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 of 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 / p 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).

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.

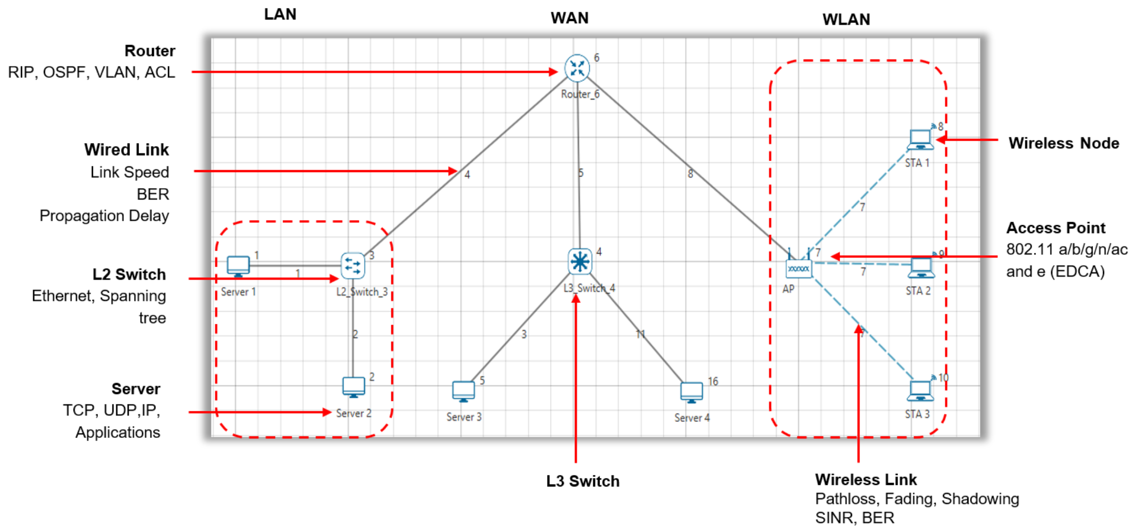


Figure 1-1: A typical Internetworks scenario in NetSim

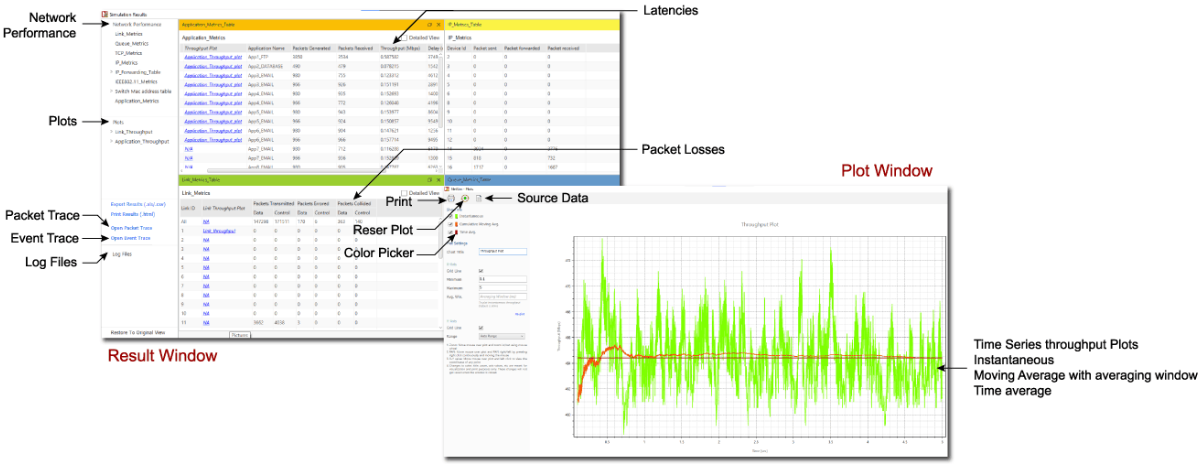
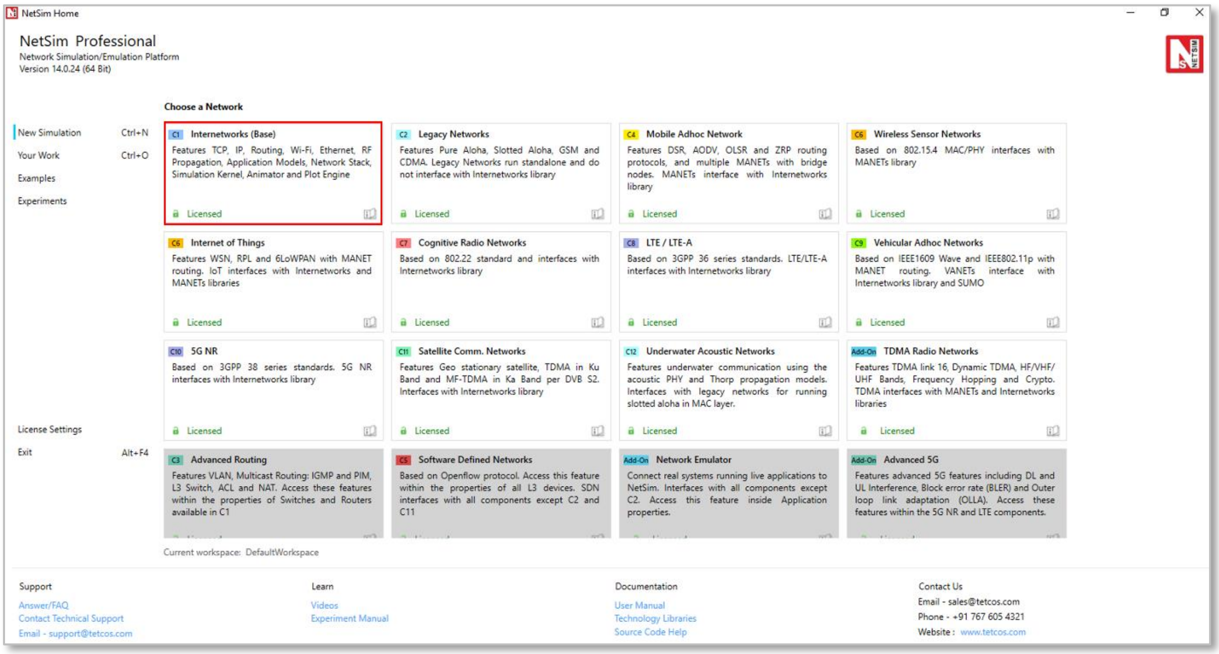


Figure 1-2: The Result dashboard and the Plots window shown in NetSim after completion of a simulation.

2 Simulation GUI

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



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 Network
Features DSR, AODV, OLSR and ZRP routing protocols, and multiple MANETs with bridge nodes. MANETs interface with Internetworks library

C6 Wireless Sensor Networks
Based on 802.15.4 MAC/PHY interfaces with MANETs library

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

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

C12 Underwater Acoustic Networks
Features underwater communication using the acoustic PHY and Thorp propagation models. Interfaces with legacy networks for running slotted aloha in MAC layer.

Add-On TDMA Radio Networks
Features TDMA link 16, Dynamic TDMA, HF/VHF/UHF Bands, Frequency Hopping and Crypto. TDMA interfaces with MANETs and Internetworks libraries

C3 Advanced Routing
Features VLAN, Multicast Routing: IGMP and PIM, L3 Switch, ACL and NAT. Access these features within the properties of Switches and Routers available in C1

C5 Software Defined Networks
Based on Openflow protocol. Access this feature within the properties of all L3 devices. SDN interfaces with all components except C2 and C11

Add-On Network Emulator
Connect real systems running live applications to NetSim. Interfaces with all components except C2. Access this feature inside Application properties.

Add-On Advanced 5G
Features advanced 5G features including DL and UL Interference, Block error rate (BLER) and Outer loop link adaptation (OLLA). Access these features within the 5G NR and LTE components.

Current workspace: DefaultWorkspace

Support
Answer/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
Website : www.tetcos.com

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.

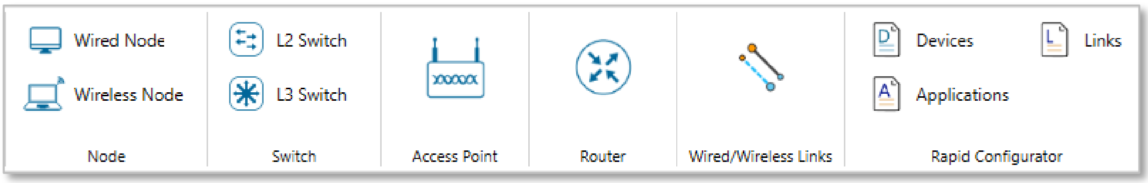


Figure 2-2: Internetworks Device Palette in GUI

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.

  Note: Wireless nodes can be effortlessly connected using the auto-connect feature, ensuring that users first drop the access point before adding the wireless node.
- **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:

  i. Click on the Set Traffic tab in the top ribbon/toolbar.

  ii. Select any application from the list and configure the traffic between source and destination.

  iii. Specify other application parameters per your model.

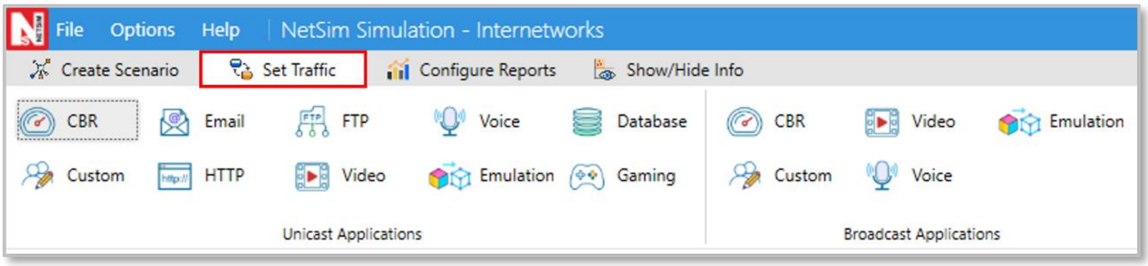


Figure 2-3: Top Ribbon/Toolbar

- Repeat (ii) to generate multiple applications. 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.

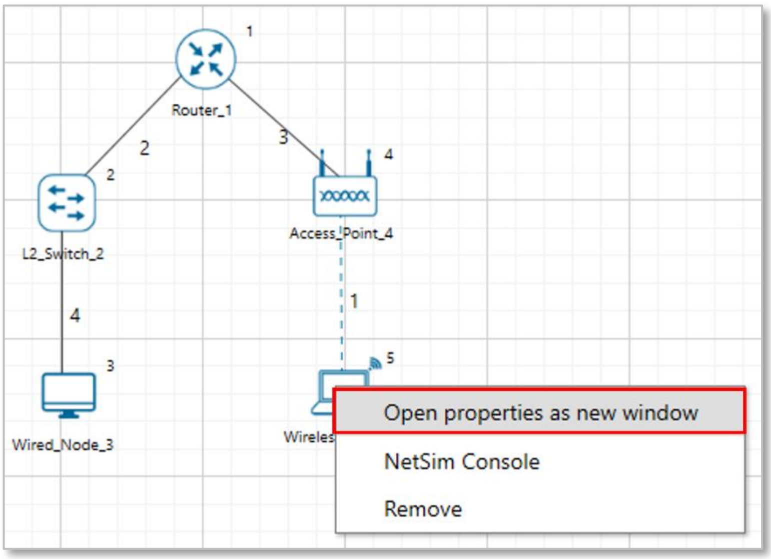
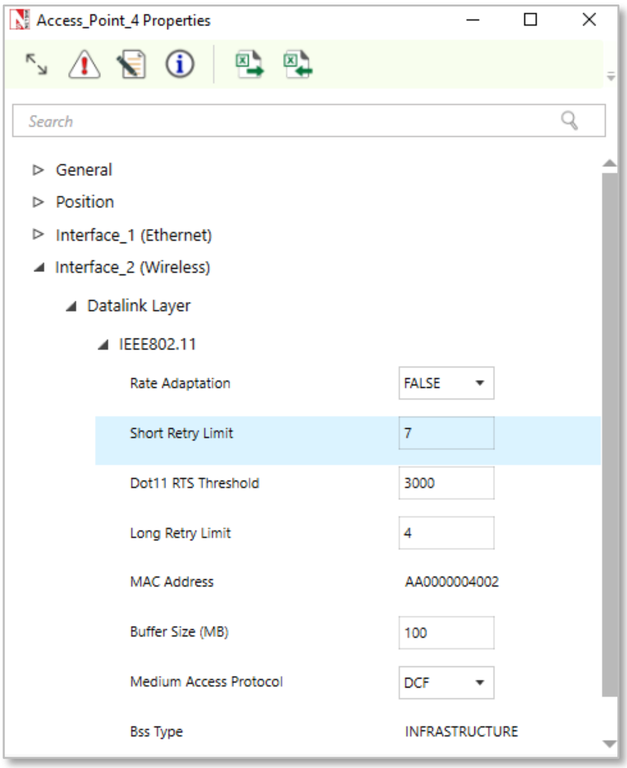


Figure 2-4: Device Properties

- Interface_Wireless’ Physical Layer and DataLink Layer parameters are local but in Physical layer Standerd parameter is global. 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 as the parameter change does not propagate to the other devices since it is local.



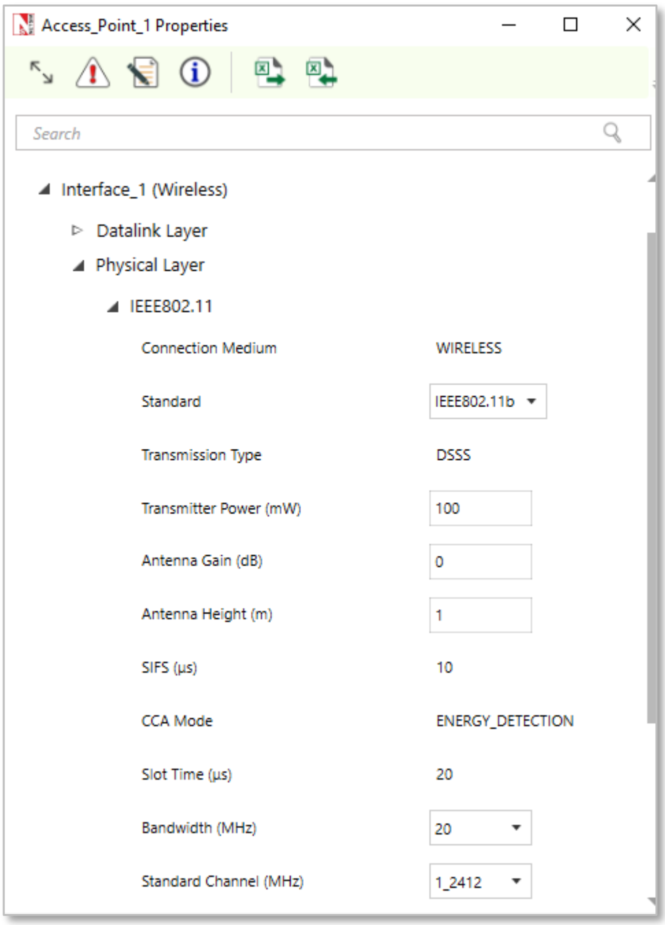
Access_Point_4 Properties

Search

- ▷ General
- ▷ Position
- ▷ Interface_1 (Ethernet)
- ◢ Interface_2 (Wireless)
  - ◢ Datalink Layer
    - ◢ IEEE802.11

Rate Adaptation	FALSE
Short Retry Limit	7
Dot11 RTS Threshold	3000
Long Retry Limit	4
MAC Address	AA0000004002
Buffer Size (MB)	100
Medium Access Protocol	DCF
Bss Type	INFRASTRUCTURE

Figure 2-5: MAC properties of Access Point



Access_Point_1 Properties

Search

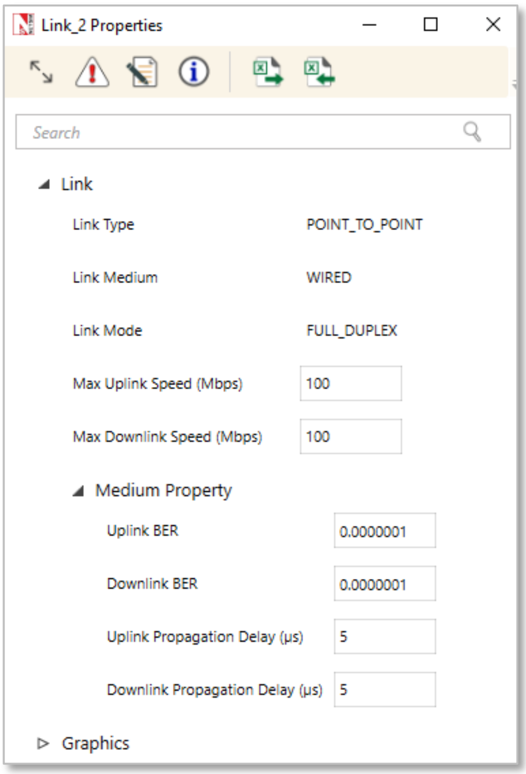
- Interface_1 (Wireless)
  - Datalink Layer
  - Physical Layer
    - IEEE802.11

Connection Medium	WIRELESS
Standard	IEEE802.11b
Transmission Type	DSSS
Transmitter Power (mW)	100
Antenna Gain (dB)	0
Antenna Height (m)	1
SIFS (µs)	10
CCA Mode	ENERGY_DETECTION
Slot Time (µs)	20
Bandwidth (MHz)	20
Standard Channel (MHz)	1_2412

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).



Link_2 Properties

Search

Link

Link Type: POINT_TO_POINT

Link Medium: WIRED

Link Mode: FULL_DUPLEX

Max Uplink Speed (Mbps): 100

Max Downlink Speed (Mbps): 100

Medium Property

Uplink BER: 0.0000001

Downlink BER: 0.0000001

Uplink Propagation Delay (µs): 5

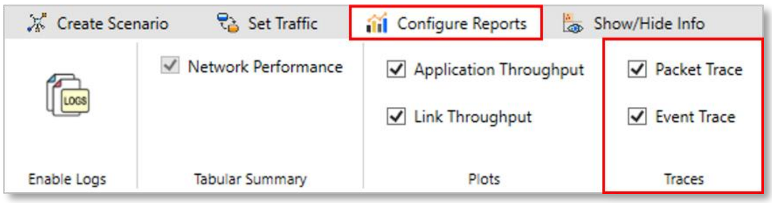
Downlink Propagation Delay (µs): 5

Graphics

Figure 2-7: Link Properties

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

Select Packet Trace / Event Trace from the Configure Reports option in the top ribbon. For detailed help, please refer **sections 8.1, 8.4** and **8.5** of the User Manual. Select Plots icon for enabling Plots and click on OK button see Figure 2-8.



☑ Network Performance

☑ Application Throughput

☑ Link Throughput

☑ Packet Trace

☑ Event Trace

Figure 2-8: Packet Trace, Event Trace & Plots options on top ribbon

2.4 Run Simulation

Click on the Run Simulation icon on the top ribbon/toolbar. For detailed help, please refer to **section 3.5** of the User Manual.

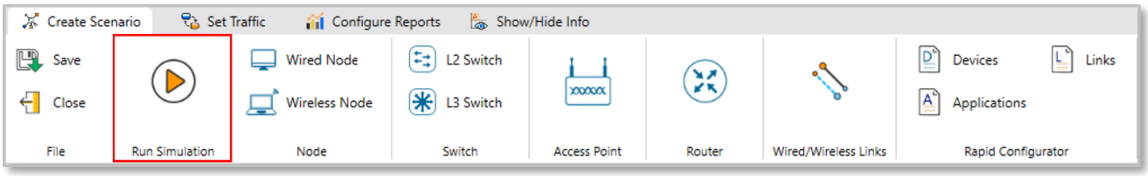
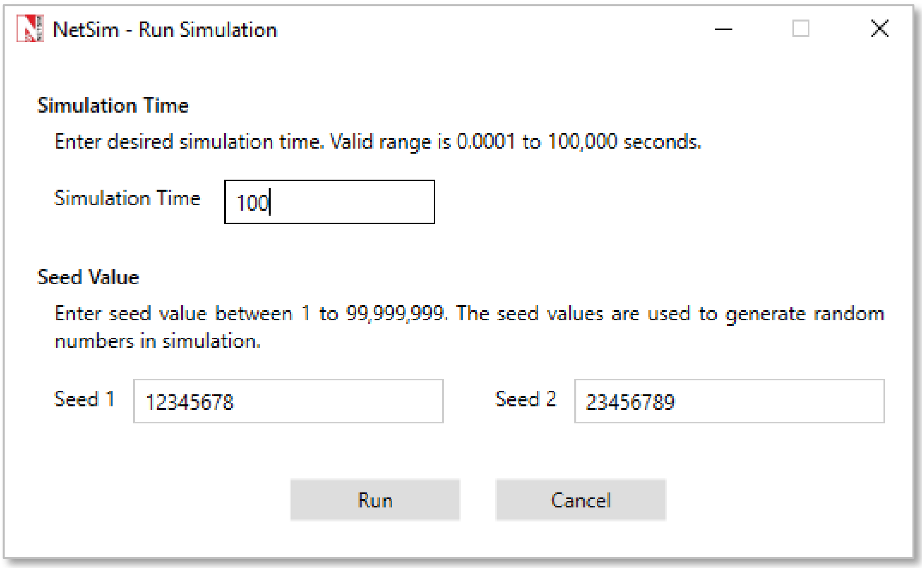


Figure 2-9: Run Simulation on top ribbon

Set the Simulation Time and click on the Run button.


NetSim - Run Simulation

Simulation Time

Enter desired simulation time. Valid range is 0.0001 to 100,000 seconds.

Simulation Time: 100

Seed Value

Enter seed value between 1 to 99,999,999. The seed values are used to generate random numbers in simulation.

Seed 1: 12345678

Seed 2: 23456789

Figure 2-10: Run Simulation window.

3 Model Features

3.1 WLAN 802.11

NetSim implements the 802.11 MAC and the 802.11 PHY abstracted at a packet-level. We start with the 3 types of nodes supported in 802.11 Wi-Fi.

- Wireless Nodes (Internetworks) or STAs. In Internetworks APs and Wireless nodes (STAs) are associated based on the connecting wireless link
- Wi-Fi Access Points (Internetworks) or APs. Every STA in the WLAN associates with exactly one AP. Each AP, along with its associated STAs, define a **cell**. Each cell operates on a specific channel.
- Standalone Wireless nodes (Mobile Adhoc networks).

The MAC Layer features:

- RTS/CTS/DATA/ACK transmissions.
- Packet queuing, aggregation, transmission, and retransmission.
- 802.11 EDCA.

The PHY layer implements:

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

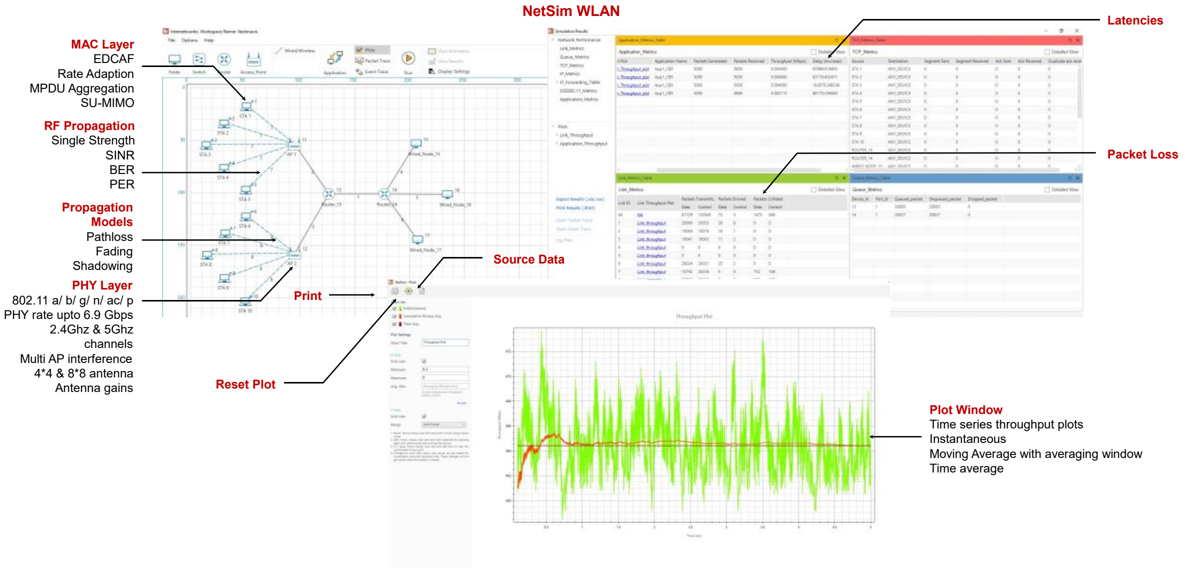


Figure 3-1: NetSim's Wi-Fi design window, the results dashboard, and the plots window

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. The operating frequencies and bandwidths are given in the Table 3-1.

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 The 2.4 GHz Channels

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

Channel	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	2484

Table 3-2: 2.4 GHz Wi-Fi Channels per IEEE Std 802.11g-2003, 802.11-2012

Channels 1 through 14 are used in 802.11b, while channels 1 through 13 are used in 802.11g/n.

3.1.3 The 5 GHz Channels

The following channel numbers are defined for 802.11a/n/ac.

Channel Number	Center Frequency (MHz)
36	5180
40	5200
44	5220
48	5240
52	5260
56	5280
60	5300

64	5320
100	5500
104	5520
108	5540
112	5560
116	5580
120	5600
124	5620
128	5640
132	5660
136	5680
140	5700
144	5720
149	5745
153	5765
157	5785
161	5805
165	5825
169	5845
173	5865
177	5885

Table 3-3: 5GHz Wi-Fi Channels per IEEE Std 802.11a -1999, 802.11n -2009, 802.11ac -2013

3.1.4 The 5.9 GHz Channels

Channel Number	Center Frequency (MHz)
100	5500
104	5520
108	5540
112	5560
116	5580
120	5600
124	5620
128	5640
132	5660
136	5680
140	5700
171	5855
172	5860
173	5865
174	5870
175	5875
176	5880
177	5885
178	5890
179	5895
180	5900
181	5905
182	5910

183	5915
184	5920

Table 3-4: 5.9 GHz Wi-Fi Channels per IEEE Std 802.11p-2010

3.1.5 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. 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, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 144, 149, 153, 157, 161, 165, 169, 173, 177
- 40MHz: 36, 44, 52, 60,100, 108, 116, 124, 132, 140, 149, 157, 165, 173
- 80MHz: 36, 52, 100, 116, 132, 149, 165
- 160MHz: 36, 100, 149

3.1.6 WLAN PHY Rate 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

3.1.7 SIFS, Slot Time, CW Min, and CW Max settings

Sub Std.	b (20MHz)
SIFS	10
Slot Time	20
CW Min	31
CW Max	1023

Table 3-6: DSSS PHY characteristics (IEEE-Std-802.11-2020 -Page no -2762)

Sub Std.	a	g	p		
Bandwidth	**20MHz**	**20MHz**	**5MHz**	**10MHz**	**20MHz**
SIFS	16	16	64	32	16
Slot Time	9	9	21	13	9
CW Min	15	15	15	15	15
CW Max	1023	1023	1023	1023	1023

Table 3-7: OFDM PHY characteristics (IEEE-Std-802.11-2020 -Page no -2846)

Sub Std.	n	
Frequency Band	2.4MHz	5
SIFS	10	16
Slot Time	20	9
CW Min	15	15
CW Max	1023	1023

Table 3-8: HT PHY characteristics (IEEE-Std-802.11-2020 -Page no -2951) and MIMO PHY characteristics (IEEE-Std-802.11n-2009 -Page no -335)

Sub Std.	ac (5GHz)
SIFS	16
Slot Time	9
CW Min	15
CW Max	1023

Table 3-9: Slot time in IEEE-Std-802.11-2020 -Page no -3094 and IEEE-Std-802.11ac-2013-Page no -297

3.1.8 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.

3.1.9 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.

3.1.10 802.11 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

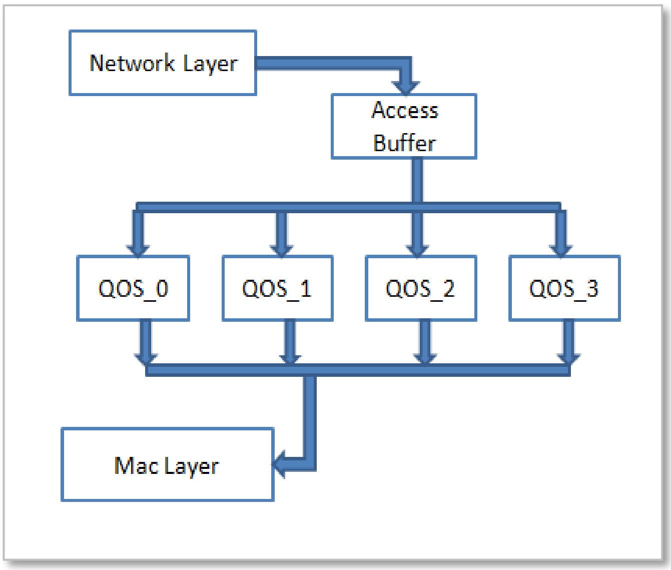


Figure 3-2: Packets transmission form Network layer to Mac Layer and how queued up in an access buffer

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.

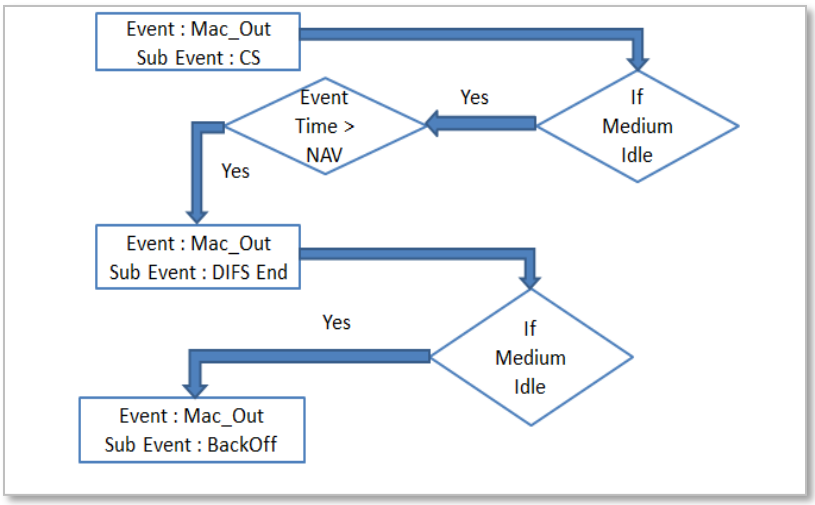


Figure 3-3: Event and SubEvent in Mac layer

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.

