Na temelju knjige:

"Network simulation experiments manual" Prepared by Emad Aboelela, Ph.D. University of Massachusetts Dartmouth

Tonko Kovačević, Marijo Nižetić

# PROTOKOLI PAKETSKIH MREŽA

Laboratorijske vježbe

(MATERIJAL U PRIPREMI)



Split: 2010.

### Dodatna literatura - redoslijed prema poglavljima (vježbama)

<u>0.5</u>	Standard Network Applications		
<u>1.5</u>	Ethernet Model Description		
<u>2.5</u>	Token Ring Model Description		
<u>3.5</u>	Building Network Topologies		
<u>4.5</u>	Configuring Applications and Profiles		
<u>5.5</u>	ATM Model Description		
<u>6.5</u>	Routing Information Protocol (RIP)	ETF RFC number 2453	( <u>www.ietf.org/rfc.html</u> )
<u>6.5</u>	Internet Control Message Protocol	ICMP. IETF RFC number 792	(www.ietf.org/rfc.html)
<u>7.5</u>	OSPF Model Description		
<u>7.5</u>	OSPF Version 2	OSPF: IETF RFC number 2328	(www.ietf.org/rfc.html)
<u>8.5</u>	A Border Gateway Protocol 4 (BGP-4)	ETF RFC number 1771	(www.ietf.org/rfc.html)
<u>8.5</u>	Application of the Border Gateway Protocol in the Internet	ETF RFC number 1772	(www.ietf.org/rfc.html).
<u>8.5</u>	BGP4 Protocol Analysis	IETF RFC number 1774	(www.ietf.org/rfc.html)
<u>9.5</u>	TCP Model Description		
<u>9.5</u>	Transmission Control Protocol	IETF RFC number 793	(www.ietf.org/rfc.html)
<u>10.5</u>	Differentiated Services Field	IETF RFC number 2474	(www.ietf.orgyrfc.html)
<u>11.5</u>	RSVP Model Description		
<u>12.5</u>	The Impact of Internet Link Capacity on Application Performance	Capacity Planning	
<u>12.5</u>	Virtual Private Networks Management: IETF RFC number 2685		(www.ietf.org/rfc.html)
<u>13.5</u>	File Transfer Protocol (FTP)	IETF RFC number 959	(www.ietf.org/rfc.html)
<u>14.5</u>	ANSI/IEEE Standard 802.11, 1999 Edition	Wireless LAN Medium Access Control (MAC) and Physical Layor (PHY) Specifications	
<u>15.5</u>	ANSI/IEEE Standard 802.11, 1999 Edition.PDF ANSI_IEEE Standard 802.11_1999 Edition.DOC	Wireless LAN Medium Access Centrel (MAC) and Physical Layer (PHY) Specifications-	
<u>15.5</u>	Transmission Control Protocol	IETF RFC number 793	(www.ietf.orgyrfc.html)

### Dodatna literatura – abecedni redoslijed

8.5	A Border Gateway Protocol 4 (BGP-4)	IETF RFC number 1771	(www.ietf.org/rfc.html)	
14.5	ANSI/IEEE Standard 802.11, 1999 Edition ANSI_IEEE Standard 802.11_1999 Edition.DOC	Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications		
15.5	ANSI/IEEE Standard 802.11, 1999 Edition	Wireless LAN Medium Access C Physical Layer (PHY) Specificati	<del>ontrol (MAC) and</del> <del>ons:</del>	
8.5	Application of the Border Gateway Protocol in the Internet	IETE REC number 1772	(www.ietf.org/rfc.html).	
5.5	ATM Model Description			
8.5	BGP4 Protocol Analysis	IETF RFC number 1774	(www.ietf.org/rfc.html)	
3.5	Building Network Topologies			
4.5	Configuring Applications and Profiles			
10.5	Differentiated Services Field	IETF RFC number 2474	(www.ietf.orgyrfc.html)	
1.5	Ethernet Model Description			
13.5	File Transfer Protocol (FTP)	IETF RFC number 959	(www.ietf.org/rfc.html)	
6.5	Internet Control Message Protocol	ICMP. IETF RFC number 792	(www.ietf.org/rfc.html)	
7.5	OSPF Model Description			
7.5	OSPF Version 2	OSPF: IETF RFC number 2328	( <u>www.ietf.org/rfc.html</u> )	
6.5	Routing Information Protocol (RIP)	IETF RFC number 2453	(www.ietf.org/rfc.html)	
11.5	RSVP Model Description			
<u>0.5</u>	Standard Network Applications			
9.5	TCP Model Description			
12.5	The Impact of Internet Link Capacity on Application Performance	Capacity Planning		
2.5	Token Ring Model Description			
9.5	Transmission Control Protocol	IETF RFC number 793	(www.ietf.org/rfc.html)	
15.5	Transmission Control Protocol	IETF RFC number 793	(www.ietf.orgyrfc.html)	
12.5	Virtual Private Networks Management	IETF RFC number 2685	(www.ietf.org/rfc.html)	

