto Rate (RBAR) algorithm. In this, the PHY rate gets set based on the target PEP (packet error probability) for a given packet size, as given in the standard. The adaptation is termed as “FALSE” since the rate is pre-determined as per standard and there is no subsequent “adaptation”.
    a. 802.11 n/ac: Target PEP = 0.1, Packet Size: 4096 B
    b. 802.11 b: Target PEP = 0.08, Packet Size: 1024B
    c. 802.11 a/g/p: Target PEP:0.1, Packet size1000B
2. GENERIC: This is similar to the Auto Rate Fall Back (ARF) algorithm. In this algorithm:
    a. Rate goes up one step for 20 consecutive packet successes
    b. Rate goes down one step for 3 consecutive packet failures
3. MINSTREL: Per the minstrel rate adaptation algorithm implemented in Linux

3.1.18 Model Limitations

1. Mobility of Wireless nodes is not available in infrastructure mode (when connected via an Access Point) and is only available in Adhoc mode. Hence mobility for wireless nodes can only be set when running MANET simulations.
2. Authentication and encryption are not supported

3. Interference with Non Wi-Fi signals is not modeled
4. While different APs can operate in different channels, all the Wireless nodes connected to one AP operate in the same channel.
5. No beacon generation, probing or association
6. RTS, CTS and ACK are always transmitted at the base rate (lowest MCS)
7. Roaming whereby a STA leaves serving AP to associate with target AP (usually based on RSSI/SNR)

3.1.19 IEEE802.11 Results

IEEE802.11 performance metrics will be displayed in the results dashboard if the network scenario simulated consisted of at least one device with WLAN protocol enabled.

Parameter	Description
Device_Id	It represents the Id's of the wireless devices which supports 802.11 (WLAN)
Interface_Id	It represents the interface Id's of the wireless nodes
Frame Sent	It is the Number of frames sent by Access Point
Frame Received	It is the number of frames received by a wireless node
RTS Sent	It is the number of Request to send (RTS) packets sent by a Wireless Node. RTS/CTS frames are sent prior to transmission when the packet size exceeds RTS threshold. The access point receives the RTS and responds with a CTS frame. The station must receive a CTS frame before sending the data frame. The CTS also contains a time value that alerts other stations to hold off from accessing the medium while the station initiating the RTS transmits its data.
RTS Received	It is the number of RTS packets received by an Access Points
CTS Sent	It is the number of Clear to send (CTS) packets sent by an Access Points
CTS Received	It is the number of CTS packets received by Wireless Nodes

Successful BackOff	It is the number of successful backoffs running at a wireless node. In the IEEE 802.11 Wireless Local Area Networks (WLANs), network nodes experiencing collisions on the shared channel need to BackOff for a random period of time, which is uniformly selected from the Contention Window (CW). BackOff is a timer which is decreased as long as the medium is sensed to be idle for a DIFS, and frozen when a transmission is detected on the medium, and resumed when the channel is detected as idle again for a DIFS interval
Failed BackOff	It is the number of failed backoffs at wireless node

Table 3-13: Description of IEEE 802.11 Metrics

3.2 Layer 2 (L2) Ethernet Switching

Layer 2 switches have a MAC address table that contains a MAC address and port number. Switches follow this simple algorithm for forwarding packets:

1. When a frame is received, the switch compares the SOURCE MAC address to the MAC address table. If the SOURCE is unknown, the switch adds it to the table along with the port number the packet was received on. In this way, the switch learns the MAC address and port of every transmitting device.
2. The switch then compares the DESTINATION MAC address with the table. If there is an entry, the switch forwards the frame out the associated port. If there is no entry, the switch sends the packet out all its ports, except the port that the frame was received on This is termed as Flooding.
3. Note that the switch does not learn the destination MAC until it receives a frame from that device

3.2.1 Spanning Tree Protocol

NetSim ethernet switches implement Spanning tree protocol to build a loop-free logical topology. This is always enabled and cannot be disabled.

3.2.2 Switch Port States

All switch ports in switches can be in one of the following states:

- Blocking: A port that would cause a switching loop if it were active. No user data is sent or received over a blocking port.

- Listening: The switch processes BPDUs and awaits possible new information that would cause it to return to the blocking state. It does not populate the MAC address table and it does not forward frames.
- Learning: While the port does not yet forward frames, it does learn source addresses from frames received and adds them to the filtering database (switching database). It populates the MAC address table but does not forward frames.
- Forwarding: A port receiving and sending data in Ethernet frames, normal operation.

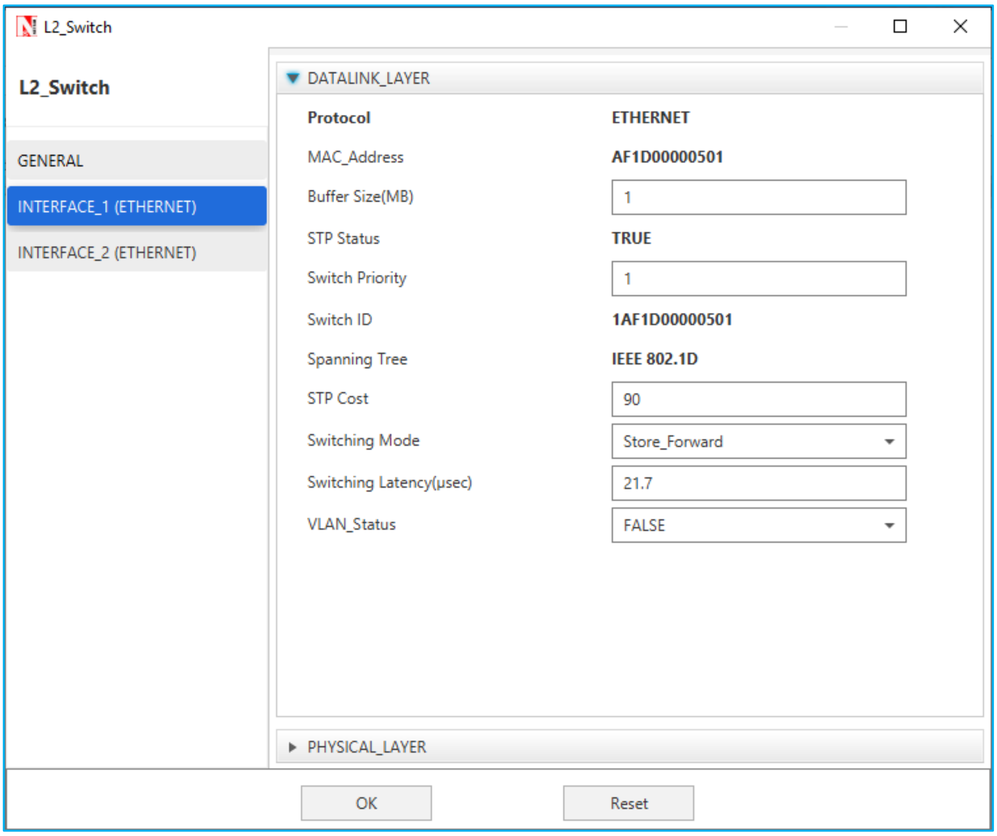
It is recommended that the application start time is set to a value that is greater than the time it takes for the spanning tree protocol to complete (typically of the order of a hundreds of milliseconds).

3.2.3 Model Limitations

1. The spanning protocol is only run at the beginning of simulation. If a link fails, the spanning protocol is not re-run.
2. If applications are started prior to completion of spanning tree protocol, then the MAC table created is not updated per the spanning tree protocol.
3. Jumbo Frames are not supported in NetSim Ethernet Protocol

3.2.4 GUI Configuration of Switch

Switch properties can be set by right clicking on a switch --> Properties --> Interface_x (Ethernet).



Protocol ETHERNET
MAC_Address AF1D00000501
Buffer Size(MB) 1
STP Status TRUE
Switch Priority 1
Switch ID 1AF1D00000501
Spanning Tree IEEE 802.1D
STP Cost 90
Switching Mode Store_Forward
Switching Latency(µsec) 21.7
VLAN_Status FALSE

Figure 3-10: Data Link Layer Properties of a Switch

The properties that can be set are:

Parameter	Type *	Range	Description
MAC ADDRESS	Fixed	Auto generated	The MAC address is a unique value associated with a network adapter. This is also known as hardware address or physical address. This is a 12-digit hexadecimal number (48 bits in length).
Buffer Size (MB)	Local	1-5	Buffer is the memory in a device which holds data packets temporarily. If the transmitting port is busy, incoming packets are stored in the buffer. NetSim models the buffer as an egress buffer and the range is 1 MB to 5MB per port of the switch.
STP Status	Fixed	TRUE	Spanning Tree Protocol is set to “True” in the Switches by default.

Switch Priority	Local	1-61440	This is the priority that can be assigned to the Switch. Priority is involved in deciding the root bridge for STP.
Switch ID	Fixed	1-15	Each switch has a unique ID for spanning tree calculation. The ID is derived by combining the priority and MAC address. Since a switch has a MAC address for each port, the least of the MAC address of the connected ports is taken while forming the unique ID.
Spanning Tree	Fixed	IEEE802.1D	The Spanning Tree Protocol (STP) ensures a loop-free topology for any bridged Ethernet local area network. The basic function of STP is to prevent bridge loops and the broadcast radiation that results from them. STP is standardized as IEEE 802.1D. As the name suggests, it creates a spanning tree within a network of connected layer-2 bridges (typically Ethernet switches) and disables those links that are not part of the spanning tree, leaving a single active path between any two network nodes.
STP Cost	Local	0-1000	Cost used by the switch to calculate spanning tree. The cost assigned to each port is based on its data rate.
Switching Mode	Local	Store Forward, Cut Through	Store and Forward: Forwarding takes place only after receipt of complete frame. This technique buffers the incoming frame and checks for errors. If no error is found it forwards the frame to the outgoing port, otherwise it discards the frame. Cut through: Switch forwards the incoming frames to its appropriate outgoing port

			immediately after receipt of destination address of the frame.
Switching Latency	Local	0-10000	Switching latency is defined as the time it takes for a switch to forward a packet from its ingress port to its egress port. The lower the latency, the less time the packet needs to stay in the switch waiting to be processed, the faster the switch, the quicker the packets can be sent to the intended destination host.
VLAN Status*	Local	TRUE, FALSE	To enable/disable VLAN

Table 3-14: Description of Datalink layer properties of switch parameter

*Requires license for Component 3 Advanced Routing and Switching

3.3 Open Shortest Path First (OSPF v2) Routing Protocol

3.3.1 OSPF Overview

OSPF is a link-state routing protocol. It is designed to be run internal to a single Autonomous System. Each OSPF router maintains an identical database describing the Autonomous System's topology. From this database, a routing table is calculated by constructing a shortest-path tree.

OSPF routes IP packets based solely on the destination IP address found in the IP packet header. IP packets are routed "as is" -- they are not encapsulated in any further protocol headers as they transit the Autonomous System. OSPF is a dynamic routing protocol. In NetSim, OSPF can detect topological changes in the AS (such as router interface failures) and calculate new loop-free routes after a period of convergence.

Each router maintains a database describing the Autonomous System's topology. This database is referred to as the link-state database. Each participating router has an identical database. Each individual piece of this database is a particular router's local state (e.g., the router's usable interfaces and reachable neighbors). The router distributes its local state throughout the Autonomous System by flooding.

All routers run the exact same algorithm, in parallel. From the link-state database, each router constructs a tree of shortest paths with itself as root. This shortest-path tree gives the route to each destination in the Autonomous System. The cost of a route is described by a single dimensionless metric.

3.3.2 OSPF Features

1. OSPF Messages – Hello, DD, LS Request, LS Update, LS Ack
2. Router LSA
3. The Neighbor Data structure features the following
    - Link state request list
    - DB summary list
    - Link state re-transmission list
    - Link state send list
    - Link state re-transmission timer
    - Inactivity timer
4. Routing table
5. Shortest path tree
6. The Interface data structure features
    - Neighbor router list
    - Flood timer
    - Update LS list
    - Network LS timer
    - Delayed ack list
7. The Protocol data structure features
    - Interface list
    - Area list
    - Max age removal timer
    - SPF timer
    - Routing table
8. The Area Data structure features
    - Associated interface list
    - Router LSA list
    - Network LSA list
    - Router summary LSA list
    - Network summary LSA list
    - Max age list
    - Router LS timer
    - Shortest path list
9. The following can be logged during simulation
    - Hello log
    - SPF log

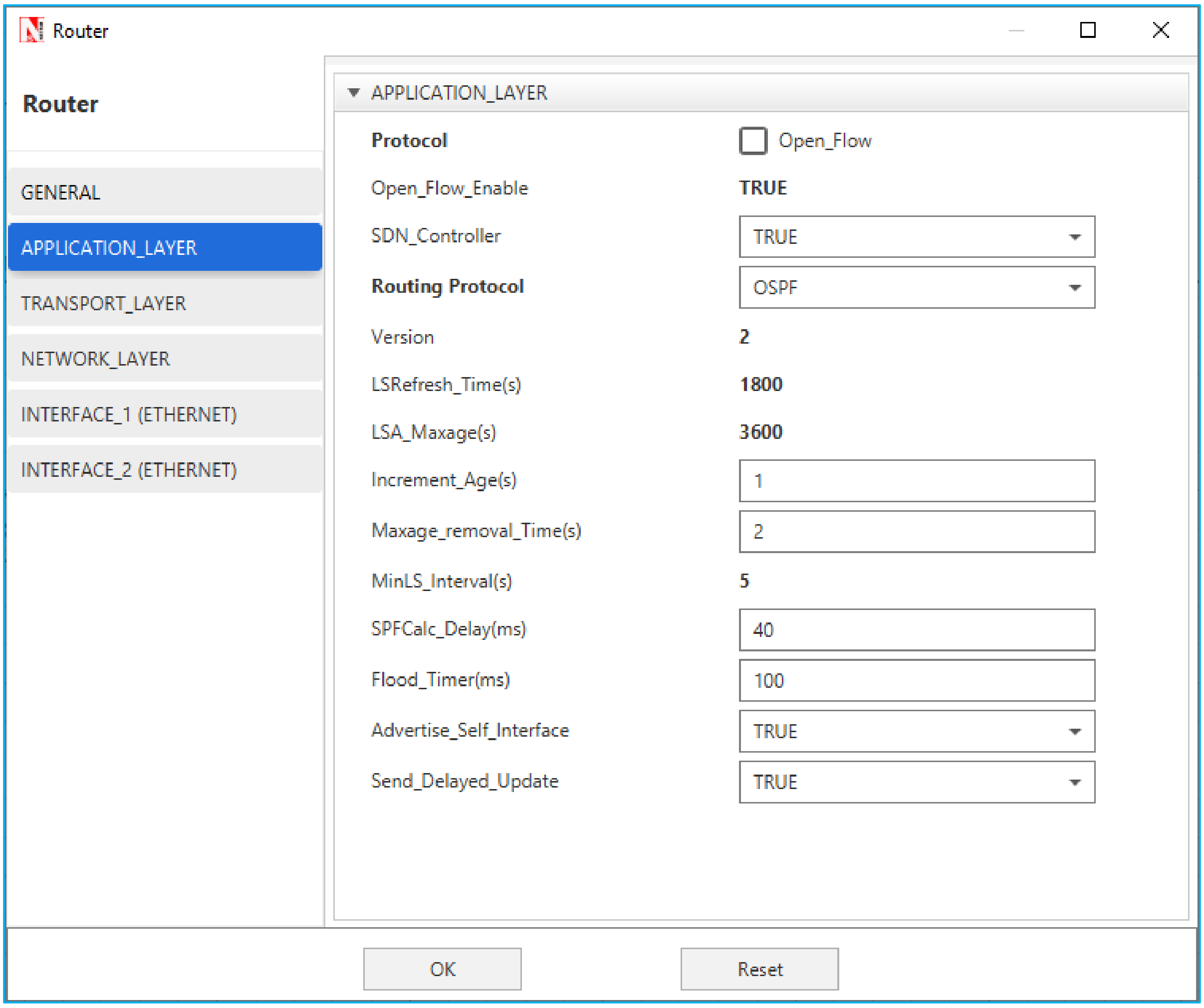
- Common log
- Debug logs – LSDB, RXList, RLSA, RCVLSU, LSULIST, Route

3.3.3 Excluded Features

The following features in OSPF have not been implemented - Multiple Areas, Network LSA, Router summary LSA, Network summary LSA, Authentication, Equal cost multipath, External AS, External routing information, Interface type – Broadcast, NBMA, Virtual, Point to multi-point

3.3.4 GUI Configuration of OSPF

OSPF properties can be set by right clicking on Router --> Properties --> Application layer see **Figure 3-11**.



Protocol □ Open_Flow

Open_Flow_Enable TRUE

SDN_Controller TRUE

Routing Protocol OSPF

Version 2

LSRefresh_Time(s) 1800

LSA_Maxage(s) 3600

Increment_Age(s) 1

Maxage_removal_Time(s) 2

MinLS_Interval(s) 5

SPFCalc_Delay(ms) 40

Flood_Timer(ms) 100

Advertise_Self_Interface TRUE

Send_Delayed_Update TRUE

Figure 3-11: Routing protocol properties of router

The properties that can be set are:

Parameter	Type *	Range	Description
Version	Global	Fixed	OSPF Version 2 as per RFC 2328 for IPv4.
LSRefresh_Time (s)	Global	Fixed	The maximum time between distinct originations of any particular Link State Advertisement (LSA). If the link state age field of one of the router's self-originated LSAs reaches the value LSRefreshTime, a new instance of the LSA is originated, even though the contents of the LSA (apart from the LSA header) will be the same. The value of LSRefreshTime is set to 30 minutes.
LSA_Maxage (s)	Global	Fixed	The maximum age that an LSA can attain. When an LSA's LS age field reaches MaxAge, it is reflooded in an attempt to flush the LSA from the routing domain. LSAs of age MaxAge are not used in the routing table calculation. The default value of MaxAge is set to 1 hour or 3600s
Increment_Age (s)	Global	0 - 100	This is an internal variable of NetSim used for simulation purposes. This value decides how often to increase the age of the LSA in the OSPF LSA Lists. A small value will cause frequent updates and provide higher accuracy but may slow down simulation, and vice versa for a large value
Maxage_removal_Time (s)	Global	0 - 9999	This variable decides the time when the LSA is removed from the MaxAgeLSA List

MinLS_Interval (s)	Global	Fixed	The minimum time between distinct originations of any particular LSA. The value of MinLSInterval is set to 5 seconds
SPFCalc_Delay (ms)	Global	0 - 9999	If SPF calculation is triggered, then the router will wait for this duration before starting the calculation. This can be used for the router to take multiple updates into account
Flood_Timer (ms)	Global	0 - 9999	The amount of time to wait before initializing the flood procedure. A random number between 0 to the set value will be chosen. The flood timer on/off is per the ISSENDDELAYUPDATE variable setting
Advertise_Self_Interface	Global	True/False	This is reserved for future use. As of NetSim v12, this should always be true. This will be used when a point-to-multipoint link is connected to the interface, and when such links are connected this should be set to false
Send_Delayed_Update	Global	True/False	This variable can be set to true to delay sending the LSU. If set to true, then the delay would be per the flooding timer. Else the update is set immediately.

Table 3-15: Description of Application layer Routing protocol properties

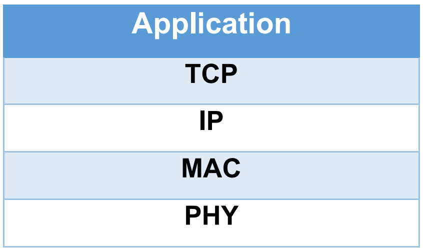
*Global – Changes in all devices of similar type. Local – Only changes in current device

3.4 Transmission Control Protocol (TCP)

3.4.1 TCP overview

TCP is a connection-oriented, end-to-end reliable protocol designed to fit into a layered hierarchy of protocols which support multi-network applications. The TCP provides for reliable communication between host computers connected computer communication networks. Very few assumptions are made as to the reliability of the communication protocols below the TCP layer. TCP assumes it can obtain a simple, potentially unreliable datagram service from the lower level protocols. In principle, the TCP should be able to operate above a wide spectrum of communication systems ranging from wired to wireless to mobile communication.

The TCP fits into a layered protocol architecture just above a basic Internet Protocol which provides a way for the TCP to send and receive variable-length segments of information enclosed in IP packets. The IP packet provides a means for addressing source and destination TCPs in different networks. The IP protocol also deals with any fragmentation or reassembly of the TCP segments required to achieve transport and delivery through multiple networks and interconnecting gateways.



Application

TCP

IP

MAC

PHY

Figure 3-12: Protocol Layering

3.4.2 TCP Features

The following features are implemented in TCP.

1. Three-way handshake (open/close)
2. Sequence Numbers
3. Slow start and congestion avoidance
4. Fast Retransmit/Fast Recovery
5. Selective Acknowledgement

3.4.3 Congestion Control Algorithms in TCP

The following congestion control algorithms are supported in NetSim.

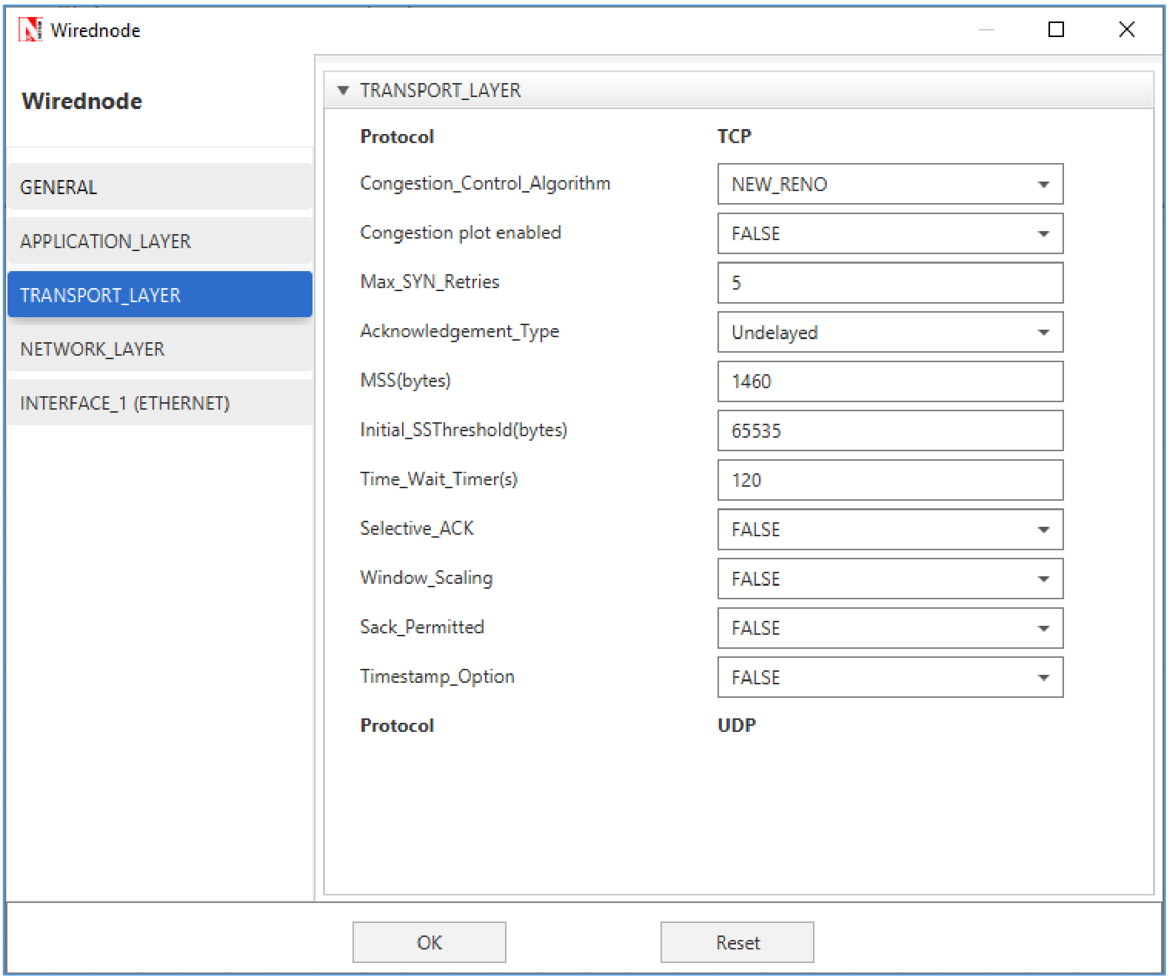
1. Old Tahoe
2. Tahoe
3. Reno
4. New Reno
5. BIC
6. CUBIC

3.4.4 Limitations of TCP

1. Send and Receive buffers are infinite

3.4.5 GUI configuration of TCP

The TCP parameters can be accessed by right clicking on a node and selecting Properties -> Transport Layer



Protocol	TCP
Congestion_Control_Algorithm	NEW_RENO
Congestion plot enabled	FALSE
Max_SYN_Retries	5
Acknowledgement_Type	Undelayed
MSS(bytes)	1460
Initial_SSThreshold(bytes)	65535
Time_Wait_Timer(s)	120
Selective_ACK	FALSE
Window_Scaling	FALSE
Sack_Permitted	FALSE
Timestamp_Option	FALSE
Protocol	UDP

Figure 3-13: Transport layer protocol properties of wired node

The properties that can be set are:

Parameter	Type *	Range	Description
Congestion Control Algorithm	Local	OLD TAHOE, TAHOE, RENO, NEW RENO, BIC, CUBIC	Congestion control algorithm is used to control the network congestion. Old Tahoe is the combination of slow start and congestion avoidance algorithm. The Fast-retransmit algorithms operating with Old Tahoe is known as

			the Tahoe. This algorithm works based on duplicate ack. When it receives three duplicate ack, which is the indication of segment loss, that segment will be retransmitted immediately without waiting for timeout. Reno implements fast recovery in case of three duplicate acknowledgements. New Reno improves retransmission during the fast-recovery phase of TCP Reno. BIC algorithm tries to find the maximum where to keep the window at for a long period of time, by using a binary search algorithm. CUBIC is an implementation of TCP with an optimized congestion control algorithm for high bandwidth networks with high latency.
Congestion plot enabled	Local	FALSE, TRUE	Congestion plot can enable or disable by selecting value as TRUE and FALSE
Max SYN Retries	Local	1-10	Maximum number of TCP SYN ACK packets that can be retransmitted. The value should in the range of 1 to 10.
Acknowledgement Type	Local	Delayed, Undelayed	If set to delayed, ACK response will be delayed improving network performance. If set to Un delayed, ACK will be sent immediately without delay.
MSS (bytes)	Local	64-1460	The maximum amount of data that a single message may contain. The MSS is the maximum data size and does not include the size of the header.

			MSS = MTU – (Network and Transport layer protocol headers).
Initial SSThreshold(bytes)	Local	5840-65535	The server-initial–ss-threshold should be in the range between 5840 and 65535 bytes.
Time Wait Timer(s)	Local	30-240	The Time wait timer default value is 120 seconds. The purpose of TIME-WAIT is to prevent delayed packets from one connection being accepted by a later connection.
Selective ACK	Local	TRUE, FALSE	In Selective Acknowledgment (SACK) mechanism, the receiving TCP sends back SACK packets to the sender informing the sender of data that has been received. The sender can then retransmit only the missing data segments.
Window Scaling	Local	TRUE, FALSE	The TCP window scaling option is to increase the receive window size allowed in Transmission Control Protocol above its former maximum value of 65,535 bytes.
Sack Permitted	Local	TRUE, FALSE	The SACK-permitted option is offered to the remote end during TCP setup as an option to an opening SYN packet. The SACK option permits selective acknowledgment of permitted data.
Timestamp Option	Local	TRUE, FALSE	TCP is a symmetric protocol, allowing data to be sent at any time in either direction. Therefore, timestamp echoing may occur in either direction. For simplicity and symmetry, we specify that timestamps always be sent and echoed in both directions. For

			efficiency, we combine the timestamp and timestamp reply fields into a single TCP Timestamps Option.

Table 3-16: Description of Transport layer protocol properties

3.4.6 TCP Performance Metrics

TCP Metrics table will be available in the Simulation Results dashboard if TCP is enabled in at least one device in the network. It provides the following information specific to TCP.

Parameter	Description
Source	It displays the name with ID of the source device which generates TCP packets
Destination	It displays the name with ID of the destination device which receives TCP packets
Local Address	It displays the local IP address with port number of the device present in source column
Remote Address	It represents the remote IP address with port number for the source and destination
Syn Sent	It is the number of syn packets sent by the source
Syn-Ack Sent	It is the number of syn ack packets sent by the destination
Segment Sent	It is the number of segments sent by a source
Segment Received	It is the number of segments received by a destination
Segment Retransmitted	It is the number of segments retransmitted by the source
Ack Sent	It is the number of acknowledgements sent by a source to destination in response to TCP syn ack and the number of acks sent by destination to source in response to the successful reception of data packet
Ack Received	It is the number of acknowledgements received by source in response to data packets and the number of acks received by destination in response to syn ack packet

Duplicate segment received	It is the number of duplicate segments received by destination
Out of order segment received	It is the number of out of ordered packets received by destination
Duplicate ack received	It is the number of duplicate acknowledgements received by source
Times RTO expired	It is the number of times RTO timer expired at source

Table 3-17: Parameter discerption of TCP Metrics table

3.4.7 TCP Reference Documents

1. RFC 793: TRANSMISSION CONTROL PROTOCOL
2. RFC 1122: Requirements for Internet Hosts -- Communication Layers
3. RFC 5681: TCP Congestion Control
4. RFC 3390: Increasing TCP's Initial Window
5. RFC 6298: Computing TCP's Retransmission Timer
6. RFC 2018: TCP Selective Acknowledgment Options
7. RFC 6582: The NewReno Modification to TCP's Fast Recovery Algorithm
8. RFC 6675: A Conservative Loss Recovery Algorithm Based on Selective Acknowledgment (SACK) for TCP
9. RFC 7323: TCP Extensions for High Performance
10. https://research.csc.ncsu.edu/netsrv/sites/default/files/cubic_a_new_tcp_2008.pdf
11. https://research.csc.ncsu.edu/netsrv/sites/default/files/bitcp.pdf
12. https://research.csc.ncsu.edu/netsrv/sites/default/files/hystart_techreport_2008.pdf

3.5 User Datagram Protocol (UDP)

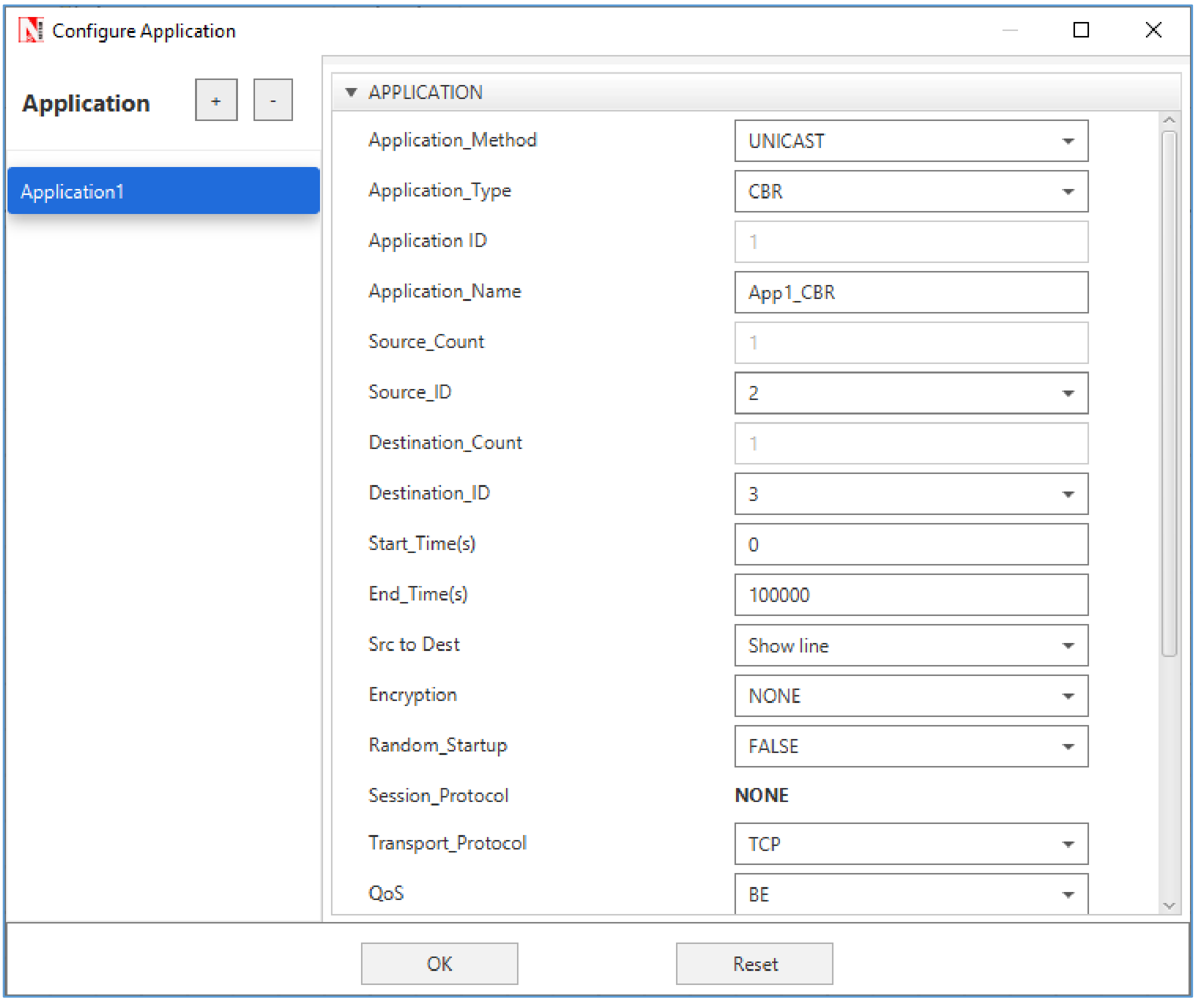
3.5.1 UDP Overview

UDP (User Datagram Protocol) is a communication protocol that offers a limited amount of service when messages are exchanged between computers in a network that uses the Internet Protocol (IP). UDP uses the Internet Protocol to get a data unit (called a datagram) from one computer to another.