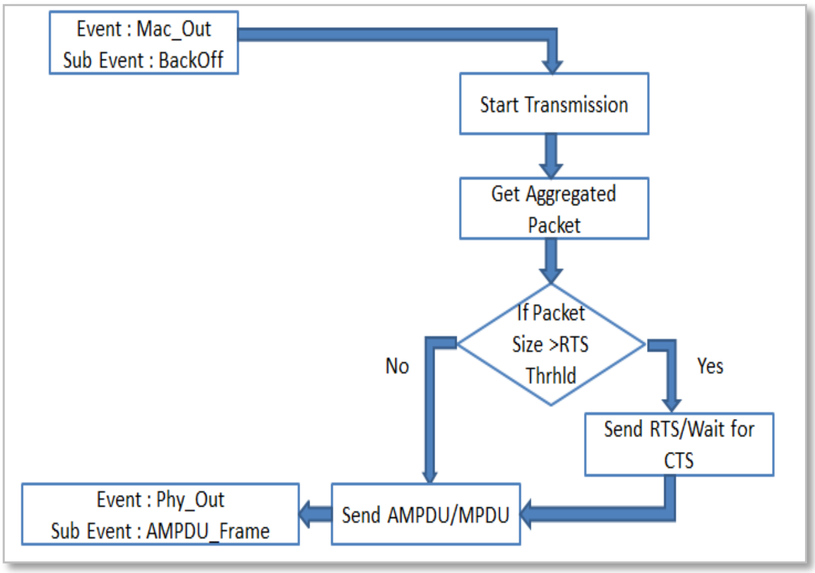


Figure 3-4: Event and SubEvent in Mac layer and Phy layer

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.

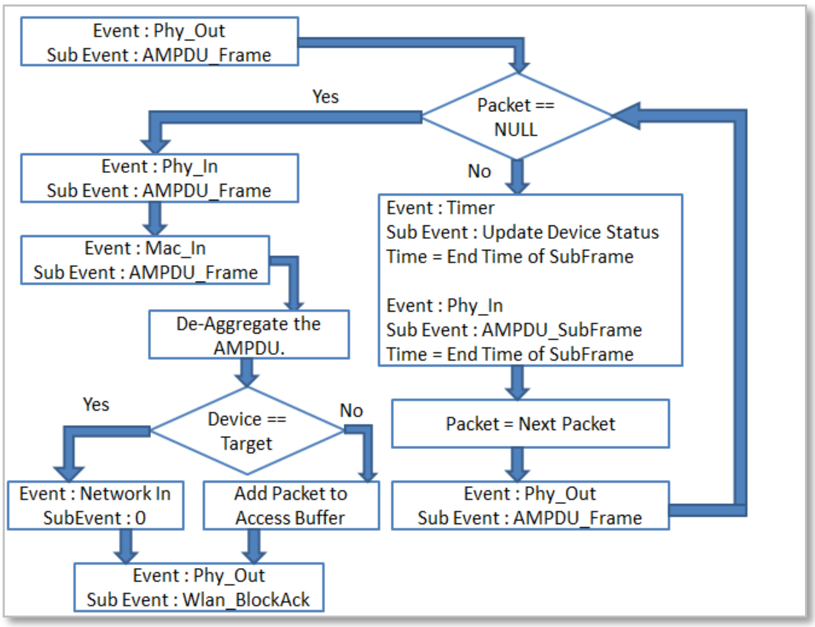


Figure 3-5: Event and SubEvent in Phy layer

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.

3.1.11 802.11ac 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 3-10: 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:

MCS index	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 3-11: Different Modulation schemes and 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 3-12: 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 3-13: 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

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

3.1.12 MAC Aggregation in NetSim

NetSim supports A-MPDU aggregation and does not support A-MSDU aggregation. MAC Aggregation is independent of MCS (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.

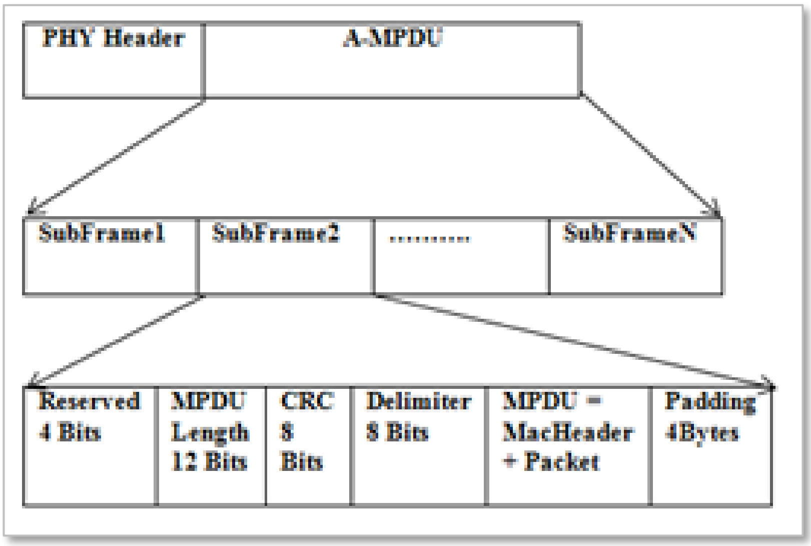
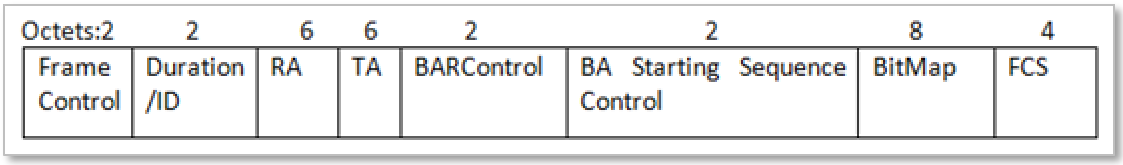


Figure 3-6: Aggregation scheme

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

$$NumberOfFramesToAggregate \times PacketSize\ (B) > 65{,}535\ (B)$$

3.1.13 Signal to interference and noise ratio (SINR)

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 transmissions. Only co-channel interference is accounted, and adjacent channel interference is not calculated. Finally, NetSim takes the ratio of the signal level, to the sum of the total interference from other transmissions plus the thermal noise. This ratio is SINR.

Once the SINR is calculated the BER is got from the SINR-BER tables for the applicable modulation scheme. This BER is then converted to Packet-Error-Rate. Packet error (Yes/No) is determined by drawing a random number in (0, 1) and comparing against PER[1].

The same is explained diagrammatically below.

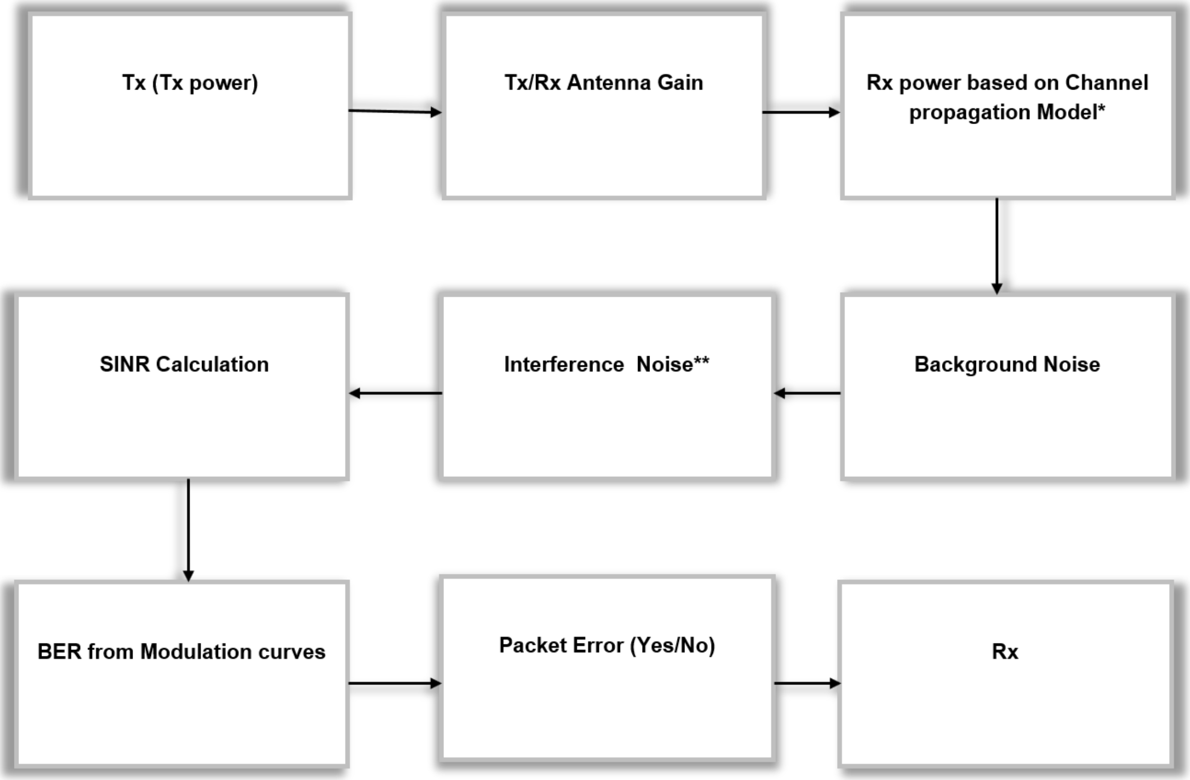


Figure 3-8: Radio Tx-Rx for one transmission

* 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

3.1.14 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.

3.1.15 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

[1] In other words, the instantaneous PER is used in a Bernoulli trial to decide whether the current packet is successfully received or not

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 on the Received power 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.

3.1.16 Transmission Range, Carrier Sense Range, and Interference Range

- Transmission Range: The transmission range is the range within which the receiver of a signal can decode the source’s transmission correctly (when no other transmitting node’s signal interferes). This is typically smaller than the carrier-sensing range of the transmitter.
- Carrier Sense Range: The carrier-sense range is the range within which the transmitter’s signal exceeds the Carrier Sense Threshold of the receiver (or another transmitter). The receiver (or another transmitter) detects the medium to be busy and does not transmit at this time.
- Interference Range: The interference range (defined by the receiver) is the range within which any signal transmitted by other sources interfere with the transmission of the intended source, thereby causing a loss (marked as a collision in NetSim) at the receiver.

These three ranges are affected by the power of the transmitter. The greater the transmission power, the further a node can receive the transmission, and also the more nodes whose communication with other nodes will be affected by this transmission. The transmission range is also affected by the MCS used by the transmitter. The higher the MCS the shorter the range, and vice versa

3.1.17 Carrier Sense (CS) Threshold

In NetSim (from v13.2 onwards) the Carrier sense (CS) threshold is set equal to Control rate receive sensitivity.

$$CSThreshold = RecieverSensitivity(ControlRate)$$

Users can modify the CS threshold using the variable CSRANGEDIFF which is set to 0 dB in code by default. This implies a 0 dB differential between the lowest MCS (Control rate) Receive sensitivity (which determines DecodeRange) and CS Threshold (which determines CarrierSenseRange). The value of CSRANGEDIFF can be modified by the user in NetSim

Standard or Pro versions, which ship with source code. We believe the term EDThreshold used in literature is the same as CSThreshold.

If the interference signal power (sum of the Received-power from all other transmitters), measured at the transmitter, is greater than ED-Threshold, then the transmitter assumes the medium is busy. Carrier is sensed by the transmitter; all CS activity occurs at the transmitter, and not at the receiver

3.1.18 Transmitter's choice of MCS

If the rate adaptation algorithm is turned off, then the transmitter chooses MCS by comparing the RSS (calculated per the equation below) against the Receiver-Sensitivity for different MCS (per the tables in the standards). The highest possible MCS is then chosen. This means the MCS is not fixed but adapts to the received signal strength, even with rate adaption turned off in the MAC layer.

NetSim exploits the AP-STA and the STA-AP channel reciprocity. Therefore, Pathloss plus Shadow loss is identical in both directions.

$$RSSI = TxPower - Pathloss - ShadowLoss$$

Note that when computing BER (from SINR) fading loss is added to this RSSI value. Thus, fading loss is not accounted when choosing MCS, but is accounted when computing BER.

NetSim has rate adaptation algorithms which take care of selecting the right MCS for a given SINR. In the simplest algorithm for every 20 successful transmissions the rate (MCS) goes up 1 step, and for every 3 continuous failures, the rate goes down one step.

3.1.19 Hidden Node Behaviour

Consider N1 and N3 transmitting to N2 whereby N1 and N3 are beyond Carrier sense (CS) range. N1 is said to be hidden from N3 and vice versa.

When N1 and N3 transmit, there are "likely" to be collisions at N2. However, collisions do not occur all the time. The CSMA/CA algorithm exponentially increases the backoff and hence after a few collisions it is possible that one of the nodes gets a low back-off number while the other draws a very high back-off number. Thus, the node with low back-off can complete transmissions (of one and even more than one packet) while the other node (with the large backoff) is still in backoff.

When N1 transmits to N2, N3 can't hear the transmission since N3 is beyond CS. Therefore, N3 can attempt if its backoff counts down to 0. However, when N2 sends back the WLAN-ACK, N3 will hear it since N3 is within range of N2. Therefore, in NetSim, N3 will sense the medium as busy and freeze its back off when N2 is sending the WLAN ACK to N1.

In case of N2 to N1/N3 transmissions, then the reverse is true for the MAC-ACK from the nodes. When N2 sends a packet to N1 (or N3) it is within range of N3 (or N1), however, when N1 (or N3) sends back the MAC ACK there is a chance of collision with a data packet of N3 (or N1).

3.1.20 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 channel contention parameters i.e., 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.

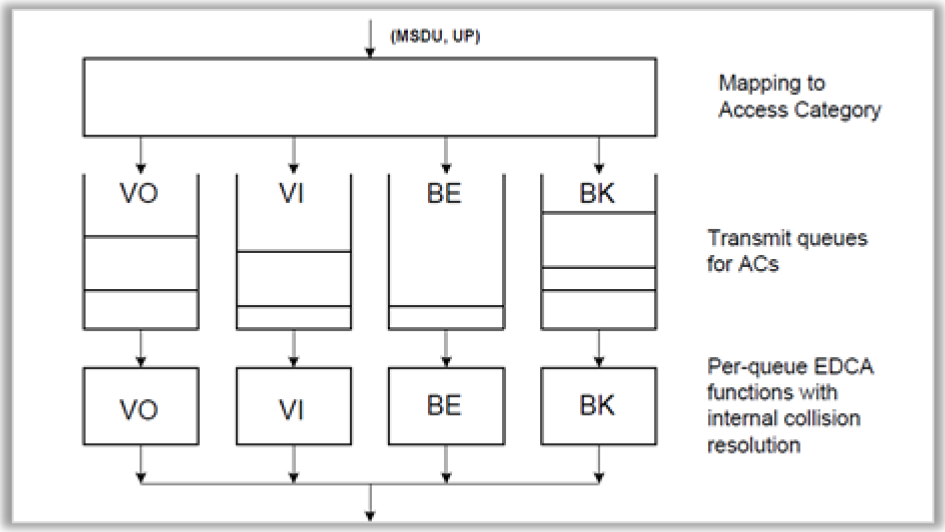

(MSDU, UP)
Mapping to Access Category
VO
VI
BE
BK
Transmit queues for ACs
VO
VI
BE
BK
Per-queue EDCA functions with internal collision resolution

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

3.1.20.1 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 3-14: 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 3-15: 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 3-16: 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).*

3.1.21 Rate Adaptation

In NetSim (with default code), rate adaptation works as follows:

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

If users, wish to set the PHY rate (MCS) by comparing the received signal strength against the Receiver minimum input sensitivity tables provided in the standards, they should comment the following line (line #38) in IEEE802_11.h, and rebuild the code

```
//#define _RECALCULATE_RX_SENSITIVITY_BASED_ON_PEP_
```

NetSim then chooses the rate at the beginning of the simulation and the rate doesn't subsequently adapt. The receiver minimum input sensitivity levels are provided in the files

- 802.11b: IEEE802_11_DSSSPhy.c
- 802.11a, 802.11g and 802.11p: IEEE802.11_OFDMPhy.c
- 802.11n and 802.11ac: IEEE802_11_HTPhy.c

Selecting the different rate adaptation options would have no impact when running this modified code.

3.1.22 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. While different APs can operate in different channels, all the Wireless nodes connected to one AP operate in the same channel.
4. No beacon generation, probing or association
5. RTS, CTS and ACK are always transmitted at the base rate (lowest MCS)
6. Roaming whereby a STA leaves serving AP to associate with target AP (usually based on RSSI/SNR)

3.1.23 Wi-Fi GUI Parameters

The WLAN parameters can be accessed by right clicking on a Access Point or Wireless Node and selecting Interface Wireless Properties ->Datalink and Physical Layers

Access Point and Wireless Node Properties			
Interface Wireless – Datalink Layer			
Parameter	**Scope**	**Range**	**Description**
Rate Adaptation	Cell	False	The algorithm 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. The adaptation is termed as "FALSE" since the rate is pre-determined as per standard and there is no subsequent "adaptation"
		Minstrel	Rate adaptation algorithm implemented in Linux
		Generic	The algorithm is similar to the Auto Rate Fall Back (ARF) algorithm. In this algorithm (i) Rate goes up one step for 20 consecutive packet successes, and (ii) Rate goes down one step after 3 consecutive packet failures
Short Retry Limit	Local	1 to 255	Determines the maximum number of transmission attempts of a frame. The length of MPDU is less than/ equal to Dot11 RTS Threshold value, made before a failure condition is indicated.
Long Retry Limit	Local	1 to 255	Determines the maximum number of transmission attempts of a frame. The length of MPDU is greater than Dot11 RTS Threshold value, made before a failure condition is indicated.
Dot11 RTS Threshold	Local	0 to 65535	The size of packets (or A-MPDU if applicable) above which RTS/CTS (Request to Send / Clear to Send) mechanism gets triggered.
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	Local	1 to 100	Buffer is the memory in a device which holds data packets temporarily. If incoming rate is higher than the outgoing rate, incoming packets are stored in the buffer. NetSim models the buffer as an egress buffer. Unit is MB.
Medium Access Protocol	Local	DCF	DCF is the process by which CSMA/CA is applied to Wi-Fi networks. DCF defines four components to ensure devices share the medium equally: Physical Carrier Sense, Virtual Carrier Sense, Random Back-off timers, and Interframe Spaces (IFS). DCF is used in non-QoS WLANs.
		EDCAF	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.
Physical Type	Local	DSSS	Direct Sequence Spread Spectrum. The physical type parameter is set to DSSS if the standard selected is IEEE802.11b.
		OFDM	Orthogonal Frequency Division Multiplexing is utilized as a digital multi-carrier modulation method. The physical type parameter is set to OFDM if the standard selected is IEEE802.11 a, g and p.
		HT	Operates in frequency bands 2.4GHz or 5GHz band. The physical type parameter is set to HT if the standard selected is IEEE802.11n.
		VHT	The physical type parameter is set to VHT if the standard selected is IEEE802.11ac.
OCBA Activated	Local	True or False	This parameter determines the type of standard to be chosen for the OFDM physical type. • The standard is set to IEEE802.11p if OCBA is True. • The standard is set to IEEE802.11a and g if OCBA is False.
BSS Type	Fixed	Auto Generated	The BSS type is fixed to Infrastructure mode. The wireless device can communicate - with each other or with a wired network - through an Access Point.
CW min (Slots)	Local	0 to 255	Specifies the initial Contention Window (CW) used by an Access Point (or STA) for a particular AC for generating a random number for the back-off.
CW max (Slots)	Local	0 to 65535	At each collision the CW is doubled. CW_{Max} specifies the final maximum CW values used by an Access Point (or STA) for a particular AC for generating a random number for the back-off.
AIFSN (Slot)	Local	2 to 15	Specifies the number of slots after a SIFS duration.
Max TXOP	Local	0 to 65535	Specifies the maximum number of microseconds of an EDCA TXOP for a given AC. Unit is microseconds.
MSDU Lifetime (TU)	Local	0 to 500	Specifies the maximum duration an MSDU would be retained by the MAC before it is discarded, for a given AC. MSDU Lifetime is specified in TU.
Interface Wireless- Physical Layer			
Protocol	Fixed	IEEE802.11	Defines the MAC and PHY specifications like IEEE802.11a/b/g/n/ac/p for wireless connectivity for fixed, portable and moving stations within a local area.
Connection Medium	Fixed	Auto Generated	Defines how the devices are connected or linked to each other.
Standard	Cell	IEEE802.11 a/b/g/n/ac/p	Refers to a family of specifications developed by IEEE for WLAN technology. The IEEE standards

			supported in NetSim are IEEE 802.11 a, b, g, n, ac and p. 802.11a provides up to 54 Mbps in 5GHz band. 802.11b provides 11 Mbps in the 2.4GHz bands. 802.11gprovides 54 Mbps transmission over short distances in the 2.4 GHz band. 802.11n adds up MIMO. 802.11ac provides support for wider channels and beamforming capabilities. 802.11p provides support to Intelligent Transportation Systems.
Transmission Type	Fixed	DSSS	The transmission type parameter is DSSS if the standard selected is IEEE802.11b.
		OFDM	The transmission type parameter is OFDM if the standard selected is IEEE802.11a, g and p.
		HT	The transmission type parameter is HT if the standard selected is IEEE802.11n.
		VHT	The transmission type parameter is VHT if the standard selected is IEEE802.11ac.
Number of Frames to Aggregate	Cell	1 to 1024 (11ac) 1 to 64 (11n)	Number of frame aggregated to form an A-MPDU. This is fixed and cannot be dynamically varied (except by modifying the code). See 3.1.12 for more information.
Transmit Power	Local	0 to 1000	Transmitted signal power. Note that the transmit power is not split among the antennas. This value is applied to each antenna in a multi-antenna transmitter. Unit is mW.
Antenna Gain	Local	0 to 1000	A relative measure of an antenna’s ability to direct or concentrate radio frequency energy in a particular direction or pattern. The measurement is typically measured in dBi (Decibels relative to an isotropic radiator).
Antenna Height	Local	0 to 1000	The height of antenna above the ground. Unit is m.
SIFS	Fixed	Auto Generated	The time interval required by a wireless device in between receiving a frame and responding to the frame. Unit is microseconds.
Frequency Band	Cell	2.4, 5 (Depends on the standard chosen)	Range of frequencies at which the device operates. The frequency band depends on the standard selected. Unit is GHz.
Bandwidth	Cell	20, 40, 60, 80, 160 (Depends on the standard chosen)	The bandwidth depends on the standard and the frequency band selected. Unit is MHz
CCA Mode	Fixed	Auto Generated	A mechanism to determine whether a medium is idle or not. It includes Carrier sensing and energy detection.
Slot Time	Fixed	Auto Generated	Time is quantized as slots in Wi-Fi. Unit is microseconds.

Standard Channel	Local	Depends on the standard chosen	The channel options defined in the standards. The options would also depend on the frequency band if the standard supports multiple bands.
CW Min	Fixed	Auto Generated	The minimum size of the Contention Window in units of slot time. The CW min is used by the MAC to calculate the back off time for channel access during a carrier sense.
CW Max	Fixed	Auto Generated	The maximum size of the Contention Window in units of slot time. The CW is doubled progressively when collisions occur.
Transmitting Antennas	Local	1 to 8	The number of transmit antennas. Note that power is not split among the transmit antennas but is assigned to each antenna. (The pair of Tx and Rx antenna present only for 802.11ac and 802.11n)
Receiving Antennas	Local	1 to 8	The number of receive antennas
Guard Interval	Local	400 and 800	Guard Interval is intended to avoid signal loss from multipath effect. Unit is nanoseconds.
Reference Distance d_0	Local	1 to 10	$PL = PL_{D_0} + 10 \times \eta \times \log(\frac{d}{d_0})$ PL: is the path loss at the reference distance d_0. Unit: Decibel (dB) d: is the distance between the transmitter and the receiver. d_0: is the reference distance defined in the standard. η: is the path loss exponent.

Table 3-17: Internetworks Config Properties

3.1.24 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 3-18: Description of IEEE 802.11 Metrics

3.1.25 Radio measurements log file

NetSim IEEE802_11 Radio measurements csv log file records pathloss, shadowing loss, fading loss, transmitted power, received power, SNR, Interference Power, SINR, BER, NSS, MCS. This log file can be enabled in NetSim GUI by clicking on icon present in the tool bar as shown below.

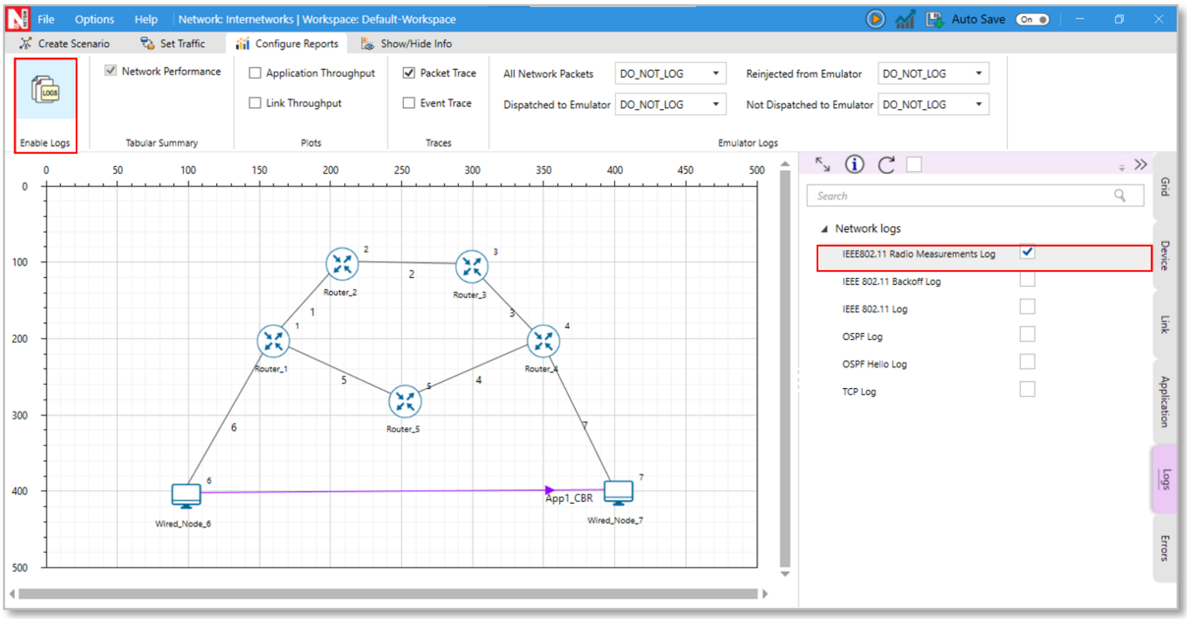


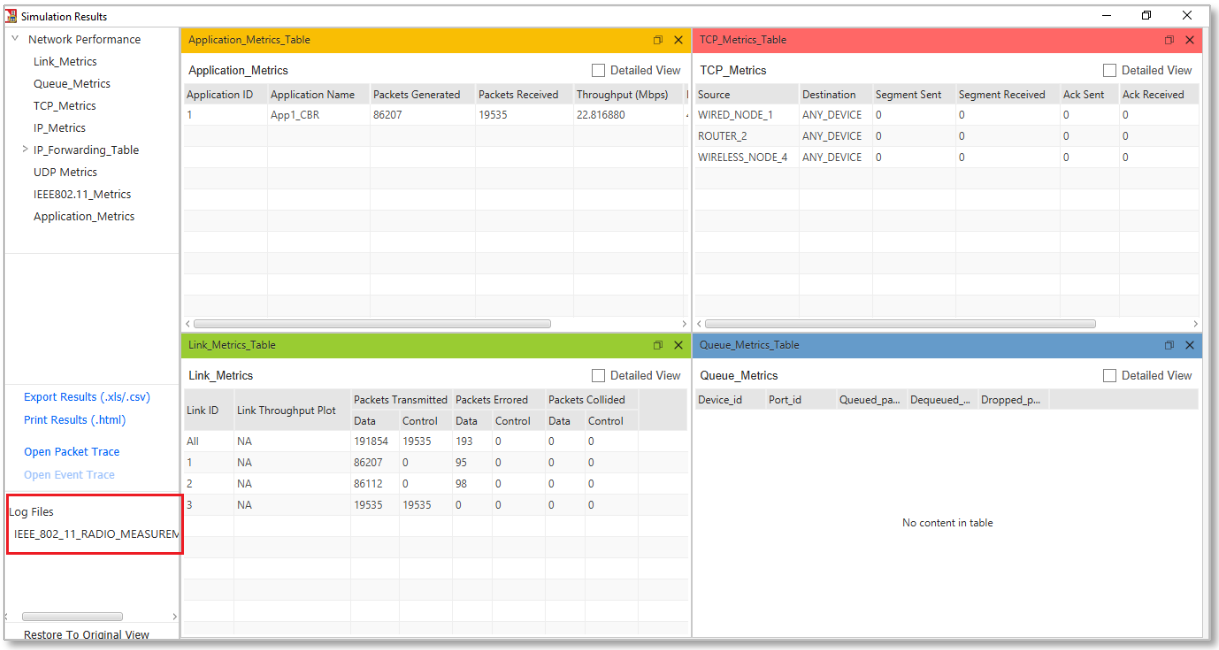
Figure 3-10: Enabling IEEE802.11 Radio Measurement logs

The IEEE802_11_RADIO_MEASUREMENTS_LOG.csv file will contain the following information:

- Time in Milliseconds
- Transmitter Name
- Receiver Name
- Distance between the Transmitter and the Receiver in meters
- Packet ID
- Packet Type

- Control Packet Type
- Transmitter Power in dBm
- Total Loss in dB
- Pathloss in dB
- Shadowing Loss in dB
- Fading Loss in dB
- Received Power in dBm
- Interference in dBm
- SNR in dB
- SINR in dB
- BER
- NSS
- MCS

The log file can be accessed from the Simulations Results Window under the log file drop down in the left pane.