## Content

0.	Labo	ratory - Introduction (Basics of OPNET IT Guru Academic Edition)	2
0.1	I. C	Dbjective	2
0.2	2. C	Overview	2
0.3	3. P	Prelab Activities	2
0.4	1. P	Procedure	3
(	0.4.1.	Start OPNET IT Guru Academic Edition	3
(	0.4.2.	Check the OPNET Preferences	3
(	0.4.3.	Run the Introduction Tutorial	4
(	0.4.4.	Run the Small Internetworks Tutorial	4
0.5	5. F	urther readings	4
0.6	5. E	xercises	5
0.7	/. L	ab Report	5
1.	Labo	ratory - Ethernet (A Direct Link Network with Media Access Control)	6
1.1	I. C	Dbjective	6
1.2	2. C		6
1.3	3. P	relab Activities	6
1.4	ł. P	rocedure	6
-	1.4.1.	Greate a New Project	6
-	1.4.2.	Create the Network	/
•	1.4.3.	Configure the Network Nodes	9
-	1.4.4.	Configure the Simulation	10
-	1.4.5.	Choose the Statistics	13
-	1.4.6.	Run the Simulation	14
- 	1.4./.	View the Results	15
1.5	). F	urther readings	16
1.6	). E	xercises	16
1./	/. L	ab Report	1/
Z.		ratory - Token Ring (A Shared-Media Network with Media Access Control)	10
Z. I	I. C		10
2.2	2. U		10
2.3	5. P	relad Activities	10 10
Z.4	₩. Γ Ω⁄/1	Create a New Project	10
4	2.4.1. 0 4 0	Create a New Project	10
4	2.4.2. 010	Configure the Network Nedeo	19
4	2.4.3.	Configure the Network Nodes	20
4	2.4.4. 015	Change the Statistics	21
4	2.4.3.	Duplicate the Scenario	23
4	2.4.0.	Duplicate the Scenario	20
4	2.4.7. วио	Null the Depute	20
25	2.4.0. 5 E	VIEW INE RESUILS	21
2.0	). Г С		21
2.0	). ⊏ 7 I	ab Deport	১। 21
2.1	∕. ∟ Ioho	ab Report	3 20)
J.	Lavu	Tatory - Switched LANS (A Set of Local Area Networks Interconnected by Switche	20) 20
21	······	) hiactiva	ง∠ วว
ວ. I ຊູງ	1. U		32 22
ວ.2 ຊີຊີ		orelah Δctivities	32 22
2.0 2.1	, г 1 D		32 22
0.4	ד. ר ק∠(1	Create a New Project	32
	J. <del>T</del> . I.		52

	3.4.2. Create the Network			
	3.4.3	3.	Configure the Network Nodes	34
	3.4.4	1.	Choose Statistics	35
	3.4.5	5.	Configure the Simulation	36
	3.4.6	6.	Duplicate the Scenario	36
	3.4.7	7.	Run the Simulation	38
	3.4.8	3.	View the Results	38
3.	.5.	Furthe	r readings	41
3.	.6.	Exerci	Ses	41
3.	.7.	Lab Re	eport	42
4.	Lab	oratory	/ - Network Design (Planning a Network with Different Users, Hosts, and	
	Ser	vices).		43
4.	.1.	Object	ive	43
4.	.2.	Overvi	ew	43
4.	.3.	Prelab	Activities	43
4.	.4.	Proced	dure	43
	4.4.1	۱.	Create a New Project	43
	4.4.2	2.	Create and Configure the Network	44
	4.	4.2.1.	Initialize the Network:	44
	4.	4.2.2.	Configure the Services:	44
	4.	4.2.3.	Configure a Subnet:	44
	4.	4.2.4.	Configure All Departments:	45
	4.	4.2.5.	Configure the Servers:	46
	4.	4.2.6.	Connect the Subnets:	47
	4.	4.2.7.	Choose the Statistics	48
	4.4.3	3.	Configure the Simulation	49
	444	1	Duplicate the Scenario	49
	44	5	Bun the Simulation	49
	446	5. S	View the Results	50
Λ	5	Furtho	r readings	51
-т. Л	6	Everci	200	51
4. 1	.0. 7		ses	51
4. 5	./. I.a.h	Laund	· ATM (A Connection Oriented, Cell Switching Technology)	52
J. 5	1	Object	ive	52
5. 5	. I. ົງ	Object	IVE	52
5. 5	.∠. ວ	Dreleh		52
ວ. ເ	.J.	Preiab		52
э.	.4. 51/	Proced	Jule Oreate a New Draiget	52
	5.4.	l.	Create a New Project	52
	5.4.2	2.	Create and Configure the Network	53
	5.4.3	5. 4 0 4		53
	5.	4.3.1.	Configure the Applications:	53
	5.	4.3.2.	Configure the Profiles:	54
	5.	4.3.3.	Configure the NorthEast Subnet:	56
	_ 5.	4.3.4.	Add Remaining Subnets:	5/
	5.4.4	1.	Choose the Statistics	59
	5.4.5	5.	Configure the Simulation	60
	5.4.6	6.	Duplicate the Scenario	60
	5.4.7	7.	Run the Simulation	61
	5.4.8	3.	View the Results	62
5.	.5.	Furthe	r readings	63
5.	.6.	Exerci	ses	63
5.	.7.	Lab Re	eport	64
6.	Lab	oratory	/ - RIP: Routing Information Protocol (A Routing Protocol Based on the	
	Dis	tance-	/ector Algorithm)	65