This protocol is transaction oriented, and delivery and duplicate protection are not guaranteed. Applications requiring ordered reliable delivery of streams of data should use the Transmission Control Protocol (TCP).

3.5.2 GUI Configuration of UDP

The UDP protocol can be set for an application by clicking on the Applications Transport Protocol option as shown below see **Figure 3-14.**



Configure Application

Application + -

Application1

APPLICATION

Application_Method	UNICAST
Application_Type	CBR
Application ID	1
Application_Name	App1_CBR
Source_Count	1
Source_ID	2
Destination_Count	1
Destination_ID	3
Start_Time(s)	0
End_Time(s)	100000
Src to Dest	Show line
Encryption	NONE
Random_Startup	FALSE
Session_Protocol	NONE
Transport_Protocol	TCP
QoS	BE

Figure 3-14: Application configuration window

3.5.3 UDP Performance Metrics

UDP Metrics table will be available in the Simulation Results dashboard if UDP is enabled in at least one device in the network. It provides the following information specific to UDP see **Table 3-18.**

Parameter	Description
Device Id	It is the Id of a device in which UDP is enabled
Local Address	It represents the IP address with port number of the local device (either source or destination)
Foreign Address	It represents the IP address with port number of the remote device (either source or destination)

Datagram sent	It is the total number of datagrams sent from the source
Datagram received	It is the total number of datagrams received at the destination

Table 3-18: Parameter discerption of UDP Metrics table

3.5.4 UDP Reference Documents

1. RFC 768: User Datagram Protocol

3.6 IP Protocol

3.6.1 IP Performance Metrics

IP Metrics table will be available in the Simulation Results dashboard if IP is enabled in at least one device in the network. It provides the following information specific to IP protocol:

Parameter	Description
Device_Id	It displays the Id's of the Layer_3 devices
Packet sent	It is the number of packets sent by a source, intermediate devices (Router or L3 switch)
Packet forwarded	It is the number of packets forwarded by intermediate devices (Router or L3 switch)
Packet received	It is the number of data packets received by destination, intermediate devices (routing packets (OSPF, RIP etc.) received by Routers)
Packet discarded	It is the number of data packets that are discarded after their TTL value is expired.
TTL expired	Time-to-live (TTL) is a value in an Internet Protocol (IP) packet that tells a network router whether or not the packet has been in the network too long and should be discarded
Firewall blocked	It is the number of packets blocked by firewall at routers

Table 3-19: Parameter discerption of IP Metrics table

3.7 Buffering, Queueing and Scheduling

3.7.1 Buffers

Devices and their Interfaces with buffers that support queuing and scheduling algorithms are:

1. Router (WAN – Network Layer)
2. EPC (WAN – Network Layer)

3. 6LOWPAN (WAN – Network Layer)
4. Satellite Gateway (WAN – Network Layer)

Queuing and scheduling in NetSim, works as follows:

1. The scheduler schedules packet transmission from the head-of-queue per the scheduling algorithm. FIFO algorithm uses a single queue while Priority, RR and WFQ use 4 queues (1 queue for each priority)
2. The buffer size is a user input. This buffer is not split among the various queues. At any point in time the cumulative size of all queues is the buffer fill.
3. The way in which the individual queues are filled up, is per the queuing algorithm selected (implemented in version 12.1)

The buffer is an egress buffer. The buffer size in Mega Bytes (MB), for each interface mentioned above is a user input. The options 8, 16, 32, 64, 128, 256, 512, 1024, 2048 and 4096 MB

3.7.2 Queuing

Drop Tail: The queue is filled up till the buffer capacity. When the queue is full if any packet arrives, it is dropped. The buffer size is a user input.

Random Early Detection (RED):

1. The queue is filled up till the average queue size is equal to minimum threshold, without dropping any packet.
2. Randomly packets are dropped when average queue size is between minimum threshold and maximum threshold. The number of packets being dropped depends on the Max Probability value.
3. All packets are dropped when average queue size is above maximum threshold.

User Inputs - Maximum threshold, minimum threshold and maximum probability.

$$Avg = \frac{t_n}{t_{n+1}} (Avg - x_n) + x_n$$

Avg – Average Queue Size. Avg is initially 0

t_n – Time when nth packet was added to the queue

t_{n+1} – Current time which is the time when the (n+1)th packet is added

x_n - Size of nth packet (B)

Packets are dropped if

$$No\ of\ Dropped\ Packets > \frac{Rand\ (0,1)}{P} \text{ where } p = C_1 \times Avg + C_2$$

$$C_1 = \frac{Max\ Probability}{(Max\ Threshold - Min\ Threshold)}$$

$$C_2 = \frac{Max\ Probability}{(Max\ Threshold - Min\ Threshold)} \times Min\ Threshold$$

Weighted Random Early Detection (WRED):

Please refer to RED explained earlier. This is modified as follows

1. There are different Max and Min threshold value for each type of priority, i.e. High, Medium, Normal, Low (The RED algorithm had only one set of Max and Min Threshold)
2. For the given threshold values of the packets, Random Early Detection (RED) algorithm is applied.

Reference Documents

1. Sally Floyd, Van Jacobson (1993). Random Early Detection Gateways for Congestion Avoidance. *IEEE/ACM Transactions on Networking.*

Queue Size: The queue depth can be obtained from the Event Trace or by modifying the protocol source code. To obtain it from the event trace, an MS Excel script would need to be written to filter by node, and at different points of time, add the number of APP-OUT events and subtract the number of TRANSPORT-OUT events. Note that deeper issues such as segmentation etc. will need to be handled appropriately based on the way the application and transport layer interact.

3.7.3 Scheduling

First In First Out (FIFO): Packets are scheduled according to their arrival time in the queue. Hence, first in packet in queue is scheduled first.

Priority: NetSim supports 4 priority queues namely High, Medium, Normal and Low. With this scheduling, first all packets in the High priority queue are served, and then those in Medium, then in normal and finally those packets in the low priority queue. Note that this could lead to situations where only higher priority packets are served and lower priority packets are never served.

Round Robin: Packet from all the 4 priorities are served in circular order. When packet arrives, they are stored in the corresponding priority list

Weighted Fair Queuing (WFQ): When packet arrives, they are stored in corresponding list according to priority. Packets are served in order of maximum weight of the priority list. In NetSim WFQ is approximated as:

$$Weight = (Number\ of\ packets\ in\ Queue) \times Priority$$ where

$$Priority = 1, 2, 3\ or\ 4$$

1 - Low priority, 2 - Normal, 3 – Medium, 4 - High

Early Deadline First (EDF): Packets are added in the queue as they arrive. While dequeuing the packets with earliest deadline are served first. The packets which have exceeded deadline are dropped.

$$Deadline = Max\ Latency - Packet\ Creation\ Time$$

Max Latency with respect to quality of service (QoS) of the packet is a user input

3.8 Links

3.8.1 Modeling Error in Wired Links

The error rates in NetSim wired links are based on a standard error measurement unit called BER or Bit Error Rate. BER represents the ratio of errored bits to total bits.

The BER value can be set by the user. A typical value of BER, say 1×10^{-6}, which equals 0.000001, means that 1 bit is in error for every one-million bits transmitted. It is important to note that Bit Error Rate is NOT equal to Packet error rate. (PER)

$$PER = 1 - (1 - BER)^L\ where\ L\ is\ the\ packet\ length\ in\ bits$$

For BER values less than 0.001, this is mathematically approximated in NetSim as

$$PER = BER * L$$

4 Featured Examples

Sample configuration files for all networks are available in the **Examples** Menu in NetSim Home Screen. These files provide examples on **How NetSim can be used** – the parameters that can be changed and the typical effect it has on performance.

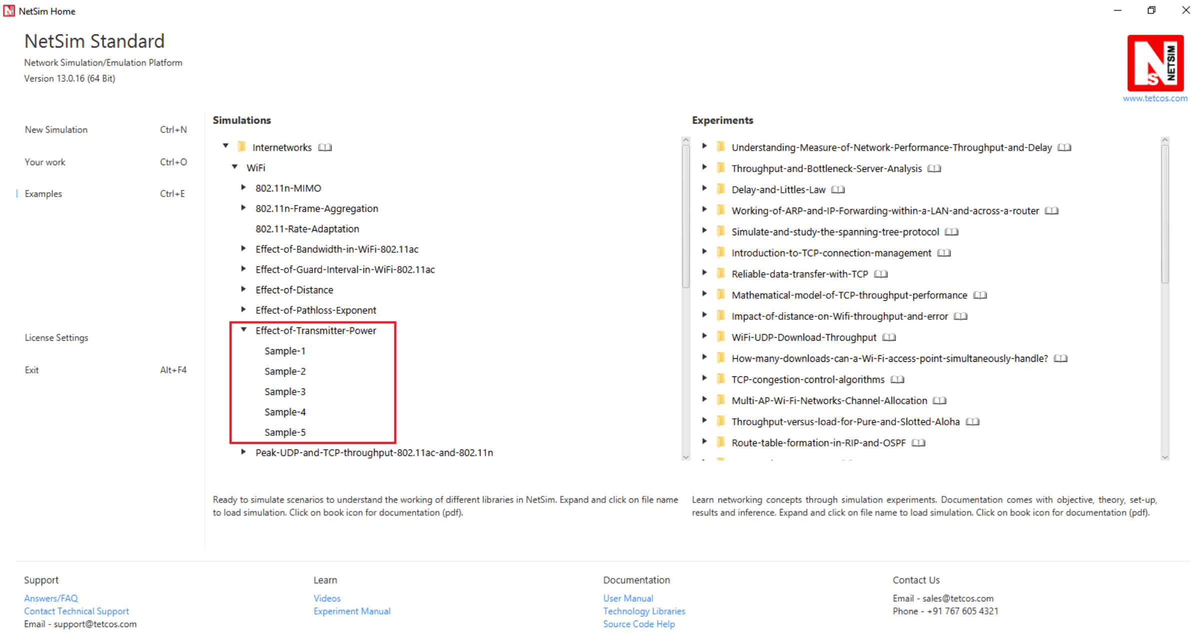
4.1 Factors affecting WLAN PHY Rate

The examples explained in this section focuses on the factors which affect the **PHY Rate/Link Throughput** of 802.11 based networks:

- Transmitter power (More Tx power leads to higher throughput)
- Channel Path loss (Higher path loss exponent leads to lower throughput)
- Receiver sensitivity (Lower Rx sensitivity leads to higher throughput)
- Distance (Higher distance between nodes leads to lower throughput)

4.1.1 Effect of Transmitter power

Open NetSim and click **Examples->Internetworks->WiFi-> Effect-of-Transmitter-Power** as shown below **Figure 4-1.**


NetSim Home
NetSim Standard
Network Simulation/Emulation Platform
Version 13.0.16 (64 Bit)
NETSIM
www.tetcos.com
New Simulation Ctrl+N
Your work Ctrl+O
Examples Ctrl+E
License Settings
Exit Alt+F4
Simulations
Internetworks
WiFi
802.11n-MIMO
802.11n-Frame-Aggregation
802.11-Rate-Adaptation
Effect-of-Bandwidth-in-WiFi-802.11ac
Effect-of-Guard-Interval-in-WiFi-802.11ac
Effect-of-Distance
Effect-of-Pathloss-Exponent
Effect-of-Transmitter-Power
Sample-1
Sample-2
Sample-3
Sample-4
Sample-5
Peak-UDP-and-TCP-throughput-802.11ac-and-802.11n
Experiments
Understanding-Measure-of-Network-Performance-Throughput-and-Delay
Throughput-and-Bottleneck-Server-Analysis
Delay-and-Littles-Law
Working-of-ARP-and-IP-Forwarding-within-a-LAN-and-across-a-router
Simulate-and-study-the-spanning-tree-protocol
Introduction-to-TCP-connection-management
Reliable-data-transfer-with-TCP
Mathematical-model-of-TCP-throughput-performance
Impact-of-distance-on-Wifi-throughput-and-error
WiFi-UDP-Download-Throughput
How-many-downloads-can-a-Wi-Fi-access-point-simultaneously-handle?
TCP-congestion-control-algorithms
Multi-AP-Wi-Fi-Networks-Channel-Allocation
Throughput-versus-load-for-Pure-and-Slotted-Aloha
Route-table-formation-in-RIP-and-OSPF
Support
Answers/FAQ
Contact Technical Support
Learn
Videos
Experiment Manual
Documentation
User Manual
Technology Libraries
Source Code Help
Contact Us

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).

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).

Email - support@tetcos.com

Email - sales@tetcos.com
Phone - +91 767 605 4321

Figure 4-1: Featured Example list

The following network diagram illustrates, what the NetSim UI displays when you open the example configuration file see **Figure 4-2.**

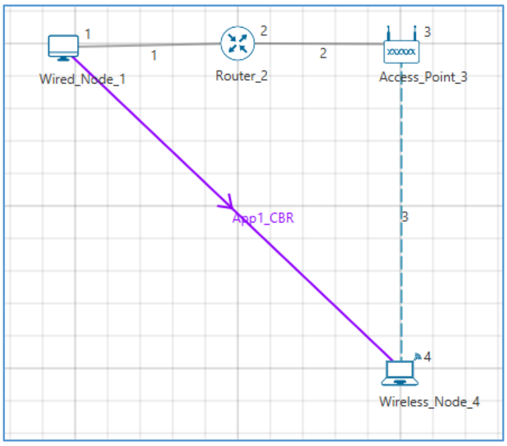


Figure 4-2: Effect of Transmitter power network topology

Increase in transmitter power increases the received power when all other parameters are constant. Increased received power leads to higher SNR and hence higher PHY Data rates, lesser error and higher throughputs.

Sample 1:

Network Settings

1. Environment Grid length: 500m x 500m
2. Distance between Access Point and the Wireless Node is set to 210m
3. Set transmitter power to 100mW under Interface Wireless > Physical layer properties of Access point
4. Set DCF as the medium access layer protocol under datalink layer properties of access point and wireless node.
5. Channel Characteristics: Path Loss Only, Path Loss Model: Log Distance, Path Loss Exponent: 2.5
6. Application Generation Rate: 10Mbps (Packet Size: 1460, Inter Arrival Time: 1168µs)
7. Click on the Application icon present in the top ribbon/toolbar and set Transport Protocol to UDP
8. In NetSim GUI Plots are Enabled. Run simulation for 10s
9. Similarly, for sample 2 to sample 5 reset the Transmitter Power to 80, 60, 40, and 20 respectively and see that, there is a decrease in the Throughput gradually.

Results and Discussion

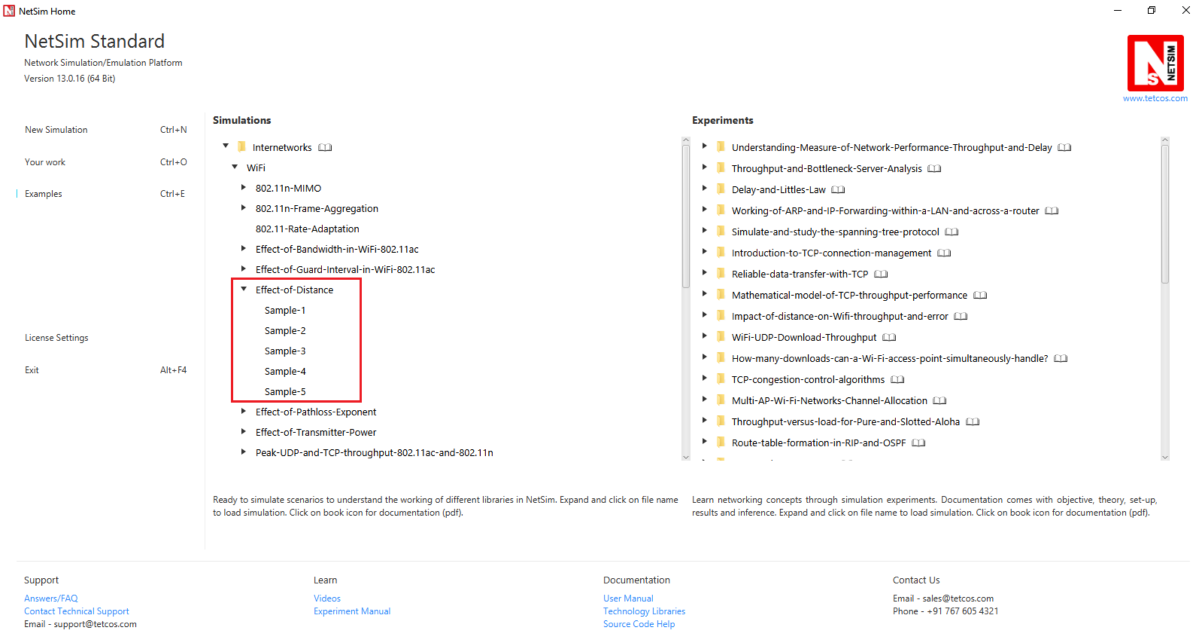
Transmitter Power (mW)	Throughput (Mbps)
100	5.82
80	5.12

60	3.80
40	3.48
20	1.68

Table 4-1: Result comparison of different transmitter power vs. Throughputs

4.1.2 Effect-of-Distance

Open NetSim and click **Examples > Internetworks > WiFi > Effect-of-Distance** as shown **Figure 4-3.**



NetSim Home

NetSim Standard

Network Simulation/Emulation Platform

Version 13.0.16 (64 Bit)

www.tetcos.com

New Simulation	Ctrl+N
Your work	Ctrl+O
Examples	Ctrl+E
License Settings	
Exit	Alt+F4

Simulations

- Internetworks
  - WiFi
    - 802.11n-MIMO
    - 802.11n-Frame-Aggregation
    - 802.11-Rate-Adaptation
    - Effect-of-Bandwidth-in-WiFi-802.11ac
    - Effect-of-Guard-Interval-in-WiFi-802.11ac
    - Effect-of-Distance
      - Sample-1
      - Sample-2
      - Sample-3
      - Sample-4
      - Sample-5
    - Effect-of-Pathloss-Exponent
    - Effect-of-Transmitter-Power
    - Peak-UDP-and-TCP-throughput-802.11ac-and-802.11n

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

- Understanding-Measure-of-Network-Performance-Throughput-and-Delay
- Throughput-and-Bottleneck-Server-Analysis
- Delay-and-Littles-Law
- Working-of-ARP-and-IP-Forwarding-within-a-LAN-and-across-a-router
- Simulate-and-study-the-spanning-tree-protocol
- Introduction-to-TCP-connection-management
- Reliable-data-transfer-with-TCP
- Mathematical-model-of-TCP-throughput-performance
- Impact-of-distance-on-Wifi-throughput-and-error
- WiFi-UDP-Download-Throughput
- How-many-downloads-can-a-Wi-Fi-access-point-simultaneously-handle?
- TCP-congestion-control-algorithms
- Multi-AP-Wi-Fi-Networks-Channel-Allocation
- Throughput-versus-load-for-Pure-and-Slotted-Aloha
- Route-table-formation-in-RIP-and-OSPF

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 4-3: Featured Example list

The following network diagram illustrates, what the NetSim UI displays when you open the example configuration file see **Figure 4-4.**

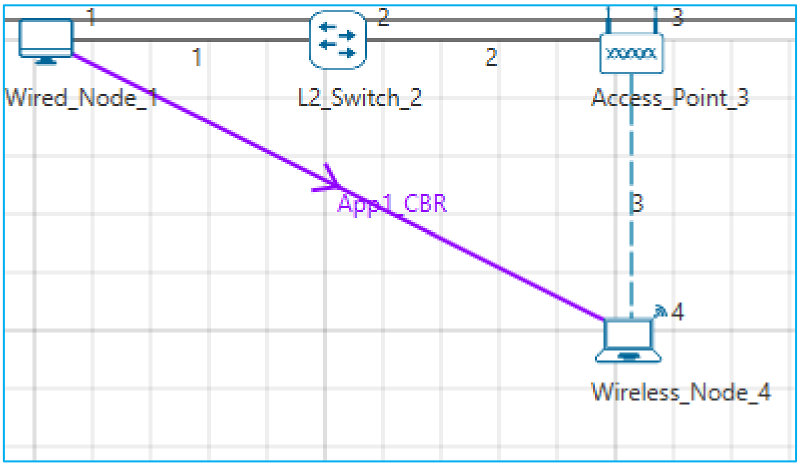


Figure 4-4: Effect of Distance network topology

As the distance between two devices increases the received signal power reduces as propagation loss increases with distance. As the received power reduces, the underlying PHY rate of the channel drops.

Sample 1:

Network Settings

1. Environment Grid length: 100m x 100m
2. Distance between Access Point and the Wireless Node is set to 10m
3. Set DCF as the medium access layer protocol under datalink layer properties of access point and wireless node.
4. WLAN Standard is set to 802.11ac and No. of Tx and Rx Antenna is set to 1 in access point and No. of Tx is 1 and Rx Antenna is set to 2 in wireless node (Right-Click Access Point or Wireless Node > Properties > Interface Wireless > Transmitting Antennas and Receiving Antennas) and Bandwidth is set to 20 MHz in both Access-point and wireless-node Transmitter Power set to 100mW in both Access-point and wireless-node.
5. Wired Link speed was set to 1Gbps and propagation delay to 10 µs in wired links.
6. Channel Characteristics: Path Loss Only, Path Loss Model: Log Distance, Path Loss Exponent: 3.5
7. Application Generation Rate: 100 Mbps (Packet Size: 1460, Inter Arrival Time: 116 µs)
8. Click on the Application icon present in the top ribbon/toolbar and set Transport Protocol to UDP
9. Run simulation for 10s
10. Similarly, in Sample-2, Sample-3, Sample-4, and Sample-5 increase the Distance from 10m to 20m, 30m, 40, and 50 respectively

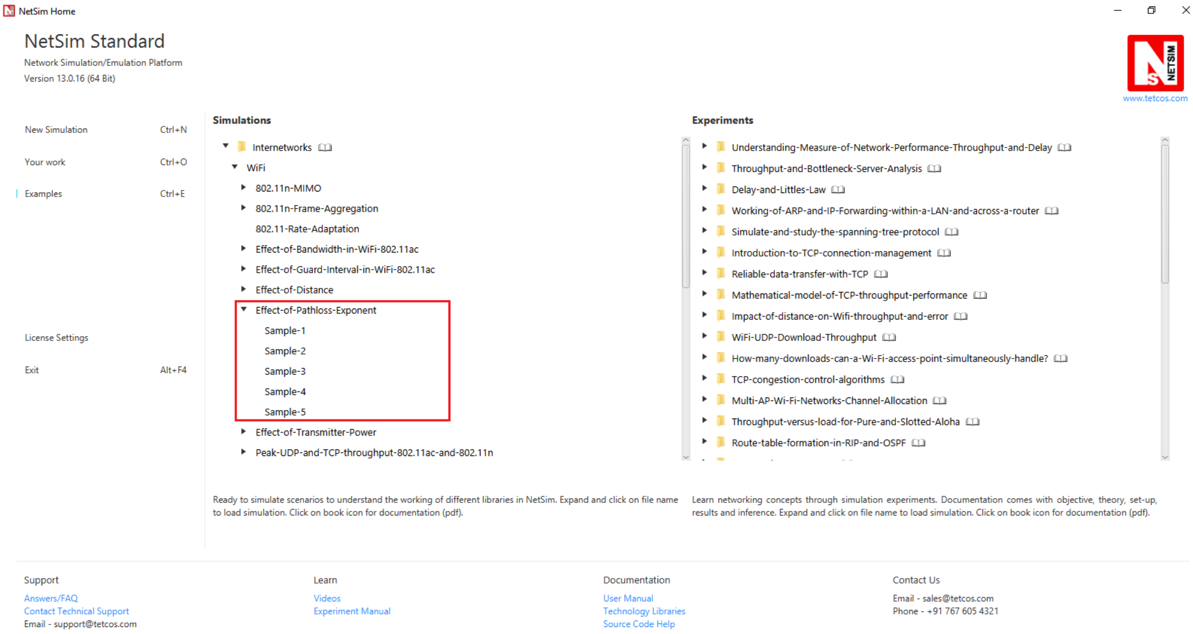
Results and Discussion

Distance (m)	Throughput (Mbps)
10	22.78
20	21.60
30	17.84
40	17.65
50	12.47

Table 4-2: Result comparison of different distance vs. throughput

4.1.3 Effect of Pathloss Exponent

Open NetSim and click **Examples > Internetworks > WiFi > Effect-of-Pathloss-Exponent** as shown **Figure 4-5**.



NetSim Home

NetSim Standard

Network Simulation/Emulation Platform

Version 13.0.16 (64 Bit)

New Simulation	Ctrl+N
Your work	Ctrl+O
Examples	Ctrl+E
License Settings	
Exit	Alt+F4

Simulations

- Internetworks
  - WiFi
    - 802.11n-MIMO
    - 802.11n-Frame-Aggregation
    - 802.11-Rate-Adaptation
    - Effect-of-Bandwidth-in-WiFi-802.11ac
    - Effect-of-Guard-Interval-in-WiFi-802.11ac
    - Effect-of-Distance
    - Effect-of-Pathloss-Exponent
      - Sample-1
      - Sample-2
      - Sample-3
      - Sample-4
      - Sample-5
    - Effect-of-Transmitter-Power
    - Peak-UDP-and-TCP-throughput-802.11ac-and-802.11n

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

- Understanding-Measure-of-Network-Performance-Throughput-and-Delay
- Throughput-and-Bottleneck-Server-Analysis
- Delay-and-Littles-Law
- Working-of-ARP-and-IP-Forwarding-within-a-LAN-and-across-a-router
- Simulate-and-study-the-spanning-tree-protocol
- Introduction-to-TCP-connection-management
- Reliable-data-transfer-with-TCP
- Mathematical-model-of-TCP-throughput-performance
- Impact-of-distance-on-Wifi-throughput-and-error
- WiFi-UDP-Download-Throughput
- How-many-downloads-can-a-Wi-Fi-access-point-simultaneously-handle?
- TCP-congestion-control-algorithms
- Multi-AP-Wi-Fi-Networks-Channel-Allocation
- Throughput-versus-load-for-Pure-and-Slotted-Aloha
- Route-table-formation-in-RIP-and-OSPF

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 4-5: Featured Example list

The following network diagram illustrates, what the NetSim UI displays when you open the example configuration file as shown **Figure 4-6.**

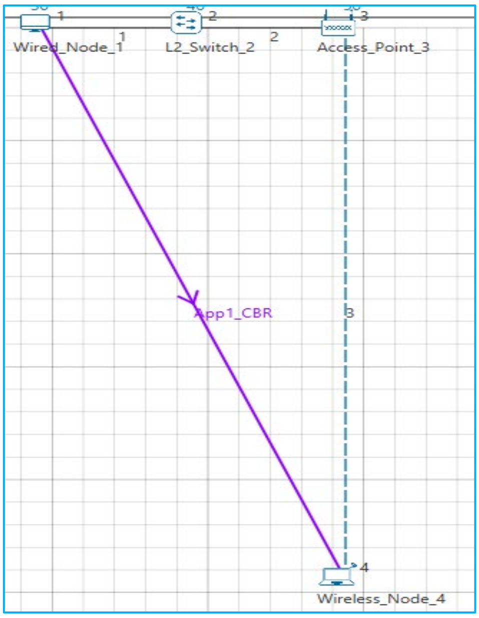


Figure 4-6: Network Topology

Path Loss or Attenuation of RF signals occurs naturally with distance. Losses can be increased by increasing the path loss exponent (η). This option is available in channel characteristics. Users can compare the results by changing the path loss exponent (η) value.

Sample 1:

Network Settings

1. Environment Grid length: 100m x 100m
2. Distance between Access Point and the Wireless Node is set to 50m
3. Set DCF as the medium access layer protocol under datalink layer properties of access point and wireless node. WLAN Standard is set to 802.11ac and No. of Tx and Rx Antenna is set to 1 in both access point and wireless node (Right-Click Access Point or Wireless Node > Properties > Interface Wireless > Transmitting Antennas and Receiving Antennas) and Bandwidth is set to 20 MHz in both Access-point and wireless-node and Transmitter Power set to 100mW in both Access-point and wireless-node.
4. Wired Link speed was set to 1Gbps and propagation delay to 10 µs in wired links.
5. Channel Characteristics: Path Loss Only, Path Loss Model: Log Distance, Path Loss Exponent: 2
6. Application Generation rate: 100 Mbps (Packet Size: 1460, Inter Arrival Time: 116 µs)
7. Click on the Application icon present in the top ribbon/toolbar and set Transport Protocol to UDP
8. Run simulation for 10s
9. Similarly, in Sample-2, Sampl-3, Sample-4, and Sample-5 increase the Path Loss Exponent from 2 to 2.5, 3, 3.5, and 4 respectively.