Application_Metrics

Application ID	Application Name	Packets Generated	Packets Received	Throughput (Mbps)
1	App1_CBR	86207	19535	22.816880

TCP_Metrics

Source	Destination	Segment Sent	Segment Received	Ack Sent	Ack Received
WIRED_NODE_1	ANY_DEVICE	0	0	0	0
ROUTER_2	ANY_DEVICE	0	0	0	0
WIRELESS_NODE_4	ANY_DEVICE	0	0	0	0

Link_Metrics

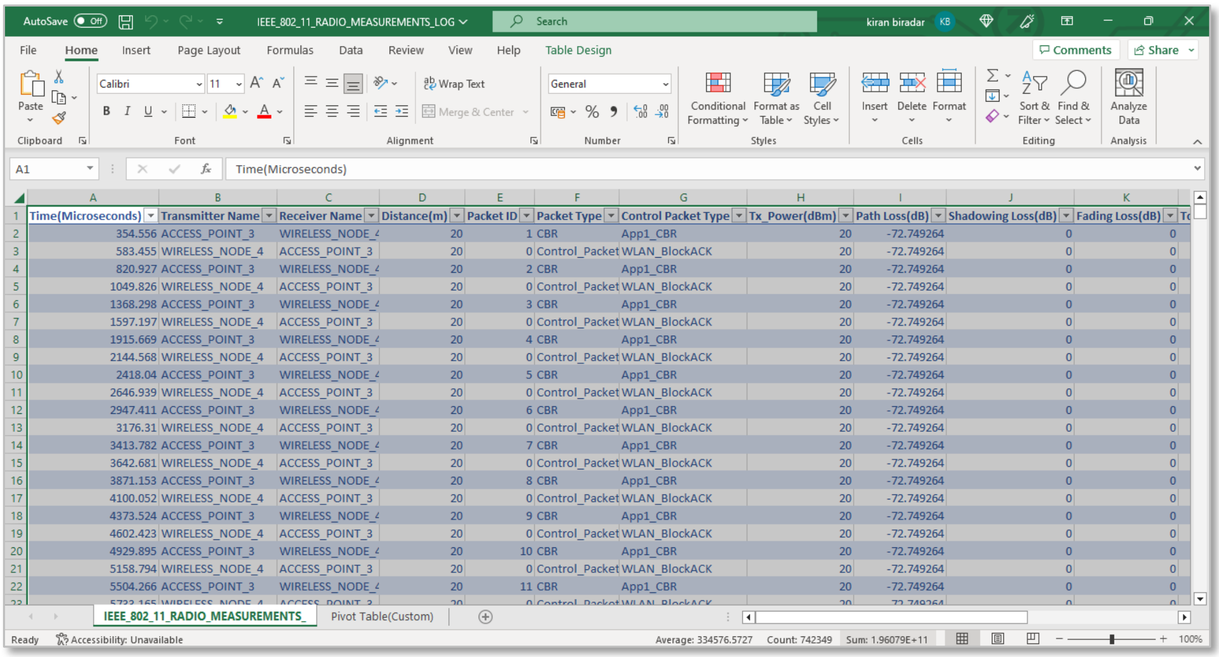
Link ID	Link Throughput Plot	Packets Transmitted		Packets Errored		Packets Collided	
		Data	Control	Data	Control	Data	Control
All	NA	191854	19535	193	0	0	0
1	NA	86207	0	95	0	0	0
2	NA	86112	0	98	0	0	0
3	NA	19535	19535	0	0	0	0

Queue_Metrics

Device_id	Port_id	Queued_pa...	Dequeued_...	Dropped_p...

No content in table

Figure 3-11: IEEE802_11_RADIO_MEASUREMENTS_LOG.csv file highlighted in the Results window.



Time(Microseconds)	Transmitter Name	Receiver Name	Distance(m)	Packet ID	Packet Type	Control Packet Type	Tx_Power(dBm)	Path Loss(dB)	Shadowing Loss(dB)	Fading Loss(dB)
354.556	ACCESS_POINT_3	WIRELESS_NODE_4	20	1	CBR	App1_CBR	20	-72.749264	0	0
583.455	WIRELESS_NODE_4	ACCESS_POINT_3	20	0	Control_Packet	WLAN_BlockACK	20	-72.749264	0	0
820.927	ACCESS_POINT_3	WIRELESS_NODE_4	20	2	CBR	App1_CBR	20	-72.749264	0	0
1049.826	WIRELESS_NODE_4	ACCESS_POINT_3	20	0	Control_Packet	WLAN_BlockACK	20	-72.749264	0	0
1368.298	ACCESS_POINT_3	WIRELESS_NODE_4	20	3	CBR	App1_CBR	20	-72.749264	0	0
1597.197	WIRELESS_NODE_4	ACCESS_POINT_3	20	0	Control_Packet	WLAN_BlockACK	20	-72.749264	0	0
1915.669	ACCESS_POINT_3	WIRELESS_NODE_4	20	4	CBR	App1_CBR	20	-72.749264	0	0
2144.568	WIRELESS_NODE_4	ACCESS_POINT_3	20	0	Control_Packet	WLAN_BlockACK	20	-72.749264	0	0
2418.04	ACCESS_POINT_3	WIRELESS_NODE_4	20	5	CBR	App1_CBR	20	-72.749264	0	0
2646.939	WIRELESS_NODE_4	ACCESS_POINT_3	20	0	Control_Packet	WLAN_BlockACK	20	-72.749264	0	0
2947.411	ACCESS_POINT_3	WIRELESS_NODE_4	20	6	CBR	App1_CBR	20	-72.749264	0	0
3176.31	WIRELESS_NODE_4	ACCESS_POINT_3	20	0	Control_Packet	WLAN_BlockACK	20	-72.749264	0	0
3413.782	ACCESS_POINT_3	WIRELESS_NODE_4	20	7	CBR	App1_CBR	20	-72.749264	0	0
3642.681	WIRELESS_NODE_4	ACCESS_POINT_3	20	0	Control_Packet	WLAN_BlockACK	20	-72.749264	0	0
3871.153	ACCESS_POINT_3	WIRELESS_NODE_4	20	8	CBR	App1_CBR	20	-72.749264	0	0
4100.052	WIRELESS_NODE_4	ACCESS_POINT_3	20	0	Control_Packet	WLAN_BlockACK	20	-72.749264	0	0
4373.524	ACCESS_POINT_3	WIRELESS_NODE_4	20	9	CBR	App1_CBR	20	-72.749264	0	0
4602.423	WIRELESS_NODE_4	ACCESS_POINT_3	20	0	Control_Packet	WLAN_BlockACK	20	-72.749264	0	0
4929.895	ACCESS_POINT_3	WIRELESS_NODE_4	20	10	CBR	App1_CBR	20	-72.749264	0	0
5158.794	WIRELESS_NODE_4	ACCESS_POINT_3	20	0	Control_Packet	WLAN_BlockACK	20	-72.749264	0	0
5504.266	ACCESS_POINT_3	WIRELESS_NODE_4	20	11	CBR	App1_CBR	20	-72.749264	0	0
5733.165	WIRELESS_NODE_4	ACCESS_POINT_3	20	0	Control_Packet	WLAN_BlockACK	20	-72.749264	0	0

Figure 3-12: IEEE802_11_RADIO_MEASUREMENTS_LOG.csv file

Implementation details and Assumptions:

- The log is written during each packet received at the physical layer (PHY_IN). Hence the number of entries will be based on the number of packets received, by all nodes or specific nodes based on values present in the DEVICE_ID_LIST array.
- MCS column displays the MCS index from the Phy parameters table in case of IEEE802.11 n and ac. However, it displays the index value from the Phy parameters table as nIndex-1 in case of DSSS based standards such as b and OFDM based standards such as a, g and p.
- The NSS value is currently set to the minimum of transmit and receive antenna counts in the same device. For example, if Transmitting Antennas is set to 2 and receiving Antennas is set to 8 then NSS is set to 2.

3.1.26 IEEE 802.11 Backoff Log

NetSim 802.11 Backoff log file records details such as the Device name, Time stamp, Packet ID, BackoffTime, contention Window size and Retry Limit. This log can be used to understand the medium access mechanism in IEEE 802.11 Protocols.

This log file can be enabled in NetSim GUI by clicking on icon present in the tool bar as shown below.

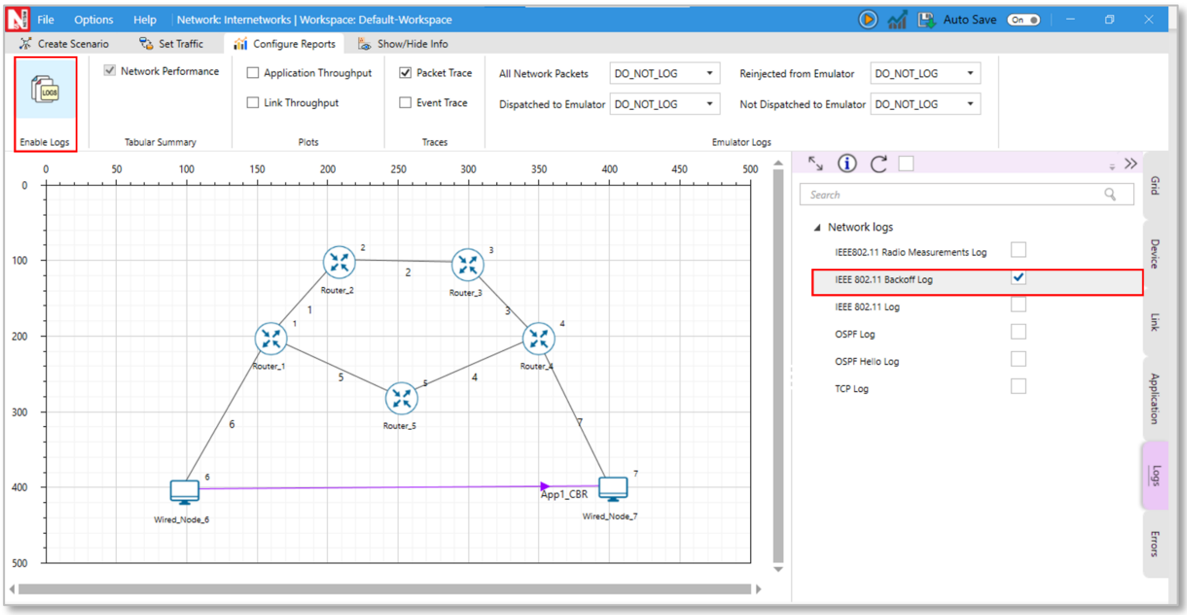
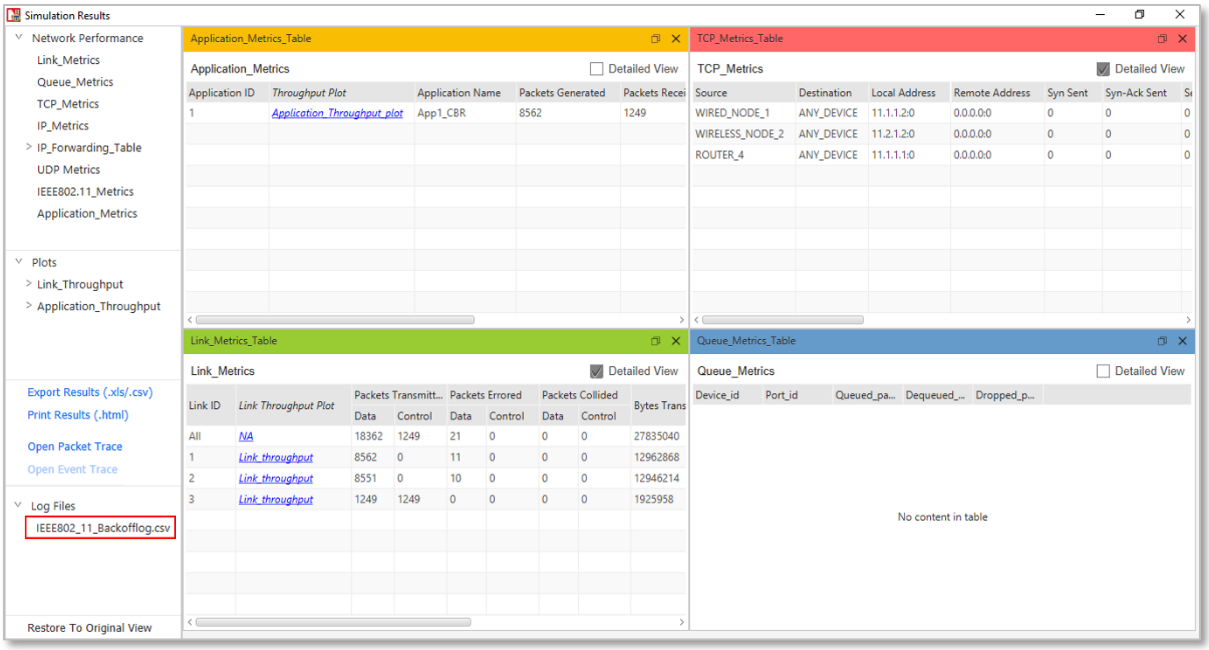


Figure 3-13: Enabling IEEE 802.11 Backoff log

The IEEE802_11_Backoff _Log.csv file will contain the following information:

- Device Name
- Timestamp
- Packet ID
- BackOffTime
- Contention Window Size
- Retry Limit

The log file can be accessed from the Simulations Results Window under the log file drop down in the left pane.



Application_Metrics_Table

Application_Metrics ☐ Detailed View

Application ID	*Throughput Plot*	Application Name	Packets Generated	Packets Recei
1	*Application_Throughput_plot*	App1_CBR	8562	1249

TCP_Metrics_Table

TCP_Metrics ☑ Detailed View

Source	Destination	Local Address	Remote Address	Syn Sent	Syn-Ack Sent	Se
WIRED_NODE_1	ANY_DEVICE	11.1.1.2:0	0.0.0.0:0	0	0	0
WIRELESS_NODE_2	ANY_DEVICE	11.2.1.2:0	0.0.0.0:0	0	0	0
ROUTER_4	ANY_DEVICE	11.1.1.1:0	0.0.0.0:0	0	0	0

Link_Metrics_Table

Link_Metrics ☑ Detailed View

Link ID	*Link Throughput Plot*	Packets Transmitt...		Packets Errored		Packets Collided		Bytes Trans
		Data	Control	Data	Control	Data	Control	
All	*NA*	18362	1249	21	0	0	0	27835040
1	*Link_throughput*	8562	0	11	0	0	0	12962868
2	*Link_throughput*	8551	0	10	0	0	0	12946214
3	*Link_throughput*	1249	1249	0	0	0	0	1925958

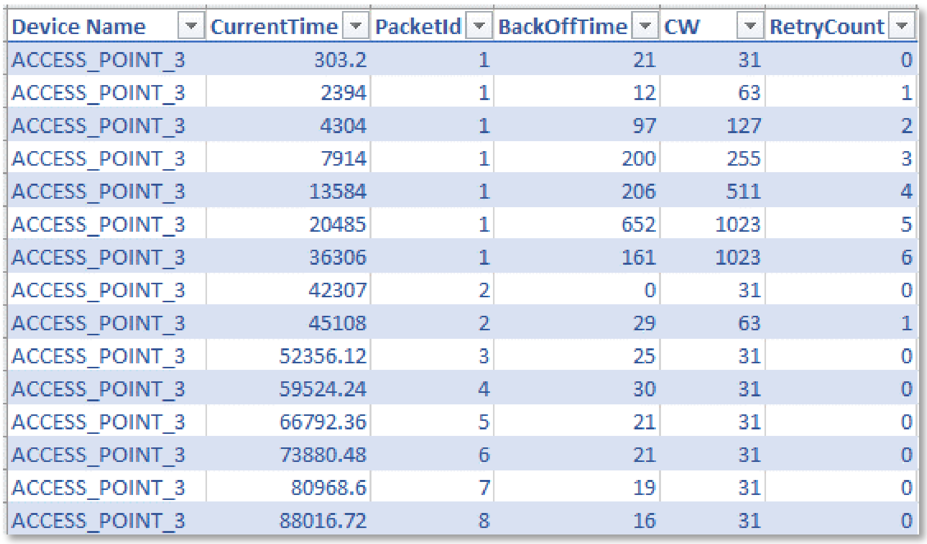
Queue_Metrics_Table

Queue_Metrics ☐ Detailed View

Device_id	Port_id	Queued_pa...	Dequeued_...	Dropped_p...

No content in table

Figure 3-14: IEEE802_11_Backoff_Log.csv file highlighted in the Results window.



Device Name	CurrentTime	PacketId	BackOffTime	CW	RetryCount
ACCESS_POINT_3	303.2	1	21	31	0
ACCESS_POINT_3	2394	1	12	63	1
ACCESS_POINT_3	4304	1	97	127	2
ACCESS_POINT_3	7914	1	200	255	3
ACCESS_POINT_3	13584	1	206	511	4
ACCESS_POINT_3	20485	1	652	1023	5
ACCESS_POINT_3	36306	1	161	1023	6
ACCESS_POINT_3	42307	2	0	31	0
ACCESS_POINT_3	45108	2	29	63	1
ACCESS_POINT_3	52356.12	3	25	31	0
ACCESS_POINT_3	59524.24	4	30	31	0
ACCESS_POINT_3	66792.36	5	21	31	0
ACCESS_POINT_3	73880.48	6	21	31	0
ACCESS_POINT_3	80968.6	7	19	31	0
ACCESS_POINT_3	88016.72	8	16	31	0

Figure 3-15: IEEE802_11_ Backoff_Log.csv file

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. It 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.

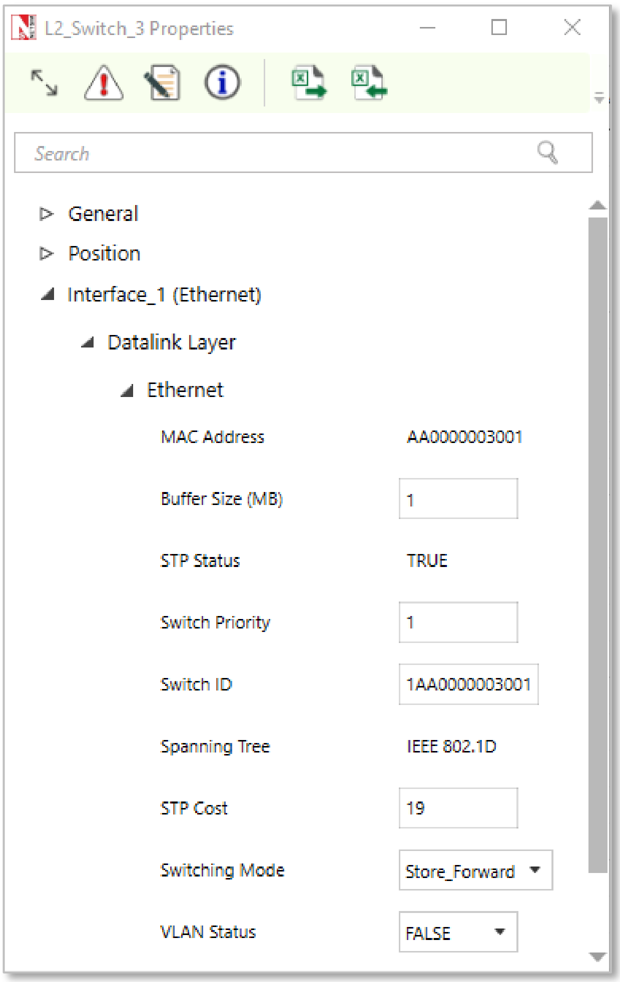
It is recommended that the application start time is set to a value that is greater than the time it takes for the spanning tree protocol to complete (of the order of a 100s of milliseconds).

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 Switch: GUI Parameters

Switch properties can be set by right clicking switch-->Properties--> Interface_1(ETHERNET).



L2_Switch_3 Properties

Search

- General
- Position
- Interface_1 (Ethernet)
  - Datalink Layer
    - Ethernet

MAC Address AA0000003001

Buffer Size (MB) 1

STP Status TRUE

Switch Priority 1

Switch ID 1AA0000003001

Spanning Tree IEEE 802.1D

STP Cost 19

Switching Mode Store_Forward

VLAN Status FALSE

Figure 3-16: 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	Local	-	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.
VLAN Status*	Local	TRUE, FALSE	To enable/disable VLAN

Table 3-19: 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

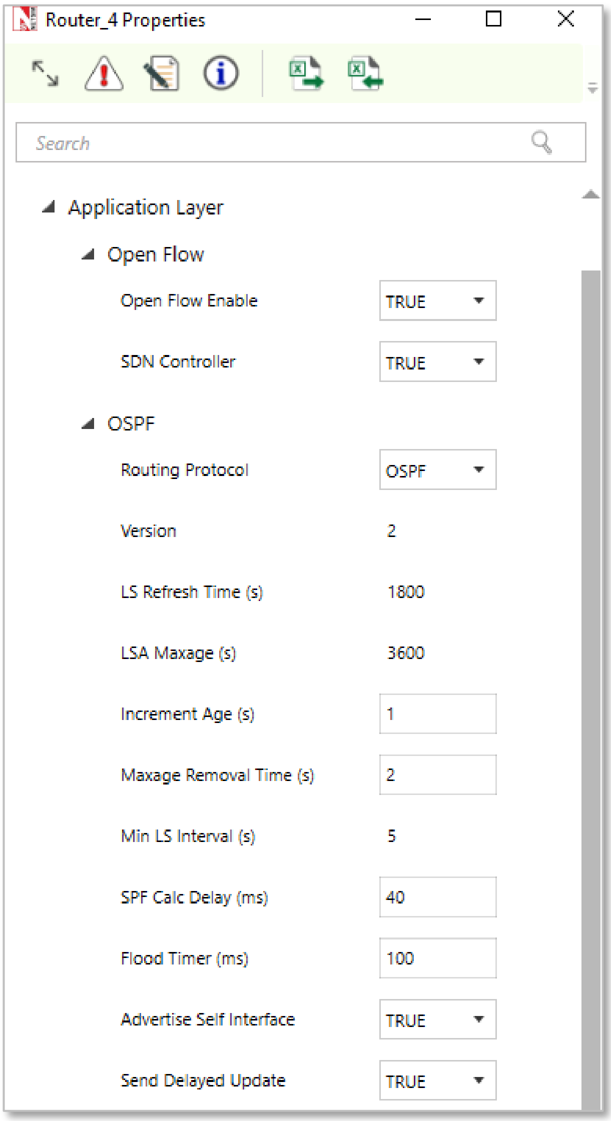
- Hello log
- SPF log
- Common log
- Debug logs – LSDB, RXList, RLSA, RCVLSU, LSULIST, Route

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 OSPF: GUI Parameters

OSPF properties can be set by right clicking on Router --> Properties --> Application layer see Figure 3-17.



Application Layer

Open Flow

Open Flow Enable: TRUE

SDN Controller: TRUE

OSPF

Routing Protocol: OSPF

Version: 2

LS Refresh Time (s): 1800

LSA Maxage (s): 3600

Increment Age (s): 1

Maxage Removal Time (s): 2

Min LS Interval (s): 5

SPF Calc Delay (ms): 40

Flood Timer (ms): 100

Advertise Self Interface: TRUE

Send Delayed Update: TRUE

Figure 3-17: 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 3-20: 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 3-18: 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.

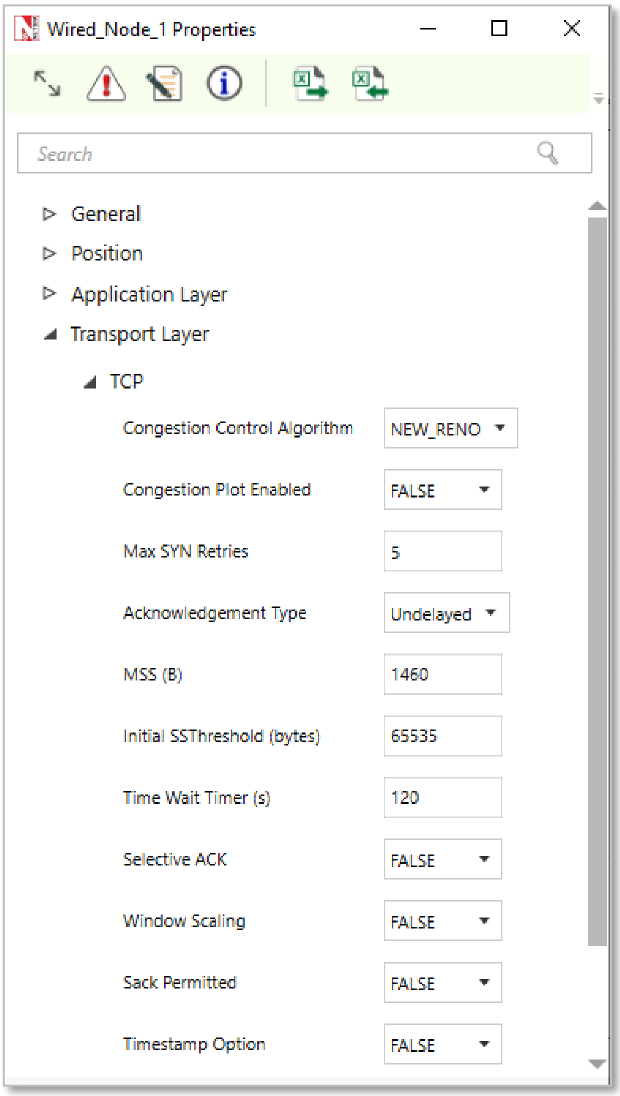
1. Old Tahoe
2. Tahoe
3. Reno
4. New Reno
5. BIC
6. CUBIC

3.4.4 Limitations of TCP

1. Send and Receive buffers are infinite

3.4.5 TCP: GUI parameters

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



Congestion Control Algorithm: NEW_RENO
Congestion Plot Enabled: FALSE
Max SYN Retries: 5
Acknowledgement Type: Undelayed
MSS (B): 1460
Initial SSThreshold (bytes): 65535
Time Wait Timer (s): 120
Selective ACK: FALSE
Window Scaling: FALSE
Sack Permitted: FALSE
Timestamp Option: FALSE

Figure 3-19: 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 3-21: 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 3-22: 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)

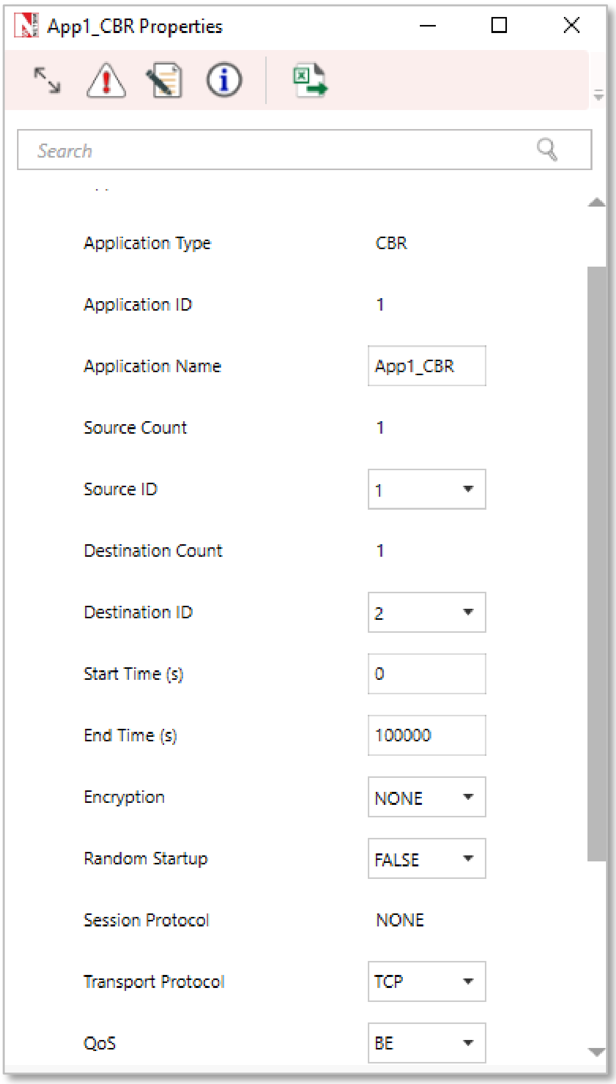
3.5.1 UDP Overview

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 reliable delivery of streams of data should use the Transmission Control Protocol (TCP).

3.5.2 UDP: GUI parameters

The UDP protocol can be set for an application by clicking on the Applications Transport Protocol option as shown below see Figure 3-20.



Application Type	CBR
Application ID	1
Application Name	App1_CBR
Source Count	1
Source ID	1
Destination Count	1
Destination ID	2
Start Time (s)	0
End Time (s)	100000
Encryption	NONE
Random Startup	FALSE
Session Protocol	NONE
Transport Protocol	TCP
QoS	BE

Figure 3-20: 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 3-23.**

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 3-23: 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 3-24: 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 the 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 the 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:

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

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

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

$$PER = BER * L$$

3.9 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 192.168.0.2 and 192.168.0.3 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 (192.168.0.0).

Similarly, if you create a network with a router and two wired nodes, the IP addresses are assigned as 192.168.0.1 and 192.169.0.1 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 192.168.0.1 and 192.169.0.1 respectively for the two interfaces. Both the nodes are in different networks (192.168.0.0 and 192.169.0.0) in this case.

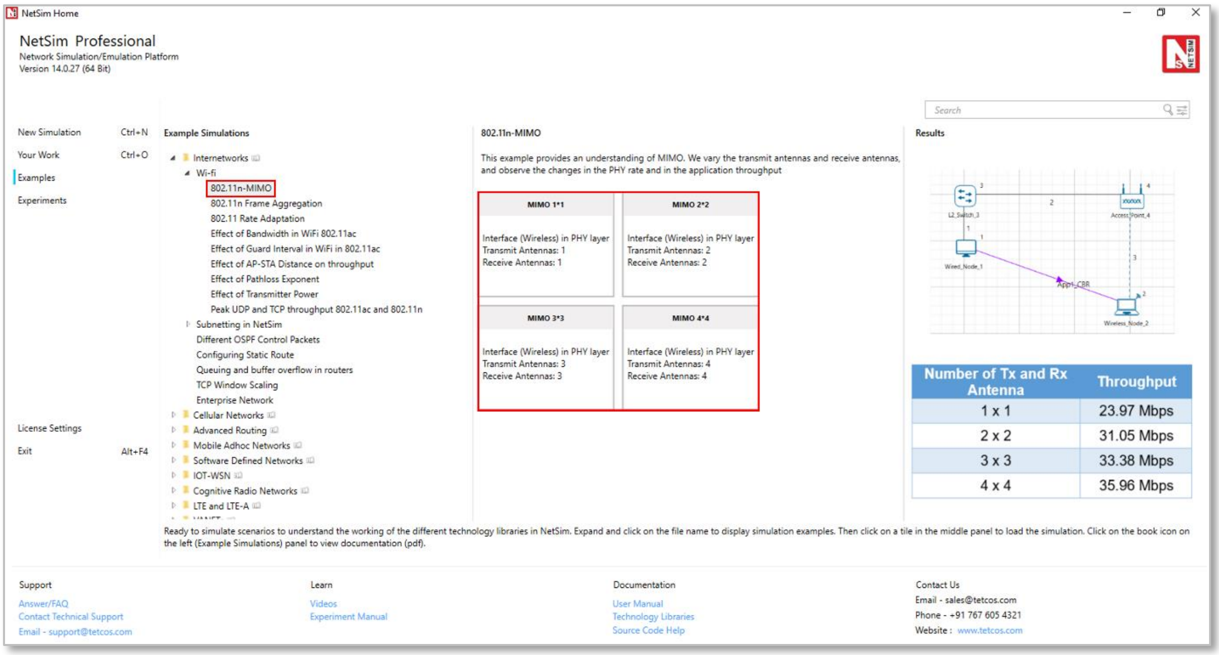
The same logic is extended as the number of devices increases.