6.1. Object	1. Objective				
6.2. Overv	iew	65			
6.3. Prelab	Activities	65			
6.4. Proce	dure	65			
6.4.1.	Create a New Project	65			
6.4.2.	Create and Configure the Network	66			
6.4.2.1.	Initialize the Network:	66			
6.4.2.2.	Configure the Router:	66			
6.4.2.3.	Add the Remaining LANs:	66			
6.4.3.	Choose the Statistics	67			
6.4.4.	Configure the Simulation	67			
6.4.5.	The Ping Scenario	68			
6.4.6.	The Failure Scenario	69			
6.4.7.	Run the Simulation	70			
6.4.8.	View the Results	71			
6.4.8.1.	Compare the Number of Updates:	71			
6.4.8.2.	Obtain the IP Addresses of the Interface:	72			
6.4.8.3.	Getting the Ping Report:	74			
6.4.8.4.	Compare the Routing Tables Content:	74			
6.5. Furthe	er readings	75			
6.6. Exerci	ses	75			
6.7. Lab R	eport	76			
7. Laborator	y - OSPF: Open Shortest Path First (A Routing Protocol Based on the				
Link-State	Algorithm)	77			
7.1. Object	live	77			
7.2. Overv	iew	77			
7.3. Prelab	Activities	77			
7.4. Proce	dure	77			
7.4.1.	Create a New Project	77			
7.4.2.	Create and Configure the Network	78			
7.4.2.1.	Initialize the Network:	78			
7.4.2.2.	Configure the Link Costs:	78			
7.4.2.3.	Configure the Traffic Demands:	79			
7.4.2.4.	Configure the Routing Protocol and Addresses:	80			
7.4.3.	Configure the Simulation	81			
7.4.4.	Duplicate the Scenario	81			
7.4.4.1.	The Areas Scenario:	81			
7.4.4.2.	The Balanced Scenario:	82			
7.4.5.	Run the Simulation	82			
7.4.6.	View the Results	83			
7.4.6.1.	The No_Areas Scenario:	83			
7.4.6.2.	The Areas Scenario:	84			
7.4.6.3.	The Balanced Scenario:	84			
7.5. Furthe	r readings	85			
7.6. Exerci	ses	85			
7.7. Lab R	eport	86			
8. Laborator	y - Border Gateway Protocol (BGP) (An Interdomain Routing Protocol)	87			
8.1. Object	tive	87			
8.2. Overv	ew	87			
8.3. Prelab	Activities	87			
8.4. Proce	dure	87			
8.4.1.	Create a New Project	87			
8.4.2.	Create and Configure the Network	88			
8.4.2.1.	Initialize the Network:	88			