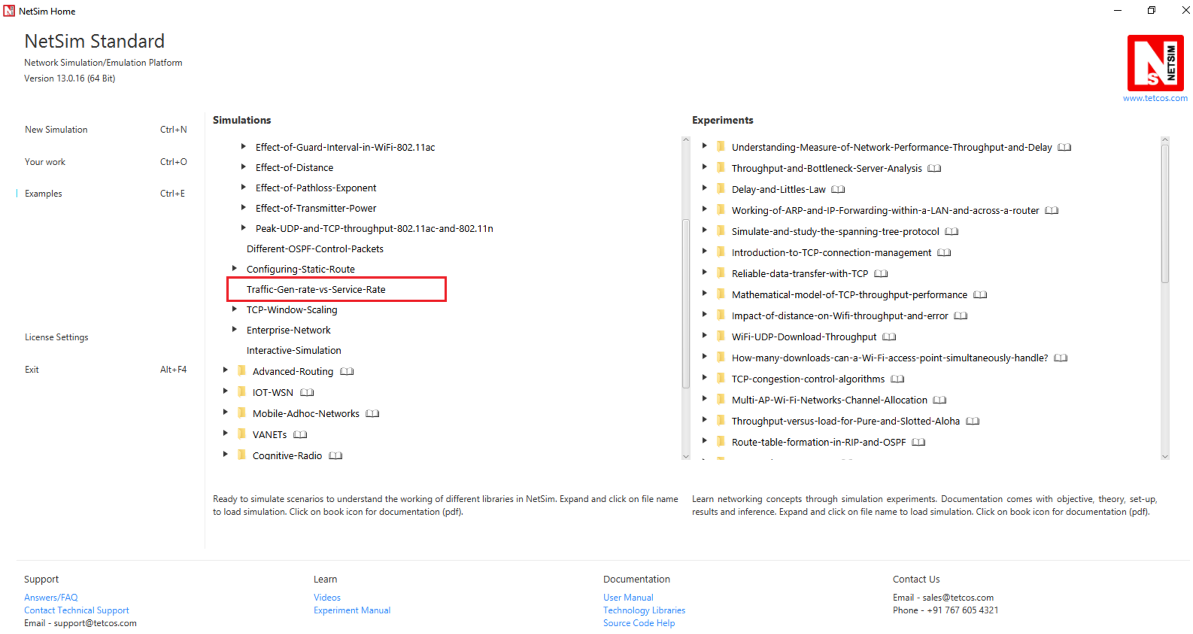
Results and Discussion

Path loss Exponent	Throughput (Mbps)
2.0	22.78
2.5	22.78
3.0	19.27
3.5	12.47
4.0	5.56

Table 4-3: Result comparison of different pathloss exponent value vs. throughput

4.2 Traffic Generation Rate and Service Rate

Open NetSim and click **Examples > Internetworks > WiFi >Traffic-Gen-Rate-vs-Service-Rate** as shown below as shown **Figure 4-7.**



NetSim Home

NetSim Standard

Network Simulation/Emulation Platform

Version 13.0.16 (64 Bit)

www.tetcos.com

New Simulation Ctrl+N

Your work Ctrl+O

Examples Ctrl+E

License Settings

Exit Alt+F4

Simulations

- Effect-of-Guard-Interval-in-WiFi-802.11ac
- Effect-of-Distance
- Effect-of-Pathloss-Exponent
- Effect-of-Transmitter-Power
- Peak-UDP-and-TCP-throughput-802.11ac-and-802.11n
- Different-OSPF-Control-Packets
- Configuring-Static-Route
- Traffic-Gen-rate-vs-Service-Rate
- TCP-Window-Scaling
- Enterprise-Network
- Interactive-Simulation
- Advanced-Routing
- IOT-WSN
- Mobile-Adhoc-Networks
- VANETs
- Cognitive-Radio

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

- Understanding-Measure-of-Network-Performance-Throughput-and-Delay
- Throughput-and-Bottleneck-Server-Analysis
- Delay-and-Littles-Law
- Working-of-ARP-and-IP-Forwarding-within-a-LAN-and-across-a-router
- Simulate-and-study-the-spanning-tree-protocol
- Introduction-to-TCP-connection-management
- Reliable-data-transfer-with-TCP
- Mathematical-model-of-TCP-throughput-performance
- Impact-of-distance-on-Wifi-throughput-and-error
- WiFi-UDP-Download-Throughput
- How-many-downloads-can-a-Wi-Fi-access-point-simultaneously-handle?
- TCP-congestion-control-algorithms
- Multi-AP-Wi-Fi-Networks-Channel-Allocation
- Throughput-versus-load-for-Pure-and-Slotted-Aloha
- Route-table-formation-in-RIP-and-OSPF

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 4-7: Featured Example list

The following network diagram illustrates, what the NetSim UI displays when you open the example configuration file as shown **Figure 4-8.**

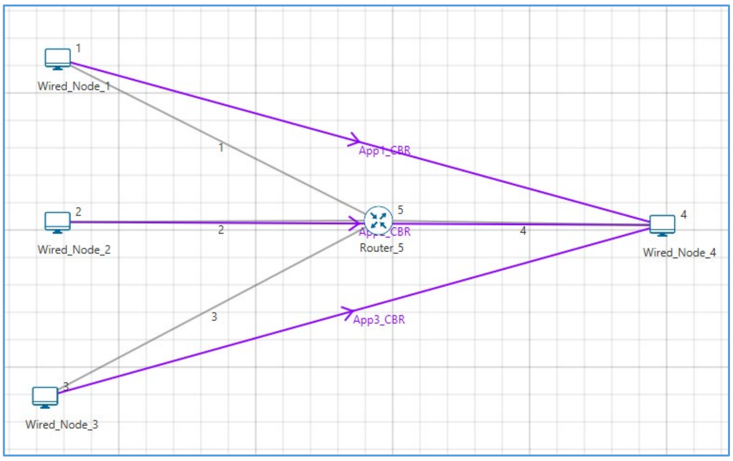


Figure 4-8: Network Topology in this experiment

Network Settings

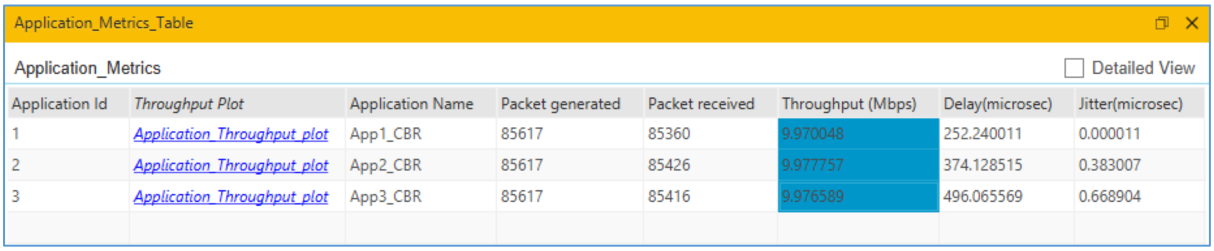
1. Click on the Application icon present in the top ribbon/toolbar and set Transport Protocol to UDP
2. Generation rate = 10Mbps for each application (Packet Size: 1460, Inter Arrival Time: 1168µs)
    a. Generation Rate (Mbps) = (Packet size (bytes) * 8) / Inter arrival time (µs))
3. The traffic generation rate can be modified by changing application properties. Note that the generation rate should be less than or equal to service rate for steady-state simulation, where the service rate is defined as the data rate supported by the Bottle-

neck link. In this case, there is no bottle neck link since all links support up to 100 Mbps

4. Plots and Packet Trace is Enabled
5. Simulate for 100s and note down the throughput
6. Go back to the scenario and change the link speed (both Uplink and Downlink Speed) between Router_5 and Wired_Node_4 from the default 100 Mbps to 25 Mbps. In this case, the link between Router_5 and Wired_Node_4 becomes a Bottle-neck link, since the link rate (i.e. service rate) is less than the generation rate of 30 Mbps (10 * 3).

Discussion

Sample1: In this scenario, router receives packets from three links at the rate of 10 Mbps each, a total of 30 Mbps. And the router-node link supports 100 Mbps. Hence there is no queuing / packet drop in the Router. The application throughput would be approximately equal to the generation rate.



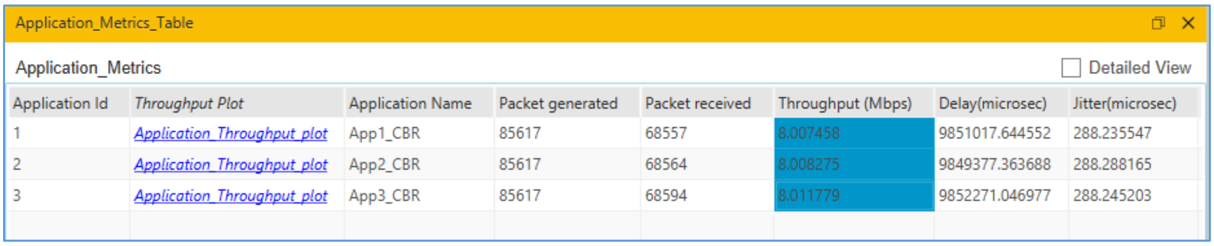
Application_Metrics_Table

Application_Metrics □ Detailed View

Application Id	Throughput Plot	Application Name	Packet generated	Packet received	Throughput (Mbps)	Delay(microsec)	Jitter(microsec)
1	*Application_Throughput_plot*	App1_CBR	85617	85360	9.970048	252.240011	0.000011
2	*Application_Throughput_plot*	App2_CBR	85617	85426	9.977757	374.128515	0.383007
3	*Application_Throughput_plot*	App3_CBR	85617	85416	9.976589	496.065569	0.668904

Figure 4-9: Application Metrics window

Sample2: In this case, the bottleneck link supports only 25 Mbps. Due to this, packets get accumulated in the router's buffer, which overflows after reaching its limit and hence router starts dropping the packets. Application throughput would be approximately equal to the bottle neck link capacity.



Application_Metrics_Table

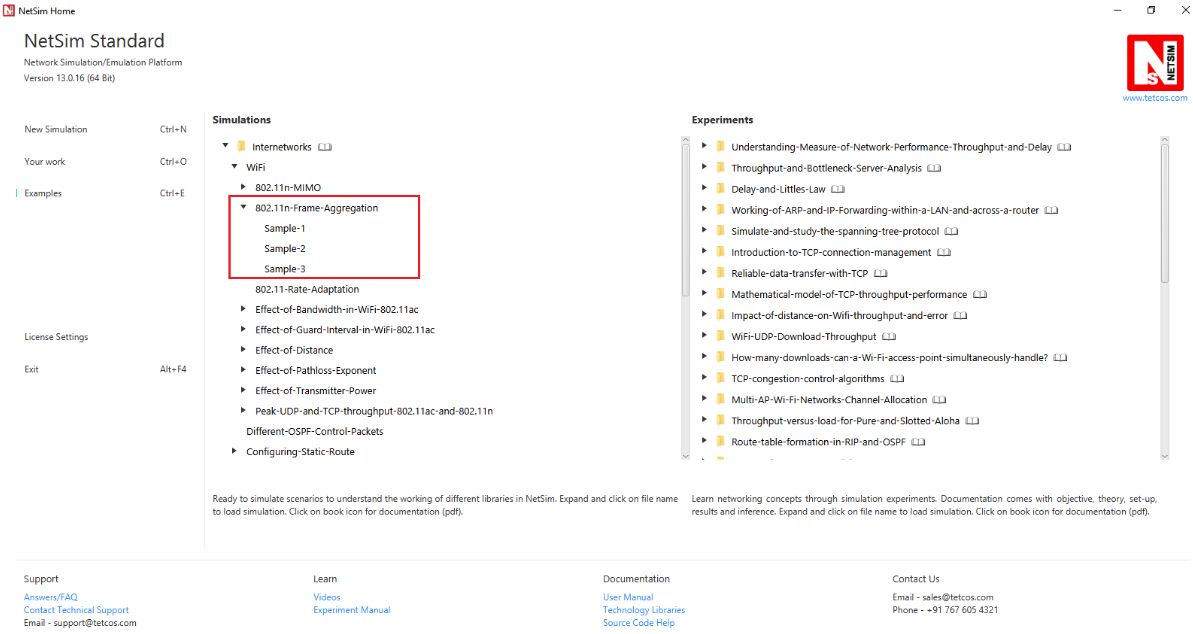
Application_Metrics □ Detailed View

Application Id	Throughput Plot	Application Name	Packet generated	Packet received	Throughput (Mbps)	Delay(microsec)	Jitter(microsec)
1	*Application_Throughput_plot*	App1_CBR	85617	68557	8.007458	9851017.644552	288.235547
2	*Application_Throughput_plot*	App2_CBR	85617	68564	8.008275	9849377.363688	288.288165
3	*Application_Throughput_plot*	App3_CBR	85617	68594	8.011779	9852271.046977	288.245203

Figure 4-10: Application Metrics window

4.3 Frame aggregation in 802.11n

Open NetSim and click **Examples > Internetworks > WiFi > 802.11n-Frame-Aggregation** as shown below **Figure 4-11.**



NetSim Home

NetSim Standard

Network Simulation/Emulation Platform

Version 13.0.16 (64 Bit)

www.tetcos.com

New Simulation	Ctrl+N
Your work	Ctrl+O
Examples	Ctrl+E
License Settings	
Exit	Alt+F4

Simulations

- Internetworks
  - WiFi
    - 802.11n-MIMO
    - 802.11n-Frame-Aggregation
      - Sample-1
      - Sample-2
      - Sample-3
    - 802.11-Rate-Adaptation
    - Effect-of-Bandwidth-in-WiFi-802.11ac
    - Effect-of-Guard-Interval-in-WiFi-802.11ac
    - Effect-of-Distance
    - Effect-of-Pathloss-Exponent
    - Effect-of-Transmitter-Power
    - Peak-UDP-and-TCP-throughput-802.11ac-and-802.11n
  - Different-OSPF-Control-Packets
  - Configuring-Static-Route

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

- Understanding-Measure-of-Network-Performance-Throughput-and-Delay
- Throughput-and-Bottleneck-Server-Analysis
- Delay-and-Littles-Law
- Working-of-ARP-and-IP-Forwarding-within-a-LAN-and-across-a-router
- Simulate-and-study-the-spanning-tree-protocol
- Introduction-to-TCP-connection-management
- Reliable-data-transfer-with-TCP
- Mathematical-model-of-TCP-throughput-performance
- Impact-of-distance-on-Wifi-throughput-and-error
- WiFi-UDP-Download-Throughput
- How-many-downloads-can-a-Wi-Fi-access-point-simultaneously-handle?
- TCP-congestion-control-algorithms
- Multi-AP-Wi-Fi-Networks-Channel-Allocation
- Throughput-versus-load-for-Pure-and-Slotted-Aloha
- Route-table-formation-in-RIP-and-OSPF

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 4-11: Featured Example list

The following network topology is shown in NetSim UI as shown **Figure 4-12.**

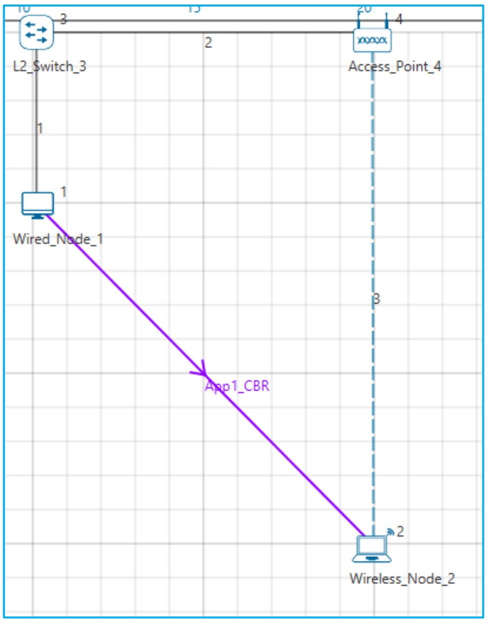


Figure 4-12: WiFi Frame-Aggregation topology

Network Settings

1. In the Environment Settings, Grid length is set to 50m * 50m
2. Distance between Access Point and the Wireless Node is 20m
3. Set DCF as the medium access layer protocol under datalink layer properties of Access point and wireless node.
4. Packet Trace option is enabled
5. Click on the Application icon present in the top ribbon/toolbar

   a. CBR Application with 100 Mbps Generation Rate (Packet Size: 1460, Inter Arrival Time: 116µs)
   b. Set Transport Protocol to UDP
6. WLAN Standard is set to 802.11n and No. of Frames to Aggregate is set to 1 in both access point and wireless node (Right-Click Access Point or Wireless Node > Properties > Interface Wireless > No. of Frame to Aggregate)
7. Channel Characteristics: Path Loss Only, Path Loss Model: Log Distance, and Path Loss Exponent: 3. (Wireless Link Properties)
8. Simulate for 10s and check the throughput in the results window
9. Go back to the scenario and increase the No. of Frames to Aggregate to 5 and 10 respectively and check the throughput in the results window.

Results and discussion

No of Frames Aggregated	Application Throughput
1	23.94 Mbps
5	44.67 Mbps
10	54.14 Mbps

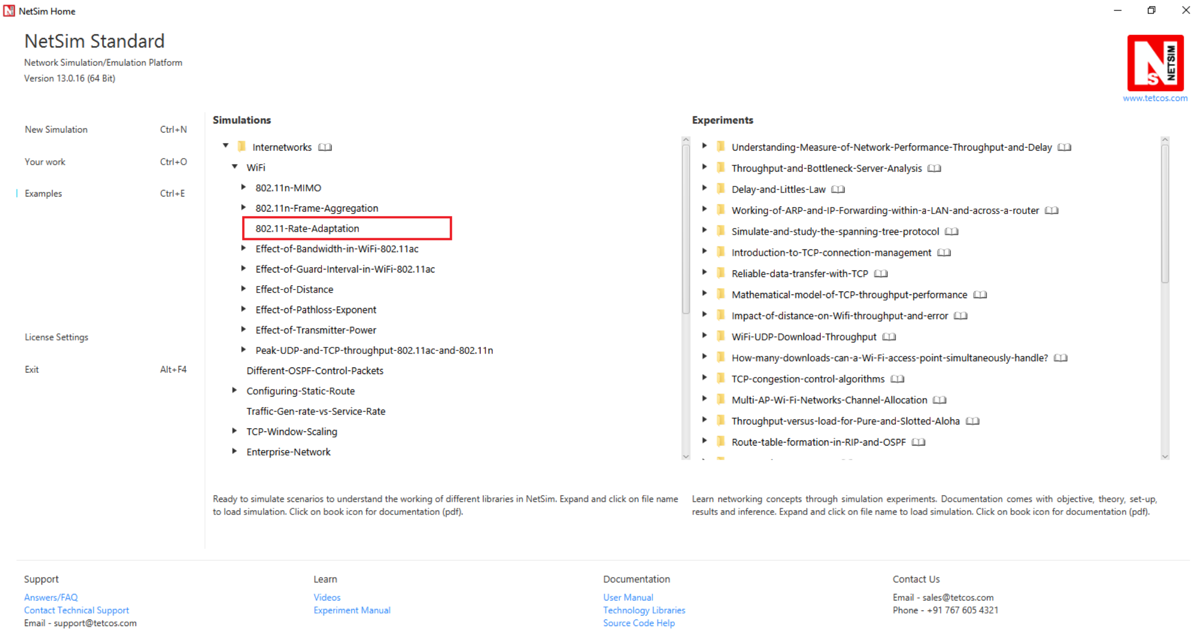
Table 4-4: No of Frames Aggregated vs. Application Throughput

- Frame aggregation is responsible for joining multiple MSDUs into a single MPDU that can be delivered to the physical layer as a single unit for transmission. As we increase the number of frames aggregated it results in lesser number of ack's. Hence, more data frames are transmitted per unit time leading to a higher application throughput.
- For No. of frames to Aggregate is set to 5, we get five successive frames followed by a WLAN_Block_Ack (which is used to acknowledge that five frames are received successfully). Users can observe this in Packet Trace by filtering Tx_ID as Access Point and Wireless Node.
- Note that in the early stages of the simulation the AP would transmit whatever the number of frames/packets in its buffer. It will not wait for 5 frames to be aggregated, if say number of frames to be aggregated is set as 5. If Access Point buffer has more than 5 frames, it will aggregate 5 frames and then send. After sending 5 frames it will receive one WLAN_Block_Ack.

4.4 Rate Adaptation in 802.11b

NetSim rate adaptation is explained in section *3.1.17* of this document.

Open NetSim, Select **Examples->Internetworks->WiFi->802.11-Rate-Adaptation** as shown below **Figure 4-13.**



NetSim Home

NetSim Standard

Network Simulation/Emulation Platform

Version 13.0.16 (64 Bit)

www.tetcos.com

New Simulation Ctrl+N

Your work Ctrl+O

Examples Ctrl+E

License Settings

Exit Alt+F4

Simulations

- Internetworks
  - WiFi
    - 802.11n-MIMO
    - 802.11n-Frame-Aggregation
    - 802.11-Rate-Adaptation
    - Effect-of-Bandwidth-in-WiFi-802.11ac
    - Effect-of-Guard-Interval-in-WiFi-802.11ac
    - Effect-of-Distance
    - Effect-of-Pathloss-Exponent
    - Effect-of-Transmitter-Power
    - Peak-UDP-and-TCP-throughput-802.11ac-and-802.11n
  - Different-OSPF-Control-Packets
  - Configuring-Static-Route
  - Traffic-Gen-rate-vs-Service-Rate
  - TCP-Window-Scaling
  - Enterprise-Network

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

- Understanding-Measure-of-Network-Performance-Throughput-and-Delay
- Throughput-and-Bottleneck-Server-Analysis
- Delay-and-Littles-Law
- Working-of-ARP-and-IP-Forwarding-within-a-LAN-and-across-a-router
- Simulate-and-study-the-spanning-tree-protocol
- Introduction-to-TCP-connection-management
- Reliable-data-transfer-with-TCP
- Mathematical-model-of-TCP-throughput-performance
- Impact-of-distance-on-Wifi-throughput-and-error
- WiFi-UDP-Download-Throughput
- How-many-downloads-can-a-Wi-Fi-access-point-simultaneously-handle?
- TCP-congestion-control-algorithms
- Multi-AP-Wi-Fi-Networks-Channel-Allocation
- Throughput-versus-load-for-Pure-and-Slotted-Aloha
- Route-table-formation-in-RIP-and-OSPF

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 4-13: Featured Example list

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

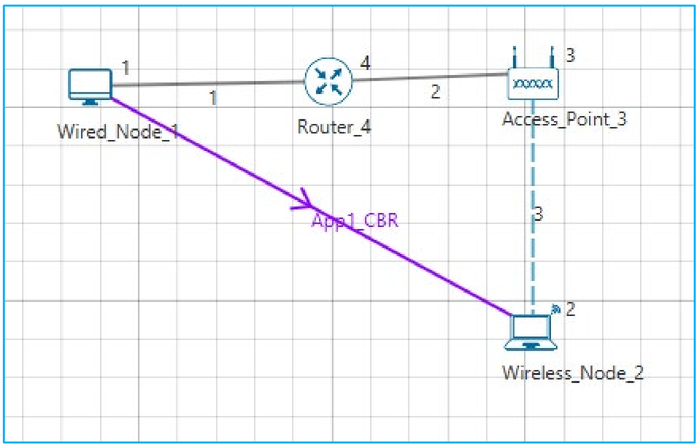


Figure 4-14: WiFi Rate Adaptation topology

Network Settings

1. Environment Grid length: 500m * 500m
2. Distance between AP and Wireless Node is 65.5m
3. Enabled Packet Trace and plot option
4. Set rate adaptation as Generic in datalink properties of access_point and wireless node
5. Set DCF as the medium access layer protocol under datalink layer properties of access_point and wireless node.
6. Click on the Application icon present in the top ribbon/toolbar and set Transport Protocol to UDP

7. Set WLAN Standard → 802.11b
8. Propagation model → Path Loss only, Path Loss Model → Log Distance and Path loss Exponent → 3.25.
9. CBR application with 10Mbps generation rate (Set Packet Size: 1460 Bytes, Inter Arrival Time: 1168 micro sec)
10. Simulate for 10 sec.

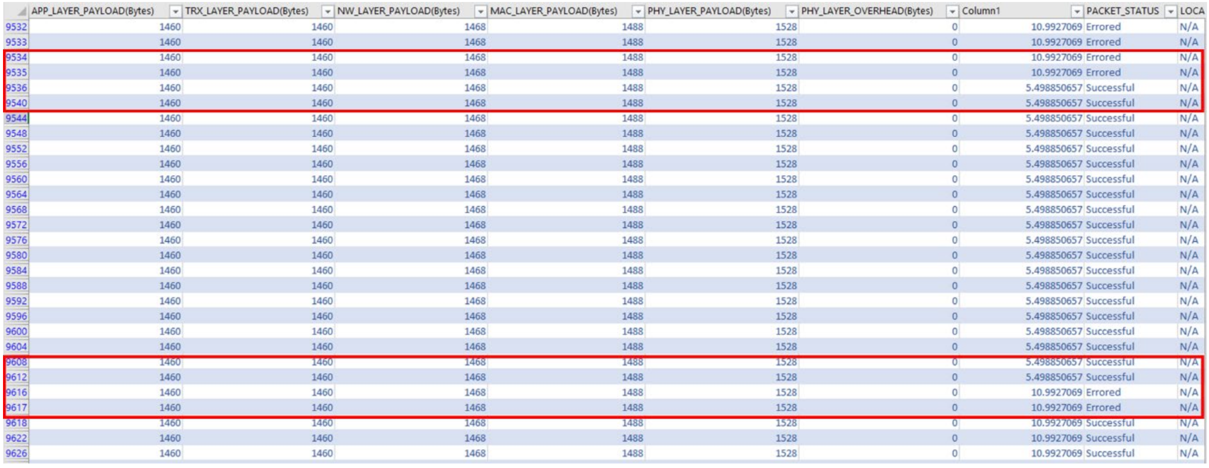
Results and Discussion

Open Packet Trace and filter Packet Type to CBR, Transmitter_ID to Access Point 3 and then calculate Phy rate. Phy rate can be calculated using packet trace by using the formula shown below:

$$Phy\ rate\ (802.11b)\ =\ Phy\_layer\_payload * 8/(phy\ end\ time - phy\ arrival\ time - 192)$$

192 μs is the approximate preamble time for 802.11b

Calculate PHY rate for all the data packets coming from Access Point to Wireless Node. For doing this please refer NetSim User Manual > Section 8.4.1 How to set filters to NetSim Trace file.



	APP_LAYER_PAYLOAD(Bytes)	TRX_LAYER_PAYLOAD(Bytes)	NW_LAYER_PAYLOAD(Bytes)	MAC_LAYER_PAYLOAD(Bytes)	PHY_LAYER_PAYLOAD(Bytes)	PHY_LAYER_OVERHEAD(Bytes)	Column1	PACKET_STATUS	LOCA
9532	1460	1460	1468	1488	1528	0	10.9927069	Errored	N/A
9533	1460	1460	1468	1488	1528	0	10.9927069	Errored	N/A
9534	1460	1460	1468	1488	1528	0	10.9927069	Errored	N/A
9535	1460	1460	1468	1488	1528	0	10.9927069	Errored	N/A
9536	1460	1460	1468	1488	1528	0	5.498850657	Successful	N/A
9540	1460	1460	1468	1488	1528	0	5.498850657	Successful	N/A
9544	1460	1460	1468	1488	1528	0	5.498850657	Successful	N/A
9548	1460	1460	1468	1488	1528	0	5.498850657	Successful	N/A
9552	1460	1460	1468	1488	1528	0	5.498850657	Successful	N/A
9556	1460	1460	1468	1488	1528	0	5.498850657	Successful	N/A
9560	1460	1460	1468	1488	1528	0	5.498850657	Successful	N/A
9564	1460	1460	1468	1488	1528	0	5.498850657	Successful	N/A
9568	1460	1460	1468	1488	1528	0	5.498850657	Successful	N/A
9572	1460	1460	1468	1488	1528	0	5.498850657	Successful	N/A
9576	1460	1460	1468	1488	1528	0	5.498850657	Successful	N/A
9580	1460	1460	1468	1488	1528	0	5.498850657	Successful	N/A
9584	1460	1460	1468	1488	1528	0	5.498850657	Successful	N/A
9588	1460	1460	1468	1488	1528	0	5.498850657	Successful	N/A
9592	1460	1460	1468	1488	1528	0	5.498850657	Successful	N/A
9596	1460	1460	1468	1488	1528	0	5.498850657	Successful	N/A
9600	1460	1460	1468	1488	1528	0	5.498850657	Successful	N/A
9604	1460	1460	1468	1488	1528	0	5.498850657	Successful	N/A
9608	1460	1460	1468	1488	1528	0	5.498850657	Successful	N/A
9612	1460	1460	1468	1488	1528	0	5.498850657	Successful	N/A
9616	1460	1460	1468	1488	1528	0	10.9927069	Errored	N/A
9617	1460	1460	1468	1488	1528	0	10.9927069	Errored	N/A
9618	1460	1460	1468	1488	1528	0	10.9927069	Successful	N/A
9622	1460	1460	1468	1488	1528	0	10.9927069	Successful	N/A
9626	1460	1460	1468	1488	1528	0	10.9927069	Successful	N/A

Figure 4-15: Packet Trace

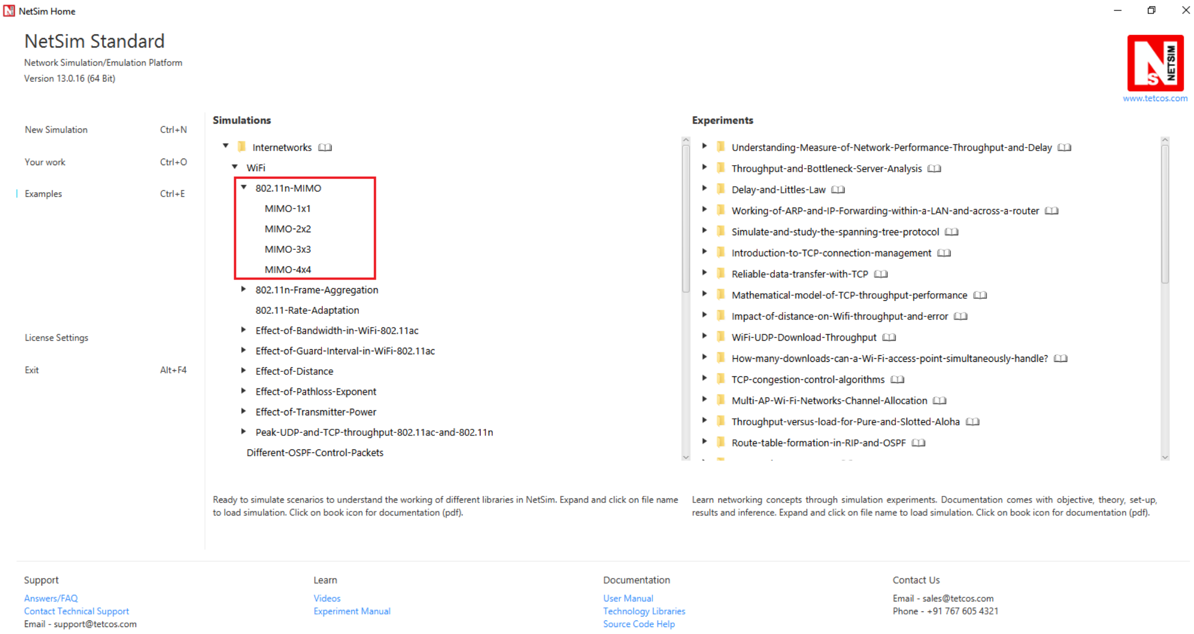
The ‘Generic’ rate adaptation algorithm is similar to the Auto Rate Fall Back (ARF) algorithm. In this algorithm:

- Rate goes up one step for 20 consecutive packet successes
- Rate goes down one step for 4 continuous packet failures

In the above screenshot, the Phy rate reduces from 11Mbps to 5.5Mbps, since there are 4 consecutive data error packets. Then the rate increases from 5.5Mbps to 11Mbps one there is 20 consecutive successful data packet transmissions.