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.

4.1 802.11n MIMO

Open NetSim, Select **Examples -> Internetworks -> Wi-Fi -> 802.11n-MIMO** then click on the tile in the middle panel to load the example shown in Figure 4-1.



NetSim Professional
Network Simulation/Emulation Platform
Version 14.0.27 (64 Bit)

Example Simulations

802.11n-MIMO

This example provides an understanding of MIMO. We vary the transmit antennas and receive antennas, and observe the changes in the PHY rate and in the application throughput

MIMO 1*1	MIMO 2*2
Interface (Wireless) in PHY layer Transmit Antennas: 1 Receive Antennas: 1	Interface (Wireless) in PHY layer Transmit Antennas: 2 Receive Antennas: 2
MIMO 3*3	**MIMO 4*4**
Interface (Wireless) in PHY layer Transmit Antennas: 3 Receive Antennas: 3	Interface (Wireless) in PHY layer Transmit Antennas: 4 Receive Antennas: 4

Results

Number of Tx and Rx Antenna	Throughput
1 x 1	23.97 Mbps
2 x 2	31.05 Mbps
3 x 3	33.38 Mbps
4 x 4	35.96 Mbps

Ready to simulate scenarios to understand the working of the different technology libraries in NetSim. Expand and click on the file name to display simulation examples. Then click on a tile in the middle panel to load the simulation. Click on the book icon on the left (Example Simulations) panel to view documentation (pdf).

Support
Answer/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
Website : www.tetcos.com

Figure 4-1: List of scenarios for the example of 802.11n-MIMO

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

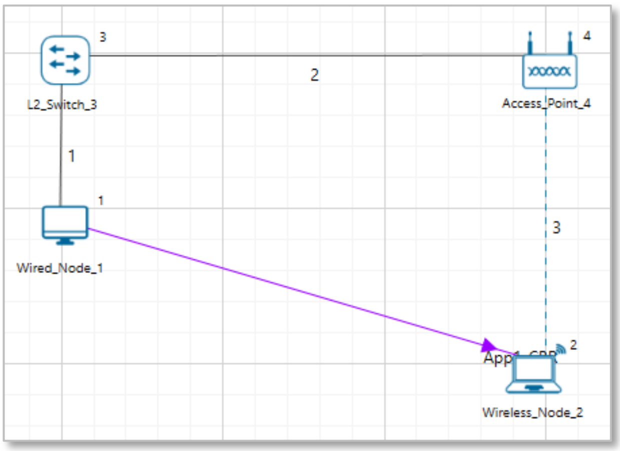


Figure 4-2: Network set up for studying the 802.11n-MIMO

Network Settings

1. Environment Grid length: 50m * 50m
2. Distance between AP and Wireless node is 20m.
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 802.11n and No. of Tx and Rx Antennas 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)
5. Channel Characteristics a Path Loss only, Path Loss Model a Log Distance and Path loss Exponent a 3. (Wireless Link Properties).
6. Click on Set Traffic tab and set CBR application with 50Mbps generation rate. (Set Inter Arrival Time: 233 (micro sec)).
7. Set transport protocol to UDP.
8. Enable Plots.
9. Simulate for 10 sec and check the throughput.
10. Go back to the scenario and increase the Number of Tx and Rx Antenna 1*1 to 2*2, 3*3, 4*4 respectively and check the throughput in the results window.

Results and Discussion

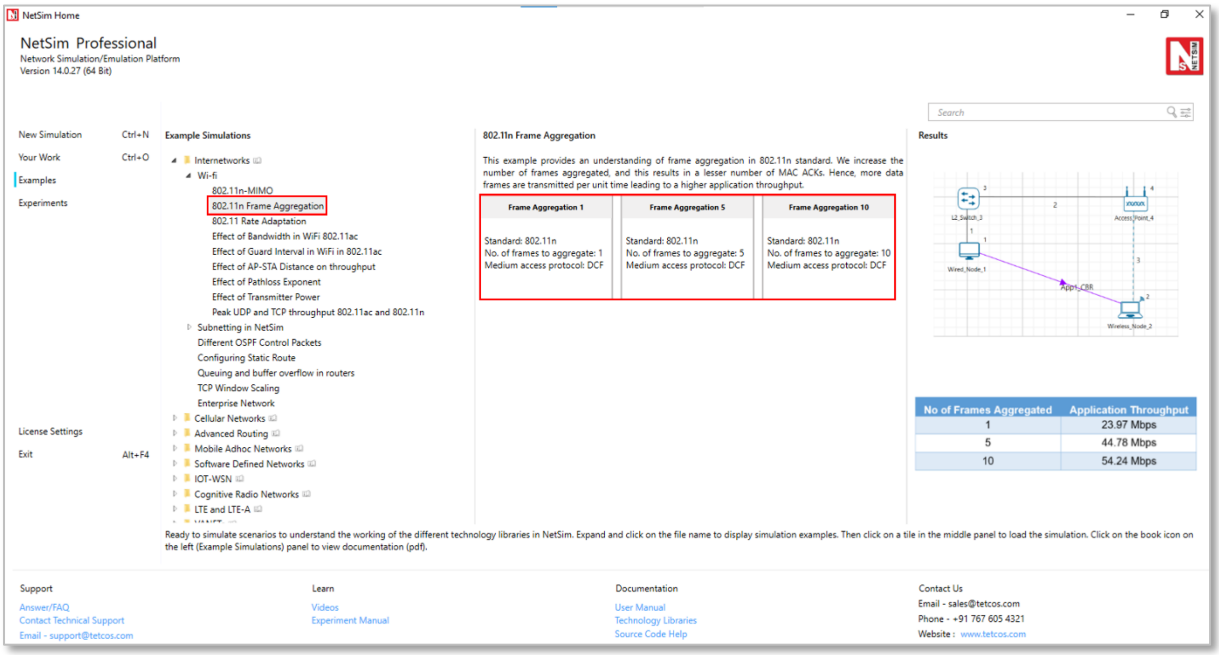
Number of Tx and Rx Antenna	Throughput
1 x 1	23.97 Mbps
2 x 2	31.04 Mbps
3 x 3	33.38 Mbps
4 x 4	35.95 Mbps

Table 4-1: 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 Transmitting Antennas and Receiving Antennas in PHY Data rate (link capacity) and hence leads to an increase in application throughput.

4.2 Frame aggregation in 802.11n

Open NetSim and Select **Examples > Internetworks > Wi-Fi > 802.11n Frame Aggregation** then click on the tile in the middle panel to load the example as shown in Figure 4-3.



NetSim Home

NetSim Professional
Network Simulation/Emulation Platform
Version 14.0.27 (64 Bit)

New Simulation Ctrl+N
Your Work Ctrl+O
Examples
Experiments
License Settings
Exit Alt+F4

Example Simulations

- Internetworks
  - Wi-fi
    - 802.11n-MIMO
    - 802.11n Frame Aggregation
    - 802.11 Rate Adaptation
    - Effect of Bandwidth in WiFi 802.11ac
    - Effect of Guard Interval in WiFi in 802.11ac
    - Effect of AP-STA Distance on throughput
    - Effect of Pathloss Exponent
    - Effect of Transmitter Power
    - Peak UDP and TCP throughput 802.11ac and 802.11n
  - Subnetting in NetSim
  - Different OSPF Control Packets
  - Configuring Static Route
  - Queuing and buffer overflow in routers
  - TCP Window Scaling
  - Enterprise Network
- Cellular Networks
- Advanced Routing
- Mobile Adhoc Networks
- Software Defined Networks
- IOT-WSN
- Cognitive Radio Networks
- LTE and LTE-A

802.11n Frame Aggregation

This example provides an understanding of frame aggregation in 802.11n standard. We increase the number of frames aggregated, and this results in a lesser number of MAC ACKs. Hence, more data frames are transmitted per unit time leading to a higher application throughput.

Frame Aggregation 1	Frame Aggregation 5	Frame Aggregation 10
Standard: 802.11n No. of frames to aggregate: 1 Medium access protocol: DCF	Standard: 802.11n No. of frames to aggregate: 5 Medium access protocol: DCF	Standard: 802.11n No. of frames to aggregate: 10 Medium access protocol: DCF

Search

Results

No of Frames Aggregated	Application Throughput
1	23.97 Mbps
5	44.78 Mbps
10	54.24 Mbps

Ready to simulate scenarios to understand the working of the different technology libraries in NetSim. Expand and click on the file name to display simulation examples. Then click on a tile in the middle panel to load the simulation. Click on the book icon on the left (Example Simulations) panel to view documentation (pdf).

Support
Answer/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
Website : www.tetcos.com

Figure 4-3: List of scenarios for the example of 802.11n frame aggregation

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

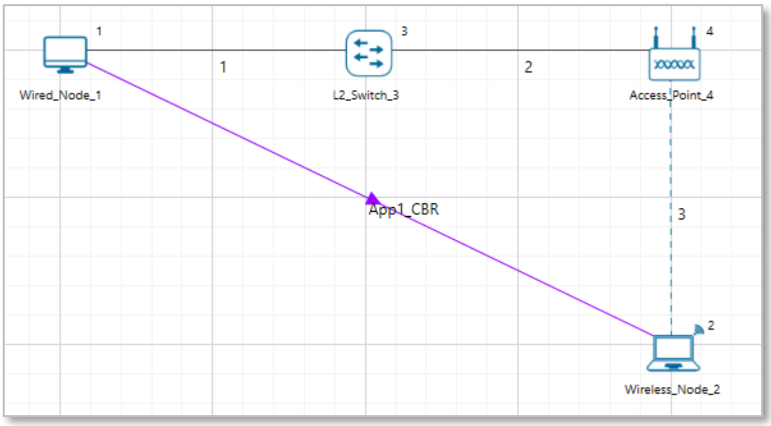


Figure 4-4: Network set up for studying the 802.11n frame aggregation

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. Click on Set Traffic tab and set CBR Application with 100 Mbps Generation Rate (Packet Size: 1460, Inter Arrival Time: 116µs)
5. 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 Frames to Aggregate)

7. Channel Characteristics: Path Loss Only, Path Loss Model: Log Distance, and Path Loss Exponent: 3. (Wireless Link Properties)
8. Enable the Plots and Packet trace and run the simulation for 10s. Then 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	23.97 Mbps
5	44.77 Mbps
10	54.24 Mbps

Table 4-2: 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 packet status to successful and 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.

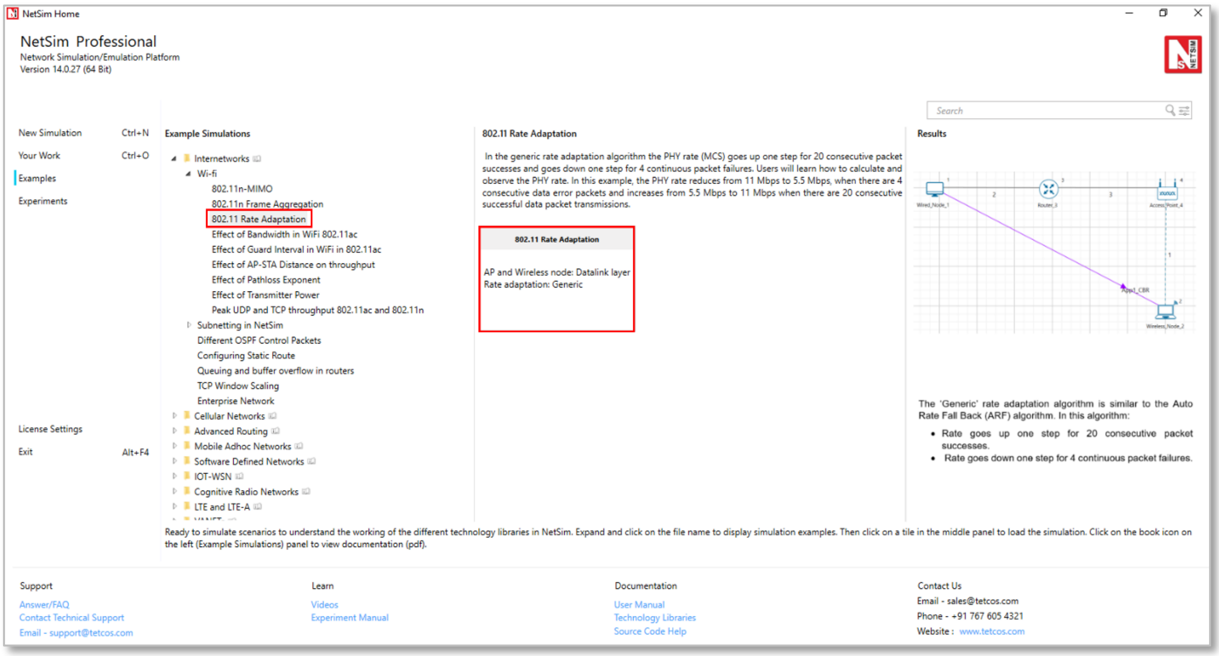
4.3 Rate Adaptation in 802.11b

NetSim rate adaptation is explained in section 3.1.21 of this document. This experiment can be performed with Standard and Pro version of NetSim since it involves code modification.

User should uncomment the following line (line #38) in IEEE802_11.h in 802.11 project and rebuild the code and then perform this example.

```
#define _RECALCULATE_RX_SENSITIVITY_BASED_ON_PEP_
```

Open NetSim, Select **Examples > Internetworks > Wi-Fi > 802.11 Rate Adaptation** then click on the tile in the middle panel to load the example as shown in Figure 4-5.



802.11 Rate Adaptation

In the generic rate adaptation algorithm the PHY rate (MCS) goes up one step for 20 consecutive packet successes and goes down one step for 4 continuous packet failures. Users will learn how to calculate and observe the PHY rate. In this example, the PHY rate reduces from 11 Mbps to 5.5 Mbps, when there are 4 consecutive data error packets and increases from 5.5 Mbps to 11 Mbps when there are 20 consecutive successful data packet transmissions.

802.11 Rate Adaptation

AP and Wireless node: Datalink layer
Rate adaptation: Generic

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.

Ready to simulate scenarios to understand the working of the different technology libraries in NetSim. Expand and click on the file name to display simulation examples. Then click on a tile in the middle panel to load the simulation. Click on the book icon on the left (Example Simulations) panel to view documentation (pdf).

Email - support@tetcos.com

Contact Us
Email - sales@tetcos.com
Phone - +91 767 605 4321
Website : www.tetcos.com

Figure 4-5: List of scenarios for the example of 802.11 rate adaptation

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

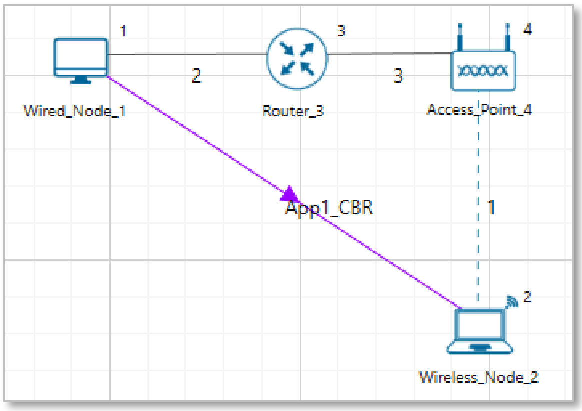


Figure 4-6: Network set up for studying the Wi-Fi Rate Adaptation

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. Channel Characteristics → Path Loss only, Path Loss Model → Log Distance and Path loss Exponent → 3.25. (Wireless Link Properties)
9. CBR application with 10Mbps generation rate (Set Packet Size: 1460 Bytes, Inter Arrival Time: 1168 micro sec)
10. Simulate for 10 sec.

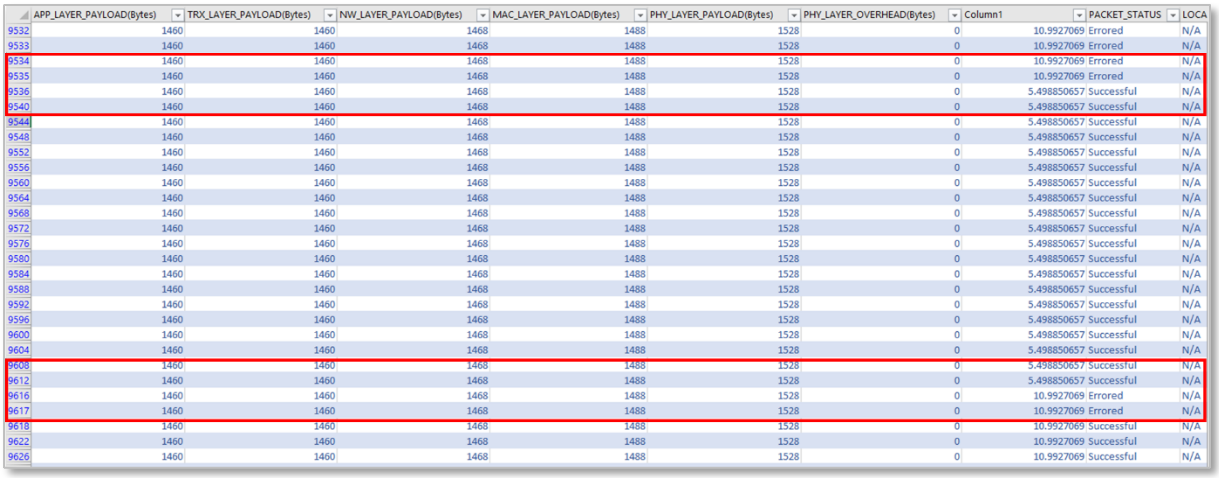
Results and Discussion

Open Packet Trace and filter Packet Type to CBR, Transmitter_ID to Access Point 3 andf filter the packet status to errored and successful 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 8.4.2 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 4-7: Packet Trace

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

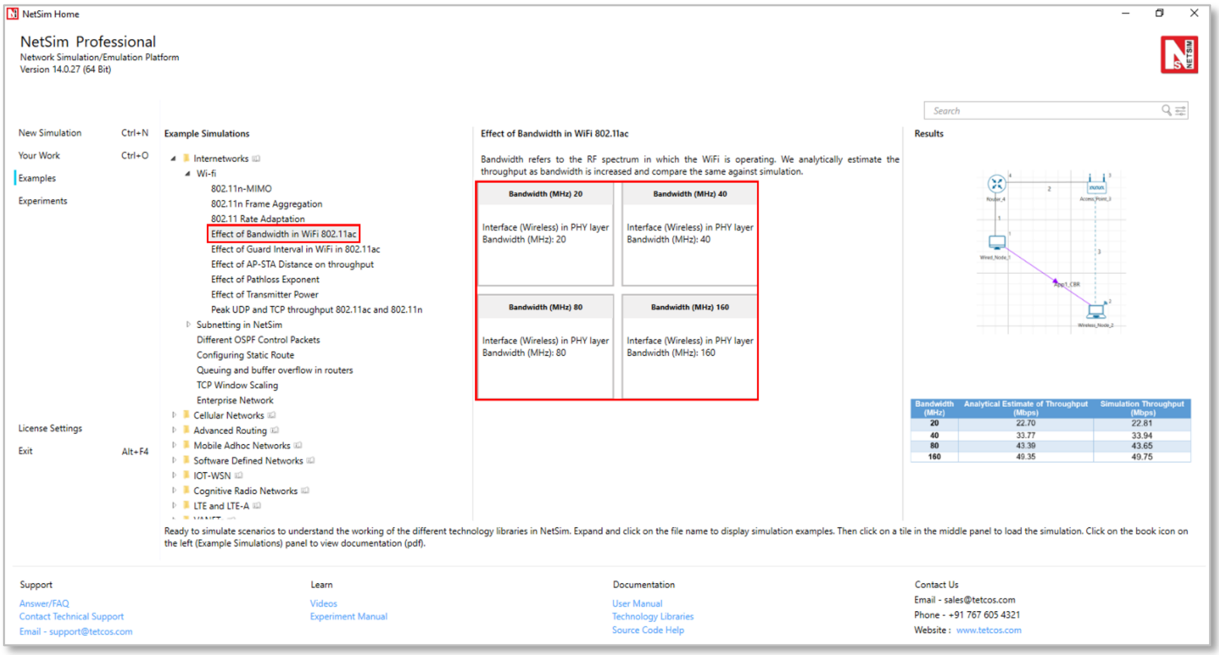
- Rate goes up one step for 20 consecutive packet successes.
- Rate goes down one step for 4 continuous packet failures

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.

4.4 Effect of Bandwidth and Guard Interval in Wi-Fi 802.11ac

4.4.1 Effect of Bandwidth

Open NetSim and Select **Examples > Internetworks > Wi-Fi > Effect of bandwidth in Wi-Fi 802.11ac** then click on the tile in the middle panel to load the example as shown in Figure 4-8.



Effect of Bandwidth in WiFi 802.11ac

Bandwidth refers to the RF spectrum in which the WiFi is operating. We analytically estimate the throughput as bandwidth is increased and compare the same against simulation.

Bandwidth (MHz) 20
Interface (Wireless) in PHY layer Bandwidth (MHz): 20

Bandwidth (MHz) 40
Interface (Wireless) in PHY layer Bandwidth (MHz): 40

Bandwidth (MHz) 80
Interface (Wireless) in PHY layer Bandwidth (MHz): 80

Bandwidth (MHz) 160
Interface (Wireless) in PHY layer Bandwidth (MHz): 160

Bandwidth (MHz)	Analytical Estimate of Throughput (Mbps)	Simulation Throughput (Mbps)
20	22.70	22.81
40	33.77	33.94
80	43.39	43.65
160	49.35	49.75

Ready to simulate scenarios to understand the working of the different technology libraries in NetSim. Expand and click on the file name to display simulation examples. Then click on a tile in the middle panel to load the simulation. Click on the book icon on the left (Example Simulations) panel to view documentation (pdf).

Email - support@tetcos.com

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

Figure 4-8: List of scenarios for the example of effect of bandwidth in Wi-Fi 802.11ac

The following network diagram illustrates what the NetSim UI displays when you open the example configuration file as shown Figure 4-9.

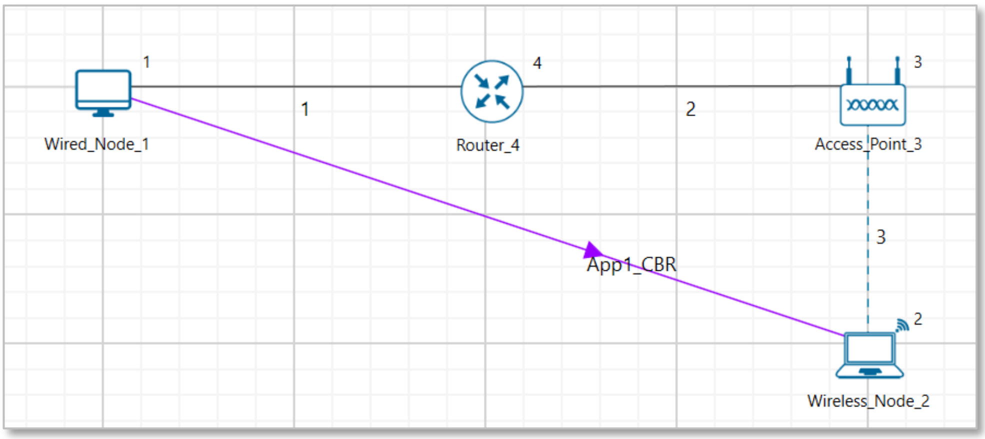


Figure 4-9: Network set up for studying the effect of bandwidth in Wi-Fi 802.11ac

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. Set transmitter power as 40mW under Wireless Interface->Transmitter Power properties of the access point and wireless node.
8. Enable packet trace and plots.
9. 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

10. Run simulation for 10s and see Application Throughput in the Results Window.
11. Go back to the scenario and increase the Bandwidth 20 to 40, 80, 160 respectively and check the 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 4-10.

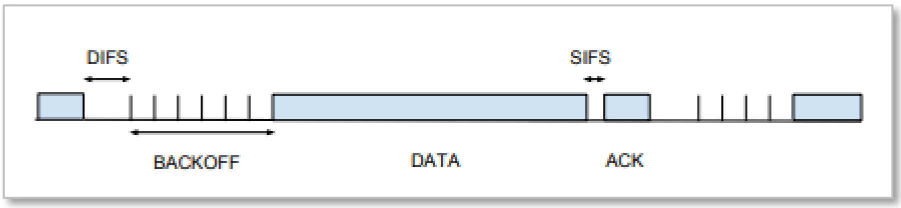


Figure 4-10: Timing diagram for WLAN

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

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

$$Average\ time\ per\ packet\ \ (\mu s)$$
$$= DIFS\ +\ Average\ Backoff\ time\ +\ Packet\ Transmission\ Time\ +\ SIFS$$
$$+\ Ack\ Transmission\ Time$$

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

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

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

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

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

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:

$$Phy\ rate\ \text{(802.11ac)} = Phy\_layer\_payload * 8/(phy\ end\ time - phy\ arrival\ time - 44)$$

Results and Discussion

Bandwidth (MHz)	Analytical Estimate of Throughput (Mbps)	Simulation Throughput (Mbps)

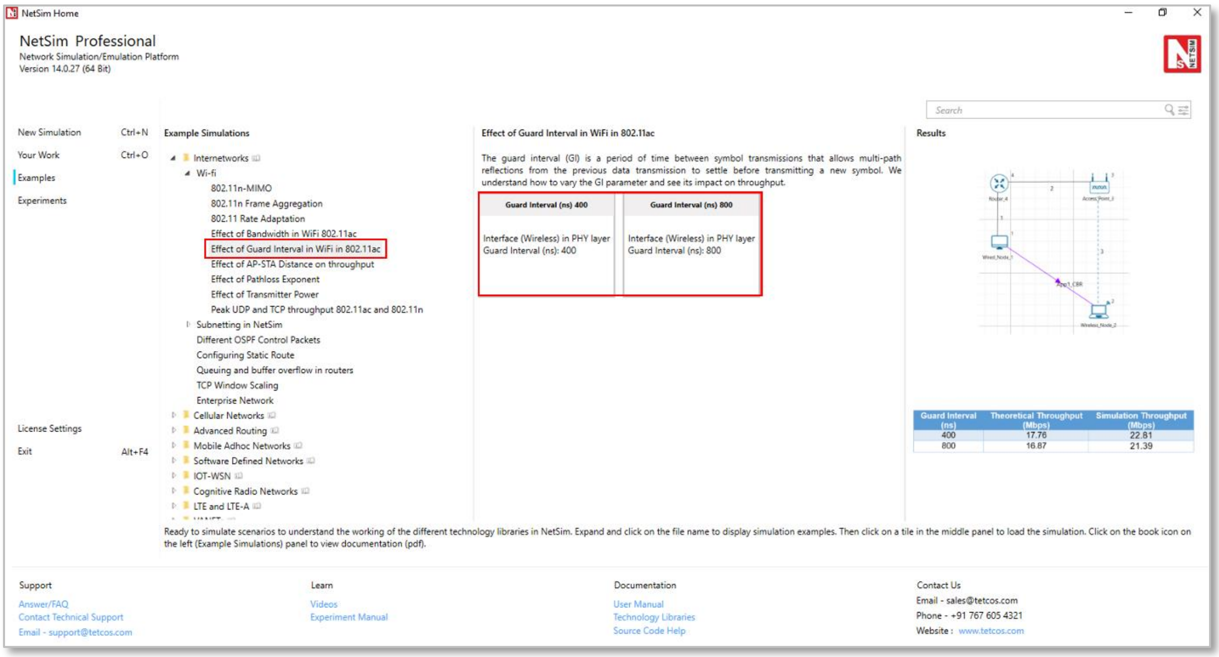
20	22.70	22.80
40	33.77	33.94
80	43.39	43.64
160	49.35	49.75

Table 4-3: Result comparison of different bandwidth vs. Analytical 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.

4.4.2 Effect of Guard Interval

Open NetSim and click on **Examples > Internetworks > Wi-Fi > Effect of Guard Interval in Wi-Fi 802.11ac** then click on the tile in the middle panel to load the example as shown in Figure 4-11.



Effect of Guard Interval in WiFi in 802.11ac

The guard interval (GI) is a period of time between symbol transmissions that allows multi-path reflections from the previous data transmission to settle before transmitting a new symbol. We understand how to vary the GI parameter and see its impact on throughput.

Guard Interval (ns) 400

Interface (Wireless) in PHY layer
Guard Interval (ns): 400

Guard Interval (ns) 800

Interface (Wireless) in PHY layer
Guard Interval (ns): 800

Guard Interval (ns)	Theoretical Throughput (Mbps)	Simulation Throughput (Mbps)
400	17.76	22.81
800	16.87	21.39

Ready to simulate scenarios to understand the working of the different technology libraries in NetSim. Expand and click on the file name to display simulation examples. Then click on a tile in the middle panel to load the simulation. Click on the book icon on the left (Example Simulations) panel to view documentation (pdf).

Figure 4-11: List of scenarios for the example of effect of guard interval in Wi-Fi 802.11ac

The following network diagram illustrates what the NetSim UI displays when you open the example configuration file as shown Figure 4-12.