8.4.2.2.	Routers Configuration:	88
8.4.2.3.	Application Configuration:	89
8.4.3.	Configure the Simulation	89
8.4.4.	Choose the Statistics	90
8.4.5.	Router Interfaces and IP Addresses	91
8.4.6.	Creating the BGP Scenario	91
8.4.7.	Configuring the BGP Neighbor Information	93
8.4.8.	Creating the BGP with Policy Scenario	94
8.4.9.	Run the Simulation	95
8.4.10.	View the Results	96
8 4 10 1	Compare the Routing Tables Content	96
8 4 10 2	Compare the load in the network	97
85 Furthe	er readings	98
	is readings	00 08
87 Lah R	enort	02
0.7. Laun	epoil	90 A
9. Laborator	y - TCP. Transmission Control Protocol (A Reliable, Connection-Onente	u,
Byle-Sirea	am Service)	99
9.1. Objec	tive	99
9.2. Overv		99
9.3. Prelat	o Activities	99
9.4. Proce	dure	100
9.4.1.	Create a New Project	100
9.4.2.	Create and Configure the Network	100
9.4.2.1.	Initialize the Network:	100
9.4.2.2.	Configure the Applications:	101
9.4.2.3.	Configure the Profiles:	101
9.4.2.4	Configure the West Subnet:	102
9425	Configure the East Subnet	102
9426	Connect the Subnets to the IP Cloud:	102
0/2	Choose the Statistics	103
9.4.3.	Configure the Simulation	103
9.4.4.	Durlighte the Openasis	104
9.4.5.		104
9.4.6.	Run the Simulation	105
9.4.7.	View the Results	105
9.5. Furthe	er readings	108
9.6. Exerci	ses	108
9.7. Lab R	eport	109
10. Laborator	y - Queuing Disciplines (Order of Packet Transmission and Dropping)	110
10.1. Obj	ective	110
10.2. Ove	erview	110
10.3. Prel	ab Activities	110
10.4. Pro	cedure	110
10.4.1.	Create a New Project	110
10.4.2	Create and Configure the Network	111
10 4 2 1	Initialize the Network	111
10.1.2.1	Configure the Applications:	111
10.4.2.2	Configure the Profiles:	112
10.4.2.3	Configure the Oueues:	11/
10.4.2.4	Configure the Workstations and Sonvers:	11/
10.4.2.3 10 / 2 C	Configure the Poutore:	1 14 115
10.4.2.0		CII
10.4.3.		115
10.4.4.		116
10.4.5.	Duplicate the Scenario	117
10.4.6.	Run the Simulation	118