4.5 802.11n MIMO

Open NetSim, Select **Examples → Internetworks → WiFi → 802.11n-MIMO** as shown below as shown **Figure 4-16.**



NetSim Home

NetSim Standard

Network Simulation/Emulation Platform

Version 13.0.16 (64 Bit)

www.tetcos.com

New Simulation	Ctrl+N
Your work	Ctrl+O
Examples	Ctrl+E
License Settings	
Exit	Alt+F4

Simulations

- Internetworks
  - WiFi
    - 802.11n-MIMO
      - MIMO-1x1
      - MIMO-2x2
      - MIMO-3x3
      - MIMO-4x4
    - 802.11n-Frame-Aggregation
    - 802.11-Rate-Adaptation
    - Effect-of-Bandwidth-in-WiFi-802.11ac
    - Effect-of-Guard-Interval-in-WiFi-802.11ac
    - Effect-of-Distance
    - Effect-of-Pathloss-Exponent
    - Effect-of-Transmitter-Power
    - Peak-UDP-and-TCP-throughput-802.11ac-and-802.11n
  - Different-OSPF-Control-Packets

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

- Understanding-Measure-of-Network-Performance-Throughput-and-Delay
- Throughput-and-Bottleneck-Server-Analysis
- Delay-and-Littles-Law
- Working-of-ARP-and-IP-Forwarding-within-a-LAN-and-across-a-router
- Simulate-and-study-the-spanning-tree-protocol
- Introduction-to-TCP-connection-management
- Reliable-data-transfer-with-TCP
- Mathematical-model-of-TCP-throughput-performance
- Impact-of-distance-on-Wifi-throughput-and-error
- WiFi-UDP-Download-Throughput
- How-many-downloads-can-a-Wi-Fi-access-point-simultaneously-handle?
- TCP-congestion-control-algorithms
- Multi-AP-Wi-Fi-Networks-Channel-Allocation
- Throughput-versus-load-for-Pure-and-Slotted-Aloha
- Route-table-formation-in-RIP-and-OSPF

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 4-16: Featured Example list

The following network diagram illustrates what the NetSim UI displays when you open the example configuration file for 802.11n-MIMO.

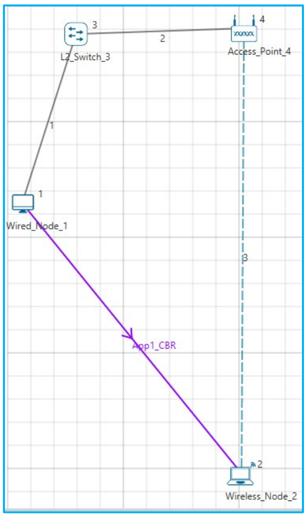


Figure 4-17: WiFi 802.11 MIMO topology

Network Settings

1. Environment Grid length: 50m * 50m
2. Distance between AP and Node is 20m.

3. Set DCF as the medium access layer protocol under datalink layer properties of access_ point and wireless node
4. Click on the Application icon present in the top ribbon/toolbar and set Transport Protocol to UDP
5. WLAN Standard is set to 802.11n and No. of Tx and Rx Antenna is set to 1 in both access point and wireless node (Right-Click Access Point or Wireless Node > Properties > Interface Wireless > Transmitting Antennas and Receiving Antennas)
6. Propagation model → Path Loss only, Path Loss Model -> Log Distance and Path loss Exponent → 3.
7. CBR application with 50Mbps generation rate.(Set Inter Arrival Time : 233 (micro sec)).
8. Enable Plots
9. Simulate for 10 sec.

Results and Discussion

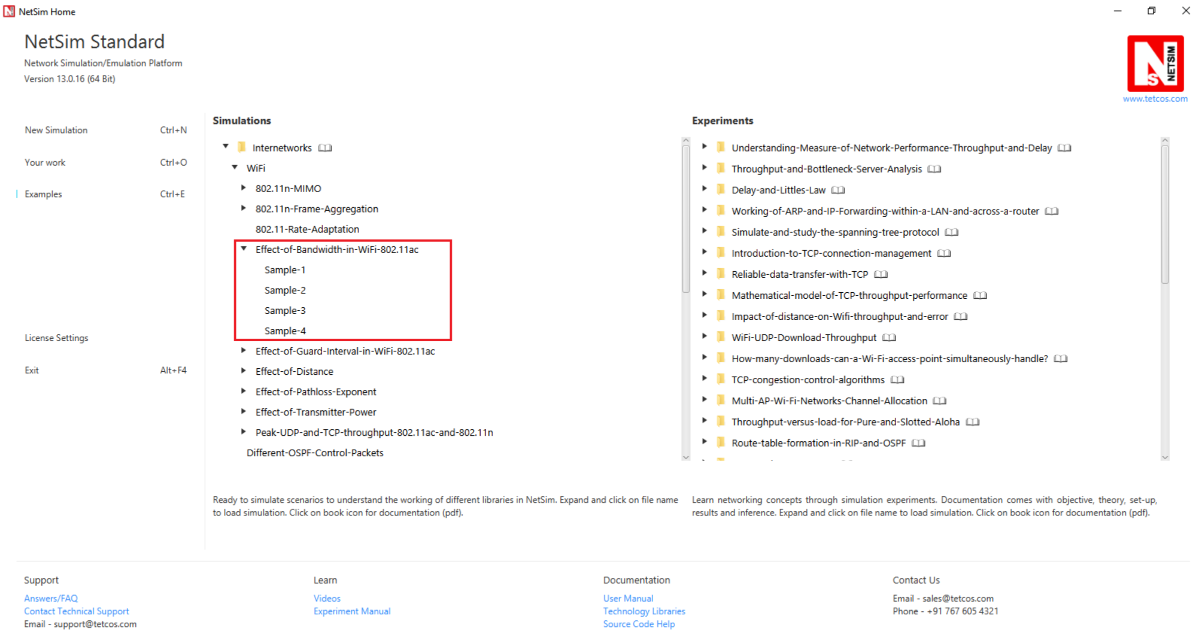
Number of Tx and Rx Antenna	Throughput
1 x 1	23.94 Mbps
2 x 2	31.02 Mbps
3 x 3	33.32 Mbps
4 x 4	35.87 Mbps

Table 4-5: Number of Tx and Rx Antenna vs. Throughput

MIMO is a method for multiplying the capacity of a radio link using multiple transmit and receive antennas. Increasing the Transmitter and Receiver Antenna count results in more PHY Data rate (link capacity) and hence leads to an increase in application throughput.

4.6 Effect of Bandwidth and Guard Interval in WiFi 802.11ac

Effect of Bandwidth: Open NetSim and click **Examples > Internetworks > WiFi > Effect-of-bandwidth-in-WiFi-802.11ac** as shown **Figure 4-18.**



NetSim Home

NetSim Standard

Network Simulation/Emulation Platform

Version 13.0.16 (64 Bit)

www.tetcos.com

New Simulation	Ctrl+N
Your work	Ctrl+O
Examples	Ctrl+E
License Settings	
Exit	Alt+F4

Simulations

- Internetworks
  - WiFi
    - 802.11n-MIMO
    - 802.11n-Frame-Aggregation
    - 802.11-Rate-Adaptation
    - Effect-of-Bandwidth-in-WiFi-802.11ac
      - Sample-1
      - Sample-2
      - Sample-3
      - Sample-4
    - Effect-of-Guard-Interval-in-WiFi-802.11ac
    - Effect-of-Distance
    - Effect-of-Pathloss-Exponent
    - Effect-of-Transmitter-Power
    - Peak-UDP-and-TCP-throughput-802.11ac-and-802.11n
  - Different-OSPF-Control-Packets

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

- Understanding-Measure-of-Network-Performance-Throughput-and-Delay
- Throughput-and-Bottleneck-Server-Analysis
- Delay-and-Littles-Law
- Working-of-ARP-and-IP-Forwarding-within-a-LAN-and-across-a-router
- Simulate-and-study-the-spanning-tree-protocol
- Introduction-to-TCP-connection-management
- Reliable-data-transfer-with-TCP
- Mathematical-model-of-TCP-throughput-performance
- Impact-of-distance-on-Wifi-throughput-and-error
- WiFi-UDP-Download-Throughput
- How-many-downloads-can-a-Wi-Fi-access-point-simultaneously-handle?
- TCP-congestion-control-algorithms
- Multi-AP-Wi-Fi-Networks-Channel-Allocation
- Throughput-versus-load-for-Pure-and-Slotted-Aloha
- Route-table-formation-in-RIP-and-OSPF

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 4-18: Featured Example list

The following network diagram illustrates what the NetSim UI displays when you open the example configuration file as shown **Figure 4-19.**

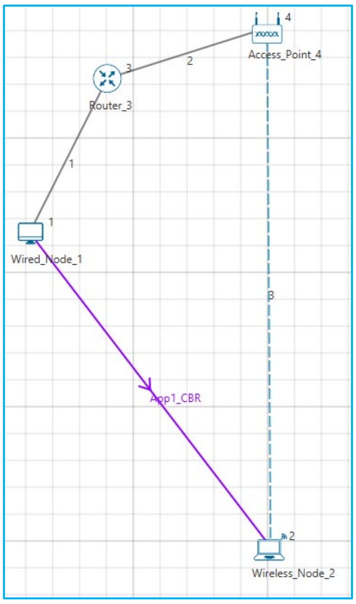


Figure 4-19: WiFi Network Topology in this experiment

Network Settings

1. Environment Grid length: 50m * 50m.
2. Click on the Application icon present in the top ribbon/toolbar and set Transport Protocol to UDP
3. Channel Characteristics: NO PATHLOSS in wireless link properties.
4. Set Bit Error rate and Propagation delay to zero under wired link properties

5. Set 802.11ac standard and Bandwidth to 20MHz under Wireless Interface->Physical Layer properties of the access point and wireless node.
6. Set DCF as the medium access layer protocol under Wireless Interface-> datalink layer properties of access point and wireless node
7. Enable packet trace and plots.
8. Set generation rate as 100 Mbps under Application properties (Packet Size = 1460 Bytes, Interarrival time = 116 microseconds). Generation rate can be calculated by using the formula below:

$$Generation\ Rate\ (Mbps) = \ Packet\ Size\ (Bytes) * \frac{8}{Interarrival} time\ (\mu s)$$

= 1460 (Bytes)*8/116 (µs) ~ 100 Mbps

9. Run simulation for 10s and see Application throughput in the Results Window

Analytical Model

The average time to transmit a packet comprises of

- DIFS
- Backoff duration
- Data packet transmission time
- SIFS
- MAC ACK transmission time

The timing diagram is as shown below **Figure 4-20.**

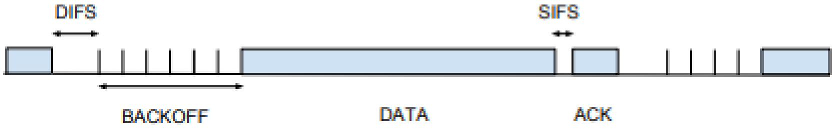


Figure 4-20: Timing diagram for WLAN

The Average throughput can be calculated by using the formula below:

$$Average\ Throughput\ (Mbps) = \frac{Application\ Payload(Bytes)}{Average\ Time\ per\ Packet(\mu s)}$$

$$\begin{aligned}&Average\ time\ per\ packet\ \ (\mu s)\\&\qquad = DIFS\ +\ Average\ Backoff\ time\ +\ Packet\ Transmission\ Time\ +\ SIFS\\&\qquad +\ Ack\ Transmission\ Time\end{aligned}$$

$$Packet\ Transmission\ Time\ (\mu s) = \ Preamble\ time\ +\ (MPDU\ Size/Data\ rate)$$

$$Average\ Backoff\ time\ (\mu s)\ =\ (CWmin/2)\ *\ Slot\ Time$$

$$Ack\ Transmission\ Time\ (\mu s) = Preamble\ time + (Ack\ Packet\ size/Ack\ data\ rate)$$

$$DIFS\ (\mu s) = SIFS + 2 * Slot\ Time$$

$$Average\ Backoff\ time\ (\mu s) = (CWmin/2) * Slot\ Time$$

where

$$Application\ payload = 1460\ Bytes$$

$$Average\ time\ per\ packet = 34 + 67.5 + 185.36 + 16 + 212.88 = 513.74\ \mu s$$

$$SIFS = 16\ \mu s$$

$$Slot\ time = 9\ \mu s$$

$$CWmin = 15\ slots\ for\ 802.11ac$$

$$DIFS = SIFS + 2 * Slot\ Time = 16\ \mu s + 2 * 9\ \mu s = 34\ \mu s$$

$$Average\ Backoff\ time = 67.5\ \mu s$$

$$Packet\ Transmission\ Time = 44\ \mu s + (1532 * 8/86.7\ Mbps) = 185.36\ \mu s$$

$$Preamble\ time = 44\ \mu s\ for\ 802.11ac\ standard$$

$$MPDU\ Size = 1460 + 8 + 20 + 44 = 1532\ Bytes$$

$$Ack\ Transmission\ Time = 44\ \mu s + (152\ Bytes * 8\ /\ 7.2Mbps) = 212.88\ \mu s$$

$$Average\ throughput = 1460 * 8/\ (513.74) = 22.7\ Mbps$$

Similarly calculate throughput theoretically for other samples by changing bandwidth and compare with Simulation throughput. Users can get the data rate by using the formula given below:

$$Phy\ rate\ (802.11b) = Phy\_layer\_payload * 8/(phy\ end\ time - phy\ arrival\ time - 44)$$

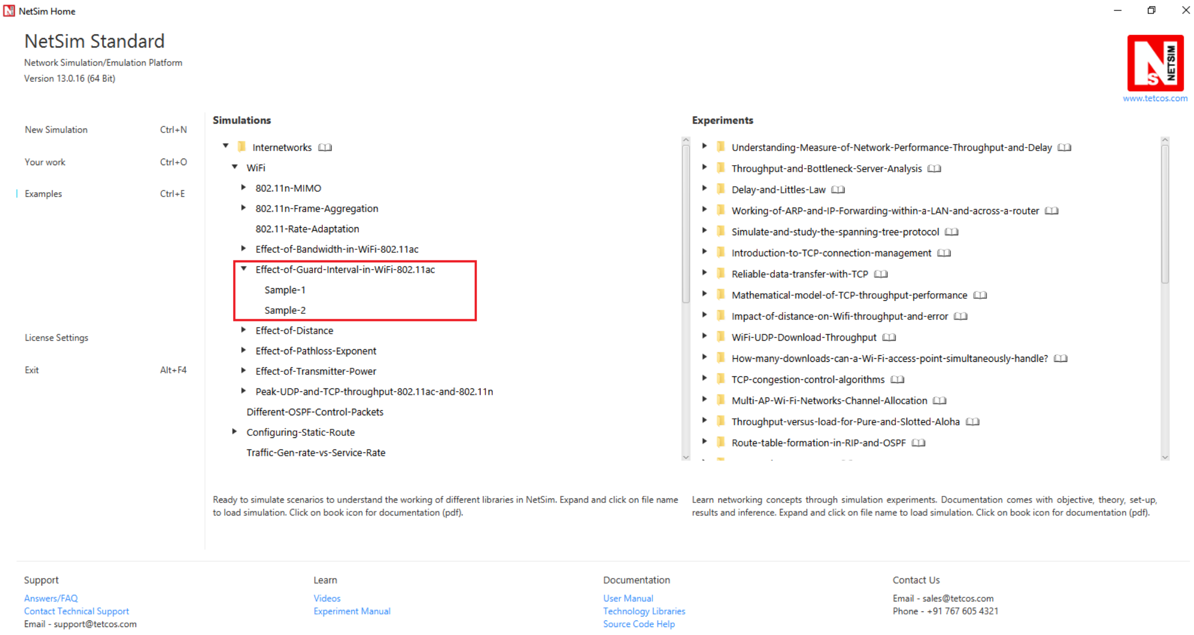
Results and Discussion

Bandwidth (MHz)	Analytical Estimate of Throughput (Mbps)	Simulation Throughput (Mbps)
20	22.70	22.77
40	33.77	33.78
80	43.39	43.44
160	49.35	49.51

Table 4-6: Result comparison of different bandwidth vs. Estimate of Throughput and Simulation Throughput

One can observe that there is an increase in throughput as we increase the bandwidth from 20MHz to 160MHz.

Effect of Guard Interval: Open NetSim and click **Examples > Internetworks > WiFi > Effect-of-Guard-Interval-in-WiFi-802.11ac** as shown **Figure 4-21.**



NetSim Home

NetSim Standard
Network Simulation/Emulation Platform
Version 13.0.16 (64 Bit)

www.tetcos.com

New Simulation Ctrl+N
Your work Ctrl+O
Examples Ctrl+E
License Settings
Exit Alt+F4

Simulations

- Internetworks
  - WiFi
    - 802.11n-MIMO
    - 802.11n-Frame-Aggregation
    - 802.11-Rate-Adaptation
    - Effect-of-Bandwidth-in-WiFi-802.11ac
    - Effect-of-Guard-Interval-in-WiFi-802.11ac
      - Sample-1
      - Sample-2
    - Effect-of-Distance
    - Effect-of-Pathloss-Exponent
    - Effect-of-Transmitter-Power
    - Peak-UDP-and-TCP-throughput-802.11ac-and-802.11n
  - Different-OSPF-Control-Packets
  - Configuring-Static-Route
  - Traffic-Gen-rate-vs-Service-Rate

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

- Understanding-Measure-of-Network-Performance-Throughput-and-Delay
- Throughput-and-Bottleneck-Server-Analysis
- Delay-and-Littles-Law
- Working-of-ARP-and-IP-Forwarding-within-a-LAN-and-across-a-router
- Simulate-and-study-the-spanning-tree-protocol
- Introduction-to-TCP-connection-management
- Reliable-data-transfer-with-TCP
- Mathematical-model-of-TCP-throughput-performance
- Impact-of-distance-on-Wifi-throughput-and-error
- WiFi-UDP-Download-Throughput
- How-many-downloads-can-a-Wi-Fi-access-point-simultaneously-handle?
- TCP-congestion-control-algorithms
- Multi-AP-Wi-Fi-Networks-Channel-Allocation
- Throughput-versus-load-for-Pure-and-Slotted-Aloha
- Route-table-formation-in-RIP-and-OSPF

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 4-21: Featured Example list

The following network diagram illustrates what the NetSim UI displays when you open the example configuration file as shown **Figure 4-22.**

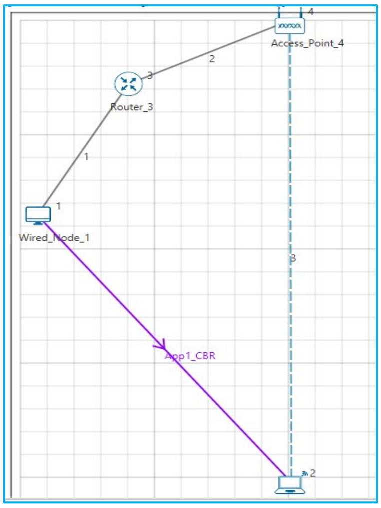


Figure 4-22: WiFi Network Topology

Network Settings

1. Environment Grid length: 50m * 50m.

2. Click on the Application icon present in the top ribbon/toolbar and set Transport Protocol to UDP
3. Channel Characteristics: NO PATHLOSS in wireless link properties.
4. Set 802.11ac standard and Bandwidth to 20MHz under Wireless Interface->Physical Layer properties of the access point and wireless node.
5. Set DCF as the medium access layer protocol under Wireless Interface-> datalink layer properties of access point and wireless node.
6. Set DCF as the medium access layer protocol under datalink layer properties of access point and wireless node.
7. Set Bit Error rate and Propagation delay to zero under wired link properties
8. Enable plots.
9. Set Guard interval to 400ns under Wireless Interface->Physical Layer properties of access point and wireless node.
10. Set generation rate as 100 Mbps under Application properties (Packet Size = 1460 Bytes, Interarrival time = 116 micro seconds). Generation rate can be calculated by using the formula below:

$$Generation\ Rate\ (Mbps) = \ Packet\ Size\ (Bytes) * \frac{8}{Interarrival} time\ (\mu s)$$

= 1460 (Bytes)*8/116 (μs) ~ 100 Mbps

11. Run simulation for 10s and note down the throughput

Calculate throughput theoretically as explained above and compare with Simulation throughput.

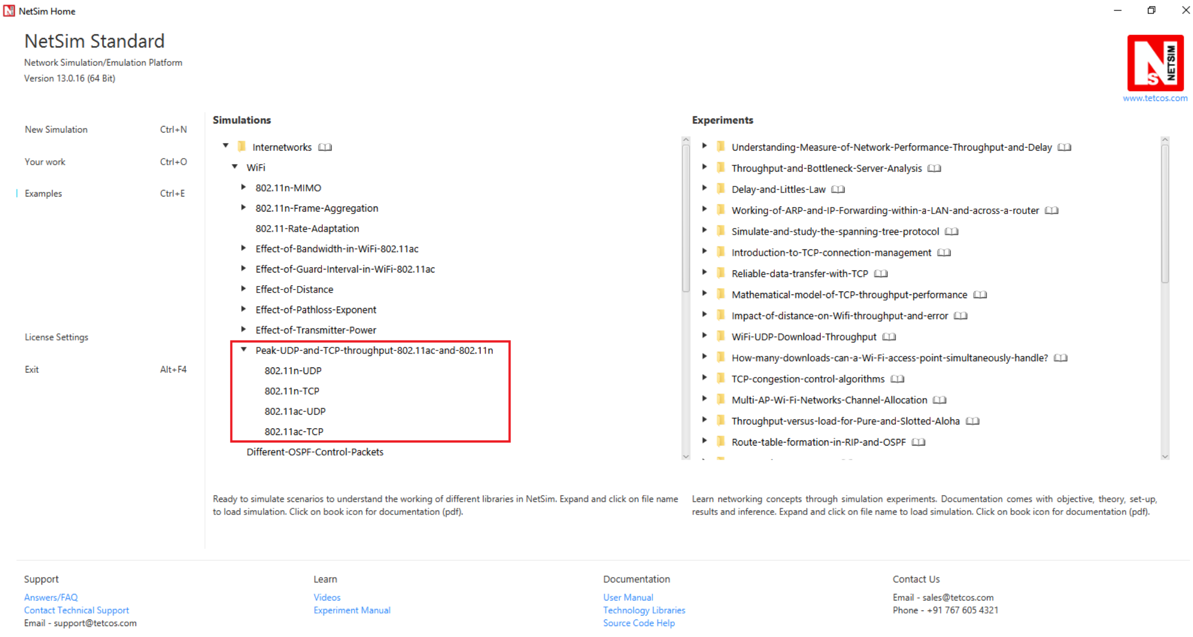
Results and Discussion

Guard Interval (ns)	Theoretical Throughput (Mbps)	Simulation Throughput (Mbps)
400	17.76	22.77
800	16.87	21.32

Table 4-7: Result comparison of different Guard Interval vs. Theoretical Throughput and Simulation Throughput

4.7 Peak UDP and TCP throughput 802.11ac and 802.11n

Open NetSim, Select **Examples ->Internetworks-> WiFi -> Peak-UDP-and-TCP-throughput-802.11ac-and-802.11n** as shown **Figure 4-23.**



NetSim Home

NetSim Standard

Network Simulation/Emulation Platform

Version 13.0.16 (64 Bit)

www.tetcos.com

New Simulation	Ctrl+N
Your work	Ctrl+O
Examples	Ctrl+E
License Settings	
Exit	Alt+F4

Simulations

- Internetworks
  - WiFi
    - 802.11n-MIMO
    - 802.11n-Frame-Aggregation
    - 802.11-Rate-Adaptation
    - Effect-of-Bandwidth-in-WiFi-802.11ac
    - Effect-of-Guard-Interval-in-WiFi-802.11ac
    - Effect-of-Distance
    - Effect-of-Pathloss-Exponent
    - Effect-of-Transmitter-Power
    - Peak-UDP-and-TCP-throughput-802.11ac-and-802.11n
      - 802.11n-UDP
      - 802.11n-TCP
      - 802.11ac-UDP
      - 802.11ac-TCP
  - Different-OSPF-Control-Packets

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

- Understanding-Measure-of-Network-Performance-Throughput-and-Delay
- Throughput-and-Bottleneck-Server-Analysis
- Delay-and-Littles-Law
- Working-of-ARP-and-IP-Forwarding-within-a-LAN-and-across-a-router
- Simulate-and-study-the-spanning-tree-protocol
- Introduction-to-TCP-connection-management
- Reliable-data-transfer-with-TCP
- Mathematical-model-of-TCP-throughput-performance
- Impact-of-distance-on-Wifi-throughput-and-error
- WiFi-UDP-Download-Throughput
- How-many-downloads-can-a-Wi-Fi-access-point-simultaneously-handle?
- TCP-congestion-control-algorithms
- Multi-AP-Wi-Fi-Networks-Channel-Allocation
- Throughput-versus-load-for-Pure-and-Slotted-Aloha
- Route-table-formation-in-RIP-and-OSPF

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 4-23: Featured Example list

The following network diagram illustrates, what the NetSim UI displays when you open the example configuration file as shown **Figure 4-24.**

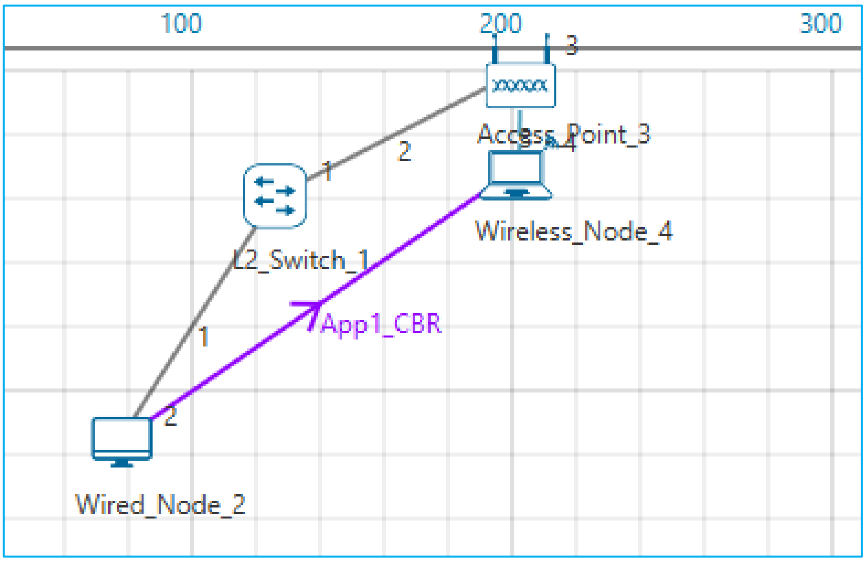


Figure 4-24: WiFi Network Topology

4.7.1 IEEE802.11n

Settings done in example config file:

1. Set the following property as shown in below given **Table 4-8.**

Interface Parameters	
Standard	IEEE802.11n
No. of Frame aggregated	64

Channel	1_2412 MHz
Rate Adaptation	False
Short Retry Limit	7
Long Retry Limit	4
Dott11_RTSThreshold	3000bytes
Medium Access Protocol	DCF
Buffer Size	1MB
Guard Interval	400ns
Bandwidth	40 MHz
Frequency Band	2.4 GHz
Transmitter Power	100mW
Antenna Gain	0
Antenna height	1m
Reference distance (d0)	1m
Transmitting Antennas	4
Receiving Antennas	4

Table 4-8: Detailed Network Parameters for IEEE802.11n

2. Set Uplink speed and Downlink speed as 1000 Mbps in wired link properties.
3. The Channel Characteristics were set as No pathloss in wireless link properties.
4. Set **Downlink** application source node as Wired Node destination node as Wireless Node.

Application Properties	
App1_CBR	
Packet Size (Byte)	1450
Inter Arrival Time (µs)	11.6
Transport Protocol	UDP

Table 4-9: Application Parameters

5. Plots are enabled in NetSim GUI.
6. Run simulation for 10 sec. After simulation completes go to metrics window and note down throughput value from application metrics.

Change Transport protocol to **TCP**, Window scaling is set to True and Scale shift count set to 5 in the transport layer of Wired node and Wireless node for the other sample (i,e 802.11n-TCP), run the simulation for 10 sec and note down throughput value from application metrics.

Results and Discussion

Transport Protocol	Throughput (Mbps)
UDP	422.48
TCP	339.75

Table 4-10: Results comparison of TCP and UDP throughputs for IEEE802.11n

4.7.2 IEEE802.11ac

Settings done in example config file:

1. Set the following property as shown in below given table:

Interface Parameters	
Standard	IEEE802.11ac
No. of Frame aggregated	64
Channel	36 (5180MHz)
Rate Adaptation	False
Short Retry Limit	7
Long Retry Limit	4
Dott11_RTSThreshold	3000bytes
Medium Access Protocol	DCF
Buffer Size	1MB
Guard Interval	400ns
Bandwidth	160 MHz
Frequency Band	5 GHz
Transmitter Power	100mW
Antenna Gain	0
Antenna height	1m
Reference distance (d0)	1m
Transmitting Antennas	8
Receiving Antennas	8

Table 4-11: Detailed Network Parameters for IEEE802.11ac

2. Set Uplink speed and Downlink speed as 10000 Mbps in wired link properties.
3. The Channel Characteristics were set as No pathloss in wireless link properties.
4. Set **Downlink** application source node as Wired Node destination node as Wireless Node.

Application Properties	
App1_CBR	
Packet Size (Byte)	1450
Inter Arrival Time (µs)	5.84
Transport Protocol	UDP

Table 4-12: Application Parameters

5. Plots are enabled in NetSim GUI.
6. Run simulation for 10 sec. After simulation completes go to metrics window and note down throughput value from application metrics.

Change Transport protocol to TCP, Window scaling is set to True and Scale shift count set to 5 in the transport layer of Wired node and Wireless node for the other sample (i,e 802.11ac-TCP), run the simulation for 10 sec and note down throughput value from application metrics.