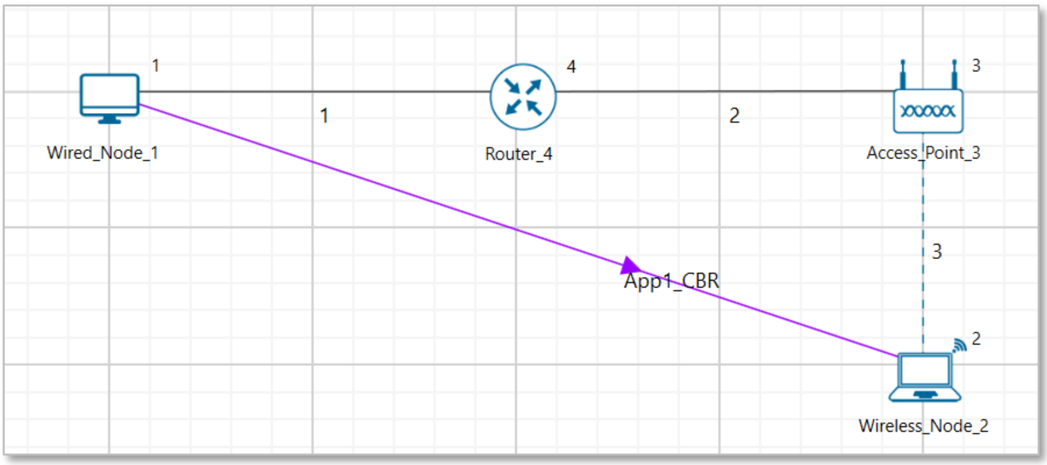


Figure 4-12: Network set up for studying the guard interval in wi-fi in Wi-Fi 802.11ac

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 Bit Error rate and Propagation delay to zero under wired link properties.
7. Set transmitter power as 40mW under Wireless Interface->Transmitter Power properties of the access point and wireless node.
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 microseconds). Generation rate can be calculated by using the formula below:

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

$$(\mu s) = 1460\ (Bytes) \times \frac{8}{116} (\mu s) {\sim} 100 Mbps$$

11. Run simulation for 10s and note down the throughput.
12. Go back to the scenario and increase the Guard interval to 400 to 800 and check the throughput in the results window

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

Results

Guard Interval (ns)	Theoretical Throughput (Mbps)	Simulation Throughput (Mbps)
400	17.76	22.80
800	16.87	21.38

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

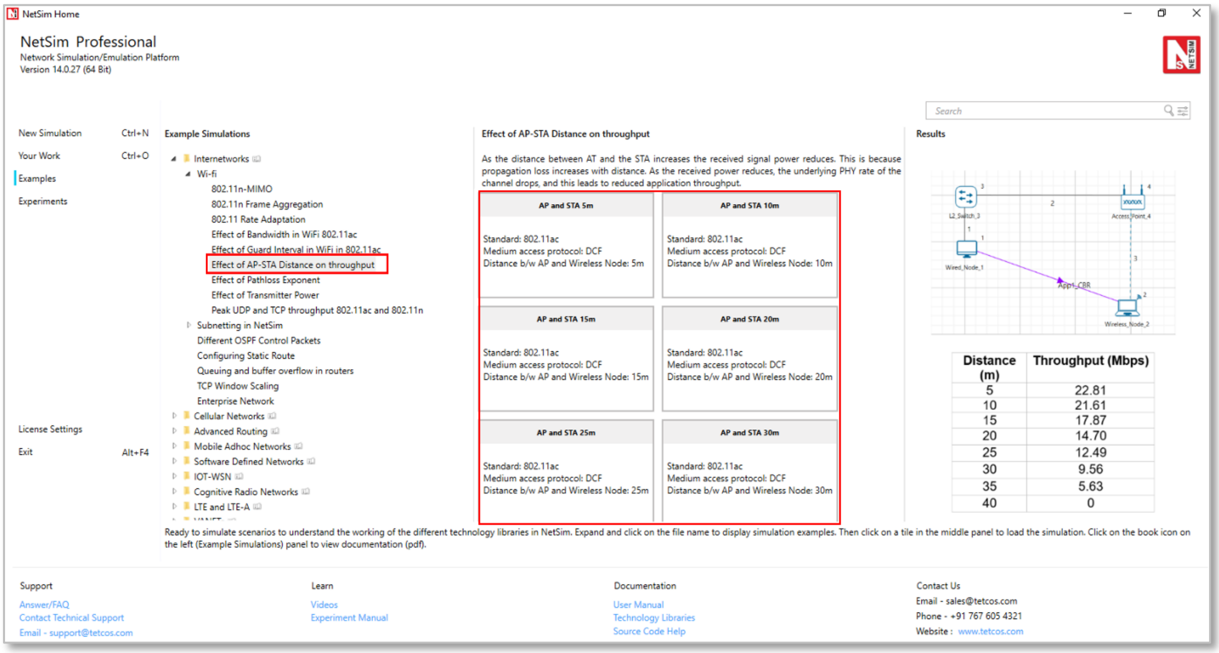
4.5 Factors affecting WLAN PHY Rate

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)

4.5.1 Effect of AP-STA Distance on throughput

Open NetSim and Select **Examples > Internetworks > Wi-Fi > Effect of AP STA Distance on throughput** then click on the tile in the middle panel to load the example as shown in Figure 4-13.



Effect of AP-STA Distance on throughput

As the distance between AT and the STA increases the received signal power reduces. This is because propagation loss increases with distance. As the received power reduces, the underlying PHY rate of the channel drops, and this leads to reduced application throughput.

AP and STA 5m
Standard: 802.11ac
Medium access protocol: DCF
Distance b/w AP and Wireless Node: 5m

AP and STA 10m
Standard: 802.11ac
Medium access protocol: DCF
Distance b/w AP and Wireless Node: 10m

AP and STA 15m
Standard: 802.11ac
Medium access protocol: DCF
Distance b/w AP and Wireless Node: 15m

AP and STA 20m
Standard: 802.11ac
Medium access protocol: DCF
Distance b/w AP and Wireless Node: 20m

AP and STA 25m
Standard: 802.11ac
Medium access protocol: DCF
Distance b/w AP and Wireless Node: 25m

AP and STA 30m
Standard: 802.11ac
Medium access protocol: DCF
Distance b/w AP and Wireless Node: 30m

Distance (m)	Throughput (Mbps)
5	22.81
10	21.61
15	17.87
20	14.70
25	12.49
30	9.56
35	5.63
40	0

Ready to simulate scenarios to understand the working of the different technology libraries in NetSim. Expand and click on the file name to display simulation examples. Then click on a tile in the middle panel to load the simulation. Click on the book icon on the left (Example Simulations) panel to view documentation (pdf).

Figure 4-13: List of scenarios for the example effect of AP-STA distance on throughput

The following network diagram illustrates, what the NetSim UI displays when you open the example configuration file see Figure 4-14.

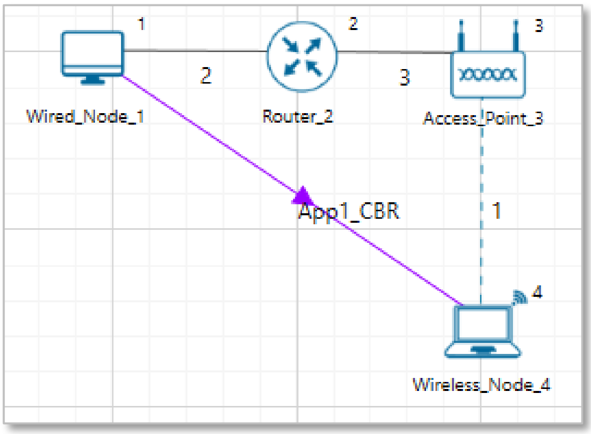


Figure 4-14: Network set up for studying the Effect of AP-STA Distance on throughput.

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.

Network Settings

1. Environment Grid length: 60m x 60m
2. Distance between Access Point and the Wireless Node is set to 5m
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. Enable the plots and run the simulation for 10s.
10. Go back to the scenario and increase the distance as per result table and Run simulation for 10s.

Results

Distance (m)	Throughput (Mbps)
5	22.81
10	21.61
15	17.87
20	14.70
25	12.49
30	9.56
35	5.63
40	0

Table 4-5: Result comparison of different distance vs. throughput

Plot

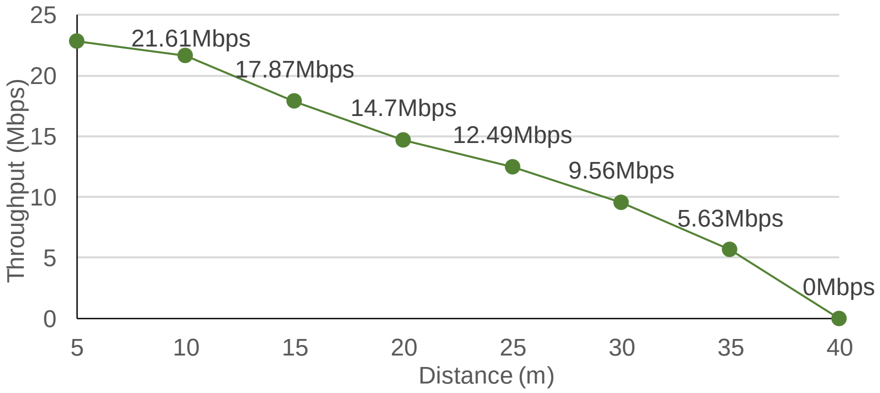
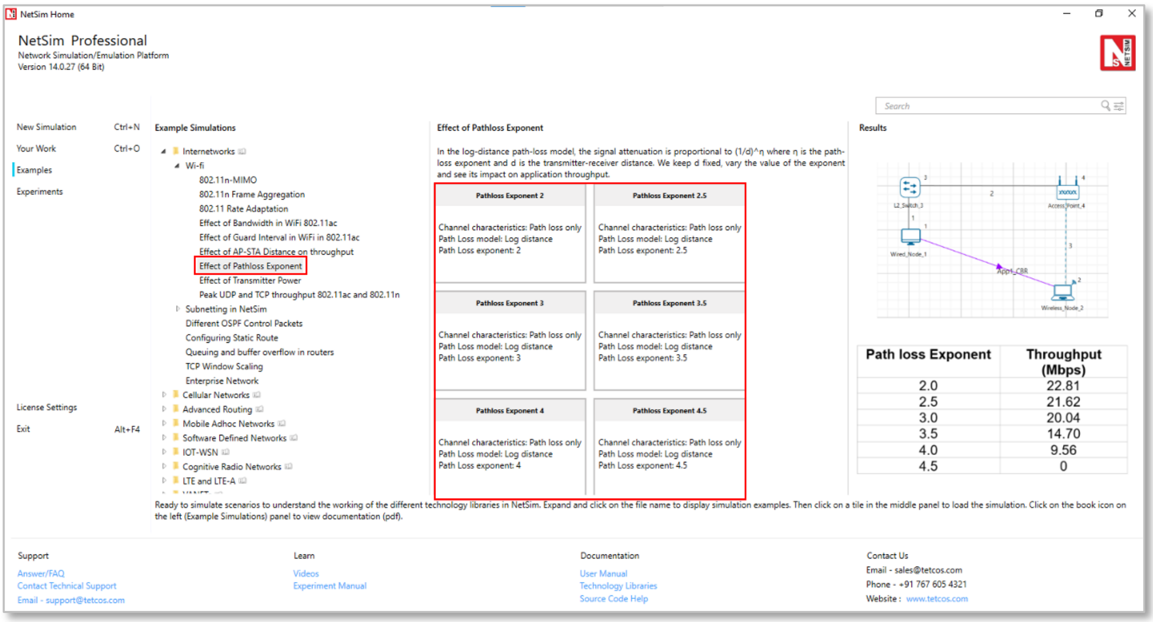


Figure 4-15: Plot of Throughput vs Distance

4.5.2 Effect of Pathloss Exponent

Open NetSim and Select **Examples > Internetworks > Wi-Fi > Effect of Pathloss Exponent** then click on the tile in the middle panel to load the example as shown in Figure 4-16.



NetSim Professional
Network Simulation/Emulation Platform
Version 14.0.27 (64 Bit)

New Simulation Ctrl+N
Your Work Ctrl+O
Examples
Experiments
License Settings
Exit Alt+F4

Example Simulations

- Internetworks
  - Wi-fi
    - 802.11n-MIMO
    - 802.11n Frame Aggregation
    - 802.11 Rate Adaptation
    - Effect of Bandwidth in WiFi 802.11ac
    - Effect of Guard Interval in WiFi in 802.11ac
    - Effect of AP-STA Distance on throughput
    - Effect of Pathloss Exponent
    - Effect of Transmitter Power
    - Peak UDP and TCP throughput 802.11ac and 802.11n
  - Subnetting in NetSim
  - Different OSPF Control Packets
  - Configuring Static Route
  - Queuing and buffer overflow in routers
  - TCP Window Scaling
  - Enterprise Network
- Cellular Networks
- Advanced Routing
- Mobile Adhoc Networks
- Software Defined Networks
- IOT-WSN
- Cognitive Radio Networks
- LTE and LTE-A

Effect of Pathloss Exponent

In the log-distance path-loss model, the signal attenuation is proportional to (1/d)^η where η is the path-loss exponent and d is the transmitter-receiver distance. We keep d fixed, vary the value of the exponent and see its impact on application throughput.

Pathloss Exponent 2
Channel characteristics: Path loss only
Path Loss model: Log distance
Path Loss exponent: 2

Pathloss Exponent 2.5
Channel characteristics: Path loss only
Path Loss model: Log distance
Path Loss exponent: 2.5

Pathloss Exponent 3
Channel characteristics: Path loss only
Path Loss model: Log distance
Path Loss exponent: 3

Pathloss Exponent 3.5
Channel characteristics: Path loss only
Path Loss model: Log distance
Path Loss exponent: 3.5

Pathloss Exponent 4
Channel characteristics: Path loss only
Path Loss model: Log distance
Path Loss exponent: 4

Pathloss Exponent 4.5
Channel characteristics: Path loss only
Path Loss model: Log distance
Path Loss exponent: 4.5

Results

Path loss Exponent	Throughput (Mbps)
2.0	22.81
2.5	21.62
3.0	20.04
3.5	14.70
4.0	9.56
4.5	0

Ready to simulate scenarios to understand the working of the different technology libraries in NetSim. Expand and click on the file name to display simulation examples. Then click on a tile in the middle panel to load the simulation. Click on the book icon on the left (Example Simulations) panel to view documentation (pdf).

Support
Answer/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
Website : www.tetcos.com

Figure 4-16: List of scenarios for the example of effect of pathloss exponent

The following network diagram illustrates, what the NetSim UI displays when you open the example configuration file as shown Figure 4-17.

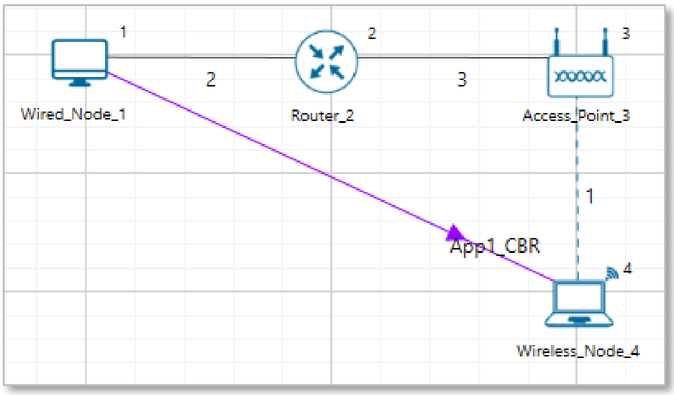


Figure 4-17: Network set up for studying the effect of pathloss exponent

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.

Network Settings

1. Environment Grid length: 40m x 40m
2. Distance between Access Point and the Wireless Node is set to 20m
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. In NetSim GUI Plots are Enabled and Run simulation for 10s.
9. Go back to the scenario and increase the Path Loss Exponent from 2 to 2.5, 3, 3.5, 4, and 4.5 respectively and Run simulation for 10s.

Results

Path loss Exponent	Throughput (Mbps)
2.0	22.81
2.5	21.61

3.0	20.04
3.5	14.70
4.0	9.56
4.5	0

Table 4-6: Result comparison of different pathloss exponent value vs. throughput

Plot

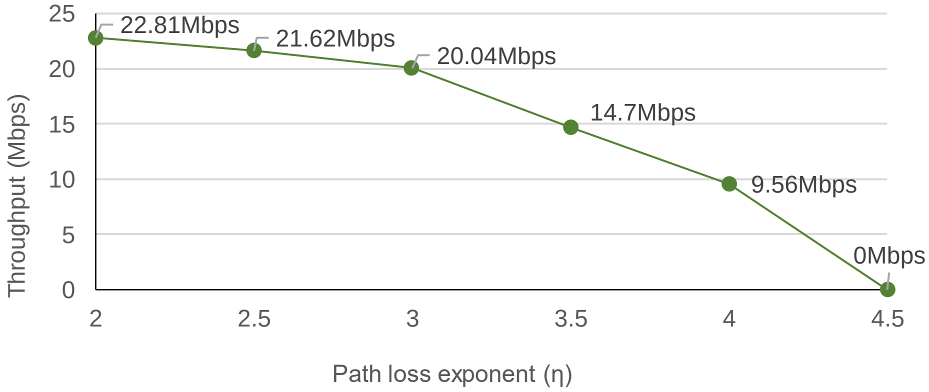
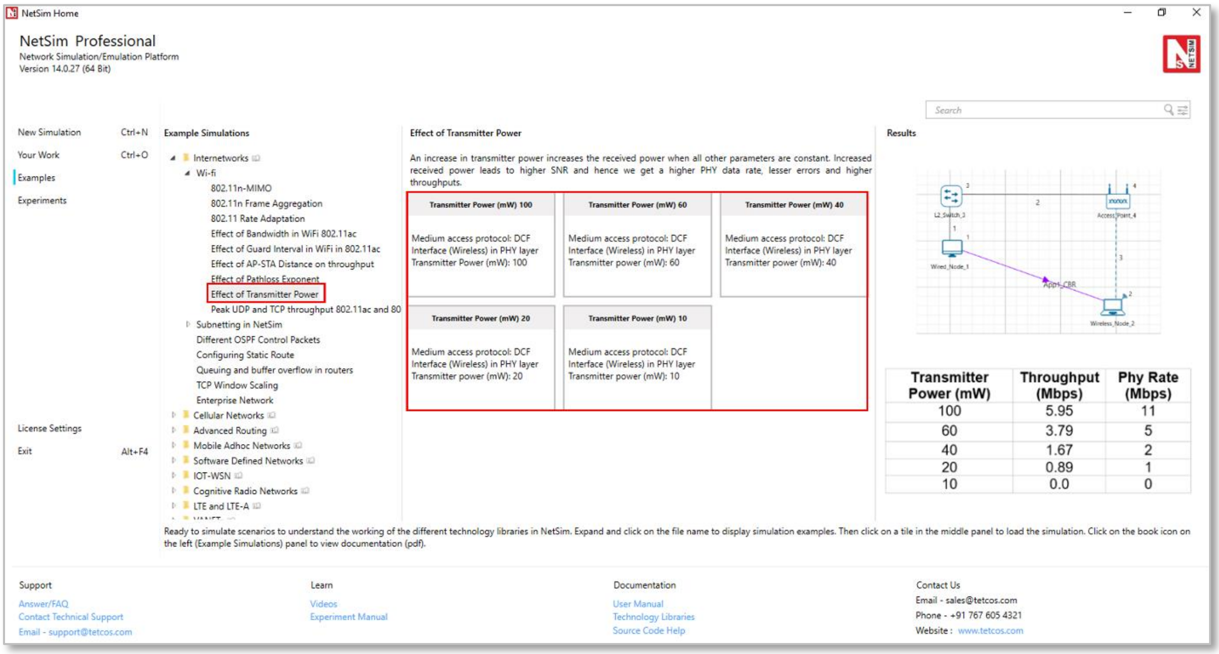


Figure 4-18: Plot of Throughput vs Path loss Exponent

4.5.3 Effect of Transmitter power

Open NetSim and Select **Examples->Internetworks->Wi-Fi-> Effect of Transmitter Power** then click on the tile in the middle panel to load the example as shown in Figure 4-19.



NetSim Home

NetSim Professional
Network Simulation/Emulation Platform
Version 14.0.27 (64 Bit)

New Simulation	Ctrl+N
Your Work	Ctrl+O
Examples	
Experiments	
License Settings	
Exit	Alt+F4

Example Simulations

- Internetworks
  - Wi-fi
    - 802.11n-MIMO
    - 802.11n Frame Aggregation
    - 802.11 Rate Adaptation
    - Effect of Bandwidth in WiFi 802.11ac
    - Effect of Guard Interval in WiFi in 802.11ac
    - Effect of AP-STA Distance on throughput
    - Effect of Pathloss Exponent
    - Effect of Transmitter Power
    - Peak UDP and TCP throughput 802.11ac and 80
  - Subnetting in NetSim
  - Different OSPF Control Packets
  - Configuring Static Route
  - Queuing and buffer overflow in routers
  - TCP Window Scaling
  - Enterprise Network
- Cellular Networks
- Advanced Routing
- Mobile Adhoc Networks
- Software Defined Networks
- IOT-WSN
- Cognitive Radio Networks
- LTE and LTE-A

Effect of Transmitter Power

An increase in transmitter power increases the received power when all other parameters are constant. Increased received power leads to higher SNR and hence we get a higher PHY data rate, lesser errors and higher throughputs.

Transmitter Power (mW) 100
Medium access protocol: DCF
Interface (Wireless) in PHY layer
Transmitter Power (mW): 100

Transmitter Power (mW) 60
Medium access protocol: DCF
Interface (Wireless) in PHY layer
Transmitter power (mW): 60

Transmitter Power (mW) 40
Medium access protocol: DCF
Interface (Wireless) in PHY layer
Transmitter power (mW): 40

Transmitter Power (mW) 20
Medium access protocol: DCF
Interface (Wireless) in PHY layer
Transmitter power (mW): 20

Transmitter Power (mW) 10
Medium access protocol: DCF
Interface (Wireless) in PHY layer
Transmitter power (mW): 10

Results

Transmitter Power (mW)	Throughput (Mbps)	Phy Rate (Mbps)
100	5.95	11
60	3.79	5
40	1.67	2
20	0.89	1
10	0.0	0

Ready to simulate scenarios to understand the working of the different technology libraries in NetSim. Expand and click on the file name to display simulation examples. Then click on a tile in the middle panel to load the simulation. Click on the book icon on the left (Example Simulations) panel to view documentation (pdf).

Support
Answer/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
Website : www.tetcos.com

Figure 4-19: List of scenarios for the example of effect of transmitter power

The following network diagram illustrates, what the NetSim UI displays when you open the example configuration file see Figure 4-20.

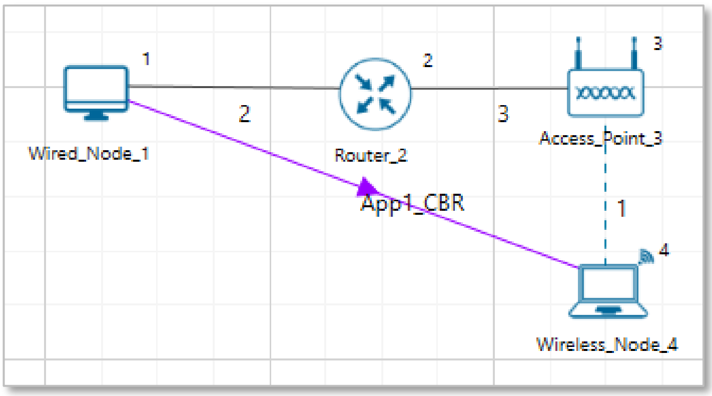


Figure 4-20: Network set up for studying the effect of transmitter power

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.

Network Settings

1. Environment Grid length: 55m x 55m
2. Distance between Access Point and the Wireless Node is set to 35m
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: 3.5
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. Enable the Plots and Run the simulation for 10s
9. Go back to the scenario and decrease the Transmitter Power to 100, 60, 40, 20 and 10 respectively and run simulation for 10s. See that, there is a decrease in the Throughput gradually.

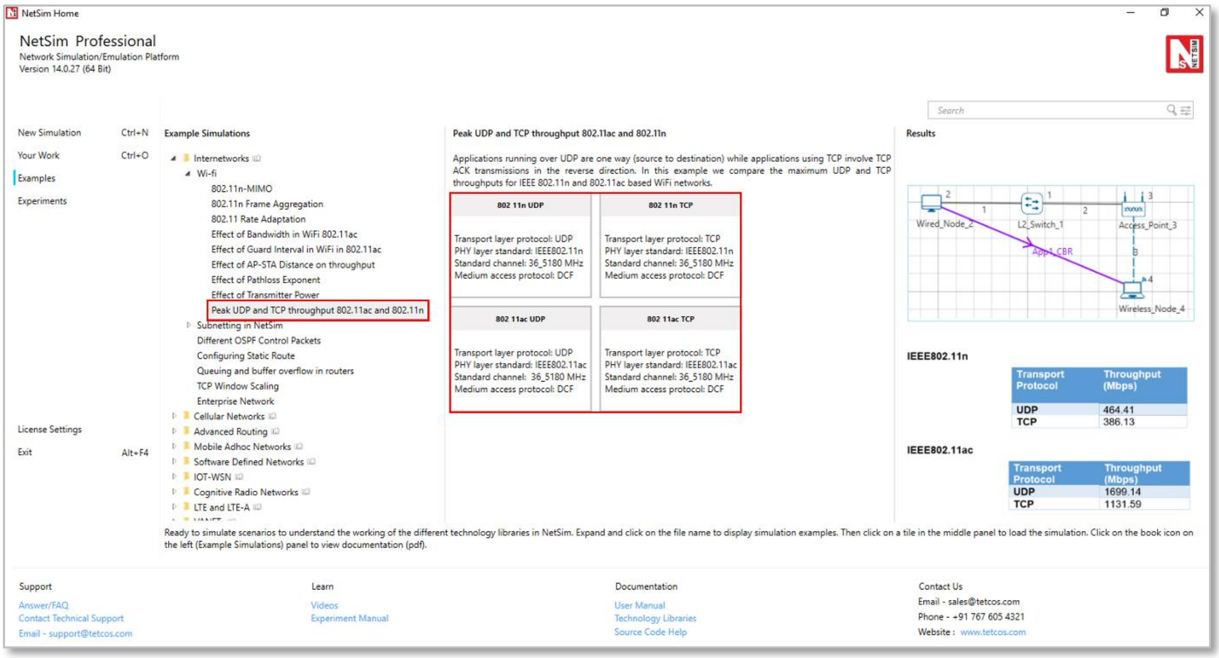
Results

Transmitter Power (mW)	Throughput (Mbps)	Phy Rate (Mbps)
100	5.94	11
60	3.79	5
40	1.67	2
20	0.89	1
10	0.0	0

Table 4-7: Result comparison of different transmitter power vs. throughput

4.6 Peak UDP and TCP throughput 802.11ac and 802.11n

Open NetSim, Select **Examples ->Internetworks-> Wi-Fi -> Peak UDP and TCP throughput 802.11ac and 802.11n** then click on the tile in the middle panel to load the example as shown Figure 4-21.



NetSim Home

NetSim Professional
Network Simulation/Emulation Platform
Version 14.0.27 (64 Bit)

New Simulation Ctrl+N
Your Work Ctrl+O
Examples
Experiments
License Settings
Exit Alt+F4

Example Simulations

- Internetworks
  - Wi-fi
    - 802.11n-MIMO
    - 802.11n Frame Aggregation
    - 802.11 Rate Adaptation
    - Effect of Bandwidth in WiFi 802.11ac
    - Effect of Guard Interval in WiFi in 802.11ac
    - Effect of AP-STA Distance on throughput
    - Effect of Pathloss Exponent
    - Effect of Transmitter Power
    - Peak UDP and TCP throughput 802.11ac and 802.11n
  - Subnetting in NetSim
  - Different OSPF Control Packets
  - Configuring Static Route
  - Queuing and buffer overflow in routers
  - TCP Window Scaling
  - Enterprise Network
- Cellular Networks
- Advanced Routing
- Mobile Adhoc Networks
- Software Defined Networks
- IOT-WSN
- Cognitive Radio Networks
- LTE and LTE-A

Peak UDP and TCP throughput 802.11ac and 802.11n

Applications running over UDP are one way (source to destination) while applications using TCP involve TCP ACK transmissions in the reverse direction. In this example we compare the maximum UDP and TCP throughputs for IEEE 802.11n and 802.11ac based WiFi networks.

802 11n UDP
Transport layer protocol: UDP
PHY layer standard: IEEE802.11n
Standard channel: 36_5180 MHz
Medium access protocol: DCF

802 11n TCP
Transport layer protocol: TCP
PHY layer standard: IEEE802.11n
Standard channel: 36_5180 MHz
Medium access protocol: DCF

802 11ac UDP
Transport layer protocol: UDP
PHY layer standard: IEEE802.11ac
Standard channel: 36_5180 MHz
Medium access protocol: DCF

802 11ac TCP
Transport layer protocol: TCP
PHY layer standard: IEEE802.11ac
Standard channel: 36_5180 MHz
Medium access protocol: DCF

Search

Results

IEEE802.11n

Transport Protocol	Throughput (Mbps)
UDP	464.41
TCP	386.13

IEEE802.11ac

Transport Protocol	Throughput (Mbps)
UDP	1699.14
TCP	1131.59

Ready to simulate scenarios to understand the working of the different technology libraries in NetSim. Expand and click on the file name to display simulation examples. Then click on a tile in the middle panel to load the simulation. Click on the book icon on the left (Example Simulations) panel to view documentation (pdf).

Support
Answer/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
Website : www.tetcos.com

Figure 4-21: List of scenarios for the example of Peak UDP and TCP throughput 802.11ac and 802.11n

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

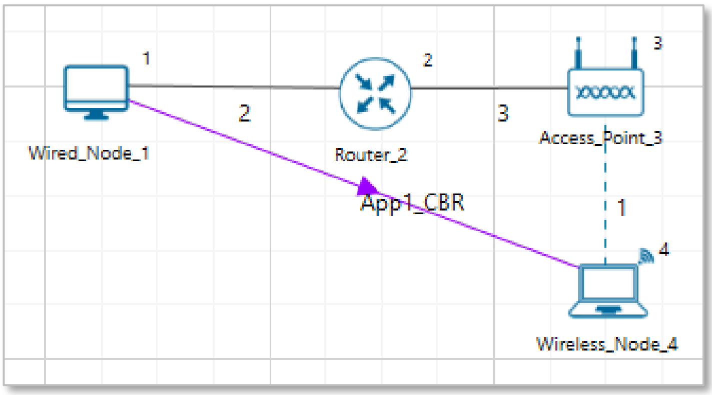


Figure 4-22: Network set up for studying the Peak UDP and TCP throughput 802.11ac and 802.11n

4.6.1 IEEE802.11n

Network Settings

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

Interface Parameters	
Physical Layer	
Standard	IEEE802.11n
No. of Frames to aggregate	64
Standard Channel	36 (5180MHz)
Buffer Size	100MB
Guard Interval	400ns
Bandwidth	40 MHz
Frequency Band	5 GHz
Transmitter Power	100mW
Antenna Gain	0
Antenna height	1m
Reference distance (d0)	1m
Transmitting Antennas	4
Receiving Antennas	4
Datalink Layer	
Rate Adaptation	False
Short Retry Limit	7
Long Retry Limit	4
Dott11_RTSThreshold	3000bytes
Medium Access Protocol	DCF

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

2. Set wired link properties as shown below.
   - Uplink speed and Downlink speed (Mbps)- 1000 Mbps.
   - Uplink BER and Downlink BER – 0.
   - Uplink and Downlink Propagation Delay(µs) – 10.
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 5 sec. After simulation completes go to metrics window and note down throughput value from application metrics.

Go Back to **802.11n UDP** Scenario and 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 5 sec and note down throughput value from application metrics.