10.5.       Further readings       120         10.6.       Exercises       120         10.7.       Lab Report       121         11.       Laboratory - RSVP. Resource Reservation Protocol (Providing QoS by Reserving Resources in the Network)       122         11.1.       Objective       122         11.1.       Objective       122         11.1.       Objective       122         11.3.       Prelab Activities       122         11.4.1.       Configure the Project       122         11.4.2.       Configure the Nodes:       123         11.4.2.1.       Add More VolP Nodes:       123         11.4.2.2.       Define the Data Flow:       126         11.4.2.3.       Configure the Profile:       127         11.4.2.4.       Configure the Profile:       127         11.4.2.5.       Configure the Posits and Routers:       128         11.4.2.6.       Configure the Instraces       128         11.4.3.1.       Voice RSVP Called Statistics:       132         11.4.3.2.       Voice RSVP Called Statistics:       132         11.4.3.4.       Voice RSVP Called Statistics:       133         11.4.5.       Further readings       136         11.4.6. </th <th>10.4.7. View the Results</th> <th>118</th>	10.4.7. View the Results	118
10.6.       Exercises       120         10.7.       Lab Report       121         11.       Laboratory - RSVP: Resource Reservation Protocol (Providing QoS by Reserving Resources in the Network)       122         11.1.       Objective       122         11.1.       Dobjective       122         11.1.       Overview       122         11.1.       Oreate the Project.       122         11.4.1.       Create the Project.       122         11.4.2.       Configure the Network.       123         11.4.2.1.       Add More VoIP Nodes:       123         11.4.2.2.       Define the Data Flow:       126         11.4.2.3.       Configure the Profile:       127         11.4.2.4.       Configure the Profile:       127         11.4.2.5.       Configure the Interfaces       128         11.4.2.6.       Configure the Statistics:       132         11.4.3.1.       Voice Caller Statistics:       132         11.4.3.2.       Voice Caller Statistics:       132         11.4.3.3.       Voice Caller Statistics:       133         11.4.4.       Configure the Statistics:       133         11.4.4.       Configure the Statistics:       133         11.4.3.1.	10.5. Further readings	120
10.7.       Lab Report.       [21]         11.       Laboratory - RSVP: Resource Reservation Protocol (Providing QoS by Reserving Resources in the Network).       [22]         11.1.       Objective       [22]         11.1.       Objective       [22]         11.3.       Prelab Activities       [22]         11.4.       Overview       [22]         11.4.       Croafigure the Project.       [22]         11.4.1.       Create the Project.       [23]         11.4.2.       Configure the Nodes:       [23]         11.4.2.1.       Add More VolP Nodes:       [23]         11.4.2.2.       Define the Data Flow:       [26]         11.4.2.3.       Configure the Application:       [26]         11.4.2.4.       Configure the Interfaces:       [28]         11.4.2.6.       Configure the Interfaces:       [32]         11.4.3.1.       Voice RSVP Caller Statistics:       [32]         11.4.3.2.       Voice RSVP Called Statistics:       [32]         11.4.3.3.       Voice RSVP Called Statistics:       [33]         11.4.4.4.       Configure the Simulation       [33]         11.4.5.       Further readings       [36]         11.4.6.       View the Results       [36]	10.6. Exercises	120
11.       Laboratory - RSVP: Resource Reservation Protocol (Providing QoS by Reserving Resources in the Network)       122         11.1.       Objective       122         11.2.       Overview       122         11.3.       Prelab Activities       122         11.4.       Procedure       122         11.4.1.       Create the Project       123         11.4.2.       Configure the Network       123         11.4.2.1.       Add More VoIP Nodes:       123         11.4.2.2.       Define the Data Flow:       125         11.4.2.3.       Configure the Profile:       126         11.4.2.4.       Configure the Hosts and Routers:       129         11.4.3.1.       Voice_RSVP Called Statistics:       132         11.4.3.2.       Voice_RSVP Called Statistics:       132         11.4.3.3.       Voice Caller Statistics:       133         11.4.3.1.       Voice_RSVP Called Statistics:       133         11.4.3.3.       Voice Caller Statistics:       133         11.4.3.4.       Voice_RSVP Called Statistics:       133         11.4.3.5.       Further Resimulation       133         11.4.4.       Configure the Simulation       133         11.4.5.       Run the Simulation <t< td=""><td>10.7. Lab Report</td><td>121</td></t<>	10.7. Lab Report	121
Resources in the Network)         122           111.         Objective         122           112.         Overview         122           113.         Prelab Activities         122           114.         Procedure         122           114.1.         Create the Project         122           114.2.         Configure the Network         123           114.2.1.         Add More VolP Nodes         123           114.2.2.         Define the Data Flow         125           114.2.3.         Configure the Profile:         127           114.2.4.         Configure the Profile:         127           114.2.5.         Configure the Profile:         129           114.3.1.         Voice, RSVP Caller Statistics:         132           114.3.1.         Voice, RSVP Called Statistics:         132           114.3.2.         Voice Caller Statistics:         133           114.4.1.         Configure the Simulation         133           114.4.2.         Configure the Simulation         133           114.4.3.         Voice Caller Statistics:         132           114.4.4.         Configure the Simulation         133           114.5.         Fun the Simulation         133	11. Laboratory - RSVP: Resource Reservation Protocol (Providing QoS by Reserving	