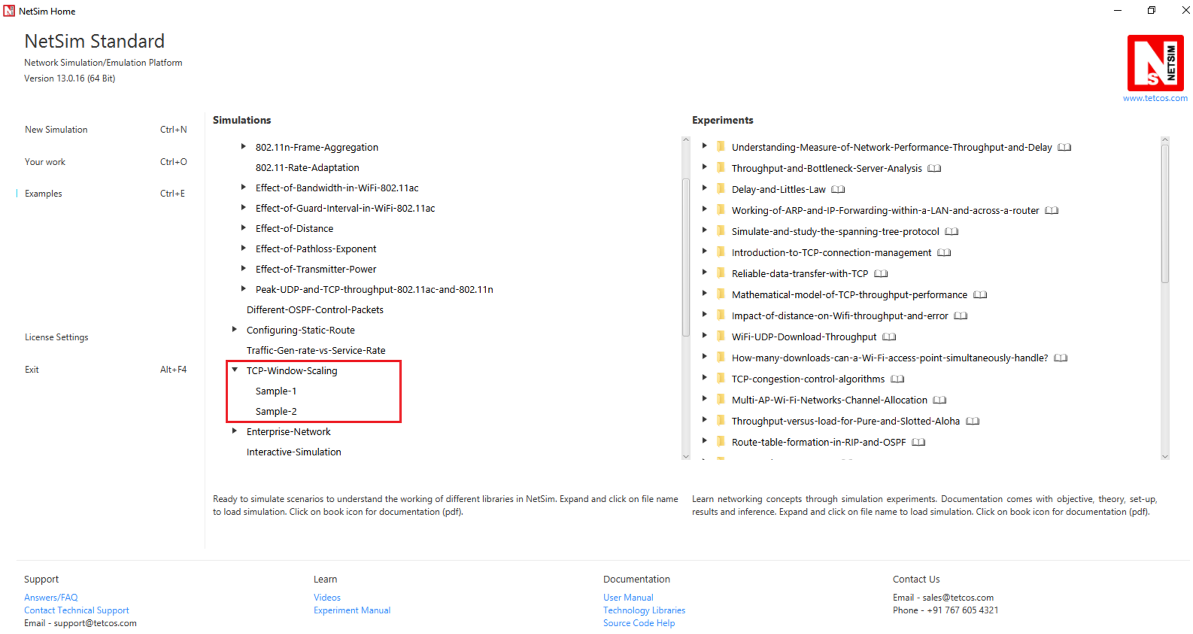
Results and Discussion

Transport Protocol	Throughput (Mbps)
UDP	1632.28
TCP	995.88

Table 4-13: Results comparison of TCP and UDP throughputs for IEEE802.11ac

4.8 TCP Window Scaling

Open NetSim, Select **Examples->Internetworks->TCP-Window-Scaling** as shown below **Figure 4-25.**



NetSim Home

NetSim Standard

Network Simulation/Emulation Platform

Version 13.0.16 (64 Bit)

www.tetcos.com

New Simulation Ctrl+N

Your work Ctrl+O

Examples Ctrl+E

License Settings

Exit Alt+F4

Simulations

- 802.11n-Frame-Aggregation
- 802.11-Rate-Adaptation
- Effect-of-Bandwidth-in-WiFi-802.11ac
- Effect-of-Guard-Interval-in-WiFi-802.11ac
- Effect-of-Distance
- Effect-of-Pathloss-Exponent
- Effect-of-Transmitter-Power
- Peak-UDP-and-TCP-throughput-802.11ac-and-802.11n
- Different-OSPF-Control-Packets
- Configuring-Static-Route
- Traffic-Gen-rate-vs-Service-Rate
- TCP-Window-Scaling
  - Sample-1
  - Sample-2
- Enterprise-Network
- Interactive-Simulation

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

- Understanding-Measure-of-Network-Performance-Throughput-and-Delay
- Throughput-and-Bottleneck-Server-Analysis
- Delay-and-Littles-Law
- Working-of-ARP-and-IP-Forwarding-within-a-LAN-and-across-a-router
- Simulate-and-study-the-spanning-tree-protocol
- Introduction-to-TCP-connection-management
- Reliable-data-transfer-with-TCP
- Mathematical-model-of-TCP-throughput-performance
- Impact-of-distance-on-Wifi-throughput-and-error
- WiFi-UDP-Download-Throughput
- How-many-downloads-can-a-Wi-Fi-access-point-simultaneously-handle?
- TCP-congestion-control-algorithms
- Multi-AP-Wi-Fi-Networks-Channel-Allocation
- Throughput-versus-load-for-Pure-and-Slotted-Aloha
- Route-table-formation-in-RIP-and-OSPF

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 4-25: Featured Example list

The following network diagram illustrates what the NetSim UI displays when you open the example configuration file for TCP Window scaling as shown **Figure 4-26.**

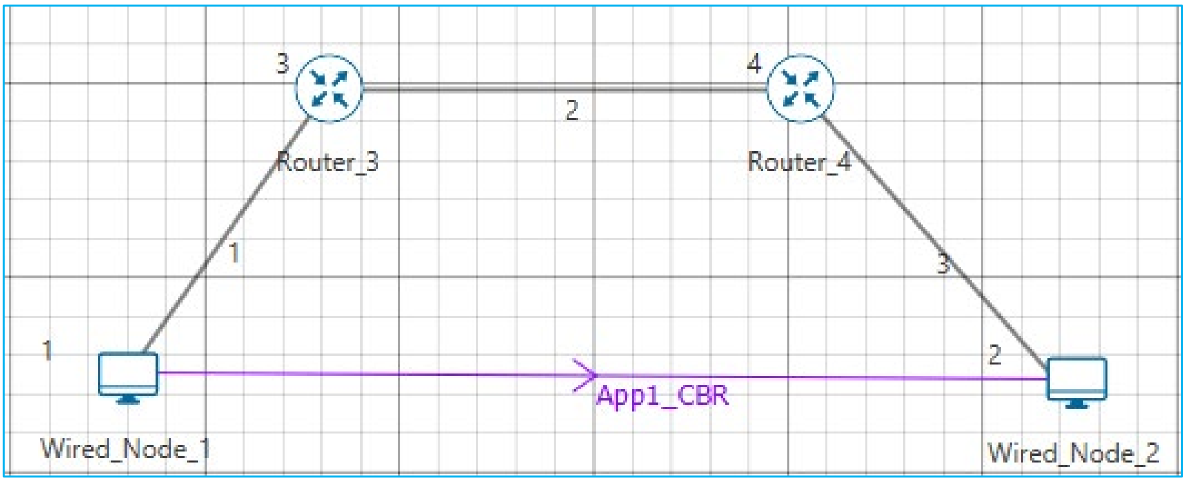


Figure 4-26: Network Topology in this experiment

The TCP throughput of a link is limited by two windows: the congestion window and the receive window. The congestion window tries not to exceed the capacity of the network (congestion control); the receive window tries not to exceed the capacity of the receiver to process data (flow control).

The **TCP window scale option** is an option to increase the receive window size allowed in Transmission Control Protocol above its former maximum value of 65,535 bytes.

TCP window scale option is needed for efficient transfer of data when the bandwidth-delay product is greater than 64K. For instance, if a https://en.wikipedia.org/wiki/Digital_Signal_1transmission line of 1.5 Mbit/second was used over a satellite link with a 513 milliseconds round trip time (RTT), the bandwidth-delay product is $1500000 \times 0.513 = 769{,}500$ bits or about 96,187 bytes.

Using a maximum window size of 64 KB only allows the buffer to be filled to $\frac{65535}{96187} = 68\ \%$ of the theoretical maximum speed of 1.5 Mbps, or 1.02 Mbps.

By using the window scale option, the receive window size may be increased up to a maximum value of 1,073,725,440 bytes. This is done by specifying a one byte shift count in the header options field. The true receive window size is left shifted by the value in shift count. A maximum value of 14 may be used for the shift count value. This would allow a single TCP connection to transfer data over the example satellite link at 1.5 Mbit/second utilizing all of the available bandwidth.

Network Settings

1. Wired Node 1 in Transport Layer TCP Window Scaling → FALSE (by default) and Congestion plot set as TRUE.
2. Application Generation rate → 10Mbps (Set Inter arrival time = 1168)
3. Bit error rate (Uplink and Downlink) → 0 in all wired links
4. Enabled Wireshark Capture in General Properties Wired Node 1 → Set as Offline
5. Link1 & Link3 Propagation delay (uplink and downlink) →5(Microsec) (by default)
6. Change the Link2 speed → 10Mbps, Propagation delay (uplink and downlink) ->100000 (Microsec)
7. Simulate for 100sec and note down the throughput
8. Now change the Window Scaling → TRUE (for all wired nodes)
9. Simulate for 100s and note down the throughput

Results and Discussion

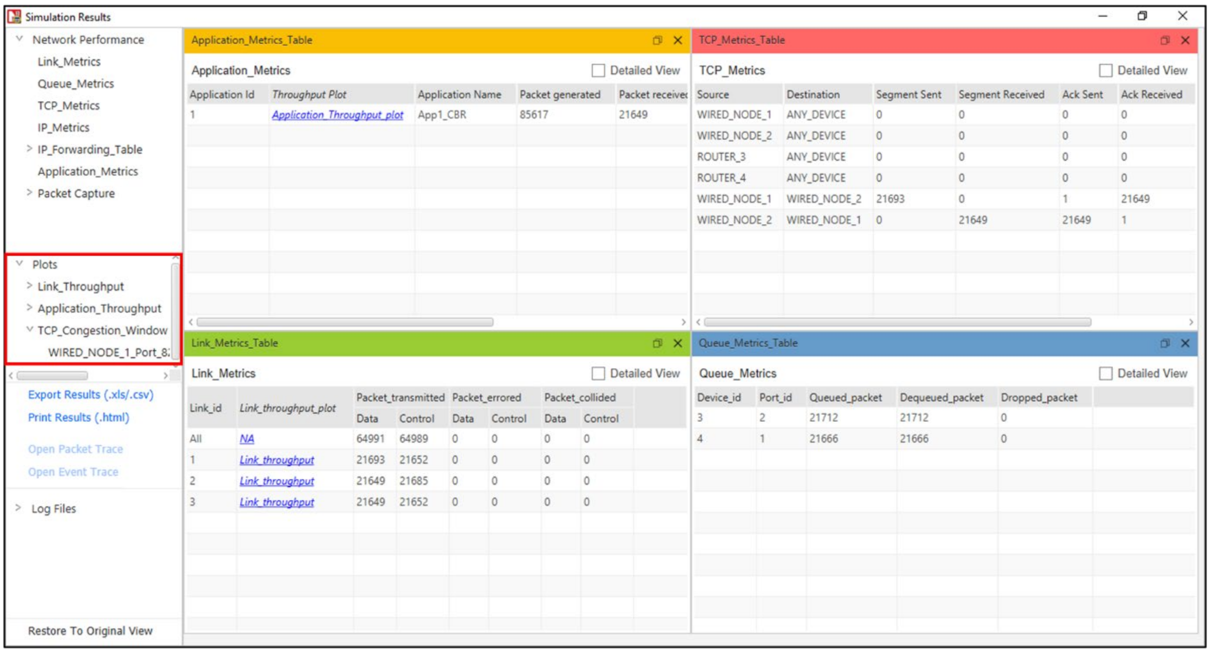
Window Scaling	Application Throughput (Mbps)
FALSE	2.5
TRUE	8.7

Table 4-14: Results comparison for with/without Window Scaling

Throughput calculation (Without Window Scaling)

Theoretical Throughput = Window size / Round trip time = $\frac{65525 * 8\ Bytes}{200ms}$ = $2.62\ Mbps$

Go to the simulation result window -> plots -> TCP Congestion Plot **Figure 4-28/Figure 4-29.**



Application_Metrics_Table

Application_Metrics □ Detailed View

Application Id	Throughput Plot	Application Name	Packet generated	Packet receive
1	Application_Throughput_plot	App1_CBR	85617	21649

TCP_Metrics_Table

TCP_Metrics □ Detailed View

Source	Destination	Segment Sent	Segment Received	Ack Sent	Ack Received
WIRED_NODE_1	ANY_DEVICE	0	0	0	0
WIRED_NODE_2	ANY_DEVICE	0	0	0	0
ROUTER_3	ANY_DEVICE	0	0	0	0
ROUTER_4	ANY_DEVICE	0	0	0	0
WIRED_NODE_1	WIRED_NODE_2	21693	0	1	21649
WIRED_NODE_2	WIRED_NODE_1	0	21649	21649	1

Link_Metrics_Table

Link_Metrics □ Detailed View

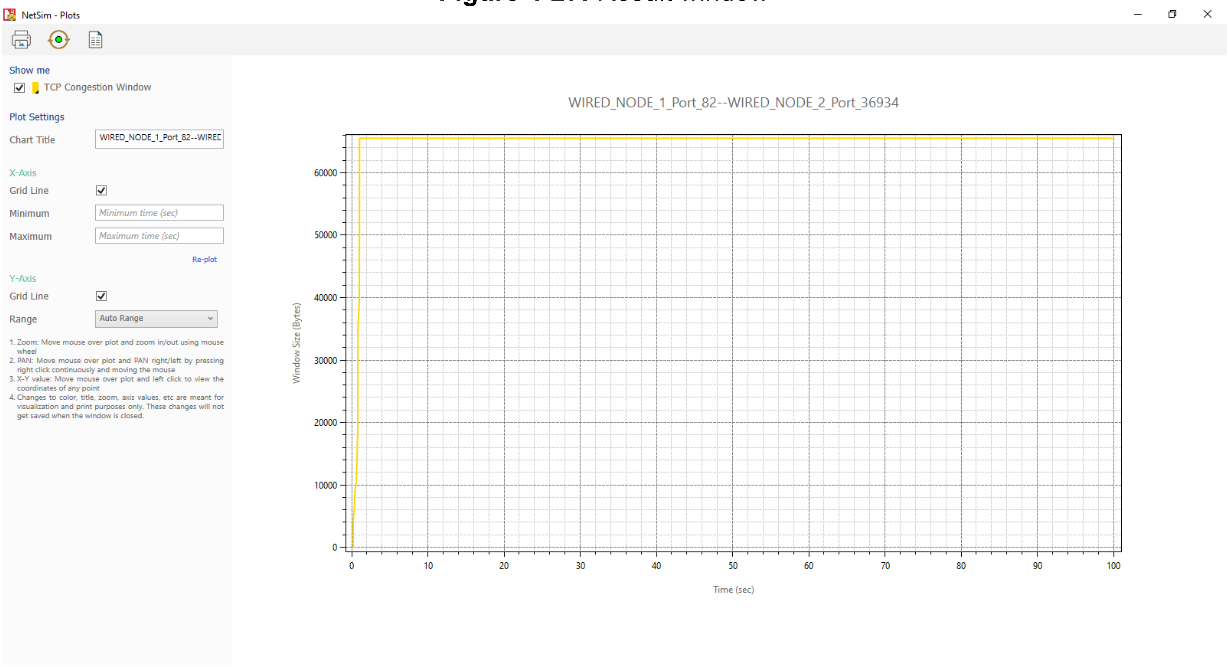
Link_id	Link_throughput_plot	Packet_transmitted		Packet_errored		Packet_collided	
		Data	Control	Data	Control	Data	Control
All	NA	64991	64989	0	0	0	0
1	Link_throughput	21693	21652	0	0	0	0
2	Link_throughput	21649	21685	0	0	0	0
3	Link_throughput	21649	21652	0	0	0	0

Queue_Metrics_Table

Queue_Metrics □ Detailed View

Device_id	Port_id	Queued_packet	Dequeued_packet	Dropped_packet
3	2	21712	21712	0
4	1	21666	21666	0

Figure 4-27: Result window



Show me

☑ TCP Congestion Window

Plot Settings

Chart Title: WIRED_NODE_1_Port_82--WIREC

X-Axis

Grid Line ☑

Minimum: Minimum time (sec)

Maximum: Maximum time (sec)

Re-plot

Y-Axis

Grid Line ☑

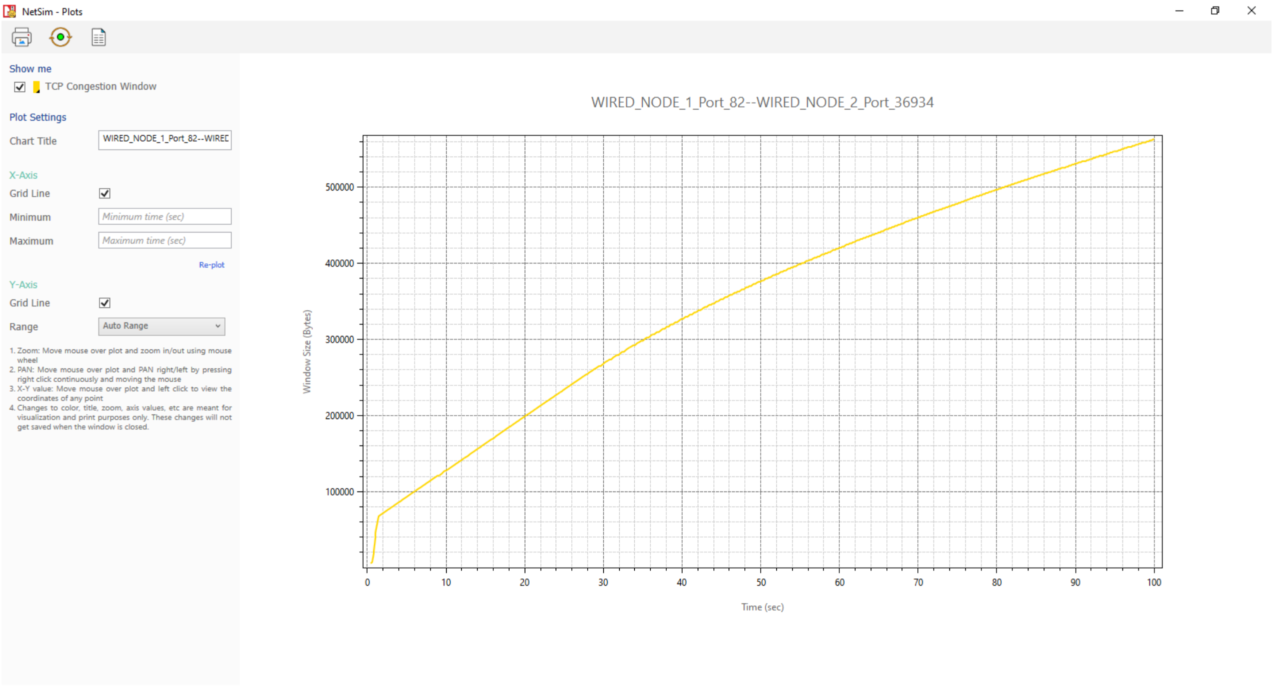
Range: Auto Range

1. Zoom: Move mouse over plot and zoom in/out using mouse wheel
2. PAN: Move mouse over plot and PAN right/left by pressing right click continuously and moving the mouse
3. X-Y value: Move mouse over plot and left click to view the coordinates of any point
4. Changes to color, title, zoom, axis values, etc are meant for visualization and print purposes only. These changes will not get saved when the window is closed.

Figure 4-28: TCP Congestion Plot for wired node_1

In case 1 the Application_Throughput is 2.5 Mbps less than the theoretical throughput since it initially takes some time for the window to reach 65535 B.

With Window Scaling



Show me

☑ 🟨 TCP Congestion Window

Plot Settings

Chart Title: WIRED_NODE_1_Port_82--WIREC

X-Axis

Grid Line ☑

Minimum: Minimum time (sec)

Maximum: Maximum time (sec)

Re-plot

Y-Axis

Grid Line ☑

Range: Auto Range

1. Zoom: Move mouse over plot and zoom in/out using mouse wheel
2. PAN: Move mouse over plot and PAN right/left by pressing right click continuously and moving the mouse
3. X-Y value: Move mouse over plot and left click to view the coordinates of any point
4. Changes to color, title, zoom, axis values, etc are meant for visualization and print purposes only. These changes will not get saved when the window is closed.

Figure 4-29: TCP Congestion Plot for wired node_2

From the above screenshot, users can notice that the window size grows up to 560192Bytes because of Window Scaling. This leads to a higher Application_Throughput compared to the case without window scaling.

We have enabled WireShark Capture in the Wired Node 1. The PCAP file is generated silently at the end of the simulation. Double click on WIRED NODE1_1.pcap file available in the result window under packet captures, In Wireshark, the window scaling graph can be obtained as follows. Select any data packet with a left click, then, go to **Statistics** > **TCP Stream Graphs** > **Window Scaling** > Select **Switch Direction**.

4.9 IP Addressing in NetSim

When you create a network using the GUI, NetSim will automatically configure the IP address to the devices in the scenario. Consider the following scenarios:

If you create a network with two wired nodes and L2_Switch, the IP addresses are assigned as 11.1.1.1 and 11.1.1.2 for the two wired nodes. The default subnet mask is assigned to be 255.255.0.0. It can be edited to 255.0.0.0 (Class A) or 255.255.255.0 (Class C) subnet masks. Both the nodes are in the same network (11.1.0.0).

Similarly, if you create a network with a router and two wired nodes, the IP addresses are assigned as 11.1.1.2 and 11.2.1.2 for the two wired nodes. The subnet mask is default as in above case, i.e., 255.255.0.0. The IP address of the router is 11.1.1.1 and 11.2.1.1

respectively for the two interfaces. Both the nodes are in different networks (11.1.0.0 and 11.2.0.0) in this case.

The same logic is extended as the number of devices is increased.

4.10 Configuring Static Routing in NetSim

Static Routing

Routers forward packets using either route information from route table entries that configured manually or the route information that is calculated using dynamic routing algorithms. Static routes, which define explicit paths between two routers, cannot be automatically updated; you must manually reconfigure static routes when network changes occur. Static routes use less bandwidth than dynamic routes. No CPU cycles are used to calculate and analyze routing updates.

Static routes are used in environments where network traffic is predictable and where the network design is simple. You should not use static routes in large, constantly changing networks because static routes cannot react to network changes. Most networks use dynamic routes to communicate between routers but might have one or two static routes configured for special cases. Static routes are also useful for specifying a gateway of last resort (a default router to which all unrouteable packets are sent).

How to Setup Static Routes

In NetSim, static routes can be configured either prior to the simulation or during the simulation.

Static route configuration prior to simulation:

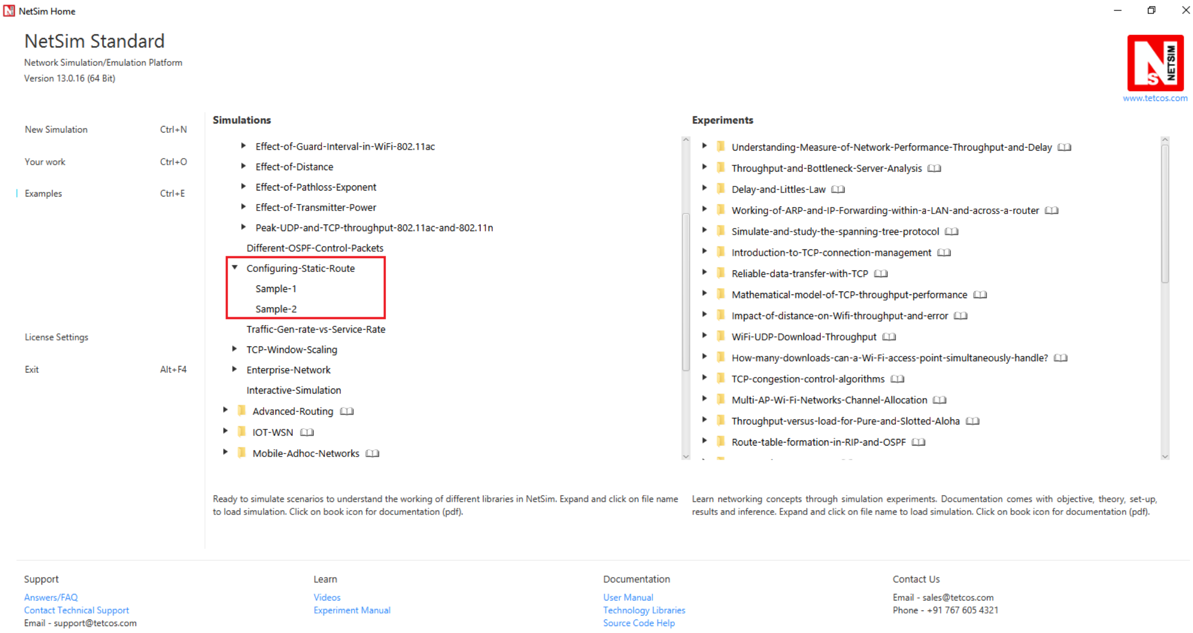
- Via static route GUI configuration
- Via file input (Interactive-Simulation/SDN)

Static route configuration during the simulation:

- Via device NetSim Console (Interactive-Simulation/ SDN)

Static route configuration via GUI

Open NetSim, Select Examples->Internetworks->Configuring-Static-Route as shown below **Figure 4-30**.



NetSim Home

NetSim Standard

Network Simulation/Emulation Platform

Version 13.0.16 (64 Bit)

www.tetcos.com

New Simulation Ctrl+N

Your work Ctrl+O

Examples Ctrl+E

License Settings

Exit Alt+F4

Simulations

- Effect-of-Guard-Interval-in-WiFi-802.11ac
- Effect-of-Distance
- Effect-of-Pathloss-Exponent
- Effect-of-Transmitter-Power
- Peak-UDP-and-TCP-throughput-802.11ac-and-802.11n
- Different-OSPF-Control-Packets
- Configuring-Static-Route
  - Sample-1
  - Sample-2
- Traffic-Gen-rate-vs-Service-Rate
- TCP-Window-Scaling
- Enterprise-Network
- Interactive-Simulation
- Advanced-Routing
- IOT-WSN
- Mobile-Adhoc-Networks

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

- Understanding-Measure-of-Network-Performance-Throughput-and-Delay
- Throughput-and-Bottleneck-Server-Analysis
- Delay-and-Littles-Law
- Working-of-ARP-and-IP-Forwarding-within-a-LAN-and-across-a-router
- Simulate-and-study-the-spanning-tree-protocol
- Introduction-to-TCP-connection-management
- Reliable-data-transfer-with-TCP
- Mathematical-model-of-TCP-throughput-performance
- Impact-of-distance-on-Wifi-throughput-and-error
- WiFi-UDP-Download-Throughput
- How-many-downloads-can-a-Wi-Fi-access-point-simultaneously-handle?
- TCP-congestion-control-algorithms
- Multi-AP-Wi-Fi-Networks-Channel-Allocation
- Throughput-versus-load-for-Pure-and-Slotted-Aloha
- Route-table-formation-in-RIP-and-OSPF

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 4-30: Featured Example list

The following network diagram illustrates what the NetSim UI displays when you open the example configuration file for Configuring Static Routing in NetSim as shown **Figure 4-31.**

4.10.1 Sample 1: Without Static Route

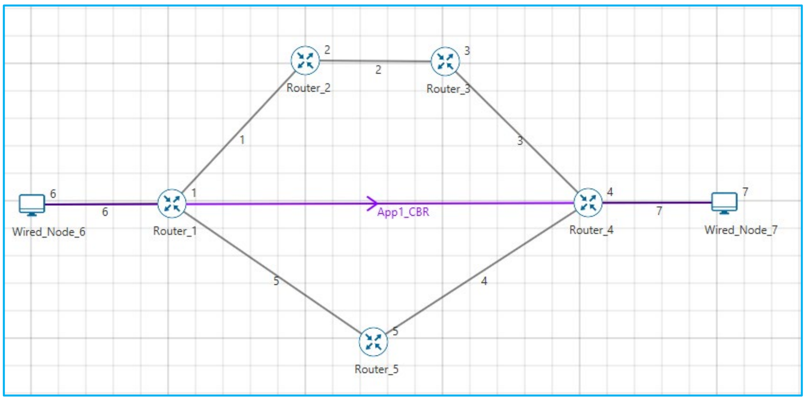
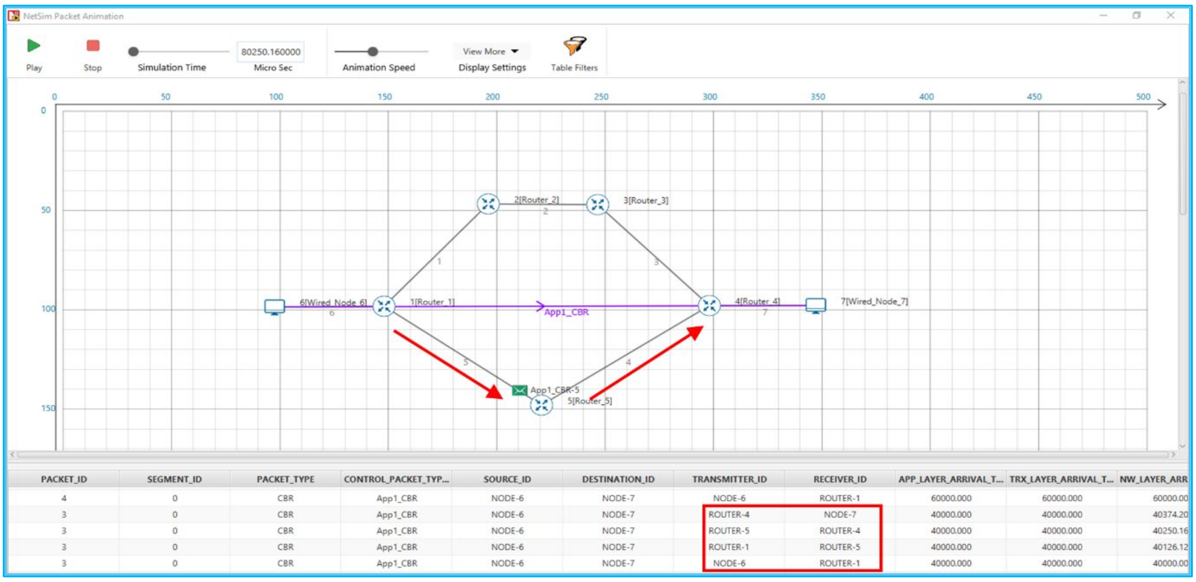


Figure 4-31: Network topology for this experiment

Network Settings

1. Environment Grid length: 500m * 500m.
2. Create a Scenario as shown in above screenshot.
3. Generate CBR Traffic Between Wired node 6 and Wired node 7 and set the transport layer protocol as UDP.
4. The default routing protocol is OSPF in application layer of Routers.
5. Wired link Properties are default.
6. Enable packet trace and plots.
7. Run simulation for 10 seconds.

8. Observe in Animation Window packet flows from Wired Node 6 -> Router 1-> Router 5-> Router 4-> Wired Node 6 as shown in below **Figure 4-32**.



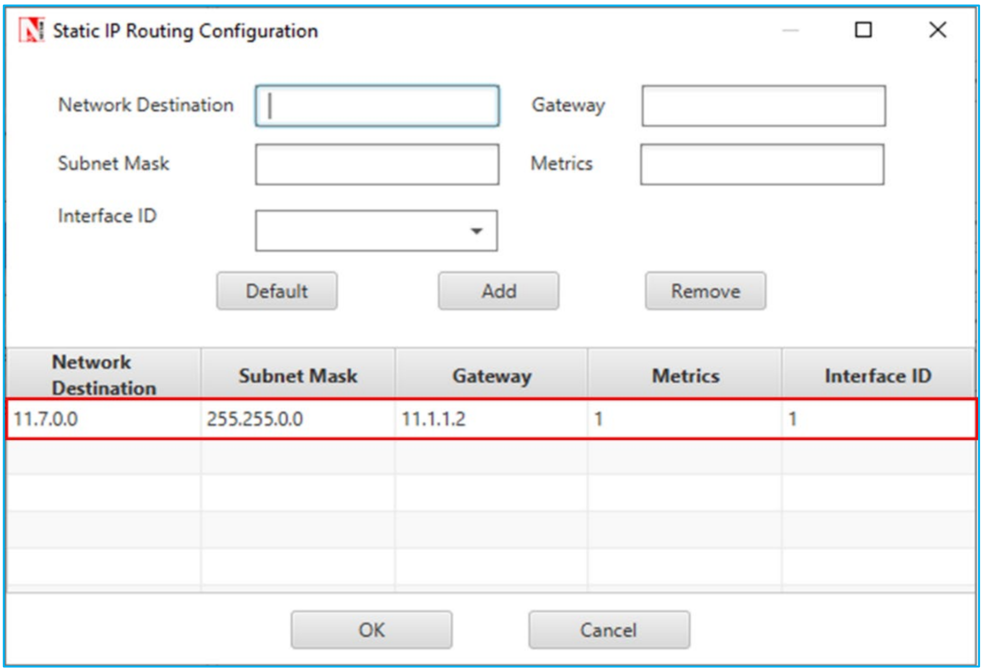
PACKET_ID	SEGMENT_ID	PACKET_TYPE	CONTROL_PACKET_TYP...	SOURCE_ID	DESTINATION_ID	TRANSMITTER_ID	RECEIVER_ID	APP_LAYER_ARRIVAL_T...	TRX_LAYER_ARRIVAL_T...	NW_LAYER_ARR
4	0	CBR	App1_CBR	NODE-6	NODE-7	NODE-6	ROUTER-1	60000.000	60000.000	60000.00
3	0	CBR	App1_CBR	NODE-6	NODE-7	ROUTER-4	NODE-7	40000.000	40000.000	40374.20
3	0	CBR	App1_CBR	NODE-6	NODE-7	ROUTER-5	ROUTER-4	40000.000	40000.000	40250.16
3	0	CBR	App1_CBR	NODE-6	NODE-7	ROUTER-1	ROUTER-5	40000.000	40000.000	40126.12
3	0	CBR	App1_CBR	NODE-6	NODE-7	NODE-6	ROUTER-1	40000.000	40000.000	40000.00

Figure 4-32: Animation Window packet flows from Wired Node 6→Router 1→Router 5→Router 4 → Wired Node 7

4.10.2 Sample 2: With Static Route

Static routing configuration

1. Open **Router 1** properties->Network_Layer. Click on **configure Static Route IP** and set the properties as per the screenshot below and click on Add and then click on OK.



Network Destination	Subnet Mask	Gateway	Metrics	Interface ID
11.7.0.0	255.255.0.0	11.1.1.2	1	1

Figure 4-33: Static IP Routing Dialogue window

This creates a text file for every router in the temp path of NetSim which is in the format below:

Router 1:

route ADD 11.7.0.0 MASK 255.255.0.0 11.1.1.2 METRIC 1 IF 1

route ADD destination_ip MASK subnet_mask gateway_ip METRIC metric_value IF Interface_Id

where

route ADD: command to add the static route.

destination_ip: is the Network address for the destination network.