Results

Transport Protocol	Throughput (Mbps)
UDP	443.16
TCP	346.85

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

Plot

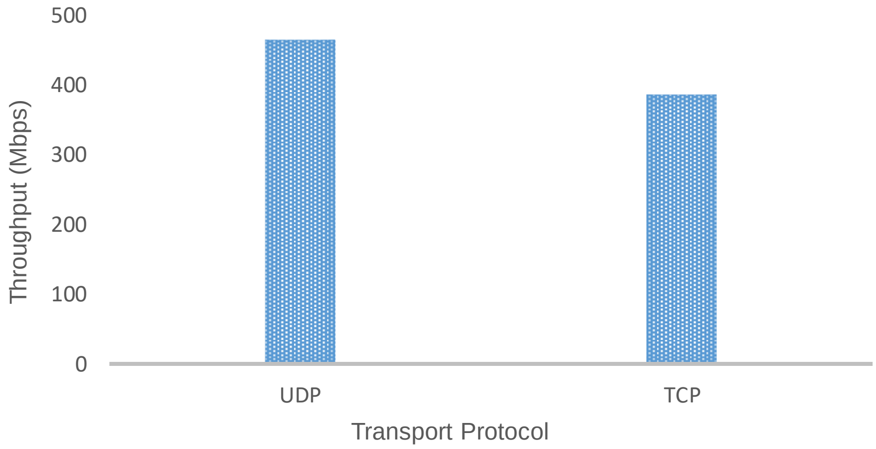


Figure 4-23: Plot of Throughput (Mbps) Vs. Transport Protocol for IEEE802.11n

4.6.2 IEEE802.11ac

Network Settings

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

Interface Parameters	
Standard	IEEE802.11ac
No. of Frames to aggregated	1024
Standard Channel	36 (5180MHz)
Rate Adaptation	False
Short Retry Limit	7
Long Retry Limit	4
Dott11_RTSThreshold	3000bytes
Medium Access Protocol	DCF
Buffer Size (Access Point)	100MB
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 wired link properties as shown below.

- Uplink speed and Downlink speed (Mbps)- 10000 Mbps.
- Uplink BER and Downlink BER – 0.
- Uplink and Downlink Propagation Delay(µs) – 10.

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)	1.93
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.

Go Back to the **802.11ac UDP** Scenario and 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

Transport Protocol	Throughput (Mbps)
UDP	5361.42
TCP	3207.06

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

Plot

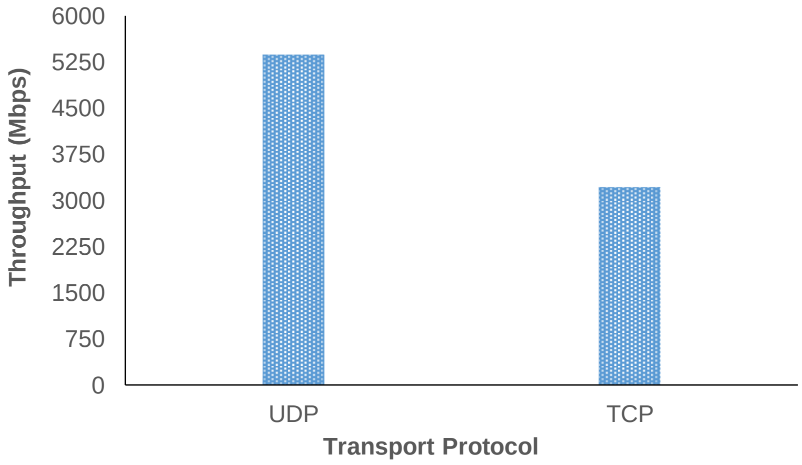


Figure 4-24: Plot of Throughput (Mbps) Vs. Transport Protocol for IEEE802.11ac

4.7 Configuring IP addresses, subnets and applying firewall rules based on subnets using Class B IP addresses

4.7.1 Introduction

4.7.1.1 IP Addressing

A unique number ID is assigned to one of the hosts or interfaces in a network. An IP address is an address used to uniquely identify a device on an IP network. An IPv4 address is made up of 32 binary bits, which can be divided into a network portion and a host portion with the help of a subnet mask. These 32 binary bits are further broken into four octets (1 octet = 8 bits). Each octet is converted to decimal and separated by a period (dot). For this reason, an IP address is said to be expressed in dotted decimal format (for example, 172.16.0.0). The value in each octet ranges from 0 to 255 in decimal, or 00000000 - 11111111 in binary.

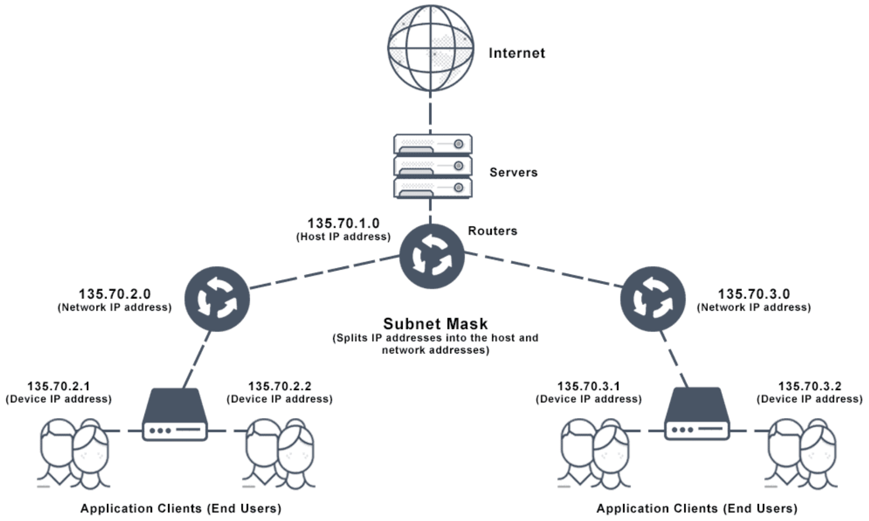


Figure 4-25: Subnet mask diagram

4.7.2 IP address classes

Class	Address range	Subnet masking	Leading Bits	Max number of Networks	Max number of Hosts	Application
IP CLASS A	1 to 126	255.0.0.0	8	128	16,777,214	Used for a large number of hosts.
IP CLASS B	128 to 191	255.255.0.0	16	16384	65,534	Used for medium-size networks.
IP CLASS C	192 to 223	255.255.255.0	24	2097157	254	Used for local area network.
IP CLASS D	224 to 239	N/A	N/A	N/A	N/A	Reserve for multi-tasking.
IP CLASS E	240 to 254	N/A	N/A	N/A	N/A	This class is reserved for R&D

Table 4-14: IP address class and its application

4.7.3 Configuring Class-B address in NetSim

The default IP addressing in NetSim is class A addressing. However, users can reconfigure (static) IP addresses with different classes. These settings are available in the network layer of end nodes, routers, and L3 switches.

Example 1: In this example, we have created a simple LAN network and modified the IP address of the routers and the users in the LAN network. Refer Figure 4-25. In this we have used the IP address of range 172.16.0.1-172.16.255.254 with a mask 255.255.0.0. When its put differently, the IP is 172.16.0.0/16.

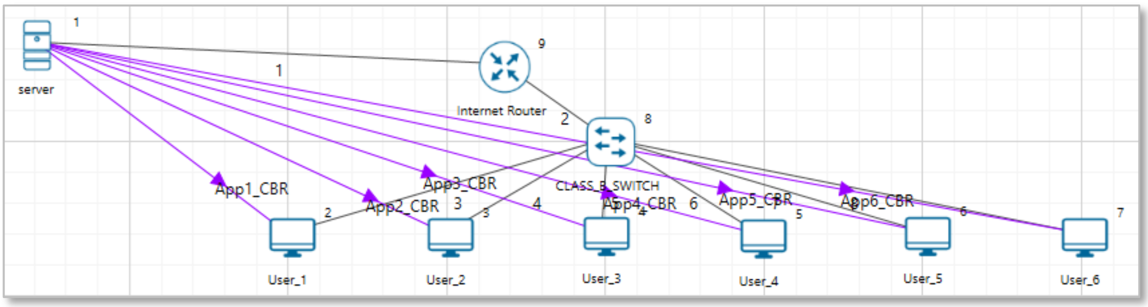


Figure 4-26: IPv4 Class B IP addressing

4.7.4 Subnetting

Subnetting is the practice of dividing a network into two or more smaller networks. It increases the routing efficiency, enhances the security of the network, and reduces the size of the broadcast domain.

A subnet mask is used to divide an IP address into two parts. One part identifies the host (computer), and the other part identifies the network to which it belongs. For better understanding of how an IP address and subnet masks work, look at an IP address and see how it's organized.

Subnet	Host	Slash Method
1	65536	/16
2	32768	/17
4	16384	/18
8	8192	/19
16	4096	/20
32	2048	/21
64	1024	/22
128	512	/23
256	256	/24
512	128	/25
1024	64	/26
2048	32	/27
4096	16	/28
8192	8	/29
16384	4	/30
32768	2	/31
65536	1	/32

Table 4-15: Class-B Subnetting using the slash method

Network ID	Subnet Mask	Host ID Range	Usable Host	Broadcast ID
172.16.0.0	/18	172.16.0.1-172.16.63.254	16382	172.16.63.255
172.16.64.0	/18	172.16.64.1-172.16.127.254	16382	172.16.127.255
172.16.128.0	/18	172.16.128.1-172.16.192.254	16382	172.16.192.255

172.16.192.0	/18	172.16.192.1-172.16.255.254	16382	172.16.255.255

Table 4-16: Using subnet mask 255.255.192.0i.e., /18 creating 4 different subnets with 16382 usable hosts

4.7.5 Configuring Class-B subnetting

We provide two examples to explain Class B sets. The example shows how to create 4 Subnets with 16382 Hosts using: (i) A single switch and (ii) Multiple switches

a. Subnets using single switch: Note that IP address and subnet masks are configured. The application (traffic) flow is configured for intra-subnet communications.

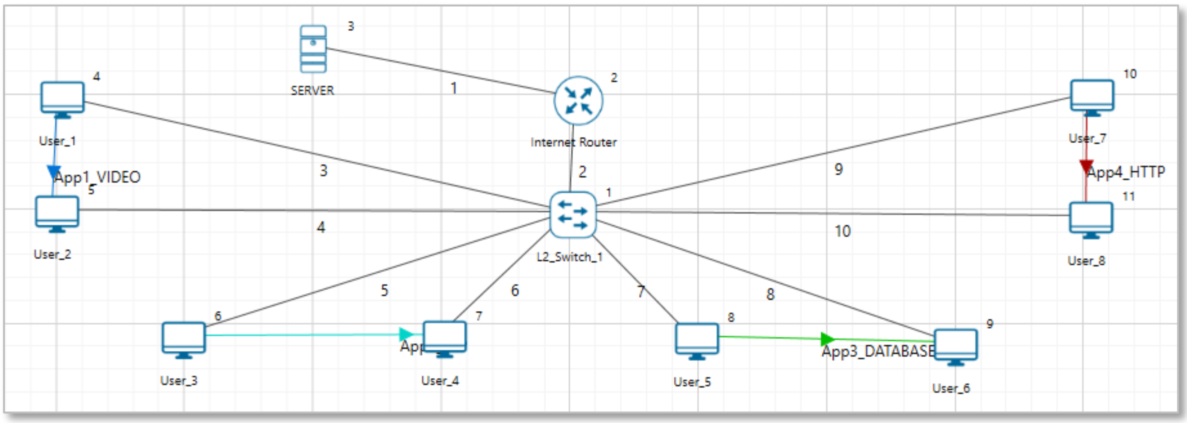
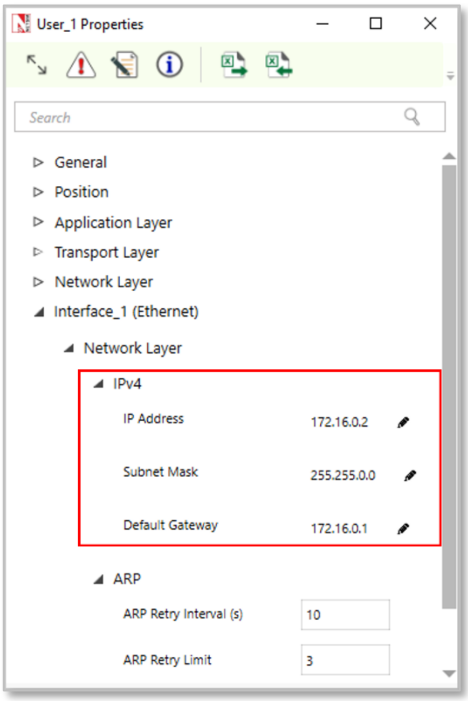


Figure 4-27: Pair of users communicating with each other belong to separate subnet per Table 4-16.

Configuring IP addresses and subnets in NetSim is as simple as configuring it in MS Operating System. The devices in NetSim are configurable via GUI, to set the IP and subnet, users need to modify the Network Layer as shown below.



IP Address 172.16.0.2

Subnet Mask 255.255.0.0

Default Gateway 172.16.0.1

ARP Retry Interval (s) 10

ARP Retry Limit 3

Figure 4-28: Configuring IP address and subnet mask in network layer of device in NetSim

b. Subnets using multiple switches: Here subnets have been configured using multiple switches. In the given example as shown in Figure 4-29, we have considered 4 departments in a university campus, by configuring subnets for CS, EC, MECH, and EE. Application (traffic flow) is set for both intra and inter-subnet communication.

Department Name	IP Address Range
Computer Science (CS)	172.16.0.1-172.16.63.254
Electronics and Communication (EC)	172.16.64.1-172.16.127.254
Mechanical Engineering (ME)	172.16.128.1-172.16.192.254
Electrical Engineering **(**EE)	172.16.192.1-172.16.255.254

Table 4-17: subnets in a university based on Table 4-16

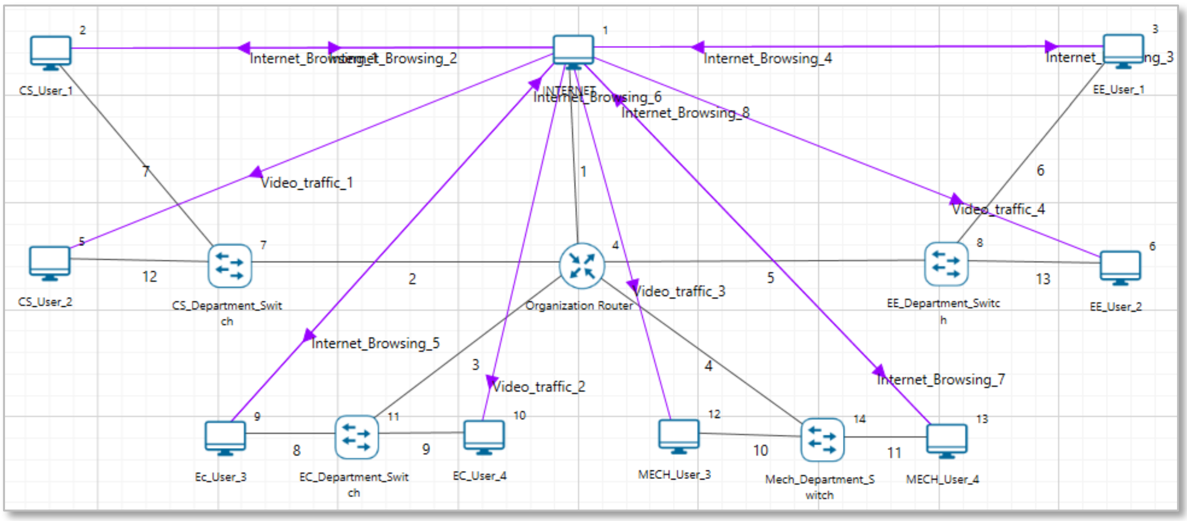


Figure 4-29: All the users are communicating from different subnets using a router and switch by configuring Class-B subnetting.

4.7.6 Firewall rules based on subnets.

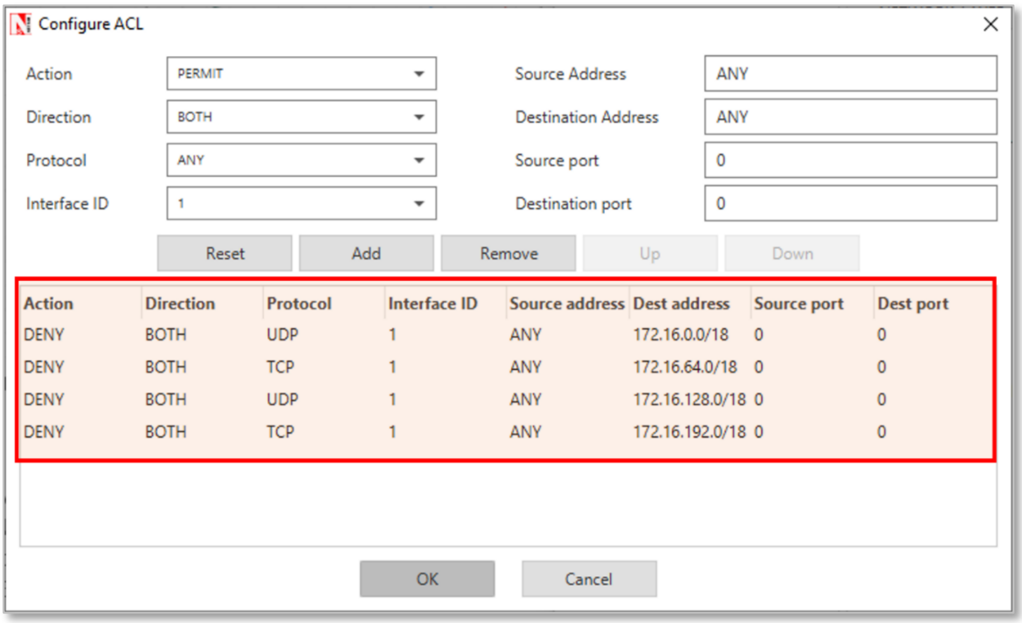
An important benefit of subnetting is security. Firewall/ACL rules can be configured at a subnet level. NetSim provides options for users to configure ACL/firewall rules i.e., to PERMIT or DENY traffic at a router based on (i) IP address/Network address (ii) Protocol (iii) Inbound / Outbound traffic.

Example 4: In this example, we have explained how users can set firewall rules to DENY traffic at a subnet level.

a. The topology considered here is the university network as shown in Figure 4-29.
b. The firewall/ACL rules are set in the Organization Router
c. ACL Rules:

  - For the CS-department Video traffic is denied
  - For the EC-department TCP traffic is denied
  - For the Mechanical department, Video Traffic is denied.
  - For the EE department TCP traffic is denied

d. These rules can be set in NetSim UI just by filling an ACL application of the router as shown below in Figure 4-30.



Action	PERMIT	Source Address	ANY
Direction	BOTH	Destination Address	ANY
Protocol	ANY	Source port	0
Interface ID	1	Destination port	0

Action	Direction	Protocol	Interface ID	Source address	Dest address	Source port	Dest port
DENY	BOTH	UDP	1	ANY	172.16.0.0/18	0	0
DENY	BOTH	TCP	1	ANY	172.16.64.0/18	0	0
DENY	BOTH	UDP	1	ANY	172.16.128.0/18	0	0
DENY	BOTH	TCP	1	ANY	172.16.192.0/18	0	0

Figure 4-30: Setting firewall rules in the organization router

4.8 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 4-18: Different OSPF Control Packets

1. The Hello packets.

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 neighbor’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.

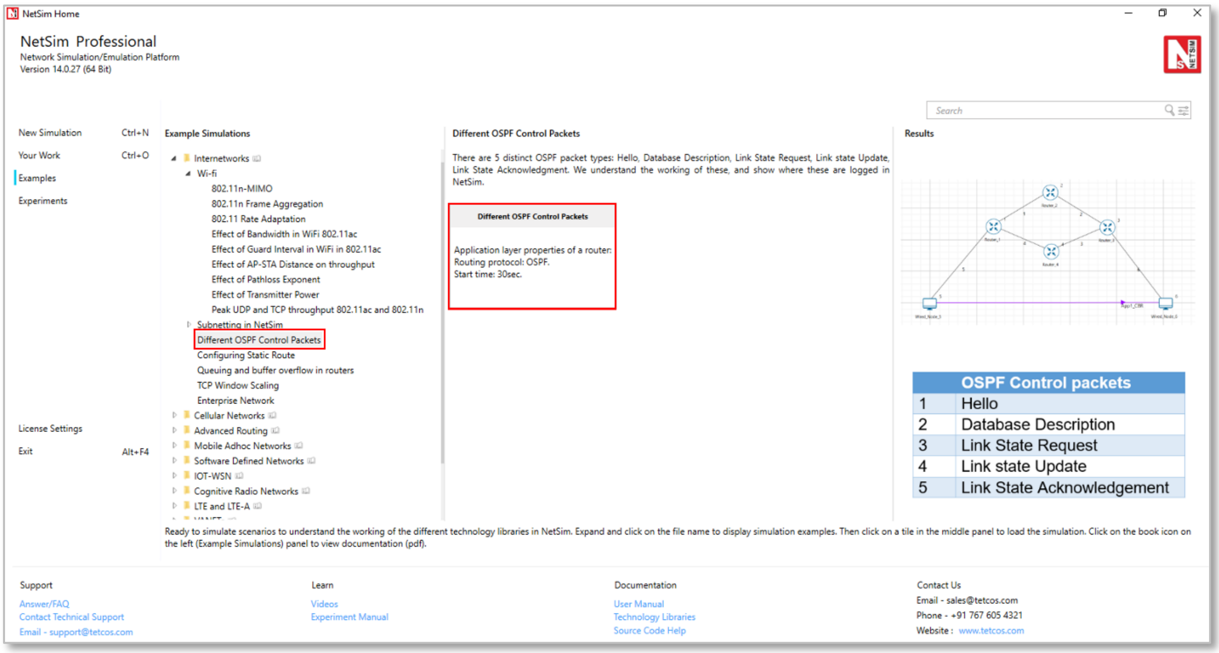
4. The Link State Update packet

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** then click on the tile in the middle panel to load the example as shown in Figure 4-31.



NetSim Home

NetSim Professional
Network Simulation/Emulation Platform
Version 14.0.27 (64 Bit)

Search

New Simulation Ctrl+N
Your Work Ctrl+O
Examples
Experiments

License Settings
Exit Alt+F4

Example Simulations

- Internetworks
  - Wi-fi
    - 802.11n-MIMO
    - 802.11n Frame Aggregation
    - 802.11 Rate Adaptation
    - Effect of Bandwidth in WiFi 802.11ac
    - Effect of Guard Interval in WiFi in 802.11ac
    - Effect of AP-STA Distance on throughput
    - Effect of Pathloss Exponent
    - Effect of Transmitter Power
    - Peak UDP and TCP throughput 802.11ac and 802.11n
  - Subnetting in NetSim
  - Different OSPF Control Packets
  - Configuring Static Route
  - Queuing and buffer overflow in routers
  - TCP Window Scaling
  - Enterprise Network
- Cellular Networks
- Advanced Routing
- Mobile Adhoc Networks
- Software Defined Networks
- IOT-WSN
- Cognitive Radio Networks
- LTE and LTE-A

Different OSPF Control Packets

There are 5 distinct OSPF packet types: Hello, Database Description, Link State Request, Link state Update, Link State Acknowledgment. We understand the working of these, and show where these are logged in NetSim.

Different OSPF Control Packets

Application layer properties of a router:
Routing protocol: OSPF.
Start time: 30sec.

Results

	OSPF Control packets
1	Hello
2	Database Description
3	Link State Request
4	Link state Update
5	Link State Acknowledgement

Ready to simulate scenarios to understand the working of the different technology libraries in NetSim. Expand and click on the file name to display simulation examples. Then click on a tile in the middle panel to load the simulation. Click on the book icon on the left (Example Simulations) panel to view documentation (pdf).

Support
Answer/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
Website : www.tetcos.com

Figure 4-31: List of scenarios for the example of different ospf control packets

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 4-32.

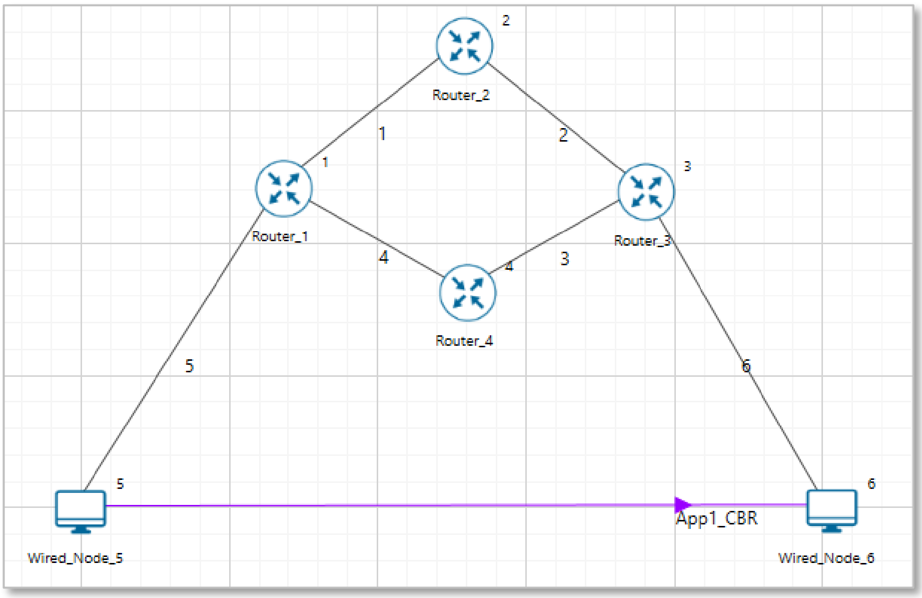


Figure 4-32: Network set up for studying the different OSPF control packets.

Network Settings

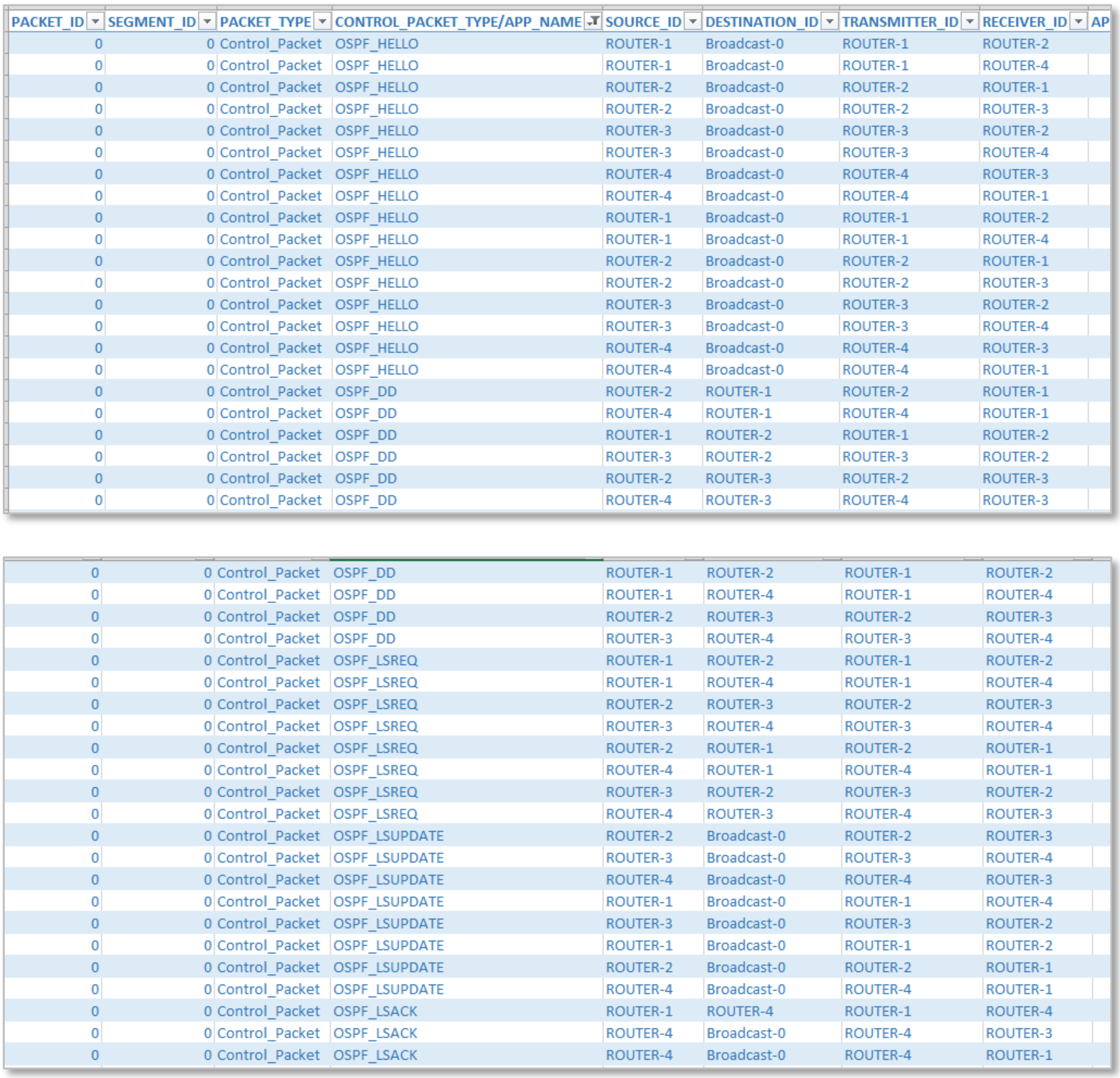
1. Set OSPF Routing protocol under Application_Layer properties of a router.
2. Configured CBR application with default properties and set application Start Time(s) to 30Sec.
3. Enabled Packet Trace and Plot.

4. Simulate for 100 sec.

Results and Discussion

The 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.

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 4-33.



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 4-33: different OSPF control packets in the packet Trace

4.9 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).

Note that the static route configuration running with TCP protocol requires reverse route configuration.