11.1.       Objective.       122         11.2.       Overview.       122         11.3.       Prelab Activities       122         11.4.       Procedure       122         11.4.1.       Create the Project       122         11.4.2.       Configure the Network.       123         11.4.2.1.       Add More VolP Nodes:       123         11.4.2.2.       Define the Data Flow.       125         11.4.2.3.       Configure the Application       126         11.4.2.4.       Configure the Porolite:       127         11.4.2.5.       Configure the Interfaces:       128         11.4.2.6.       Configure the Hosts and Routers:       131         11.4.3.1.       Voice RSVP Called Statistics:       132         11.4.3.2.       Voice RSVP Called Statistics:       132         11.4.3.1.       Voice Caller Statistics:       133         11.4.4.       Configure the Simulation       133         11.4.5.       Run the Results.       133         11.4.6.       View the Results.       136         11.6.       Exercises       136         11.7.       Lab Report.       137         12.4.       Oreceta and Configure the Network       137	Resources in the Network)	122
11.2.       Overview.       122         11.3.       Prelab Activities.       122         11.4.       Procedure.       122         11.4.1.       Create the Project.       122         11.4.2.       Configure the Project.       123         11.4.2.1.       Add More VolP Nodes:       123         11.4.2.2.       Define the Data Flow.       125         11.4.2.3.       Configure the Application:       126         11.4.2.4.       Configure the Profile:       127         11.4.2.5.       Configure the Hosts and Routers:       128         11.4.3.1.       Voice_RSVP Caller Statistics:       132         11.4.3.2.       Voice_RSVP Called Statistics:       132         11.4.3.1.       Voice_RSVP Called Statistics:       133         11.4.3.1.       Voice_RSVP Called Statistics:       133         11.4.3.2.       Voice_RSVP Called Statistics:       133         11.4.3.3.1.       Voice_RSVP Called Statistics:       133         11.4.4.2.       Configure the Simulation       133         11.4.4.3.4.       Configure the Simulation       133         11.4.5.       Run the Simulation       136         11.7.       Lab Report       136         11.7	11.1. Objective	122
11.3.       Prelab Activities       122         11.4.       Procedure       122         11.4.1.       Configure the Network       123         11.4.2.1.       Add More VoIP Nodes:       123         11.4.2.2.       Define the Data Flow.       125         11.4.2.3.       Configure the Application:       126         11.4.2.4.       Configure the Profile       127         11.4.2.5.       Configure the Hosts and Routers:       129         11.4.2.6.       Configure the Hosts and Routers:       131         11.4.3.1.       Voice Called Statistics:       132         11.4.3.2.       Voice Called Statistics:       132         11.4.3.3.       Voice Caller Statistics:       133         11.4.4.       Configure the Simulation       133         11.4.5.       Run the Simulation       133         11.4.6.       View the Results       133         11.4.5.       Run the Simulation       133         11.4.6.       View the Results       133         11.4.6.       View the Results       136         11.4.1.5.       Further readings       136         11.4.2.6.       Configure the Network Security and Virtual Private Networks)       137         12	11.2. Overview	122
114.       Procedure       122         114.1.       Create the Project.       122         114.2.       Configure the Network.       123         114.2.1.       Add More VoIP Nodes:       123         114.2.2.       Define the Data Flow.       125         114.2.2.       Define the Data Flow.       126         114.2.3.       Configure the Application:       126         114.2.4.       Configure the Hosts and Routers:       128         114.2.5.       Configure the Hosts and Routers:       129         114.3.1.       Voice RSVP Called Statistics:       131         114.3.2.       Voice RSVP Called Statistics:       132         114.3.3.       Voice Called Statistics:       132         114.4.       Configure the Simulation       133         11.4.5.       Run the Simulation       133         11.4.6.       View the Results.       133         11.5.       Further readings       136         11.6.       Exercises       136         11.7.       Lab Report       137         12.4.       Oreate a New Project       137         12.4.       Procedure       137         12.4.       Create a New Project       138	11.3. Prelab Activities	122
114.1       Create the Project.       122         114.2       Configure the Network.       123         114.2.1       Add More VoIP Nodes:       123         114.2.2       Define the Data Flow:       125         114.2.3       Configure the Application:       126         114.2.4       Configure the Porfile:       127         114.2.5       Configure the Hosts and Routers:       128         114.2.6       Configure the Hosts and Routers:       129         114.3.1       Voice RSVP Called Statistics:       132         114.3.2       Voice Called Statistics:       132         114.3.3       Voice Called Statistics:       133         114.3.4       Configure the Simulation       133         114.4.6       View the Results       133         114.5       Rut the Simulation       133         114.6       View the Results       136         11.6       Exercises       136         11.7       Lab Report       136         12.1       Objective       137         12.2       Overview       137         12.3       Prelab Activities       137         12.4       Create and Configure the Network       138	11.4. Procedure	122
11.4.2.       Configure the Network       123         11.4.2.1.       Add More VolP Nodes:       123         11.4.2.2.       Define the Data Flow:       125         11.4.2.3.       Configure the Application:       126         11.4.2.4.       Configure the Profile:       127         11.4.2.5.       Configure the Hosts and Routers:       128         11.4.2.6.       Configure the Hosts and Routers:       131         11.4.3.       Choose the Statistics:       132         11.4.3.       Voice Caller Statistics:       132         11.4.3.1.       Voice Caller Statistics:       133         11.4.3.2.       Voice Caller Statistics:       133         11.4.3.3.       Voice Caller Statistics:       133         11.4.3.4.       Configure the Simulation       133         11.4.4.6.       View the Results       133         11.4.6.       View the Results       136         11.5.       Further readings       136         11.7.       Lab Report       137         12.1.       Objective       137         12.2.       Overview       137         12.3.       Prelab Activities       137         12.4.1.       Create and Configure the Network	11.4.1. Create the Project	122