MASK: is the Subnet mask for the destination network.

gateway_ip: is the IP address of the next-hop router/node.

METRIC: is the value used to choose between two routes.

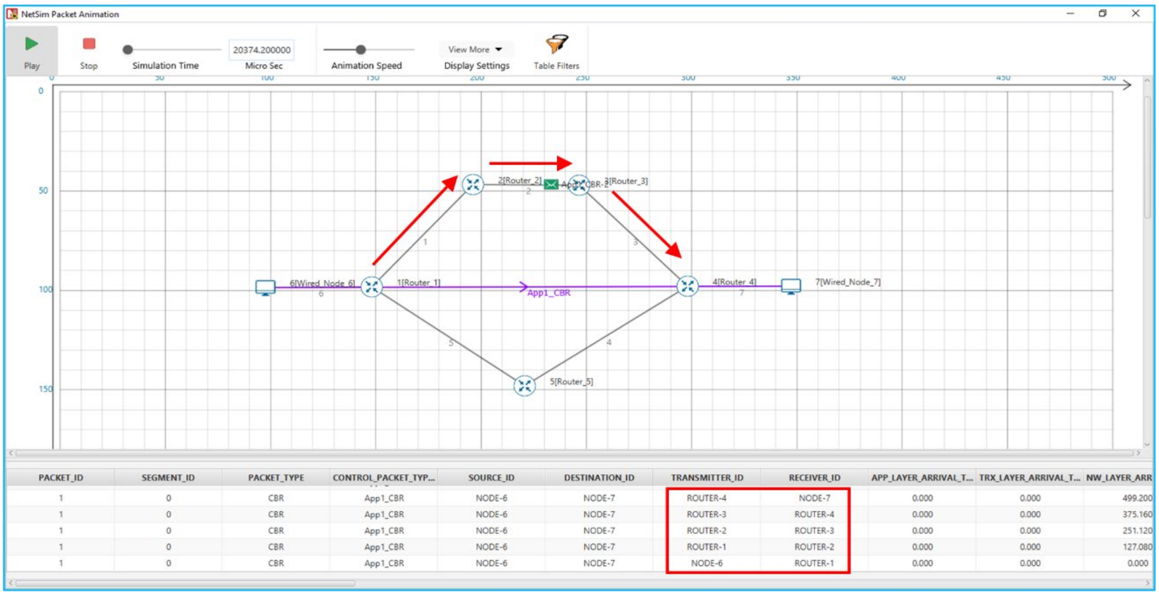
IF: is the Interface to which the gateway_ip is connected. The default value is 1.

1. Similarly Configure Static Route for all the routers as given in below **Table 4-15.**

Devices	Network Destination	Gateway	Subnet Mask	Metrics	Interface ID
Router 1	11.7.0.0	11.1.1.2	255.255.0.0	1	1
Router 2	11.7.0.0	11.2.1.2	255.255.0.0	1	2
Router 3	11.7.0.0	11.3.1.2	255.255.0.0	1	2
Router 4	11.7.0.0	11.7.1.2	255.255.0.0	1	3

Table 4-15: Static Route configuration for routers

2. After configuring the router properties.
3. Run the simulation for 10 seconds and check packet animation window.
4. Observe in Animation Window packet flows from Wired Node 6 -> Router 1-> Router 2-> Router 3-> Router 4-> Wired Node 7 as shown in below Figure 4-34 as shown in **Figure 4-34.**



PACKET_ID	SEGMENT_ID	PACKET_TYPE	CONTROL_PACKET_TYP...	SOURCE_ID	DESTINATION_ID	TRANSMITTER_ID	RECEIVER_ID	APP_LAYER_ARRIVAL_T...	TRX_LAYER_ARRIVAL_T...	NW_LAYER_ARR
1	0	CBR	App1_CBR	NODE-6	NODE-7	ROUTER-4	NODE-7	0.000	0.000	499.200
1	0	CBR	App1_CBR	NODE-6	NODE-7	ROUTER-3	ROUTER-4	0.000	0.000	375.160
1	0	CBR	App1_CBR	NODE-6	NODE-7	ROUTER-2	ROUTER-3	0.000	0.000	251.120
1	0	CBR	App1_CBR	NODE-6	NODE-7	ROUTER-1	ROUTER-2	0.000	0.000	127.080
1	0	CBR	App1_CBR	NODE-6	NODE-7	NODE-6	ROUTER-1	0.000	0.000	0.000

Figure 4-34: Observe in Animation Window packet flows from Wired Node 6→Router 1→Router 2→Router 3→Router 4→Wired Node 7

Disabling Static Routing

- If static routes were configured via GUI, it can be manually removed prior to the simulation from the Static IP Routing Dialogue or from the file input.
- If static routes were configured during the run time, the entries can be deleted using route delete command during runtime.

4.11 Different OSPF Control Packets

There are five distinct OSPF packet types.

Type	Description
1	Hello
2	Database Description
3	Link State Request
4	Link state Update
5	Link State Acknowledgement

Table 4-16: Different OSPF Control Packets

1. The Hello packet

Hello packets are OSPF packet type 1. These packets are sent periodically on all interfaces in order to establish and maintain neighbor relationships. In addition, Hello Packets are multicast on those physical networks having a multicast or broadcast capability, enabling dynamic discovery of neighboring routers. All routers connected to a common network must agree on certain parameters (Network mask, Hello Interval and Router Dead Interval). These parameters are included in Hello packets, so that differences can inhibit the forming of neighbor relationships.

2. The Database Description packet

Database Description packets are OSPF packet type 2. These packets are exchanged when an adjacency is being initialized. They describe the contents of the link-state database. Multiple packets may be used to describe the database. For this purpose a poll-response procedure is used. One of the routers is designated to be the master, the other the slave. The master sends Database Description packets (polls) which are acknowledged by Database Description packets sent by the slave (responses). The responses are linked to the polls via the packets DD sequence numbers.

3. The Link State Request packet

Link State Request packets are OSPF packet type 3. After exchanging Database Description packets with a neighboring router, a router may find that parts of its link-state database are out-of-date. The Link State Request packet is used to request the pieces of the neighbour's database that are more up-to-date. Multiple Link State Request packets may need to be used. A router that sends a Link State Request packet has in mind the precise instance of the database pieces it is requesting. Each instance is defined by its LS sequence number, LS checksum, and LS age, although these fields are not specified in the Link State Request Packet itself. The router may receive even more recent instances in response.

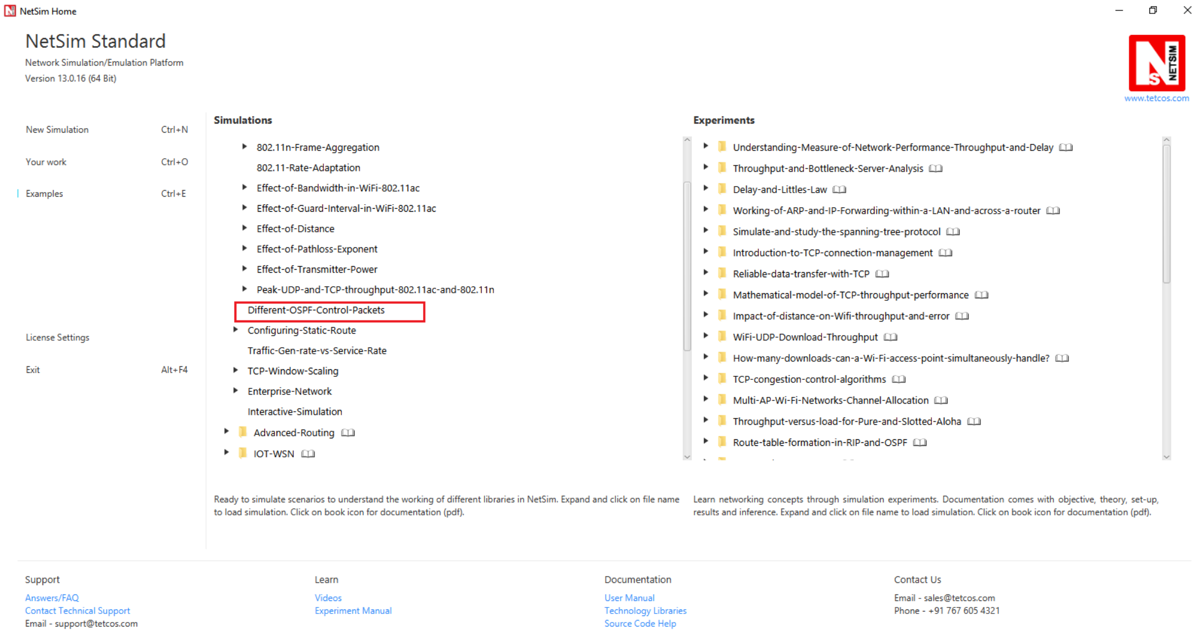
4. The Link State Update packet

Link State Update packets are OSPF packet type 4. These packets implement the flooding of LSAs. Each Link State Update packet carries a collection of LSAs one hop further from their origin. Several LSAs may be included in a single packet. Link State Update packets are multicast on those physical networks that support multicast/broadcast. In order to make the flooding procedure reliable, flooded LSAs are acknowledged in Link State Acknowledgment packets. If retransmission of certain LSAs is necessary, the retransmitted LSAs are always sent directly to the neighbor.

5. The Link State Acknowledgment packet

Link State Acknowledgment Packets are OSPF packet type 5. To make the flooding of LSAs reliable, flooded LSAs are explicitly acknowledged. This acknowledgment is accomplished through the sending and receiving of Link State Acknowledgment packets. Multiple LSAs can be acknowledged in a single Link State Acknowledgment packet.

Open NetSim, Select **Examples->Internetworks->Different-OSPF-Control-Packets** as shown



NetSim Home

NetSim Standard
Network Simulation/Emulation Platform
Version 13.0.16 (64 Bit)

www.tetcos.com

New Simulation	Ctrl+N
Your work	Ctrl+O
Examples	Ctrl+E
License Settings	
Exit	Alt+F4

Simulations

- 802.11n-Frame-Aggregation
- 802.11-Rate-Adaptation
- Effect-of-Bandwidth-in-WiFi-802.11ac
- Effect-of-Guard-Interval-in-WiFi-802.11ac
- Effect-of-Distance
- Effect-of-Pathloss-Exponent
- Effect-of-Transmitter-Power
- Peak-UDP-and-TCP-throughput-802.11ac-and-802.11n
- Different-OSPF-Control-Packets
- Configuring-Static-Route
- Traffic-Gen-rate-vs-Service-Rate
- TCP-Window-Scaling
- Enterprise-Network
- Interactive-Simulation
- Advanced-Routing
- IOT-WSN

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

- Understanding-Measure-of-Network-Performance-Throughput-and-Delay
- Throughput-and-Bottleneck-Server-Analysis
- Delay-and-Littles-Law
- Working-of-ARP-and-IP-Forwarding-within-a-LAN-and-across-a-router
- Simulate-and-study-the-spanning-tree-protocol
- Introduction-to-TCP-connection-management
- Reliable-data-transfer-with-TCP
- Mathematical-model-of-TCP-throughput-performance
- Impact-of-distance-on-Wifi-throughput-and-error
- WiFi-UDP-Download-Throughput
- How-many-downloads-can-a-Wi-Fi-access-point-simultaneously-handle?
- TCP-congestion-control-algorithms
- Multi-AP-Wi-Fi-Networks-Channel-Allocation
- Throughput-versus-load-for-Pure-and-Slotted-Aloha
- Route-table-formation-in-RIP-and-OSPF

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 4-35: Featured Example list

The following network diagram illustrates what the NetSim UI displays when you open the example configuration file for Different-OSPF-Control-Packets in NetSim as shown **Figure 4-36.**

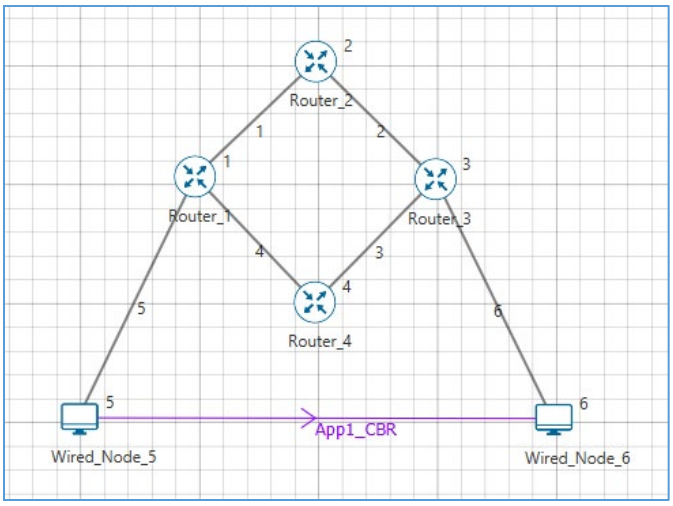


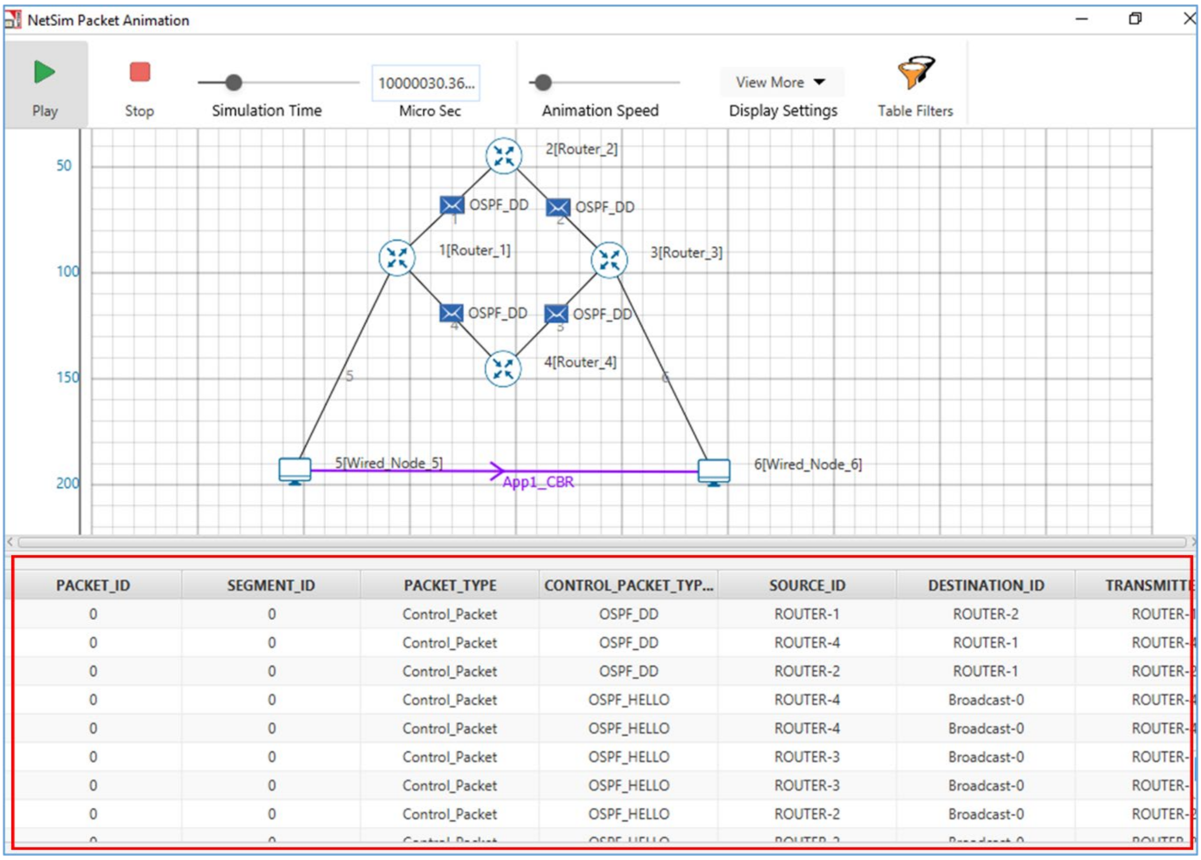
Figure 4-36: Network topology for Different OSPF Control Packets

Network Settings

1. Set OSPF Routing protocol under Application_Layer properties of a router
2. Configured CBR application with default properties
3. Enabled Packet Trace
4. Simulate for 100 sec.

Results and Discussion

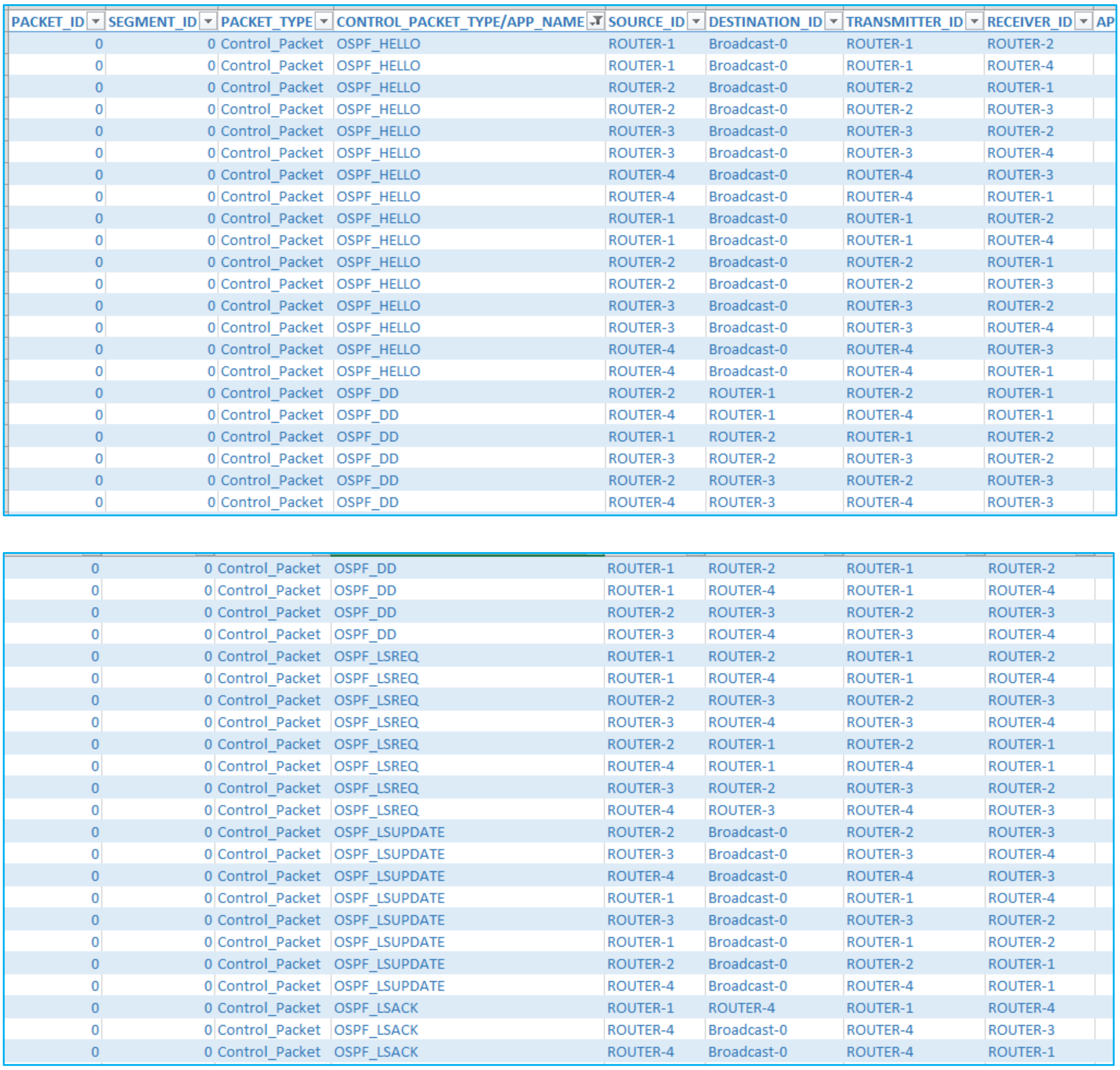
Open Packet animation window and click on play button. Users can observe all the OSPF packets. OSPF neighbors are dynamically discovered by sending Hello packets out each OSPF-enabled interface on a router. Then Database description packets are exchanged when an adjacency is being initialized. They describe the contents of the topological database. After exchanging Database Description packets with a neighboring router, a router may find that parts of its topological database are out of date. The Link State Request packet is used to request the pieces of the neighbor's database that are more up to date. The sending of Link State Request packets is the last step in bringing up an adjacency. A packet that contains fully detailed LSAs, typically sent in response to an LSR message. LSAck is sent to confirm receipt of an LSU message.



PACKET_ID	SEGMENT_ID	PACKET_TYPE	CONTROL_PACKET_TYP...	SOURCE_ID	DESTINATION_ID	TRANSMITTE
0	0	Control_Packet	OSPF_DD	ROUTER-1	ROUTER-2	ROUTER-1
0	0	Control_Packet	OSPF_DD	ROUTER-4	ROUTER-1	ROUTER-4
0	0	Control_Packet	OSPF_DD	ROUTER-2	ROUTER-1	ROUTER-2
0	0	Control_Packet	OSPF_HELLO	ROUTER-4	Broadcast-0	ROUTER-4
0	0	Control_Packet	OSPF_HELLO	ROUTER-4	Broadcast-0	ROUTER-4
0	0	Control_Packet	OSPF_HELLO	ROUTER-3	Broadcast-0	ROUTER-
0	0	Control_Packet	OSPF_HELLO	ROUTER-3	Broadcast-0	ROUTER-
0	0	Control_Packet	OSPF_HELLO	ROUTER-2	Broadcast-0	ROUTER-2
0	0	Control_Packet	OSPF_HELLO	ROUTER-2	Broadcast-0	ROUTER-

Figure 4-37: OSPF Control Packet in the animation window

The same can be observed in Packet trace by filtering CONTROL_PACKET_TYPE/ APP_NAME to OSPF_HELLO, OSPF_DD, OSPF_LSACK, OSPF_LSUPDATE and OSPF_LSREQ packets as shown below **Figure 4-38.**



PACKET_ID	SEGMENT_ID	PACKET_TYPE	CONTROL_PACKET_TYPE/APP_NAME	SOURCE_ID	DESTINATION_ID	TRANSMITTER_ID	RECEIVER_ID	AP
0	0	Control_Packet	OSPF_HELLO	ROUTER-1	Broadcast-0	ROUTER-1	ROUTER-2	
0	0	Control_Packet	OSPF_HELLO	ROUTER-1	Broadcast-0	ROUTER-1	ROUTER-4	
0	0	Control_Packet	OSPF_HELLO	ROUTER-2	Broadcast-0	ROUTER-2	ROUTER-1	
0	0	Control_Packet	OSPF_HELLO	ROUTER-2	Broadcast-0	ROUTER-2	ROUTER-3	
0	0	Control_Packet	OSPF_HELLO	ROUTER-3	Broadcast-0	ROUTER-3	ROUTER-2	
0	0	Control_Packet	OSPF_HELLO	ROUTER-3	Broadcast-0	ROUTER-3	ROUTER-4	
0	0	Control_Packet	OSPF_HELLO	ROUTER-4	Broadcast-0	ROUTER-4	ROUTER-3	
0	0	Control_Packet	OSPF_HELLO	ROUTER-4	Broadcast-0	ROUTER-4	ROUTER-1	
0	0	Control_Packet	OSPF_HELLO	ROUTER-1	Broadcast-0	ROUTER-1	ROUTER-2	
0	0	Control_Packet	OSPF_HELLO	ROUTER-1	Broadcast-0	ROUTER-1	ROUTER-4	
0	0	Control_Packet	OSPF_HELLO	ROUTER-2	Broadcast-0	ROUTER-2	ROUTER-1	
0	0	Control_Packet	OSPF_HELLO	ROUTER-2	Broadcast-0	ROUTER-2	ROUTER-3	
0	0	Control_Packet	OSPF_HELLO	ROUTER-3	Broadcast-0	ROUTER-3	ROUTER-2	
0	0	Control_Packet	OSPF_HELLO	ROUTER-3	Broadcast-0	ROUTER-3	ROUTER-4	
0	0	Control_Packet	OSPF_HELLO	ROUTER-4	Broadcast-0	ROUTER-4	ROUTER-3	
0	0	Control_Packet	OSPF_HELLO	ROUTER-4	Broadcast-0	ROUTER-4	ROUTER-1	
0	0	Control_Packet	OSPF_DD	ROUTER-2	ROUTER-1	ROUTER-2	ROUTER-1	
0	0	Control_Packet	OSPF_DD	ROUTER-4	ROUTER-1	ROUTER-4	ROUTER-1	
0	0	Control_Packet	OSPF_DD	ROUTER-1	ROUTER-2	ROUTER-1	ROUTER-2	
0	0	Control_Packet	OSPF_DD	ROUTER-3	ROUTER-2	ROUTER-3	ROUTER-2	
0	0	Control_Packet	OSPF_DD	ROUTER-2	ROUTER-3	ROUTER-2	ROUTER-3	
0	0	Control_Packet	OSPF_DD	ROUTER-4	ROUTER-3	ROUTER-4	ROUTER-3	
0	0	Control_Packet	OSPF_DD	ROUTER-1	ROUTER-2	ROUTER-1	ROUTER-2	
0	0	Control_Packet	OSPF_DD	ROUTER-1	ROUTER-4	ROUTER-1	ROUTER-4	
0	0	Control_Packet	OSPF_DD	ROUTER-2	ROUTER-3	ROUTER-2	ROUTER-3	
0	0	Control_Packet	OSPF_DD	ROUTER-3	ROUTER-4	ROUTER-3	ROUTER-4	
0	0	Control_Packet	OSPF_LSREQ	ROUTER-1	ROUTER-2	ROUTER-1	ROUTER-2	
0	0	Control_Packet	OSPF_LSREQ	ROUTER-1	ROUTER-4	ROUTER-1	ROUTER-4	
0	0	Control_Packet	OSPF_LSREQ	ROUTER-2	ROUTER-3	ROUTER-2	ROUTER-3	
0	0	Control_Packet	OSPF_LSREQ	ROUTER-3	ROUTER-4	ROUTER-3	ROUTER-4	
0	0	Control_Packet	OSPF_LSREQ	ROUTER-2	ROUTER-1	ROUTER-2	ROUTER-1	
0	0	Control_Packet	OSPF_LSREQ	ROUTER-4	ROUTER-1	ROUTER-4	ROUTER-1	
0	0	Control_Packet	OSPF_LSREQ	ROUTER-3	ROUTER-2	ROUTER-3	ROUTER-2	
0	0	Control_Packet	OSPF_LSREQ	ROUTER-4	ROUTER-3	ROUTER-4	ROUTER-3	
0	0	Control_Packet	OSPF_LSUPDATE	ROUTER-2	Broadcast-0	ROUTER-2	ROUTER-3	
0	0	Control_Packet	OSPF_LSUPDATE	ROUTER-3	Broadcast-0	ROUTER-3	ROUTER-4	
0	0	Control_Packet	OSPF_LSUPDATE	ROUTER-4	Broadcast-0	ROUTER-4	ROUTER-3	
0	0	Control_Packet	OSPF_LSUPDATE	ROUTER-1	Broadcast-0	ROUTER-1	ROUTER-4	
0	0	Control_Packet	OSPF_LSUPDATE	ROUTER-3	Broadcast-0	ROUTER-3	ROUTER-2	
0	0	Control_Packet	OSPF_LSUPDATE	ROUTER-1	Broadcast-0	ROUTER-1	ROUTER-2	
0	0	Control_Packet	OSPF_LSUPDATE	ROUTER-2	Broadcast-0	ROUTER-2	ROUTER-1	
0	0	Control_Packet	OSPF_LSUPDATE	ROUTER-4	Broadcast-0	ROUTER-4	ROUTER-1	
0	0	Control_Packet	OSPF_LSACK	ROUTER-1	ROUTER-4	ROUTER-1	ROUTER-4	
0	0	Control_Packet	OSPF_LSACK	ROUTER-4	Broadcast-0	ROUTER-4	ROUTER-3	
0	0	Control_Packet	OSPF_LSACK	ROUTER-4	Broadcast-0	ROUTER-4	ROUTER-1	

Figure 4-38: OSPF Control Packet in the packet Trace

4.12 Enterprise Network

Create a simple enterprise network, comprising of, two branches, head-quarters and a data center. Branches and headquarters are connected to the data center over the public cloud. In NetSim, users can model the network, by just adding the network elements, through click and drop, and renaming them suitably as shown below **Figure 4-39.**

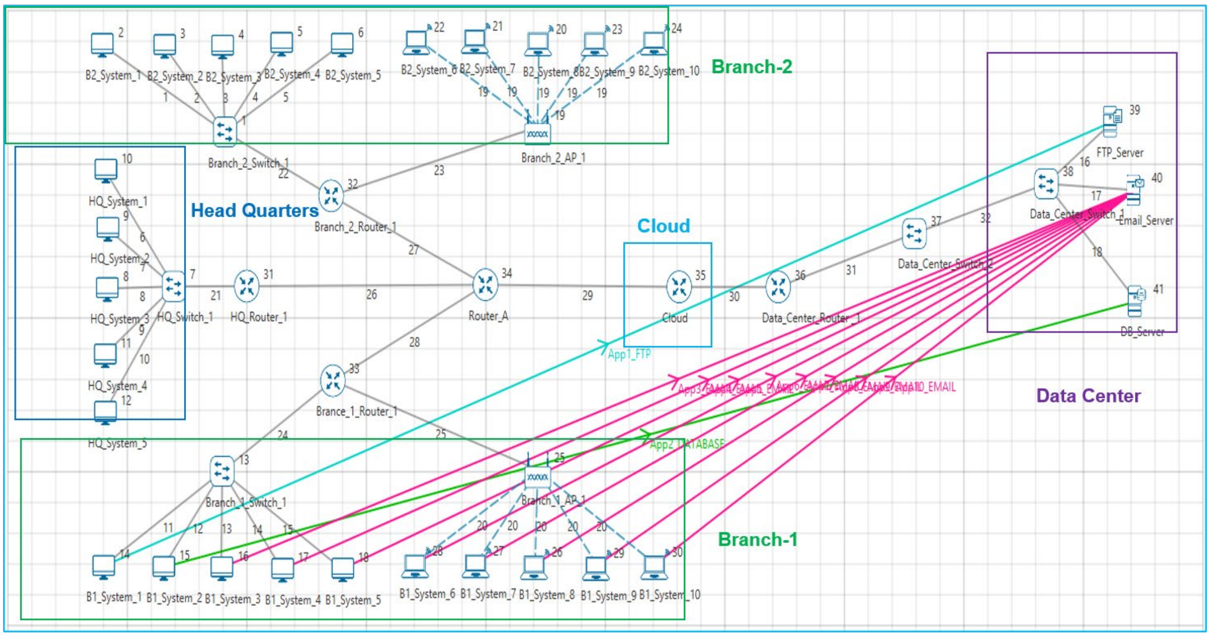


Figure 4-39: Enterprise Network - Sample 1

Network Settings

Sample1: Open NetSim, Select **Examples->Internetworks->Enterprise-Network ->Sample-1**

1. We have changed the link rate for the outbound link i.e. Link 28 from Branch 1 as 2Mbps.
2. Configured one FTP application from 14 to the file server 39, a Database application from 15 to the Database server 41, and eight email applications running between 16, 17, 18, 26, 27, 28, 29, 30 and the Email server 40.
3. Enabled Plots and Simulated for 100s .

Sample2: Open NetSim, Select **Examples->Internetworks->Enterprise-Network ->Sample-2**

1. In this sample, we have added more nodes via the switch and configured 3 FTP applications from systems 43, 45, 46 to FTP server 39 as shown in the below screenshot **Figure 4-40**.