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:

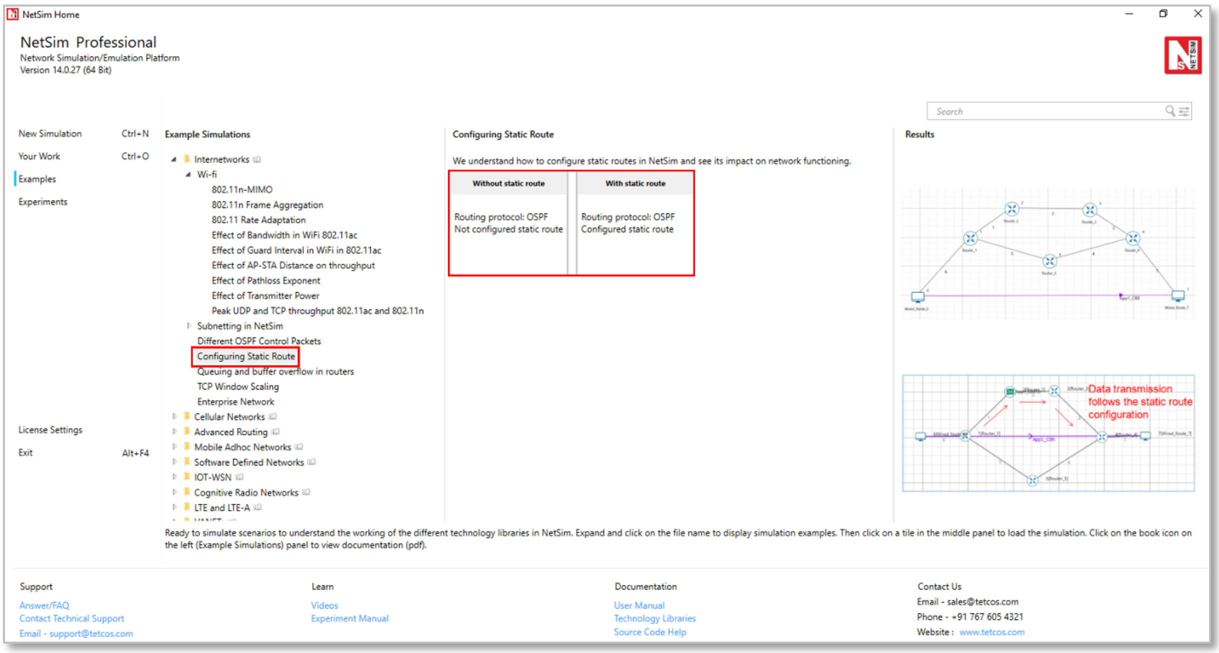
- Via static route GUI configuration
- Via file input (Interactive-Simulation/SDN)

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** then click on the tile in the middle panel to load the example as shown in Figure 4-34.



Configuring Static Route

We understand how to configure static routes in NetSim and see its impact on network functioning.

Without static route	With static route
Routing protocol: OSPF Not configured static route	Routing protocol: OSPF Configured static route

Ready to simulate scenarios to understand the working of the different technology libraries in NetSim. Expand and click on the file name to display simulation examples. Then click on a tile in the middle panel to load the simulation. Click on the book icon on the left (Example Simulations) panel to view documentation (pdf).

Email - support@tetcos.com

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

Figure 4-34: List of scenarios for the example of Configuring Static Route

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 4-35.

4.9.1 Without Static Route

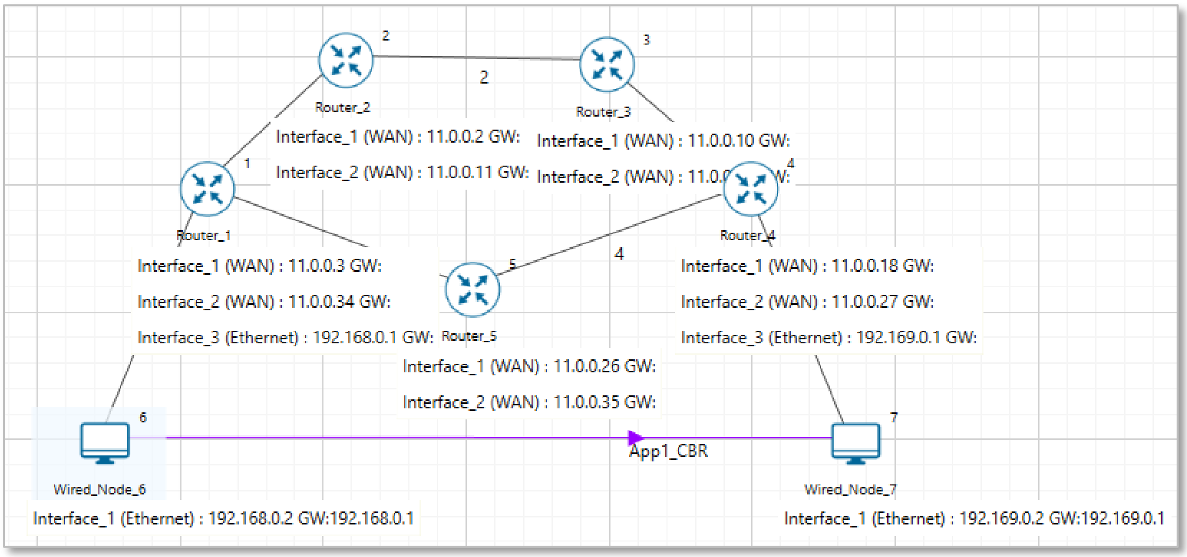
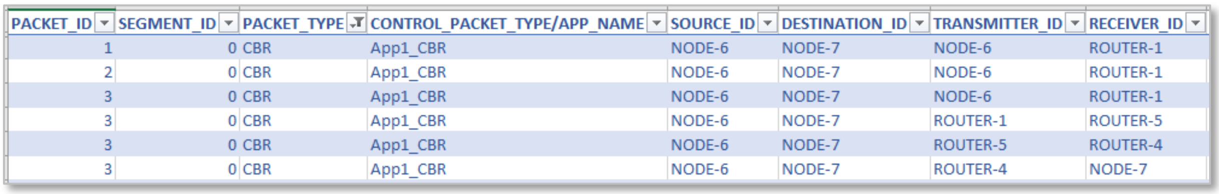

2
3
Router_2
2
Router_3
Interface_1 (WAN) : 11.0.0.2 GW:
Interface_2 (WAN) : 11.0.0.11 GW:
Interface_1 (WAN) : 11.0.0.10 GW:
Interface_2 (WAN) : 11.0.
W:
1
4
Router_1
Router_4
Interface_1 (WAN) : 11.0.0.3 GW:
Interface_2 (WAN) : 11.0.0.34 GW:
Interface_3 (Ethernet) : 192.168.0.1 GW:
5
4
Router_5
Interface_1 (WAN) : 11.0.0.26 GW:
Interface_2 (WAN) : 11.0.0.35 GW:
Interface_1 (WAN) : 11.0.0.18 GW:
Interface_2 (WAN) : 11.0.0.27 GW:
Interface_3 (Ethernet) : 192.169.0.1 GW:
6
7
App1_CBR
Wired_Node_6
Wired_Node_7
Interface_1 (Ethernet) : 192.168.0.2 GW:192.168.0.1
Interface_1 (Ethernet) : 192.169.0.2 GW:192.169.0.1

Figure 4-35: Network set up for studying the Configuring Static Route

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. In packet trace, filter the CONTROL_PACKET_TYPE to APP1_CBR and observe the packet flow from Wired Node 6 -> Router 1-> Router 5-> Router 4-> Wired Node 7 as shown in below Figure 4-36.



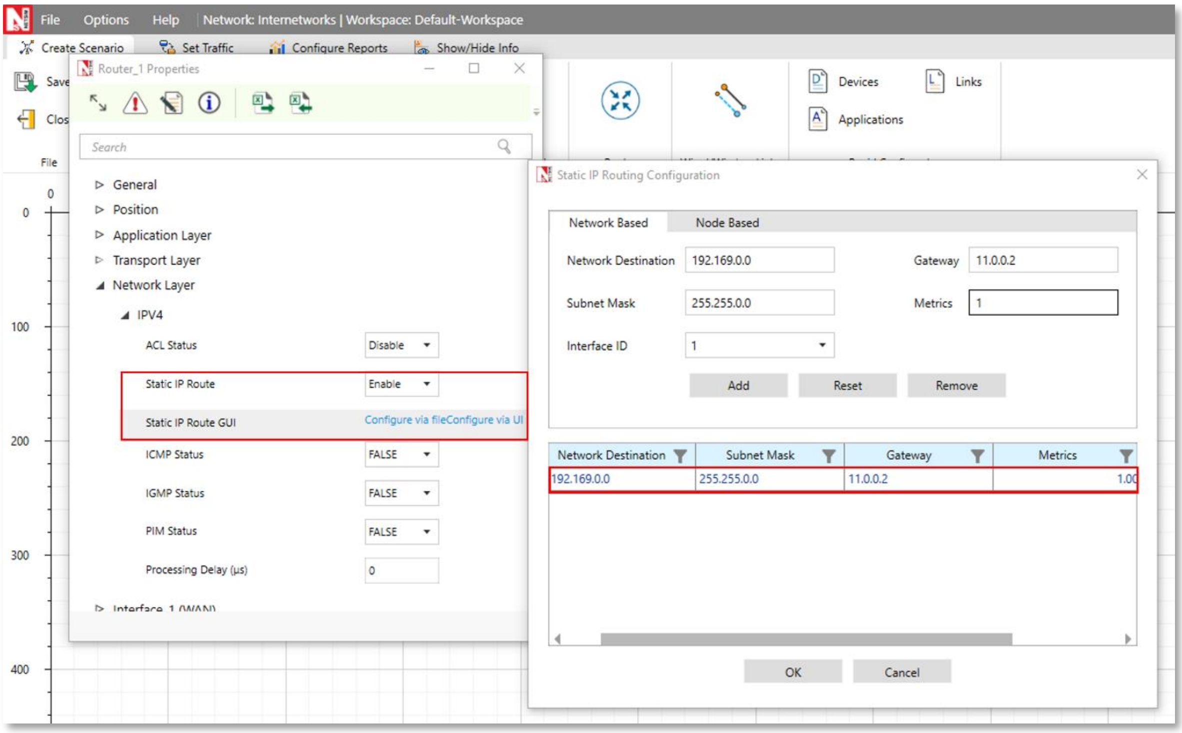
PACKET_ID	SEGMENT_ID	PACKET_TYPE	CONTROL_PACKET_TYPE/APP_NAME	SOURCE_ID	DESTINATION_ID	TRANSMITTER_ID	RECEIVER_ID
1	0	CBR	App1_CBR	NODE-6	NODE-7	NODE-6	ROUTER-1
2	0	CBR	App1_CBR	NODE-6	NODE-7	NODE-6	ROUTER-1
3	0	CBR	App1_CBR	NODE-6	NODE-7	NODE-6	ROUTER-1
3	0	CBR	App1_CBR	NODE-6	NODE-7	ROUTER-1	ROUTER-5
3	0	CBR	App1_CBR	NODE-6	NODE-7	ROUTER-5	ROUTER-4
3	0	CBR	App1_CBR	NODE-6	NODE-7	ROUTER-4	NODE-7

Figure 4-36: Packet flows from Wired Node 6 -> Router 1 -> Router 5 -> Router 4 -> Wired Node 7

4.9.2 With Static Route

Static routing configuration

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



Router_1 Properties – Network Layer – IPV4:

ACL Status	Disable
Static IP Route	Enable
Static IP Route GUI	Configure via fileConfigure via UI
ICMP Status	FALSE
IGMP Status	FALSE
PIM Status	FALSE
Processing Delay (µs)	0

Static IP Routing Configuration – Network Based:

Network Destination: 192.169.0.0 Gateway: 11.0.0.2

Subnet Mask: 255.255.0.0 Metrics: 1

Interface ID: 1

Network Destination	Subnet Mask	Gateway	Metrics
192.169.0.0	255.255.0.0	11.0.0.2	1.00

Figure 4-37: 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.

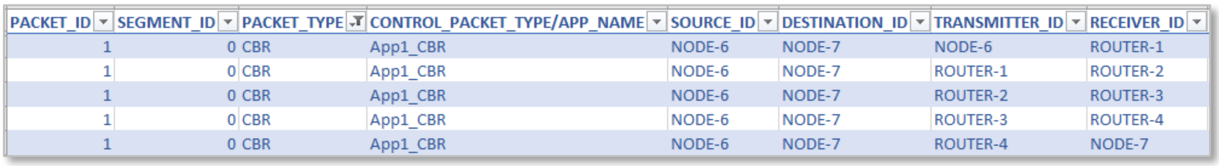
IF: is the Interface to which the gateway_ip is connected. The default value is 1.

1. Similarly Configure Static Route for all the routers as given in below Table 4-19.

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 4-19: Static Route configuration for routers

2. After configuring the router properties.
3. Run the simulation for 10 seconds.
4. In packet trace, filter the CONTROL_PACKET_TYPE to APP1_CBR and observe the change in the packet flow from Wired Node 6 -> Router 1-> Router 2-> Router 3-> Router 4-> Wired Node 7 due to static route configurations as shown in Figure 4-38.



PACKET_ID	SEGMENT_ID	PACKET_TYPE	CONTROL_PACKET_TYPE/APP_NAME	SOURCE_ID	DESTINATION_ID	TRANSMITTER_ID	RECEIVER_ID
1	0	CBR	App1_CBR	NODE-6	NODE-7	NODE-6	ROUTER-1
1	0	CBR	App1_CBR	NODE-6	NODE-7	ROUTER-1	ROUTER-2
1	0	CBR	App1_CBR	NODE-6	NODE-7	ROUTER-2	ROUTER-3
1	0	CBR	App1_CBR	NODE-6	NODE-7	ROUTER-3	ROUTER-4
1	0	CBR	App1_CBR	NODE-6	NODE-7	ROUTER-4	NODE-7

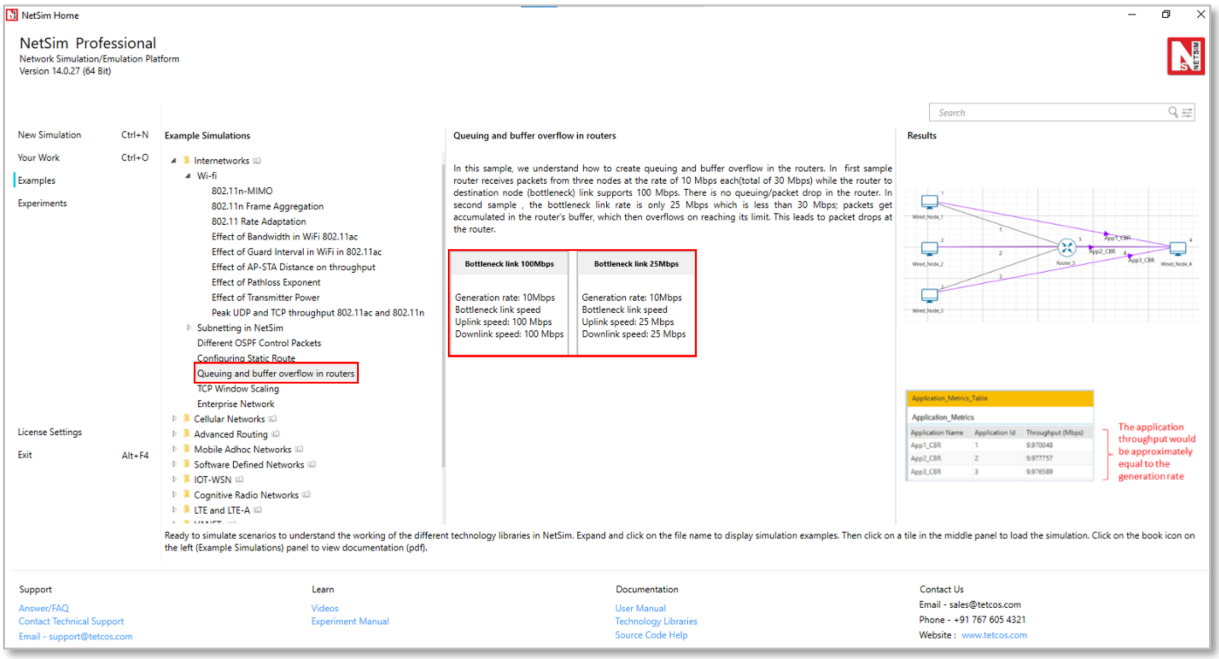
Figure 4-38: Observe in Packet Trace, the packet flows from Wired Node 6 -> Router 1 -> Router 2 -> Router 3 -> Router 4 -> Wired Node 7

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.

4.10 Queuing and buffer overflow in routers

Open NetSim and Select **Examples > Internetworks >Queuing and buffer overflow in routers** then click on the tile in the middle panel to load the example as shown in Figure 4-39.



Queuing and buffer overflow in routers

In this sample, we understand how to create queuing and buffer overflow in the routers. In first sample router receives packets from three nodes at the rate of 10 Mbps each(total of 30 Mbps) while the router to destination node (bottleneck) link supports 100 Mbps. There is no queuing/packet drop in the router. In second sample , the bottleneck link rate is only 25 Mbps which is less than 30 Mbps; packets get accumulated in the router's buffer, which then overflows on reaching its limit. This leads to packet drops at the router.

Bottleneck link 100Mbps	Bottleneck link 25Mbps
Generation rate: 10Mbps Bottleneck link speed Uplink speed: 100 Mbps Downlink speed: 100 Mbps	Generation rate: 10Mbps Bottleneck link speed Uplink speed: 25 Mbps Downlink speed: 25 Mbps

Application_Metrics_Table

Application_Metrics

Application Name	Application Id	Throughput (Mbps)
App1_CBR	1	9.970048
App2_CBR	2	9.977757
App3_CBR	3	9.976589

The application throughput would be approximately equal to the generation rate

Ready to simulate scenarios to understand the working of the different technology libraries in NetSim. Expand and click on the file name to display simulation examples. Then click on a tile in the middle panel to load the simulation. Click on the book icon on the left (Example Simulations) panel to view documentation (pdf).

Email - support@tetcos.com

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

Figure 4-39: List of scenarios for the example of queuing and buffer overflow in routers

The following network diagram illustrates, what the NetSim UI displays when you open the example configuration file as shown Figure 4-40.

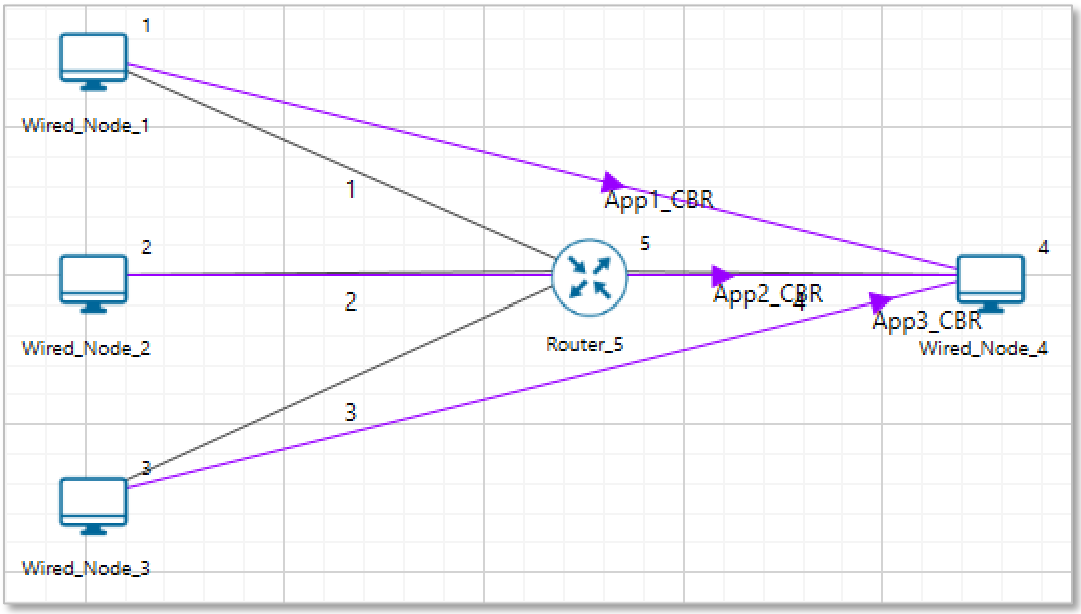


Figure 4-40: Network set up for studying the queuing and buffer overflow in routers

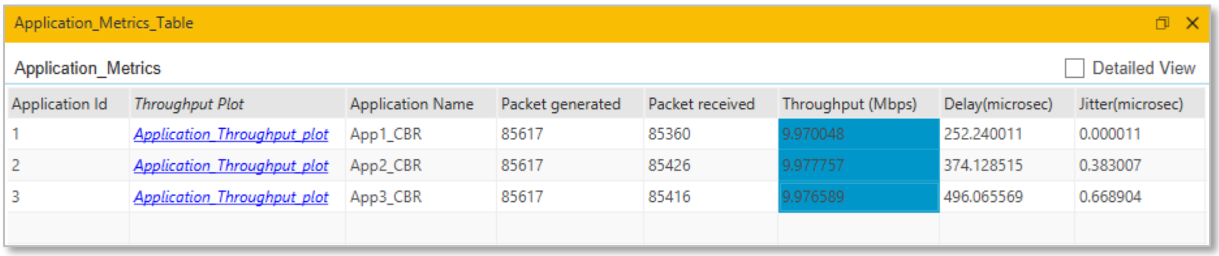
Network Settings

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)
3. Generation Rate (Mbps) = (Packet size (bytes) * 8) / Inter arrival time (µs))

4. 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
5. Plots and Packet Trace is Enabled
6. Simulate for 100s and note down the throughput
7. 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

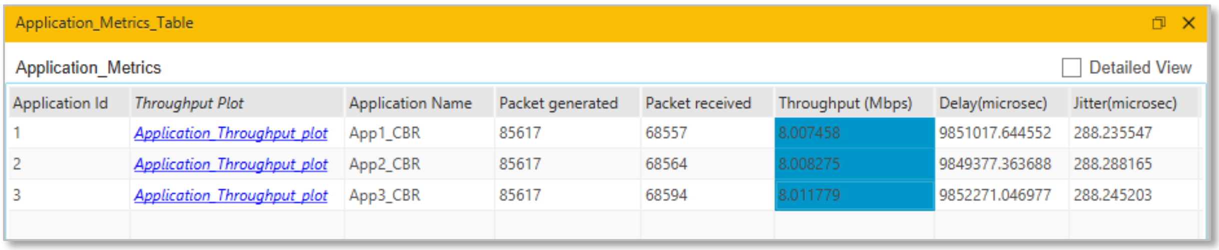
Bottleneck link 100Mbps: In this scenario, router receives packets from three links at the rate of 10 Mbps each, a total of 30 Mbps. And the router-node link supports 100 Mbps. Hence there is no queuing / packet drop in the Router. The application throughput would be approximately equal to the generation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



Application 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 4-41: Application Metrics window for Bottleneck link 100Mbps

Bottleneck link 25Mbps: 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.

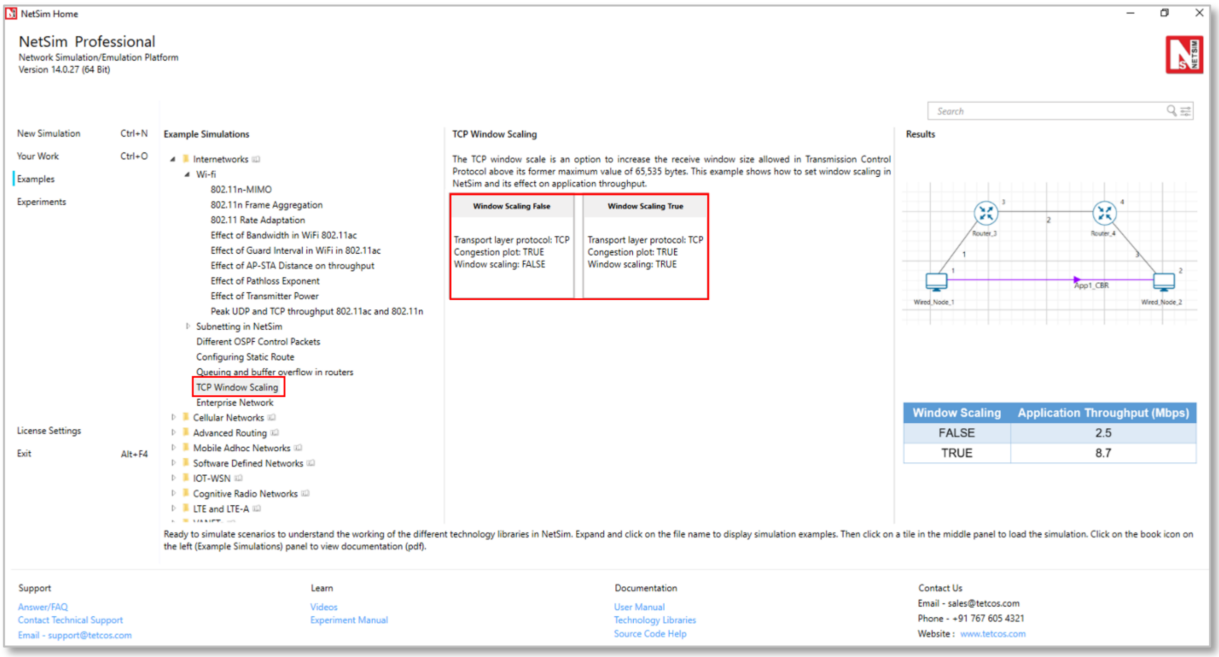


Application Id	Throughput Plot	Application Name	Packet generated	Packet received	Throughput (Mbps)	Delay(microsec)	Jitter(microsec)
1	Application_Throughput_plot	App1_CBR	85617	68557	8.007458	9851017.644552	288.235547
2	Application_Throughput_plot	App2_CBR	85617	68564	8.008275	9849377.363688	288.288165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

Figure 4-42: Application Metrics window for Bottleneck link 25Mbps

4.11 TCP Window Scaling

Open NetSim, Select **Examples->Internetworks->TCP Window Scaling** then click on the tile in the middle panel to load the example as shown in Figure 4-43.



TCP Window Scaling

The TCP window scale is an option to increase the receive window size allowed in Transmission Control Protocol above its former maximum value of 65,535 bytes. This example shows how to set window scaling in NetSim and its effect on application throughput.

Window Scaling False	Window Scaling True
Transport layer protocol: TCP Congestion plot: TRUE Window scaling: FALSE	Transport layer protocol: TCP Congestion plot: TRUE Window scaling: TRUE

Window Scaling	Application Throughput (Mbps)
FALSE	2.5
TRUE	8.7

Ready to simulate scenarios to understand the working of the different technology libraries in NetSim. Expand and click on the file name to display simulation examples. Then click on a tile in the middle panel to load the simulation. Click on the book icon on the left (Example Simulations) panel to view documentation (pdf).

Contact Us
Email - sales@tetcos.com
Phone - +91 767 605 4321
Website : www.tetcos.com

Figure 4-43: List of scenarios for the example of TCP Window Scaling

The following network diagram illustrates what the NetSim UI displays when you open the example configuration file for TCP Window scaling as shown Figure 4-44.

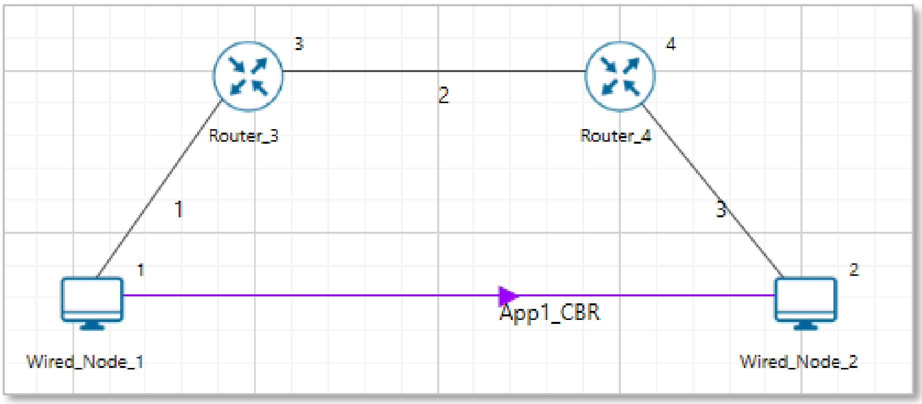


Figure 4-44: Network set up for studying the TCP Window Scaling

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 transmission 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

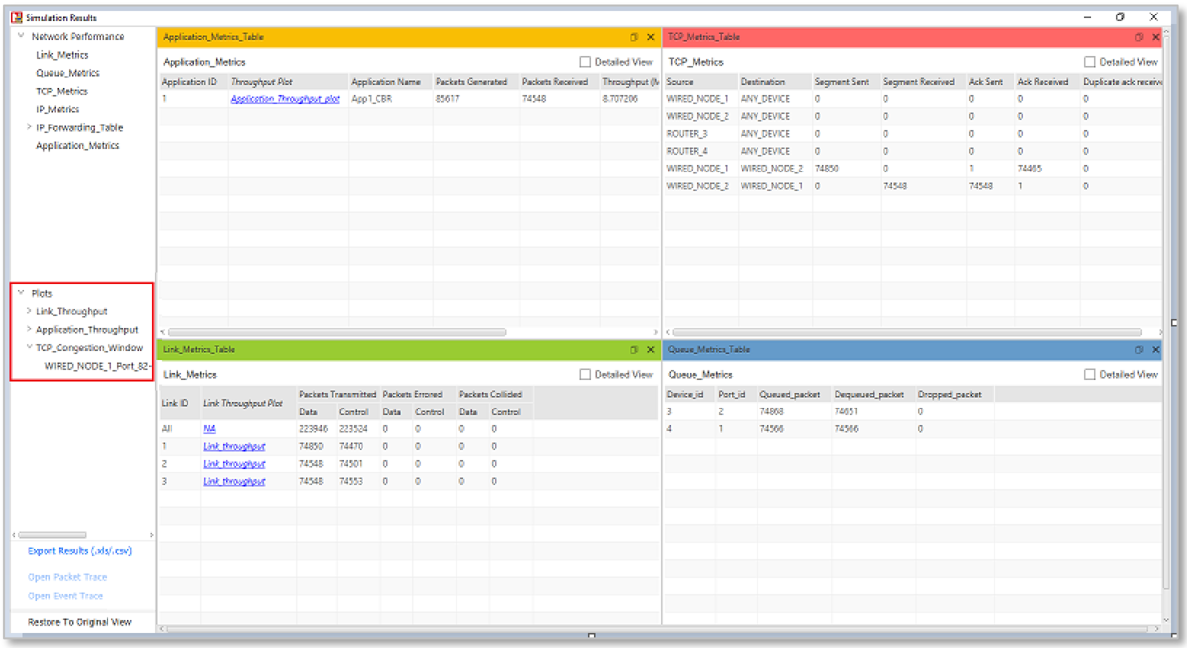
Window Scaling	Application Throughput (Mbps)
FALSE	2.5
TRUE	8.7

Table 4-20: 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 4-46/Figure 4-47.