11.4.2.1       Add More VolP Nodes:       123         11.4.2.2       Define the Data Flow:       125         11.4.2.3       Configure the Profile:       127         11.4.2.4       Configure the Profile:       127         11.4.2.5       Configure the Hosts and Routers:       128         11.4.2.6       Configure the Hosts and Routers:       129         11.4.3       Choose the Statistics       131         11.4.3.1       Voice RSVP Caller Statistics:       132         11.4.3.2       Voice RSVP Caller Statistics:       132         11.4.3.3       Voice Caller Statistics:       133         11.4.4       Configure the Simulation       133         11.4.5       Run the Simulation       133         11.4.6       View the Results       133         11.4.6       View the Results       136         11.7       Lab Report       136         11.7       Lab Report       137         12.1       Objective       137         12.2       Overview       137         12.4       Procedure       137         12.4       Procedure       137         12.4       Procedure       137         12.4.1       Cre	11.4.2. Configure the Network	123
11.4.2.3.       Configure the Application:       125         11.4.2.4.       Configure the Application:       126         11.4.2.5.       Configure the Profile:       127         11.4.2.6.       Configure the Hosts and Routers:       129         11.4.3.       Choose the Statistics:       131         11.4.3.       Choose the Statistics:       132         11.4.3.       Voice RSVP Caller Statistics:       132         11.4.3.       Voice Caller Statistics:       133         11.4.4.       Configure the Simulation       133         11.4.5.       Run the Simulation       133         11.4.6.       View the Results       133         11.5.       Further readings       136         11.6.       Exercises       136         11.7.       Laboratory - Firewalls and VPN (Network Security and Virtual Private Networks)       137         12.1.       Objective       137         12.4.       Procedure       137         12.4.       Procedure       137         12.4.1.       Create a New Project       138         12.4.2.2.       Coreate and Configure the Network       138         12.4.3.       Choose the Statistics       139         12.4.4.	11.4.2.1. Add More VoIP Nodes:	123
11.4.2.4.       Configure the Application:       126         11.4.2.4.       Configure the Interfaces:       127         11.4.2.5.       Configure the Hosts and Routers:       128         11.4.2.6.       Configure the Hosts and Routers:       129         11.4.3.       Choose the Statistics:       131         11.4.3.       Choose the Statistics:       132         11.4.3.       Voice RSVP Called Statistics:       132         11.4.3.       Voice Caller Statistics:       132         11.4.4.       Configure the Simulation       133         11.4.5.       Run the Simulation       133         11.4.6.       View the Results       133         11.4.6.       View the Results       136         11.6.       Exercises       136         11.7.       Lab Report       137         12.4.       Objective       137         12.2.       Overview       137         12.4.       Create and Configure the Network       138         12.4.1.       Create and Project       137         12.4.2.       Create and VPN (Network Security and Virtual Private Networks)       137         12.4.1.       Initialize the Network:       138         12.4.2.       <	11.4.2.2. Define the Data Flow:	125
11.4.2.4.       Configure the Profile:       127         11.4.2.5.       Configure the Hosts and Routers:       129         11.4.3.1.       Voice RSVP Caller Statistics:       132         11.4.3.2.       Voice RSVP Called Statistics:       132         11.4.3.3.       Voice Caller Statistics:       132         11.4.3.1.       Voice Caller Statistics:       132         11.4.3.2.       Voice Caller Statistics:       133         11.4.4.       Configure the Simulation       133         11.4.5.       Run the Simulation       133         11.4.6.       View the Results       133         11.5.       Further readings       136         11.6.       Exercises       136         11.7.       Lab Report       136         12.1.       Objective       137         12.2.       Overview       137         12.3.       Prelab Activities       137         12.4.1.       Create and Configure the Network       138         12.4.2.2.       Configure the Nodes:       138         12.4.3.       Choose the Statistics       139         12.4.4.       The Firewall Scenario       141         12.4.5.       Firemalls and VPN       140	11.4.2.3. Configure the Application:	126
11.4.2.5.       Configure the Interaces:       128         11.4.3.1.       Choose the Statistics       131         11.4.3.2.       Voice_RSVP Called Statistics:       132         11.4.3.3.       Voice Called Statistics:       132         11.4.3.4.       Configure the Simulation       133         11.4.3.3.       Voice Called Statistics:       132         11.4.4.       Configure the Simulation       133         11.4.5.       Run the Simulation       133         11.4.6.       View the Results       133         11.4.5.       Further readings       136         11.6.       Exercises       136         11.7.       Lab Report       136         12.       Laboratory - Firewalls and VPN (Network Security and Virtual Private Networks)       137         12.1.       Objective       137         12.2.       Overview       137         12.4.1.       Create a New Project       137         12.4.2.       Create a New Project       138         12.4.2.1.       Initialize the Network       138         12.4.2.2.       Configure the Network       138         12.4.3.       Choose the Statistics       139         12.4.4.       The Firewa	11.4.2.4. Configure the Profile:	12/