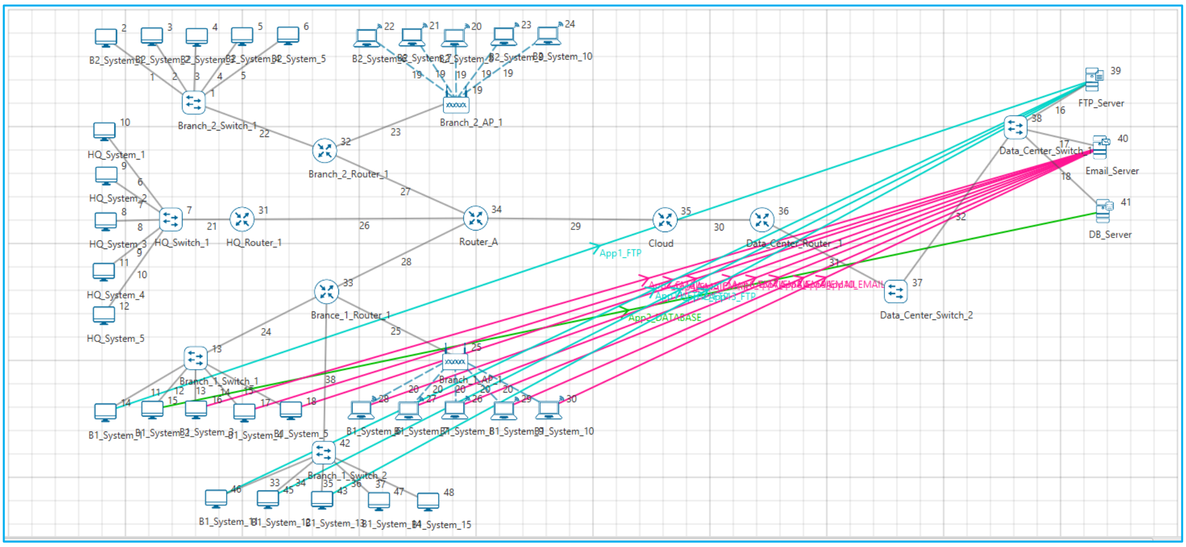


Figure 4-40: Enterprise Network - Sample 2

2. Simulated for 100 seconds.

Sample3: Open NetSim, Select **Examples->Internetworks->Enterprise-Network ->Sample-3**

1. In this sample, we have changed the outbound link speed i.e. Link 28 to 4Mbps and simulated for 100 seconds.

Sample4: Open NetSim, Select **Examples->Internetworks->Enterprise-Network ->Sample-4**

1. In this sample, we have changed the outbound link speed i.e. Link 28 to 2Mbps and configured Voice applications from 14, 15, 46, 45 and 43 to Head office 10 as shown in the below screenshot **Figure 4-41**.

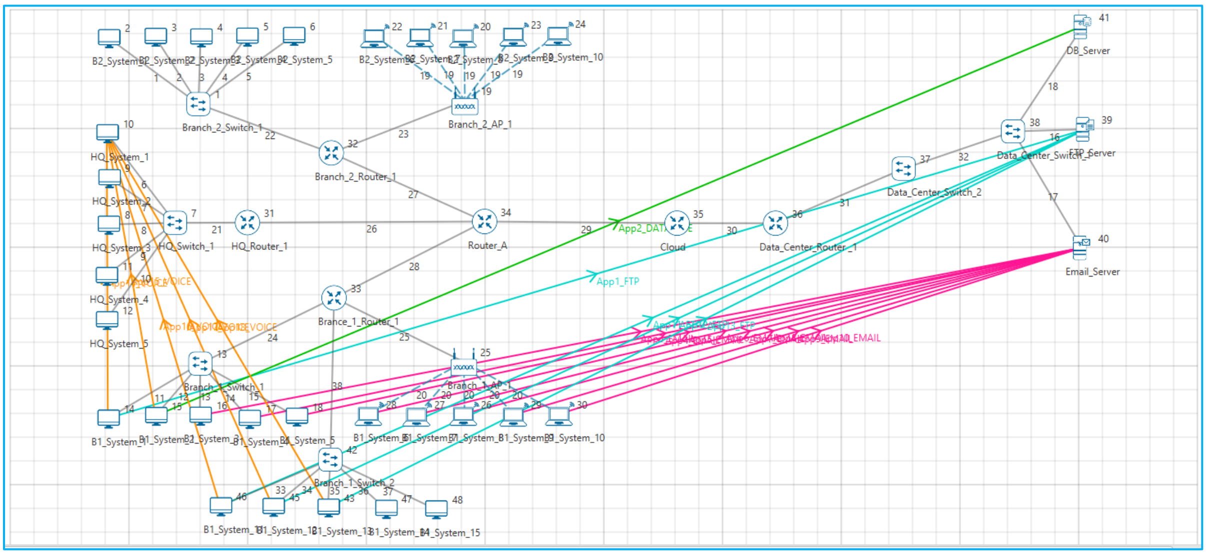
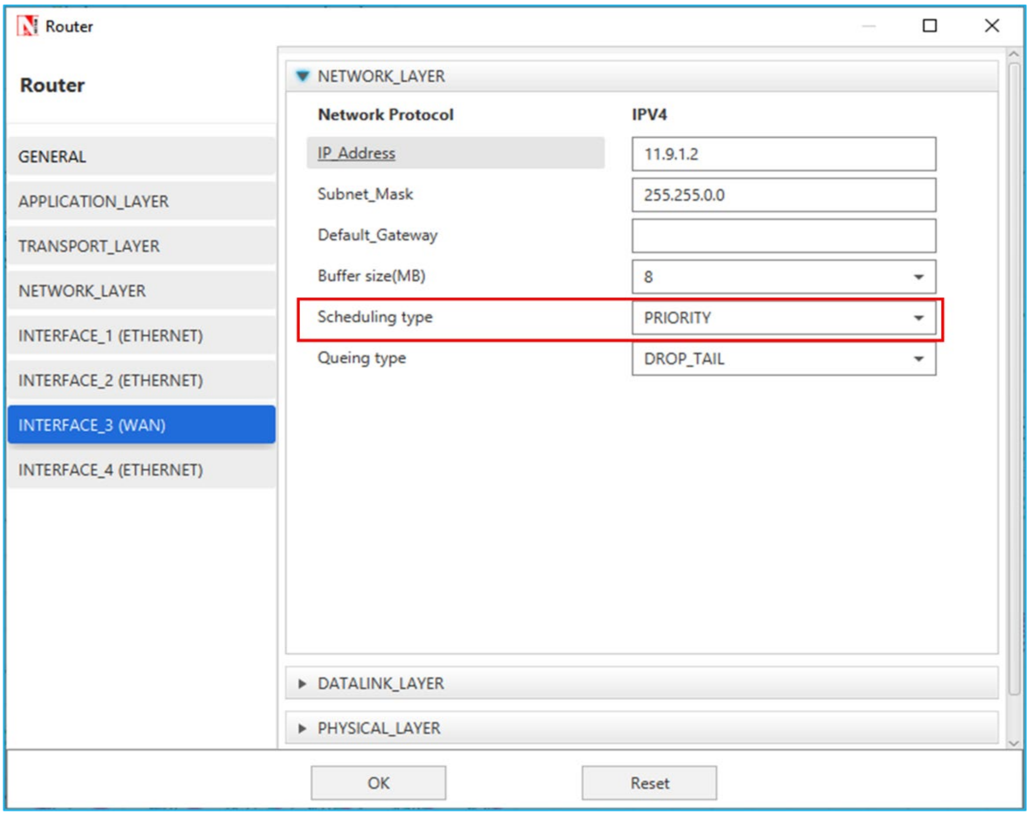


Figure 4-41: Enterprise Network - Sample 4

2. Also changed Scheduling type to Priority under Network Layer Properties of Router33 Interface_WAN properties as shown below **Figure 4-42.**



Network Protocol: IPV4
IP_Address: 11.9.1.2
Subnet_Mask: 255.255.0.0
Default_Gateway:
Buffer size(MB): 8
Scheduling type: PRIORITY
Queing type: DROP_TAIL

Figure 4-42: WAN Interface – Network layer properties window

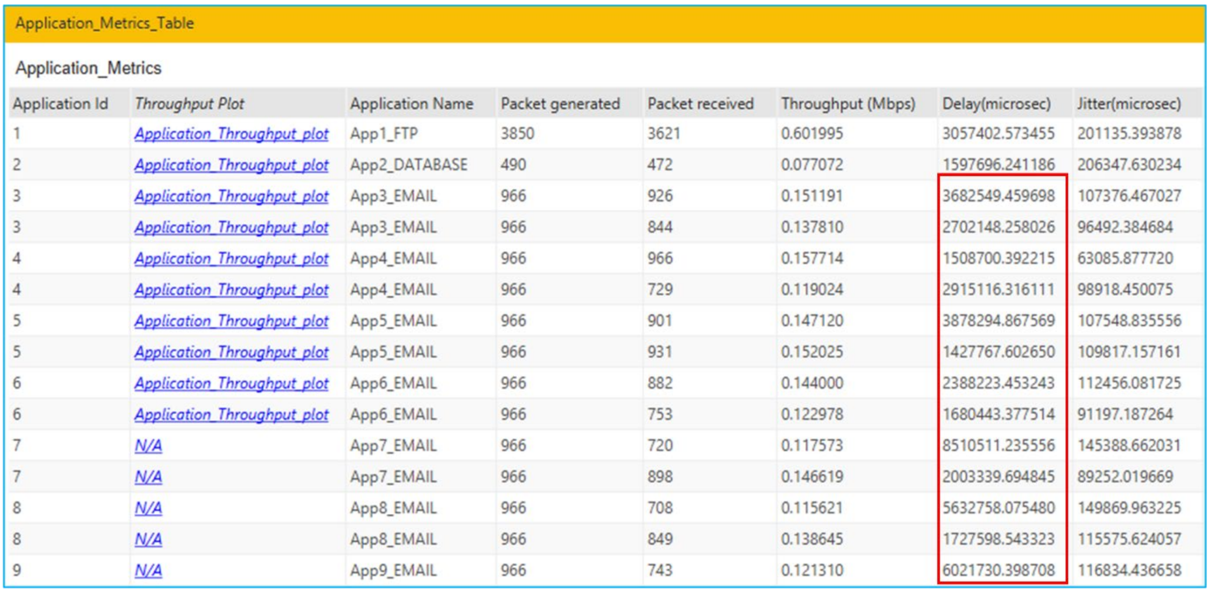
3. Simulated for 100 seconds.

Sample5: Open NetSim, Select **Examples->Internetworks->Enterprise-Network ->Sample-5**

1. In this sample, we have changed the start time for Voice and FTP applications to 40 seconds, email application to 30 seconds and database application to 40 seconds.
2. Enabled Plots and simulated for 100 seconds.

Results and Discussion

Sample1: Open metrics window and calculate the average delay for e-mail application present under Application properties shown below **Figure 4-43.**



Application_Metrics_Table

Application_Metrics

Application Id	Throughput Plot	Application Name	Packet generated	Packet received	Throughput (Mbps)	Delay(microsec)	Jitter(microsec)
1	Application_Throughput_plot	App1_FTP	3850	3621	0.601995	3057402.573455	201135.393878
2	Application_Throughput_plot	App2_DATABASE	490	472	0.077072	1597696.241186	206347.630234
3	Application_Throughput_plot	App3_EMAIL	966	926	0.151191	3682549.459698	107376.467027
3	Application_Throughput_plot	App3_EMAIL	966	844	0.137810	2702148.258026	96492.384684
4	Application_Throughput_plot	App4_EMAIL	966	966	0.157714	1508700.392215	63085.877720
4	Application_Throughput_plot	App4_EMAIL	966	729	0.119024	2915116.316111	98918.450075
5	Application_Throughput_plot	App5_EMAIL	966	901	0.147120	3878294.867569	107548.835556
5	Application_Throughput_plot	App5_EMAIL	966	931	0.152025	1427767.602650	109817.157161
6	Application_Throughput_plot	App6_EMAIL	966	882	0.144000	2388223.453243	112456.081725
6	Application_Throughput_plot	App6_EMAIL	966	753	0.122978	1680443.377514	91197.187264
7	N/A	App7_EMAIL	966	720	0.117573	8510511.235556	145388.662031
7	N/A	App7_EMAIL	966	898	0.146619	2003339.694845	89252.019669
8	N/A	App8_EMAIL	966	708	0.115621	5632758.075480	149869.963225
8	N/A	App8_EMAIL	966	849	0.138645	1727598.543323	115575.624057
9	N/A	App9_EMAIL	966	743	0.121310	6021730.398708	116834.436658

Figure 4-43: Application metrics table for sample 1

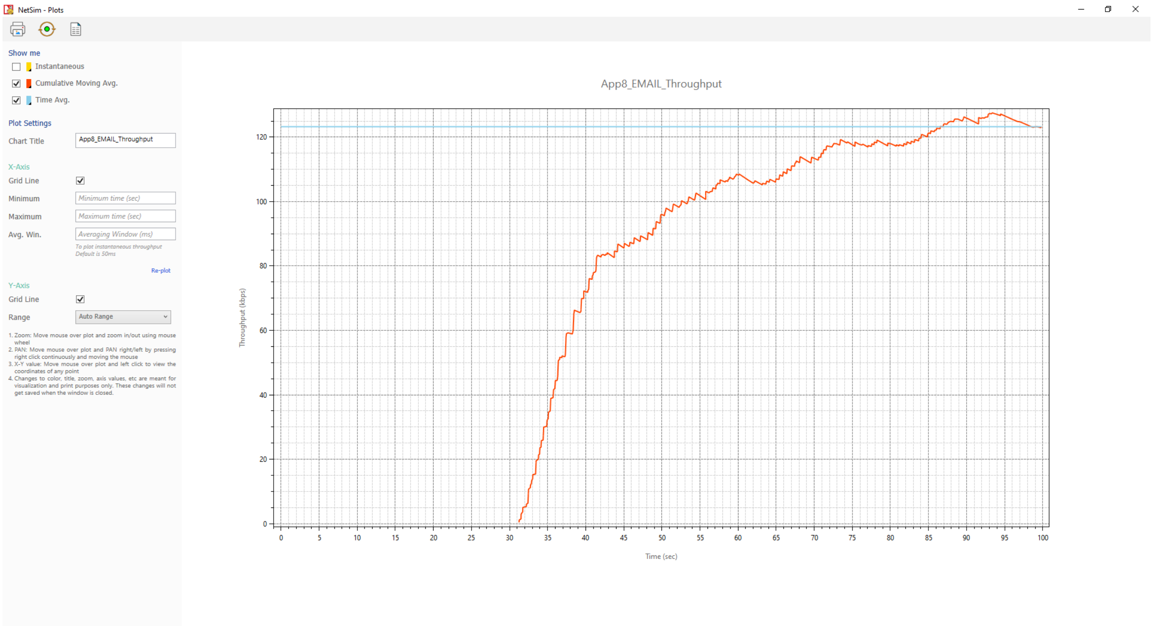
The delay experienced by the e-mail applications would be **3.48 seconds**

Sample 2: In this Sample, the average delay for email applications has increased to **14.36 seconds** due to the impact of additional load on the network.

Sample 3: In this Sample, the average delay for e-mail applications has dropped down to **2.11 seconds** due to the increased link speed.

Sample 4: In this Sample, the average delay for the e-mail application has increased to **5.11 seconds** since voice has a higher priority over data, and the routers will first serve the voice packets in its queue and only then route the data packets.

Sample 5: In this Sample, users can notice that email application sees good throughput initially after which it is flat. On the other hand, the voice application throughput is 0 till 40 seconds, since it has no traffic, and starts picking up 40 seconds onwards. Note that these are moving average graphs and not instantaneous value plots.



Show me

- ☐ Instantaneous
- ☑ Cumulative Moving Avg.
- ☑ Time Avg.

Plot Settings

Chart Title: App8_EMAIL_Throughput

X-Axis

Grid Line ☑

Minimum: Minimum time (sec)

Maximum: Maximum time (sec)

Avg. Win.: Averaging Window (ms)

To plot instantaneous throughput Default is 50ms

Re-plot

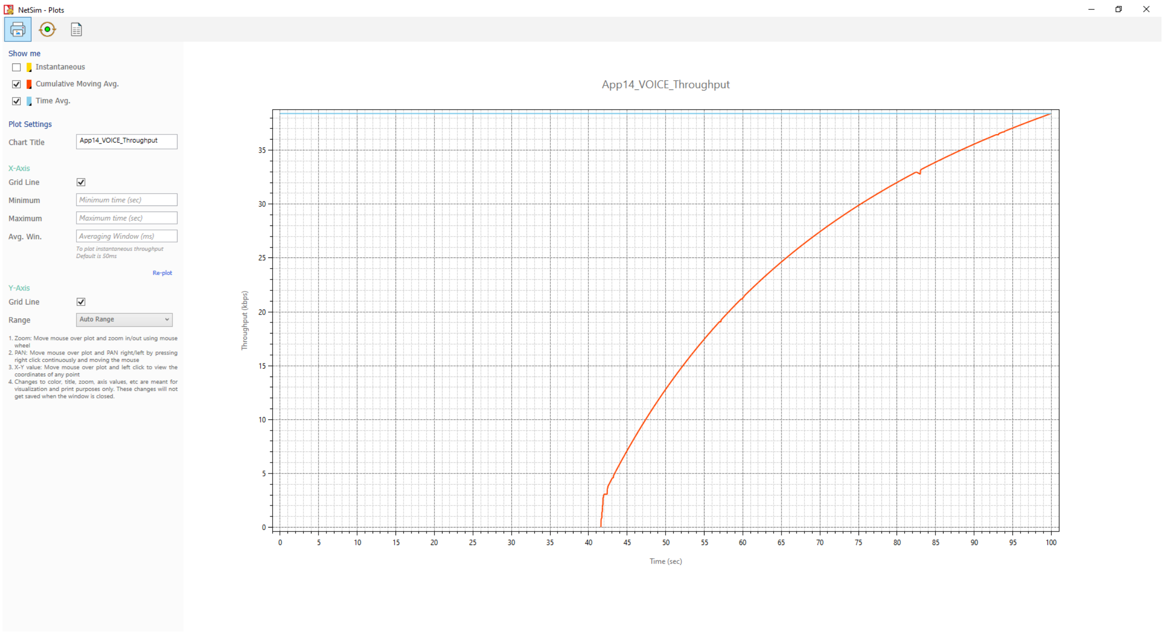
Y-Axis

Grid Line ☑

Range: Auto Range

1. Zoom: Move mouse over plot and zoom in/out using mouse wheel
2. PAN: Move mouse over plot and PAN right/left by pressing right click continuously and moving the mouse
3. X-Y value: Move mouse over plot and left click to view the coordinates of any point
4. Changes to color, title, zoom, axis values, etc are meant for visualization and print purposes only. These changes will not get saved when the window is closed.

Figure 4-44: EMAIL Throughput Plot for Application 8



Show me

- ☐ Instantaneous
- ☑ Cumulative Moving Avg.
- ☑ Time Avg.

Plot Settings

Chart Title: App14_VOICE_Throughput

X-Axis

Grid Line ☑

Minimum: Minimum time (sec)

Maximum: Maximum time (sec)

Avg. Win.: Averaging Window (ms)

To plot instantaneous throughput Default is 50ms

Re-plot

Y-Axis

Grid Line ☑

Range: Auto Range

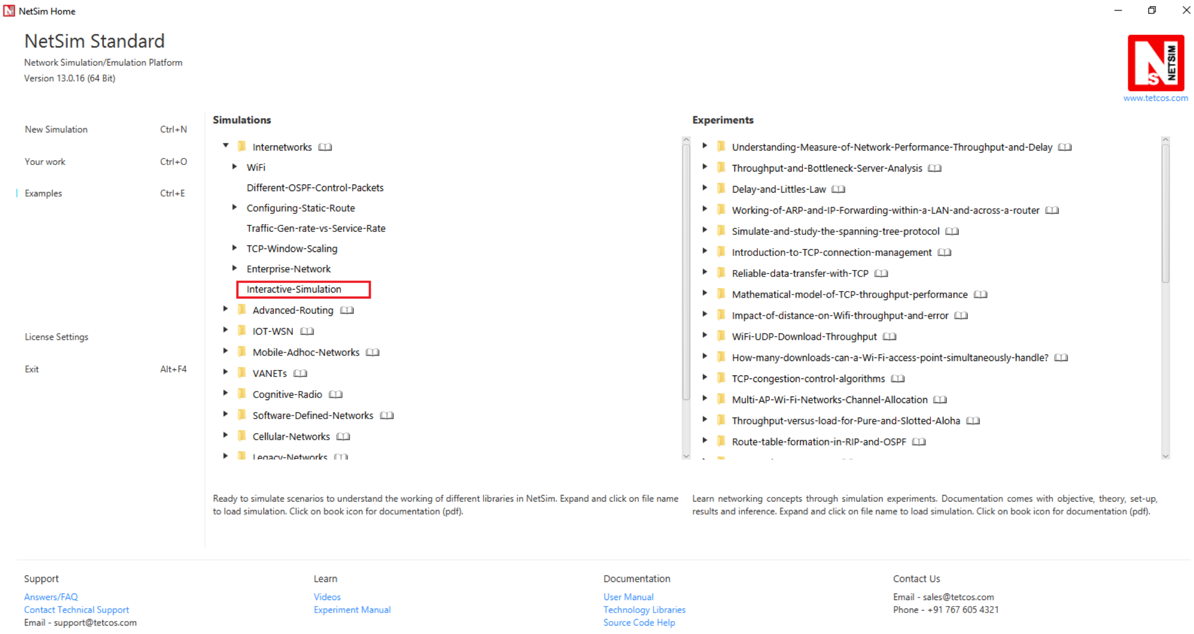
1. Zoom: Move mouse over plot and zoom in/out using mouse wheel
2. PAN: Move mouse over plot and PAN right/left by pressing right click continuously and moving the mouse
3. X-Y value: Move mouse over plot and left click to view the coordinates of any point
4. Changes to color, title, zoom, axis values, etc are meant for visualization and print purposes only. These changes will not get saved when the window is closed.

Figure 4-45: VOICE Throughput Plot for Application 14

4.13 NetSim Interactive Simulation

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.

Working: This section will demonstrate how to perform Interactive simulation for a simple network scenario. Open NetSim and click **Examples > Simulations > Internetworks > Interactive-Simulation** as shown below **Figure 4-46.**



NetSim Home

NetSim Standard

Network Simulation/Emulation Platform

Version 13.0.16 (64 Bit)

www.tetcos.com

New Simulation	Ctrl+N
Your work	Ctrl+O
Examples	Ctrl+E
License Settings	
Exit	Alt+F4

Simulations

- Internetworks
  - WiFi
  - Different-OSPF-Control-Packets
  - Configuring-Static-Route
  - Traffic-Gen-rate-vs-Service-Rate
  - TCP-Window-Scaling
  - Enterprise-Network
  - Interactive-Simulation
- Advanced-Routing
- IOT-WSN
- Mobile-Adhoc-Networks
- VANETs
- Cognitive-Radio
- Software-Defined-Networks
- Cellular-Networks
- Legacy-Networks

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

- Understanding-Measure-of-Network-Performance-Throughput-and-Delay
- Throughput-and-Bottleneck-Server-Analysis
- Delay-and-Littles-Law
- Working-of-ARP-and-IP-Forwarding-within-a-LAN-and-across-a-router
- Simulate-and-study-the-spanning-tree-protocol
- Introduction-to-TCP-connection-management
- Reliable-data-transfer-with-TCP
- Mathematical-model-of-TCP-throughput-performance
- Impact-of-distance-on-Wifi-throughput-and-error
- WiFi-UDP-Download-Throughput
- How-many-downloads-can-a-Wi-Fi-access-point-simultaneously-handle?
- TCP-congestion-control-algorithms
- Multi-AP-Wi-Fi-Networks-Channel-Allocation
- Throughput-versus-load-for-Pure-and-Slotted-Aloha
- Route-table-formation-in-RIP-and-OSPF

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 4-46: Featured Example list

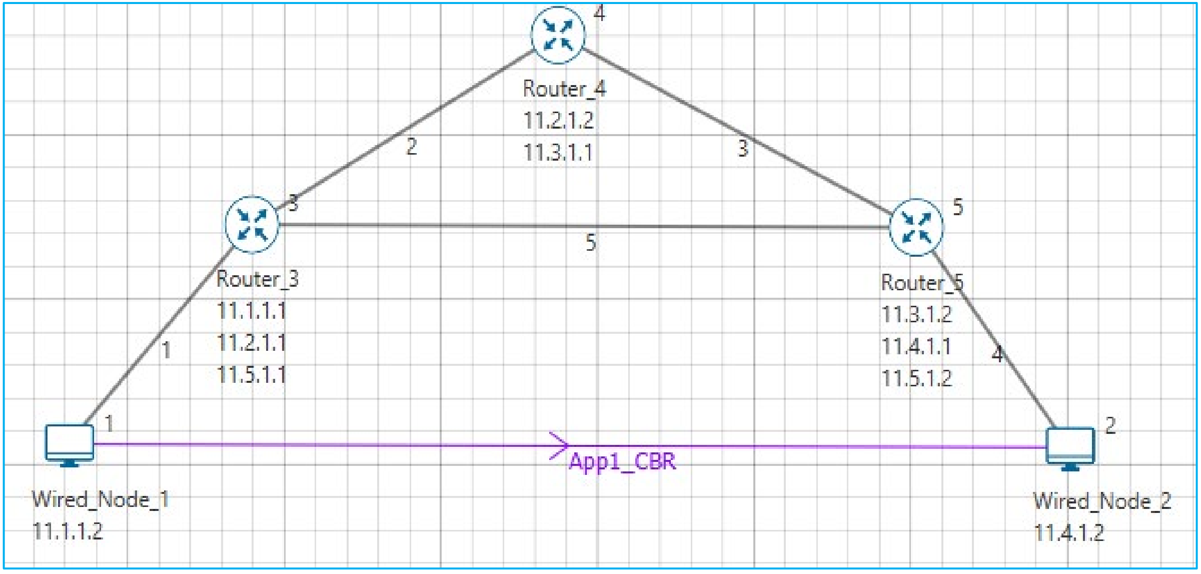
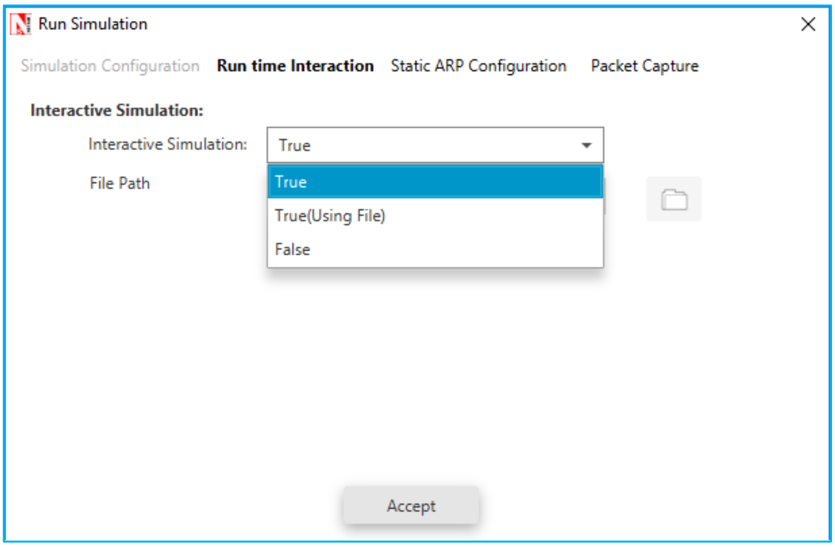


Figure 4-47: Interactive Simulation topology

- Click on Application icon present in the top ribbon and set the Application type as CBR. The Source_Id is 1 and Destination_Id is 2.
- Set Start Time as 30 Sec
- Enable Packet trace. In NetSim GUI Plots are Enabled.
- Enable Wireshark in Wired_Node_1
- Click on run simulation option and In the Run time Interaction tab set Interactive Simulation as True and click on Accept as shown **Figure 4-48.**



Interactive Simulation:

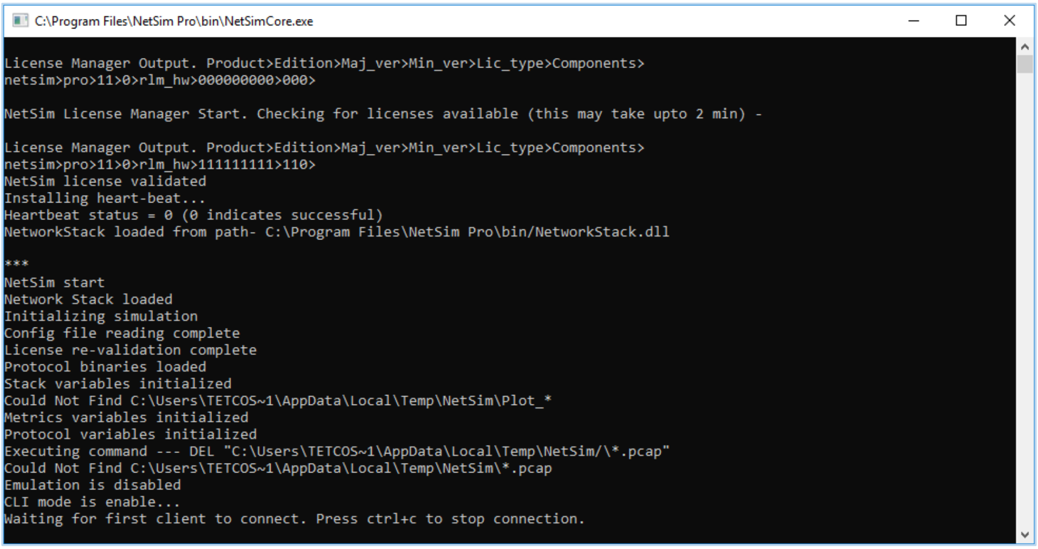
Interactive Simulation: True

File Path

True
True(Using File)
False

Figure 4-48: Run time Interaction window

- In NetSim GUI Plots are Enabled. Click on run simulation and set Simulation Time as 500 sec. (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 Simulation ends) and click OK
- Simulation (NetSimCore.exe) will start running and will display a message "waiting for first client to connect" as shown below **Figure 4-49.**



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

```
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 4-49: Waiting for first client to connect a console

- After the Simulation window opened go to Network scenario and right click on Router_3 or any other node and select NetSim Console option as shown **Figure 4-50.**

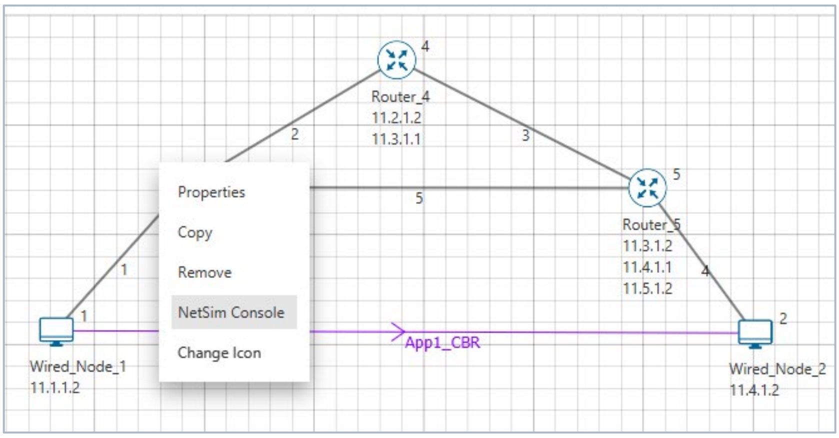
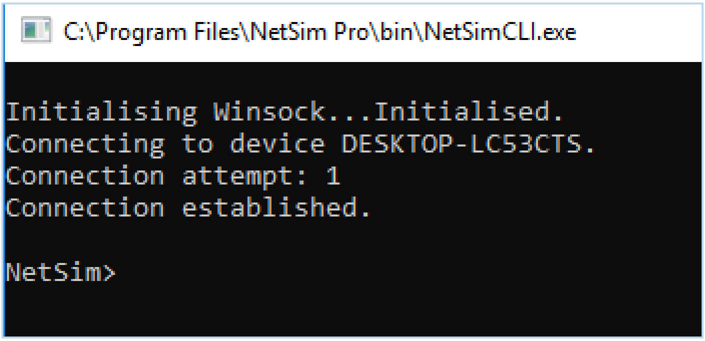


Figure 4-50: NetSim Console option

- Now Client (NetSimCLI.exe) will start running and it will try to establish connection with NetSimCore.exe. After connection is established the window will look similar like this shown below **Figure 4-51.**



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

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

NetSim>
```