Application_Metrics_Table

Application_Metrics ☐ Detailed View

Application ID	Throughput Plot	Application Name	Packets Generated	Packets Received	Throughput (M
1	Application_Throughput_plot	App1_CBR	85617	74548	8.707206

TCP_Metrics_Table

TCP_Metrics ☐ Detailed View

Source	Destination	Segment Sent	Segment Received	Ack Sent	Ack Received	Duplicate ack receiv
WIRED_NODE_1	ANY_DEVICE	0	0	0	0	0
WIRED_NODE_2	ANY_DEVICE	0	0	0	0	0
ROUTER_3	ANY_DEVICE	0	0	0	0	0
ROUTER_4	ANY_DEVICE	0	0	0	0	0
WIRED_NODE_1	WIRED_NODE_2	74850	0	1	74465	0
WIRED_NODE_2	WIRED_NODE_1	0	74548	74548	1	0

Link_Metrics_Table

Link_Metrics ☐ Detailed View

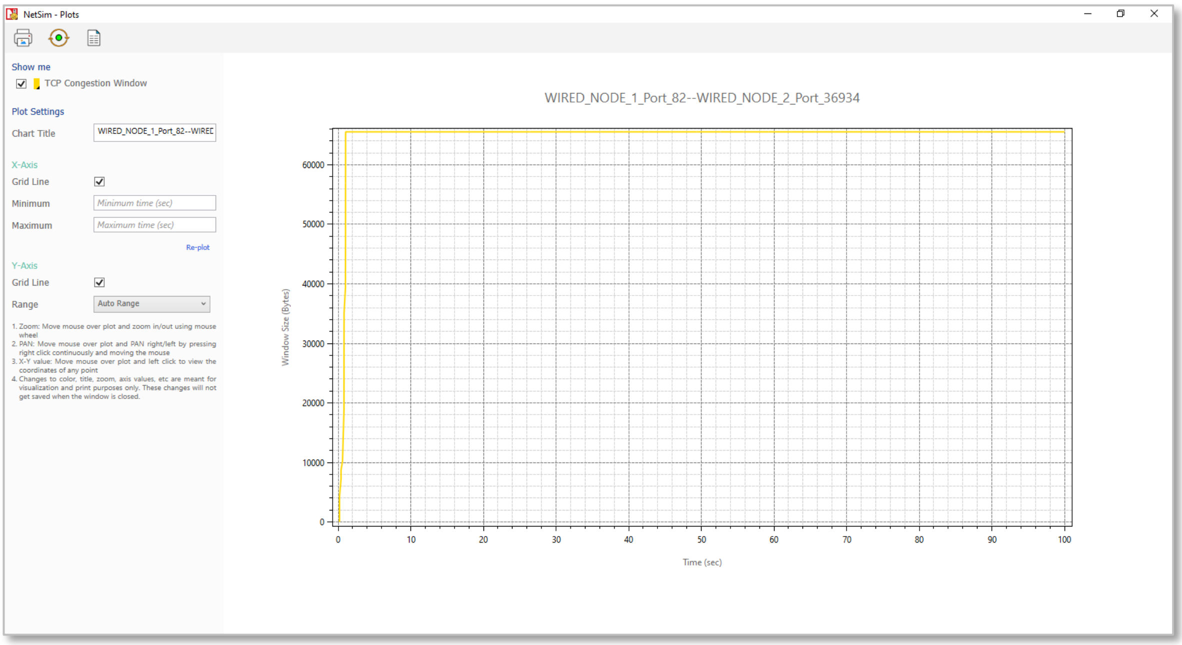
Link ID	Link Throughput Plot	Packets Transmitted		Packets Errored		Packets Collided	
		Data	Control	Data	Control	Data	Control
All	NA	223946	223524	0	0	0	0
1	Link_throughput	74850	74470	0	0	0	0
2	Link_throughput	74548	74501	0	0	0	0
3	Link_throughput	74548	74553	0	0	0	0

Queue_Metrics_Table

Queue_Metrics ☐ Detailed View

Device_id	Port_id	Queued_packet	Dequeued_packet	Dropped_packet
3	2	74868	74851	0
4	1	74566	74566	0

Figure 4-45: Result window



Show me

☑ TCP Congestion Window

Plot Settings

Chart Title: WIRED_NODE_1_Port_82--WIRED

X-Axis

Grid Line ☑

Minimum: Minimum time (sec)

Maximum: Maximum time (sec)

Y-Axis

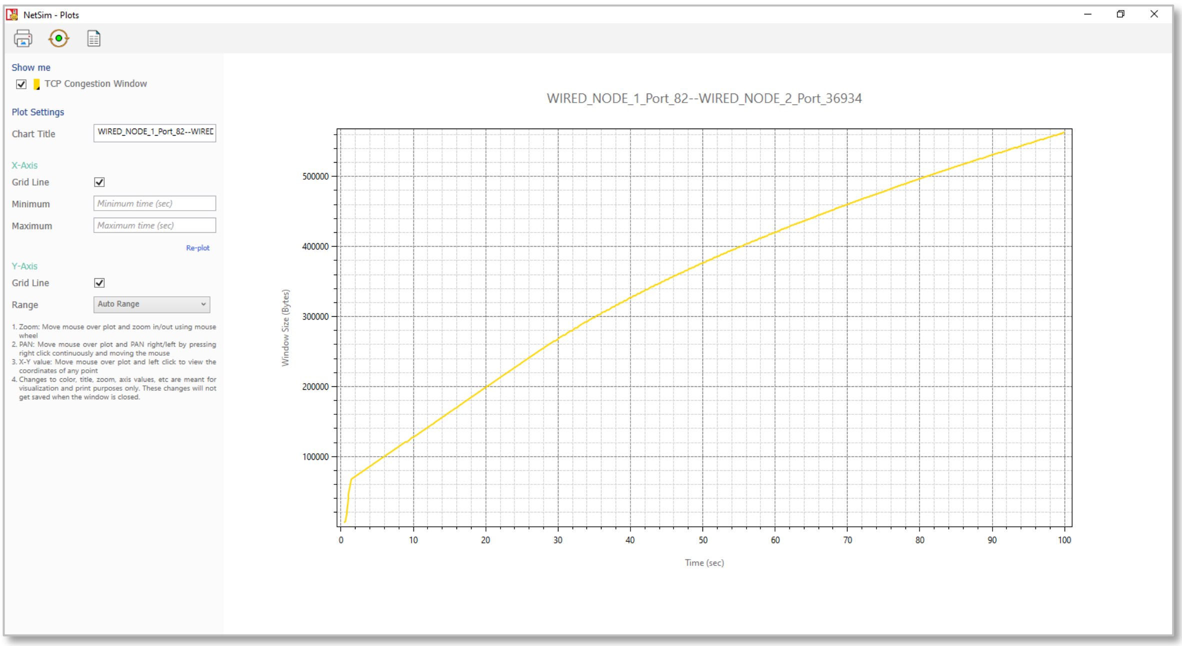
Grid Line ☑

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 4-46: TCP Congestion Plot for wired node_1

In **Window Scaling False,** 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.



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 ☑

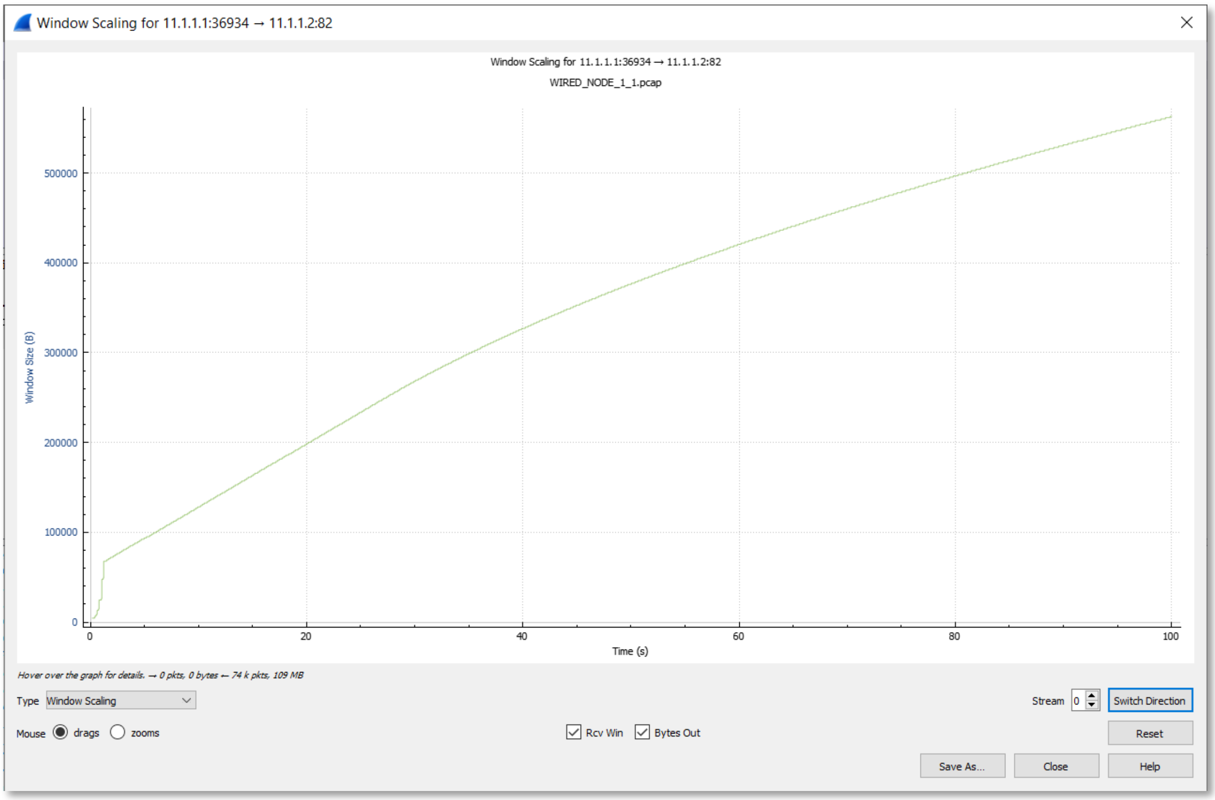
Range: Auto Range

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 4-47: TCP Congestion Plot for wired node_2

In **Window Scaling TRUE**, 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**.



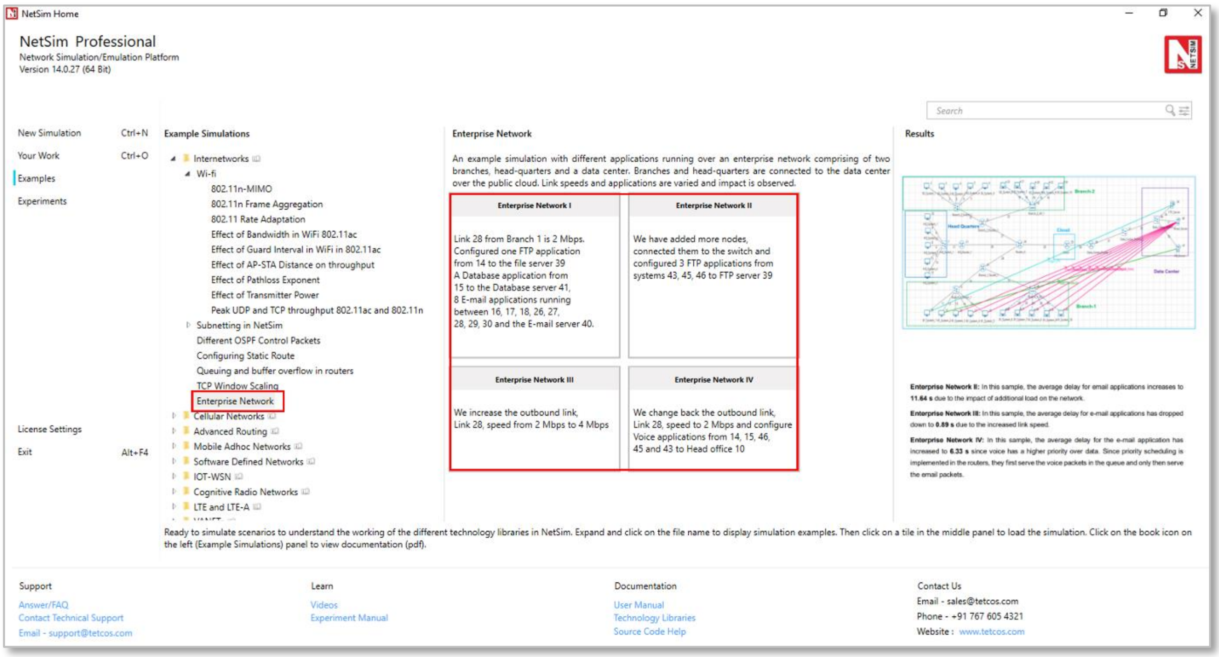
Hover over the graph for details. → 0 pkts, 0 bytes ← 74 k pkts, 109 MB

Figure 4-48: Wireshark Window when Window Scaling is TRUE

4.12 An enterprise network comprising of different subnets and running various applications

We consider a simple enterprise network, comprising of two branches, headquarters and a data center. Branches and headquarters are connected to the data center over the public cloud. Branch 1 has 10 systems, branch 2 has 10 systems, HQ has 5 systems, and they connect to a data center which houses a DB server, an email server, and an FTP server.

Open NetSim, Select **Examples->Internetworks->Enterprise Network** then click on the tile in the middle panel to load the example as shown in Figure 4-49.



NetSim Home

NetSim Professional
Network Simulation/Emulation Platform
Version 14.0.27 (64 Bit)

New Simulation Ctrl+N
Your Work Ctrl+O
Examples
Experiments

License Settings
Exit Alt+F4

Example Simulations

- Internetworks
  - Wi-fi
    - 802.11n-MIMO
    - 802.11n Frame Aggregation
    - 802.11 Rate Adaptation
    - Effect of Bandwidth in WiFi 802.11ac
    - Effect of Guard Interval in WiFi in 802.11ac
    - Effect of AP-STA Distance on throughput
    - Effect of Pathloss Exponent
    - Effect of Transmitter Power
    - Peak UDP and TCP throughput 802.11ac and 802.11n
  - Subnetting in NetSim
  - Different OSPF Control Packets
  - Configuring Static Route
  - Queuing and buffer overflow in routers
  - TCP Window Scaling
  - Enterprise Network
- Cellular Networks
- Advanced Routing
- Mobile Adhoc Networks
- Software Defined Networks
- IOT-WSN
- Cognitive Radio Networks
- LTE and LTE-A

Enterprise Network

An example simulation with different applications running over an enterprise network comprising of two branches, head-quarters and a data center. Branches and head-quarters are connected to the data center over the public cloud. Link speeds and applications are varied and impact is observed.

Enterprise Network I	Enterprise Network II
Link 28 from Branch 1 is 2 Mbps. Configured one FTP application from 14 to the file server 39 A Database application from 15 to the Database server 41, 8 E-mail applications running between 16, 17, 18, 26, 27, 28, 29, 30 and the E-mail server 40.	We have added more nodes, connected them to the switch and configured 3 FTP applications from systems 43, 45, 46 to FTP server 39
Enterprise Network III	**Enterprise Network IV**
We increase the outbound link, Link 28, speed from 2 Mbps to 4 Mbps	We change back the outbound link, Link 28, speed to 2 Mbps and configure Voice applications from 14, 15, 46, 45 and 43 to Head office 10

Search

Results

Enterprise Network II: In this sample, the average delay for email applications increases to **11.64 s** due to the impact of additional load on the network.

Enterprise Network III: In this sample, the average delay for e-mail applications has dropped down to **0.89 s** due to the increased link speed.

Enterprise Network IV: In this sample, the average delay for the e-mail application has increased to **6.33 s** since voice has a higher priority over data. Since priority scheduling is implemented in the routers, they first serve the voice packets in the queue and only then serve the email packets.

Ready to simulate scenarios to understand the working of the different technology libraries in NetSim. Expand and click on the file name to display simulation examples. Then click on a tile in the middle panel to load the simulation. Click on the book icon on the left (Example Simulations) panel to view documentation (pdf).

Support
Answer/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
Website : www.tetcos.com

Figure 4-49: List of scenarios for the example of enterprise networks

The following network diagram illustrates what the NetSim UI displays when you open the example configuration file for **Enterprise Network** in NetSim as shown in Figure 4-50.

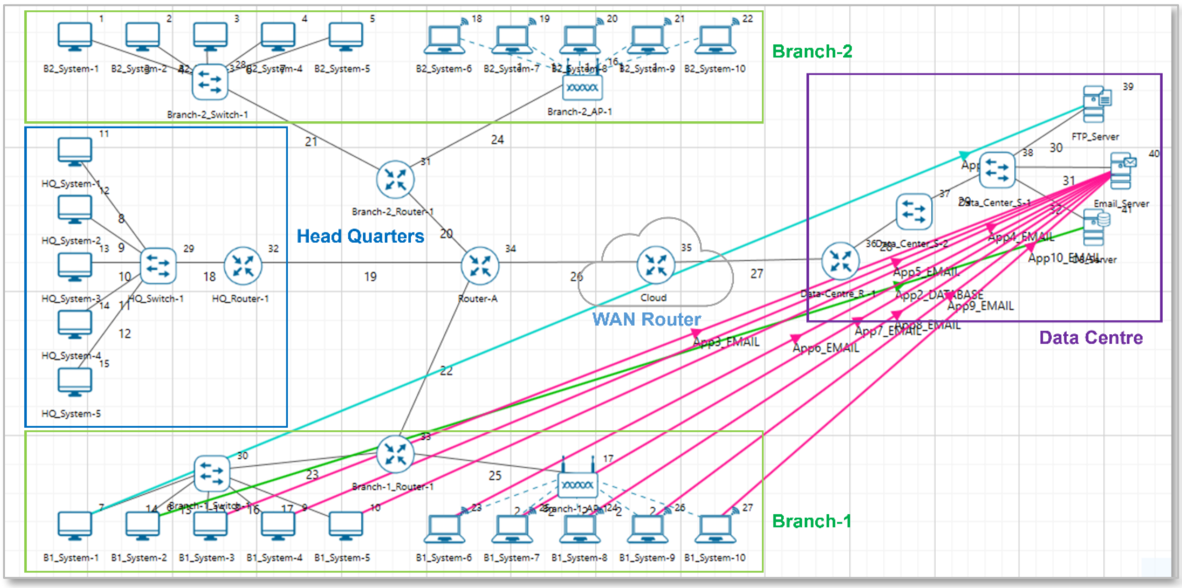


Figure 4-50: Network set up for studying the enterprise network. Labelling (Branch-1, Branch-2, HQ, Data center) has been added to the screen shot. Links 29, 30 and the WAN Router can be thought of as the internet cloud over which traffic flows to reach the data center.

Network Settings

Enterprise Network I

1. Link rate for the outbound link i.e., link 28 from Branch 1 is set to 2 Mbps.

2. Configure one FTP application from 14 to the file server 39, a DB 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. Enable plots and simulate for 100s.

Enterprise Network II

1. In this sample, we add more nodes via the switch and configured 3 FTP applications from systems 43, 45, 46 to FTP server 39, as shown in Figure 4-51.

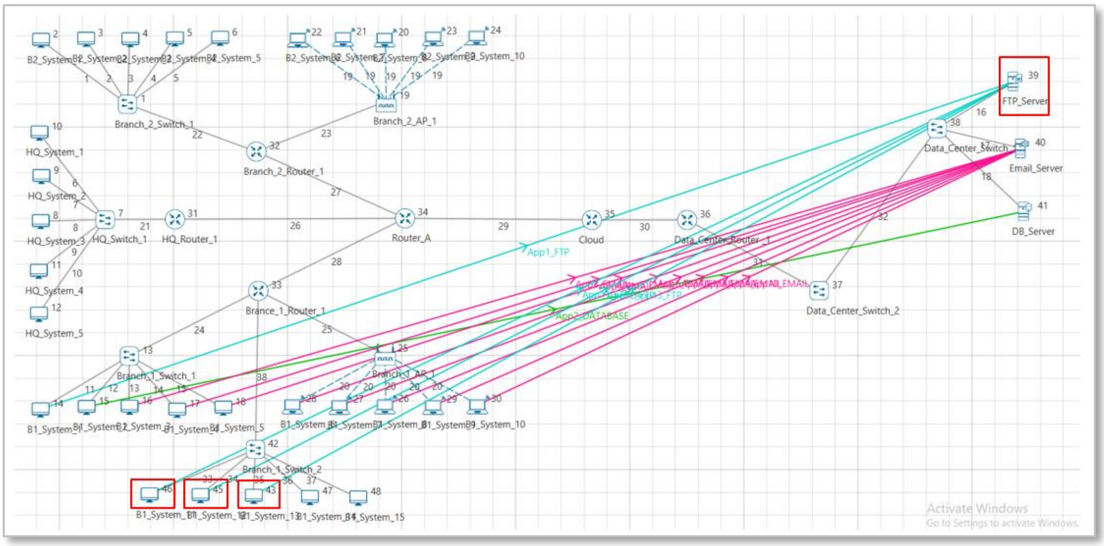


Figure 4-51: Configuring FTP applications from systems 43,45,46 to FTP server 39

2. Simulate for 100 seconds.

Enterprise Network III

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

Enterprise Network IV

1. In this sample, we change the outbound link speed i.e., Link 28 to 2Mbps and configure Voice applications from 14, 15, 46, 45 and 43 to Head office 10 as shown in Figure 4-52.

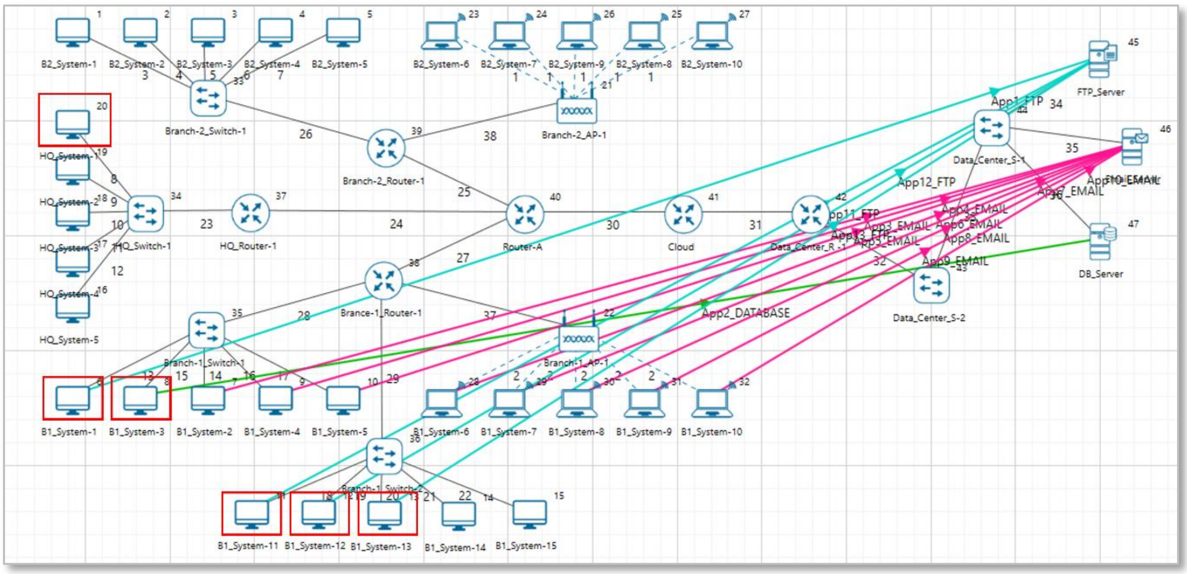
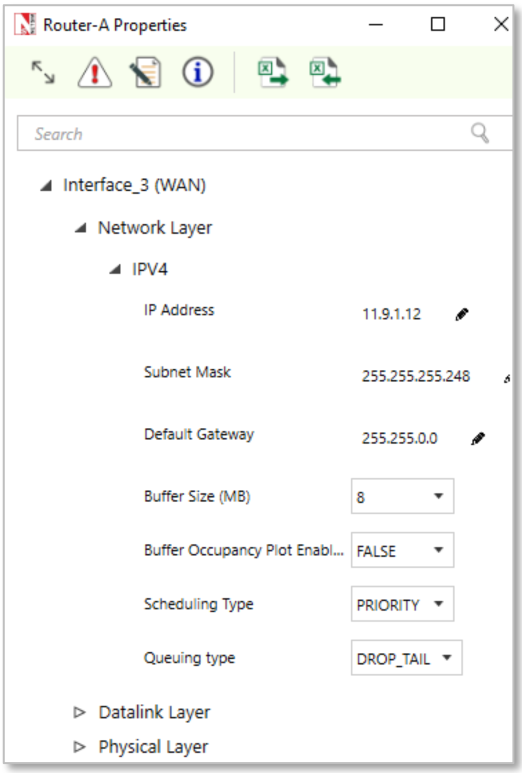


Figure 4-52: Configuring voice applications from 14, 15, 43, 45, 46 to HO 10

2. Also changed Scheduling type to Priority under Network Layer Properties of Router33 Interface WAN properties as shown below Figure 4-53.



Router-A Properties

Search

◢ Interface_3 (WAN)

◢ Network Layer

◢ IPV4

IP Address	11.9.1.12
Subnet Mask	255.255.255.248
Default Gateway	255.255.0.0
Buffer Size (MB)	8
Buffer Occupancy Plot Enabl...	FALSE
Scheduling Type	PRIORITY
Queuing type	DROP_TAIL

▷ Datalink Layer

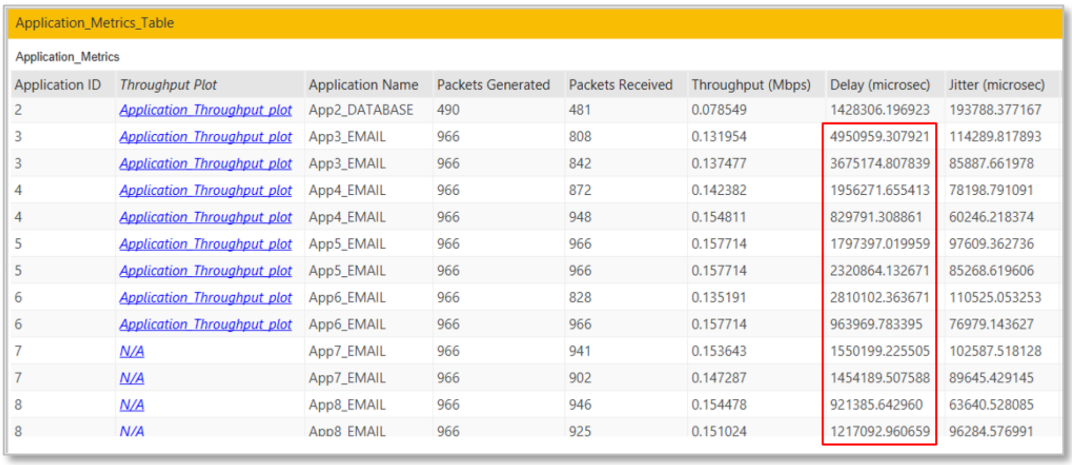
▷ Physical Layer

Figure 4-53: WAN Interface – Network layer properties window

3. Simulate for 100 seconds.

Results and Discussion

Enterprise Network I Open metrics window and calculate the average delay for e-mail application present under Application properties shown below in Figure 4-54.



Application_Metrics_Table

Application_Metrics

Application ID	*Throughput Plot*	Application Name	Packets Generated	Packets Received	Throughput (Mbps)	Delay (microsec)	Jitter (microsec)
2	*Application_Throughput_plot*	App2_DATABASE	490	481	0.078549	1428306.196923	193788.377167
3	*Application_Throughput_plot*	App3_EMAIL	966	808	0.131954	4950959.307921	114289.817893
3	*Application_Throughput_plot*	App3_EMAIL	966	842	0.137477	3675174.807839	85887.661978
4	*Application_Throughput_plot*	App4_EMAIL	966	872	0.142382	1956271.655413	78198.791091
4	*Application_Throughput_plot*	App4_EMAIL	966	948	0.154811	829791.308861	60246.218374
5	*Application_Throughput_plot*	App5_EMAIL	966	966	0.157714	1797397.019959	97609.362736
5	*Application_Throughput_plot*	App5_EMAIL	966	966	0.157714	2320864.132671	85268.619606
6	*Application_Throughput_plot*	App6_EMAIL	966	828	0.135191	2810102.363671	110525.053253
6	*Application_Throughput_plot*	App6_EMAIL	966	966	0.157714	963969.783395	76979.143627
7	*N/A*	App7_EMAIL	966	941	0.153643	1550199.225505	102587.518128
7	*N/A*	App7_EMAIL	966	902	0.147287	1454189.507588	89645.429145
8	*N/A*	App8_EMAIL	966	946	0.154478	921385.642960	63640.528085
8	*N/A*	App8_EMAIL	966	925	0.151024	1217092.960659	96284.576991

Figure 4-54: Application metrics table for Enterprise Network I

The average delay experienced by the e-mail applications is **1.90 s**

Enterprise Network II: In this sample, the average delay for email applications increases to **11.64 s** due to the impact of additional load on the network.

Enterprise Network III: In this sample, the average delay for e-mail applications has dropped down to **0.89 s** due to the increased link speed.

Enterprise Network IV: In this sample, the average delay for the e-mail application has increased to **6.33 s** since voice has a higher priority over data. Since priority scheduling is implemented in the routers, they first serve the voice packets in the queue and only then serve the email packets.

5 Internetworks Experiments in NetSim

Apart from examples, in-built experiments are also available in NetSim. Examples help the user understand the working of features in NetSim. Experiments are designed to help the user (usually students) learn networking concepts through simulation. The experiments contain objective, theory, set-up, results, and inference. The following experiments are available in the Experiments manual (pdf file).

1. Understand Measures of Network Performance: Throughput and Delay
2. Throughput and Bottleneck Server Analysis
3. Delay and Little's Law
4. Understand working of ARP, and IP Forwarding within a LAN and across a router
5. Simulate and study the spanning tree protocol.
6. Introduction to TCP connection management
7. Reliable data transfer with TCP
8. Mathematical Modelling of TCP Throughput Performance
9. Study how throughput and error of a Wireless LAN network changes as the distance between the Access Point and the wireless nodes is varied.
10. WiFi: UDP Download Throughput
11. How many downloads can a Wi-Fi access point simultaneously handle?
12. TCP Congestion Control Algorithms
13. Multi-AP Wi-Fi Networks: Channel Allocation
14. Study the working and routing table formation of Interior routing protocols, i.e. Routing Information Protocol (RIP) and Open Shortest Path First (OSPF)
15. M/D/1 and M/G/1 Queues
16. Wi-Fi Multimedia Extension (IEEE 802.11 EDCA)
17. Understand the working of OSPF.
18. Understand the events involved in NetSim DES (Discrete Event Simulator) in simulating the flow of one packet from a Wired node to a Wireless node.
19. Understand the working of TCP BIC Congestion control algorithm, simulate and plot the TCP congestion window.
20. Simulating Link Failure

6 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)

7 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