Figure 4-51: Connection established

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

<u>Note: Commands are not a case sensitive</u>

1. Simulation specific (Not applicable for file based interactive simulation)

1. Pause
2. PauseAt
3. Continue
4. Stop
5. Exit
6. Reconnect

Pause: To pause the currently running simulation

PauseAt: To pause the currently running simulation with respect to particular time (Ex: To Pause simulation at 70.2 sec use command as **PauseAt 70.2**)

Continue: To start the currently paused simulation

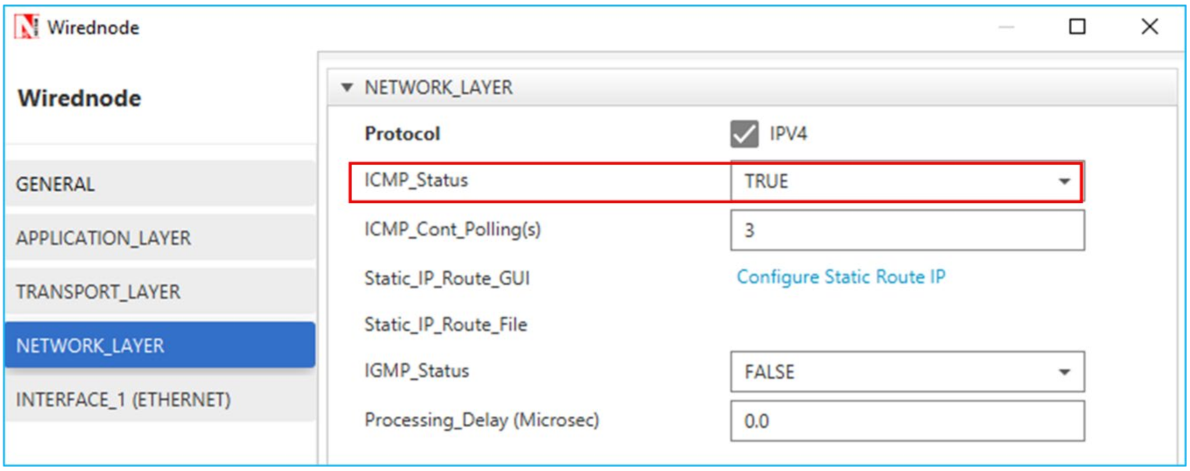
Stop: To stop the currently running simulation (NetSimCore.exe)

Exit: To exit from the client (NetSimCLI.exe)

Reconnect: To reconnect client (NetSimCLI.exe) to simulation (NetSimCore.exe) when we rerun simulation again

2. 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 Network, if you don’t then the device is faulty, disconnected, switched off, incorrectly configured
- You can use the ***ping*** command with an IP address or Device name
- **ICMP_Status** should be set as True in all nodes(Wired_Node and Router)



Protocol ☑ IPV4

ICMP_Status TRUE

ICMP_Cont_Polling(s) 3

Static_IP_Route_GUI

Static_IP_Route_File

IGMP_Status FALSE

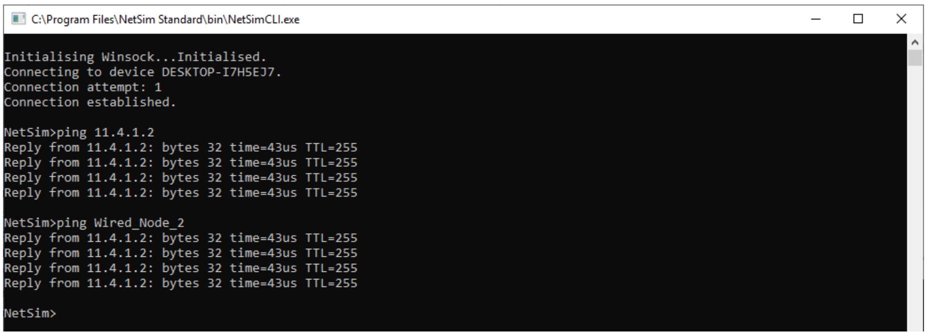
Processing_Delay (Microsec) 0.0

Figure 4-52: Network Layer window for wired node

- Right click on Wired_Node_1 and go to properties. Under General properties enable Wireshark Capture option as “Online”

```
Ping <IP address> e.g. ping 11.4.1.2
Ping <Node Name> e.g. ping Wired_Node_2
```

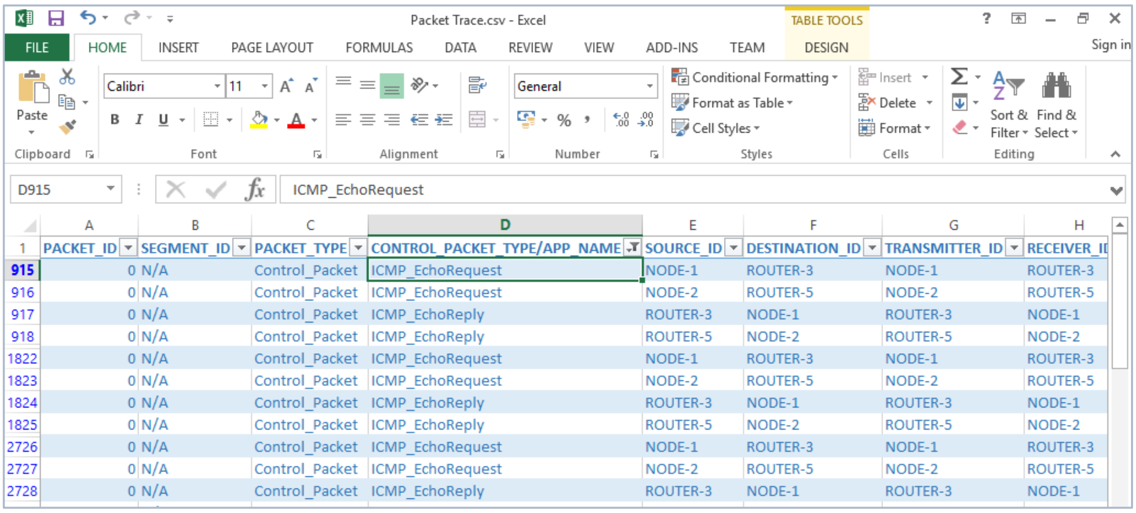
Ping Command Results



```
Initialising Winsock...Initialised.
Connecting to device DESKTOP-I7H5EJ7.
Connection attempt: 1
Connection established.

NetSim>ping 11.4.1.2
Reply from 11.4.1.2: bytes 32 time=43us TTL=255
Reply from 11.4.1.2: bytes 32 time=43us TTL=255
Reply from 11.4.1.2: bytes 32 time=43us TTL=255
Reply from 11.4.1.2: bytes 32 time=43us TTL=255

NetSim>ping Wired_Node_2
Reply from 11.4.1.2: bytes 32 time=43us TTL=255
Reply from 11.4.1.2: bytes 32 time=43us TTL=255
Reply from 11.4.1.2: bytes 32 time=43us TTL=255
Reply from 11.4.1.2: bytes 32 time=43us TTL=255

NetSim>
```

Figure 4-53: Pinging to Wired_Node_2

- After simulation open packet trace and filter ICMP_EchoRequest and ICMP_EchoReply from CONTROL_PACKET_TYPE/APP_NAME column

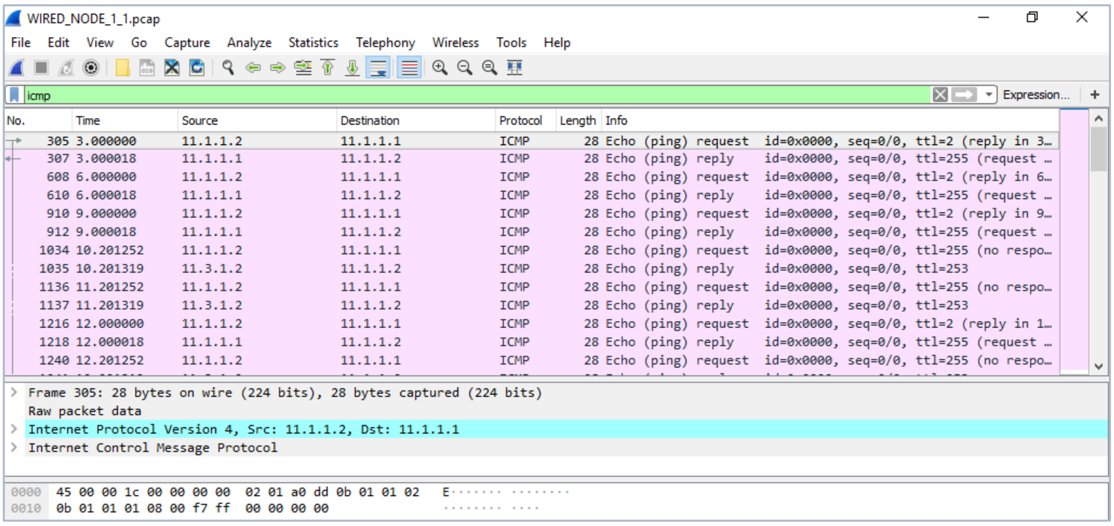


D915 | ICMP_EchoRequest

	A	B	C	D	E	F	G	H
1	PACKET_ID	SEGMENT_ID	PACKET_TYPE	CONTROL_PACKET_TYPE/APP_NAME	SOURCE_ID	DESTINATION_ID	TRANSMITTER_ID	RECEIVER_I
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 4-54: Packet Trace - ICMP Control Packets

- Open Wireshark and apply filter ICMP. we can see the ping request and reply packets in Wireshark as shown **Figure 4-55.**



Filter: icmp

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               ········ ····
```

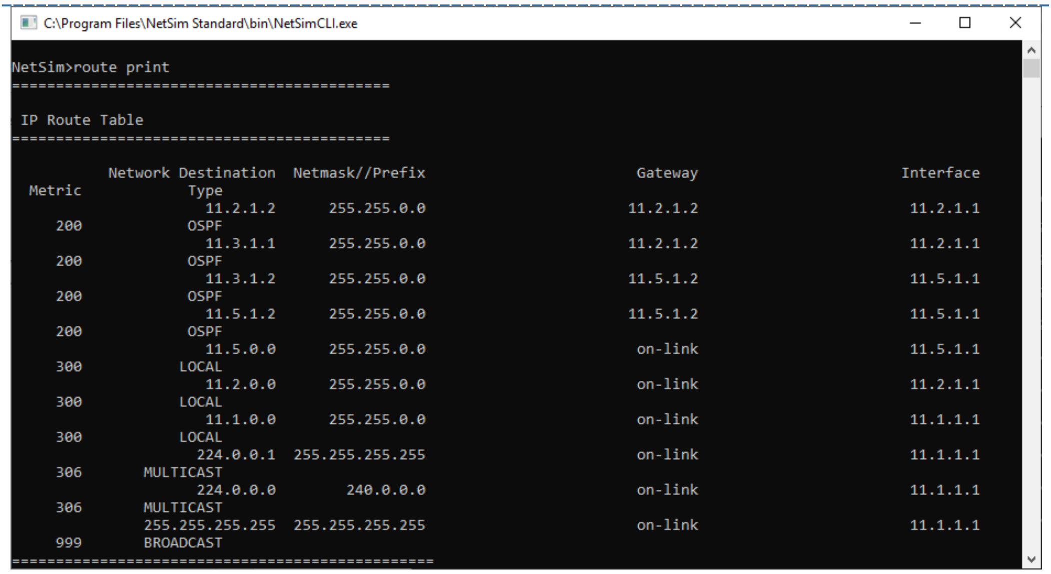
Figure 4-55: ICMP Control packets in Wireshark

3. Route Commands

1. route print
2. route delete
3. route add

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

```
route print
```



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

```
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
================================================
```

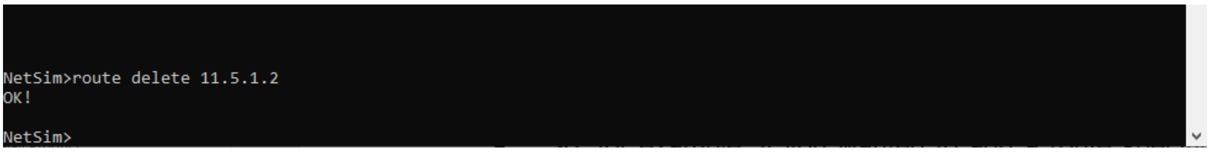
Figure 4-56: Network Route Print

- You will 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 will be dynamically generated
- In order to delete route in the IP routing table you will type a command using the following syntax

```
route delete destination_network
```

- So, to delete the route with destination network 11.5.0.0, all we'd have to do is type this command

```
route delete 11.5.1.2
```



```
NetSim>route delete 11.5.1.2
OK!

NetSim>
```

Figure 4-57: Network Route Delete

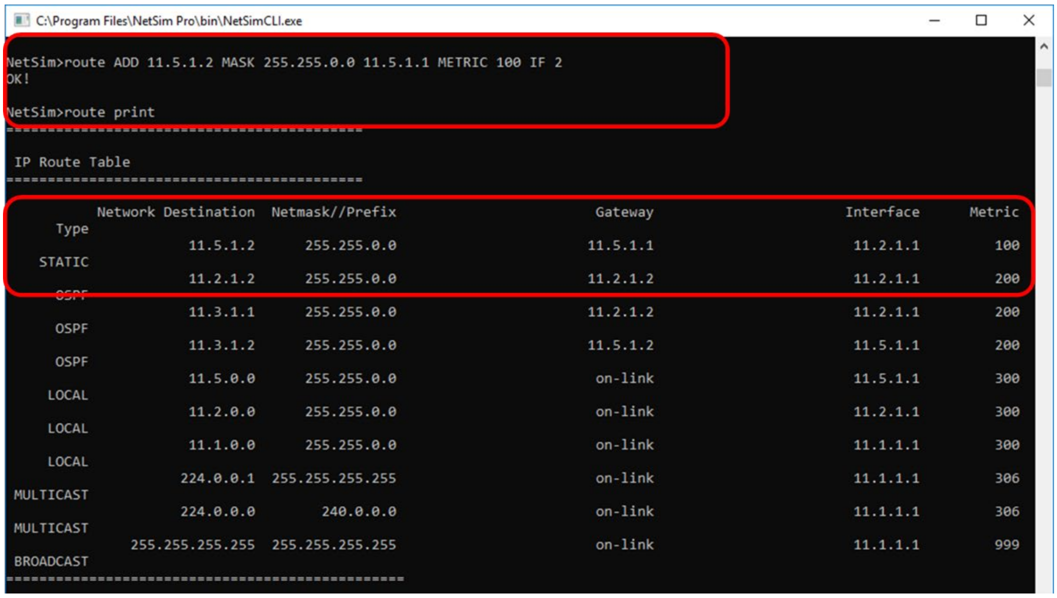
- To check whether route has been deleted or not check again using **route print** command
- To add a static route to the table, you will type a command using the following syntax

```
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 would see your new static route



```
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 4-58: Route added into Network

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.

3. ACL Configuration

Routers provide basic traffic filtering capabilities, such as blocking 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.

Commands to configure ACL

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

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

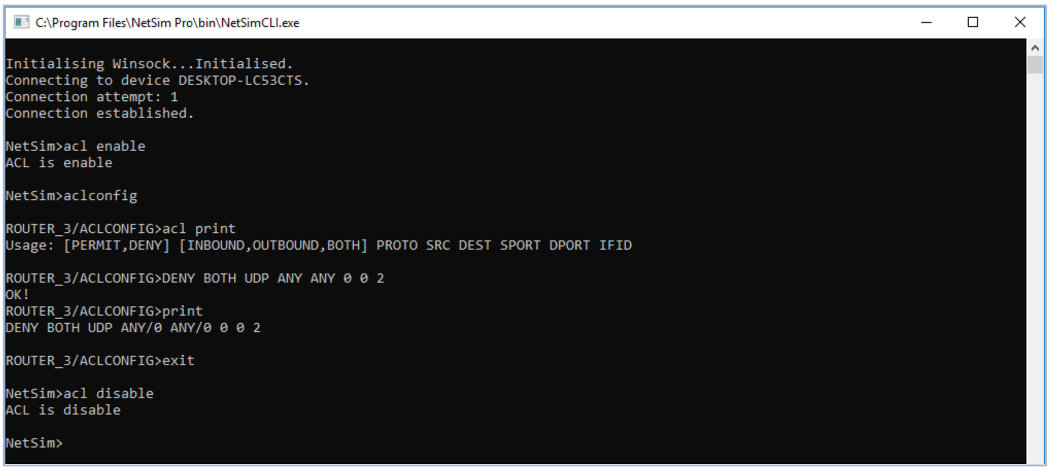
```
[PERMIT, DENY] [INBOUND, OUTBOUND, BOTH] PROTO SRC DEST SPORT DPORT IFID
```

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 the Router_3
- Click on the Application icon present in the top ribbon/toolbar and set Transport Protocol to UDP
- In NetSim GUI Plots are Enabled. Click on run simulation option and In the Run time Interaction tab set Interactive Simulation as True and click on Accept
- Set the Simulation Time as 500 sec or more. Click Ok
- Right click on Router_3 and select NetSim Console. Use the command as follows:

```
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
ROUTER_3/ACLCONFIG>exit
NetSim>acl disable
ACL is disable
NetSim>
```

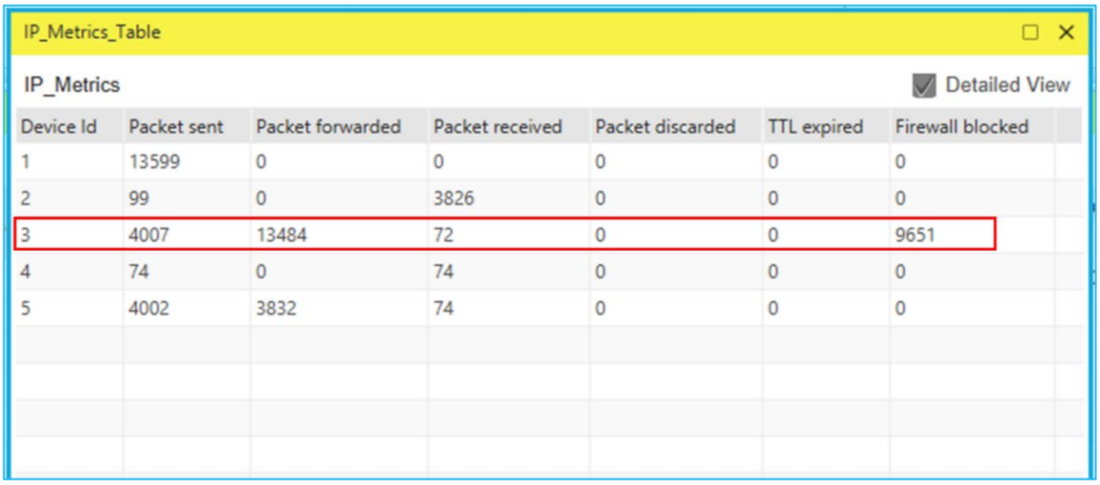


```
Initialising Winsock...Initialised.
Connecting to device DESKTOP-LC53CTS.
Connection attempt: 1
Connection established.

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>print
DENY BOTH UDP ANY/0 ANY/0 0 0 2

ROUTER_3/ACLCONFIG>exit

NetSim>acl disable
ACL is disable

NetSim>
```

Figure 4-59: ACL Configuration command

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 no of packets blocked by firewall has been shown below **Figure 4-60.**

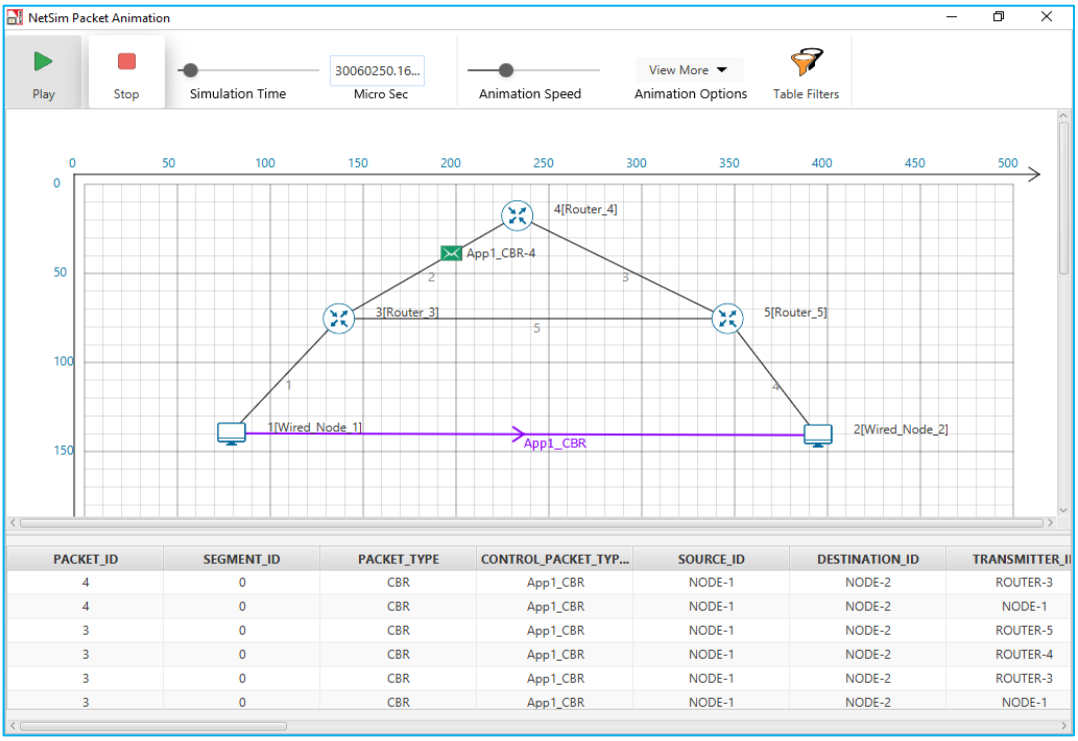
Note: Results will vary based on time of ACL command are executed



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 4-60: IP Metrics Table in result window

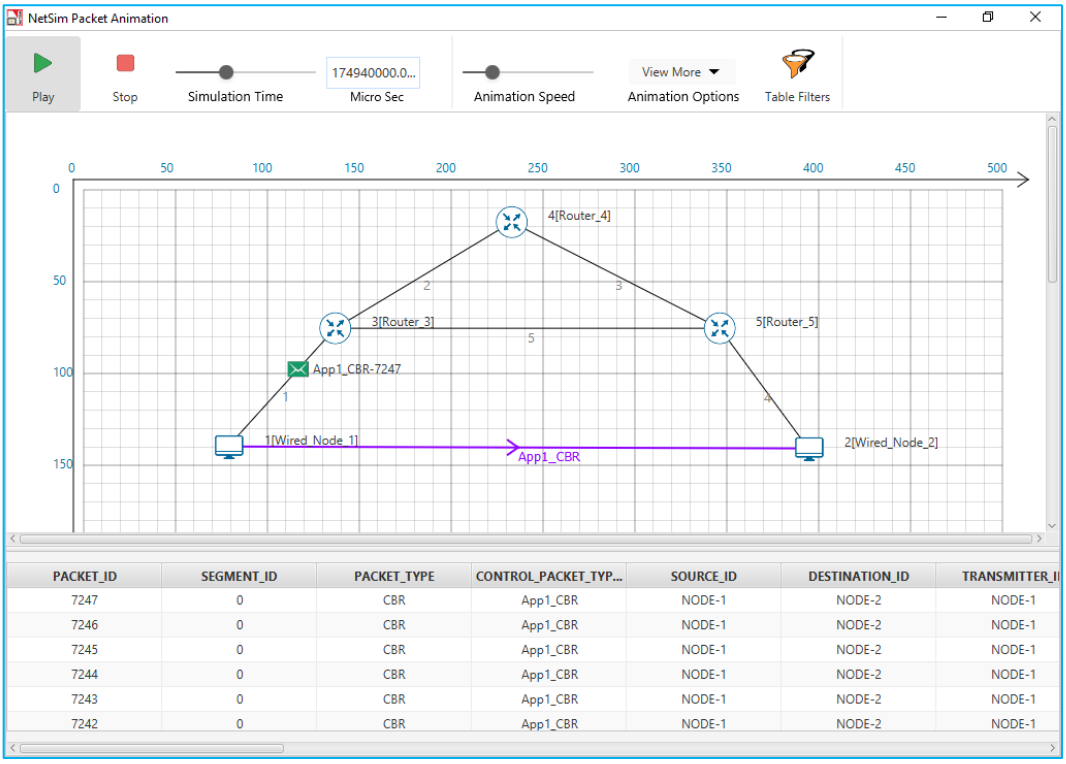
- Check Packet animation window whether packets has been blocked in Router_3 or not after entering ACL command to deny UDP traffic.
- Before applying ACL rule there is packet flow from Wired_Node_1 to Wired_Node_2.



PACKET_ID	SEGMENT_ID	PACKET_TYPE	CONTROL_PACKET_TYP...	SOURCE_ID	DESTINATION_ID	TRANSMITTER_I
4	0	CBR	App1_CBR	NODE-1	NODE-2	ROUTER-3
4	0	CBR	App1_CBR	NODE-1	NODE-2	NODE-1
3	0	CBR	App1_CBR	NODE-1	NODE-2	ROUTER-5
3	0	CBR	App1_CBR	NODE-1	NODE-2	ROUTER-4
3	0	CBR	App1_CBR	NODE-1	NODE-2	ROUTER-3
3	0	CBR	App1_CBR	NODE-1	NODE-2	NODE-1

Figure 4-61: In Animation Window before applying ACL rules see the packet flow

- After applying ACL rule Packet flows up to Router_3 only.

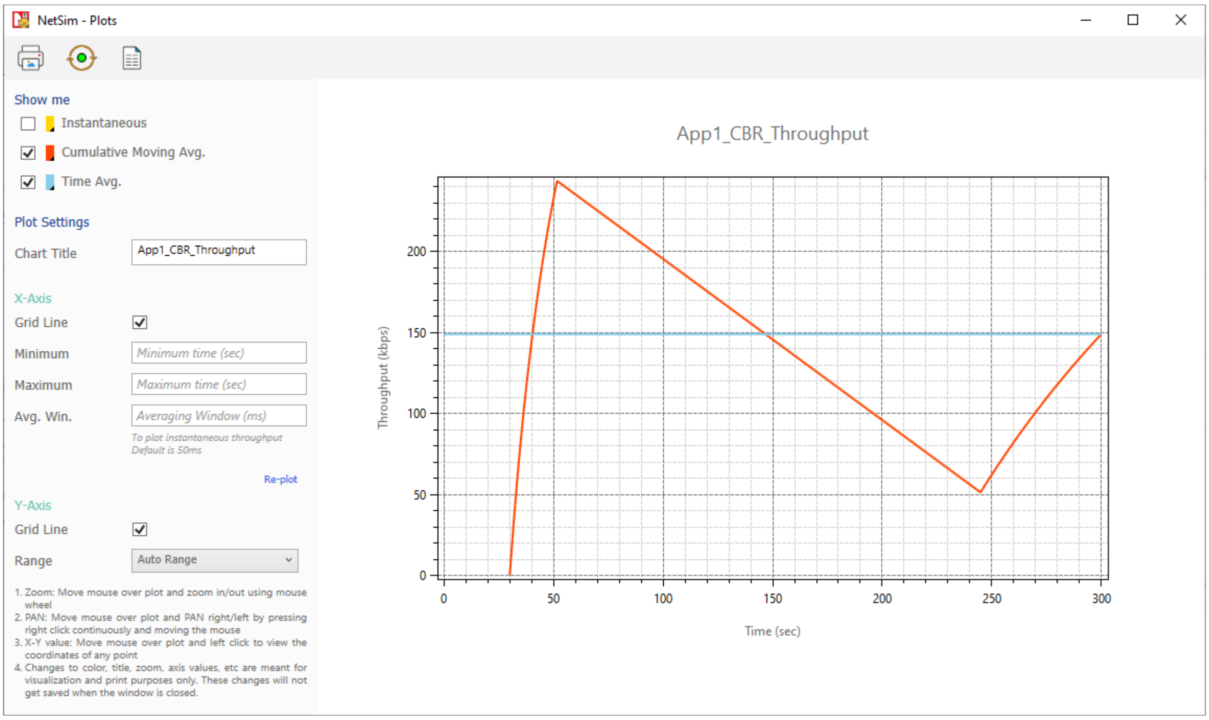


PACKET_ID	SEGMENT_ID	PACKET_TYPE	CONTROL_PACKET_TYP...	SOURCE_ID	DESTINATION_ID	TRANSMITTER_I
7247	0	CBR	App1_CBR	NODE-1	NODE-2	NODE-1
7246	0	CBR	App1_CBR	NODE-1	NODE-2	NODE-1
7245	0	CBR	App1_CBR	NODE-1	NODE-2	NODE-1
7244	0	CBR	App1_CBR	NODE-1	NODE-2	NODE-1
7243	0	CBR	App1_CBR	NODE-1	NODE-2	NODE-1
7242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

Figure 4-62: In Animation Window after applying ACL rules see the packet flow

The impact of ACL rule applied over the simulation traffic can be observed in the Application throughput plot. Throughput graph will show a drop after ACL is set. If ACL is disabled after a while, application packets will start flowing across the router. The Application throughput plot will show a drop and increase(Moving througput graph) in throughput after setting ACL and disabling ACL respectively.

Following is an example: ACL rule applied at around 50sec user can see the drop in throughput in the graph, since router blocks UDP packets in the plot. Once ACL has been disabled at around 240sec router permits packets and hence throughput can be observed in the plot shown below **Figure 4-63.**



Show me

☐ 🟨 Instantaneous

☑ 🟥 Cumulative Moving Avg.

☑ 🟦 Time Avg.

Plot Settings

Chart Title: App1_CBR_Throughput

X-Axis

Grid Line ☑

Minimum: Minimum time (sec)

Maximum: Maximum time (sec)

Avg. Win.: Averaging Window (ms)

To plot instantaneous throughput
Default is 50ms

Re-plot

Y-Axis

Grid Line ☑

Range: Auto Range

1. Zoom: Move mouse over plot and zoom in/out using mouse wheel
2. PAN: Move mouse over plot and PAN right/left by pressing right click continuously and moving the mouse
3. X-Y value: Move mouse over plot and left click to view the coordinates of any point
4. Changes to color, title, zoom, axis values, etc are meant for visualization and print purposes only. These changes will not get saved when the window is closed.

Figure 4-63: Application throughput plot

5 Reference Documents

1. IEEE 802.3 standard for Ethernet
2. IEEE 802.11 standards for Wireless LAN
3. RFCs 777, 760, 792 for Internet Control Message Protocol
4. IENs 108, 128 for Internet Control Message Protocol
5. RFC 2328 for Open Shortest Path First (OSPF)

6 Latest FAQs

Up to date FAQs on NetSim’s Internetworks library is available at

https://tetcos.freshdesk.com/support/solutions/folders/14000108665

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

https://tetcos.freshdesk.com/support/solutions/folders/14000119396