11.4.2.6.       Configure the Prosts and Routers:       129         11.4.3.1.       Voice_RSVP Caller Statistics:       132         11.4.3.2.       Voice_RSVP Called Statistics:       132         11.4.3.3.       Voice Caller Statistics:       132         11.4.3.3.       Voice Caller Statistics:       132         11.4.4.       Configure the Simulation       133         11.4.5.       Run the Simulation       133         11.4.6.       View the Results       133         11.4.6.       View the Results       133         11.6.       Exercises       136         11.7.       Lab Report       136         12.       Objective       137         12.1.       Objective       137         12.2.       Overview       137         12.4.       Create and VPN (Network Security and Virtual Private Networks)       137         12.2.       Overview       137         12.4.       Procedure       137         12.4.       Create and Configure the Network       138         12.4.1.       Initialize the Network       138         12.4.2.2.       Configure the Nodes:       138         12.4.3.       Choose the Statistics       139	11.4.2.5. Configure the Interfaces:	128
11.4.3.1.       Voice_RSVP Caller Statistics:       132         11.4.3.1.       Voice_RSVP Called Statistics:       132         11.4.3.2.       Voice Caller Statistics:       132         11.4.3.3.       Voice Caller Statistics:       132         11.4.4.       Configure the Simulation       133         11.4.5.       Run the Simulation       133         11.4.6.       View the Results       133         11.5.       Further readings       136         11.6.       Exercises       136         11.7.       Lab Report       136         12.       Laboratory - Firewalls and VPN (Network Security and Virtual Private Networks)       137         12.1.       Objective       137         12.2.       Overview       137         12.4.       Create and Configure the Network       138         12.4.1.       Create and Configure the Network       138         12.4.2.       Configure the Network       138         12.4.2.       Configure the Network       138         12.4.3.       Choose the Statistics       139         12.4.4.       The Firewall Scenario       141         12.4.5.       Firewall Scenario       141         12.4.6.1. <td< td=""><td>11.4.2.6. Configure the Hosts and Routers:</td><td>129</td></td<>	11.4.2.6. Configure the Hosts and Routers:	129
11.4.3.1.       Voice_RSVP Called Statistics:       132         11.4.3.2.       Voice_RSVP Called Statistics:       132         11.4.3.3.       Voice Caller Statistics:       132         11.4.4.       Configure the Simulation       133         11.4.4.       Configure the Simulation       133         11.4.5.       Run the Simulation       133         11.4.6.       View the Results       133         11.4.6.       View the Results       133         11.6.       Exercises       136         11.7.       Lab Report       136         12.       Laboratory - Firewalls and VPN (Network Security and Virtual Private Networks)       137         12.1.       Objective       137         12.2.       Overview       137         12.4.       Procedure       137         12.4.       Procedure       137         12.4.1.       Create and Configure the Network       138         12.4.2.2.       Configure the Network       138         12.4.3.       Choose the Statistics       138         12.4.4.       The Firewall Scenario       139         12.4.5.       Firewall Scenario       140         12.4.6.       The Firewall VPN Scenario	11.4.3. Choose the Statistics	131
11.4.3.2.       Voice Caller Statistics:       132         11.4.3.3.       Voice Caller Statistics:       133         11.4.4.       Configure the Simulation       133         11.4.5.       Run the Simulation       133         11.4.6.       View the Results       133         11.5.       Further readings       136         11.6.       Exercises       136         11.7.       Lab Report       136         12.1.       Objective       137         12.1.       Objective       137         12.2.       Overview       137         12.3.       Prelab Activities       137         12.4.       Objective       137         12.4.       Create a New Project       137         12.4.1.       Create and Configure the Network       138         12.4.2.       Corefigure the Network       138         12.4.2.       Configure the Nodes:       138         12.4.3.       Choose the Statistics       139         12.4.4.       The Firewall Scenario       139         12.4.5.       Firewall Scenario       141         12.4.6.1.       Configure the VPN:       141         12.4.6.2.       Simulation	11.4.3.1. VOICE_RSVP Caller Statistics:	132
11.4.3.3.       Voice Caller Statistics:       132         11.4.4.       Configure the Simulation       133         11.4.5.       Run the Simulation       133         11.4.6.       View the Results       133         11.5.       Further readings       136         11.6.       Exercises       136         11.7.       Lab Report       136         12.       Laboratory - Firewalls and VPN (Network Security and Virtual Private Networks)       137         12.1.       Objective       137         12.2.       Overview       137         12.3.       Prelab Activities       137         12.4.       Procedure       137         12.4.1.       Create and Configure the Network       138         12.4.2.1.       Initialize the Network:       138         12.4.2.2.       Configure the Nodes:       138         12.4.3.       Choose the Statistics       139         12.4.4.       The Firewall VPN       140         12.4.5.       Firewall VPN Scenario       141         12.4.6.       The Firewall VPN Scenario       141         12.4.6.       The Firewall VPN Scenario       141         12.4.6.       The Firewall VPN Scenario       14	11.4.3.2. Voice_RSVP Called Statistics:	132
11.4.4.       Configure the Simulation       133         11.4.5.       Run the Simulation       133         11.4.6.       View the Results       133         11.5.       Further readings       136         11.6.       Exercises       136         11.7.       Lab Report       136         12.       Laboratory - Firewalls and VPN (Network Security and Virtual Private Networks)       137         12.1.       Objective       137         12.2.       Overview       137         12.4.       Procedure       137         12.4.       Procedure       137         12.4.1.       Create and Configure the Network       138         12.4.2.1.       Initialize the Network:       138         12.4.2.1.       Initialize the Network:       138         12.4.2.2.       Configure the Nodes:       138         12.4.3.       Choose the Statistics       139         12.4.4.       The Firewall Scenario       140         12.4.5.       Firewall VPN       140         12.4.6.1.       Configure the VPN:       141         12.4.6.2.       Simulation       143         12.4.6.1.       Configure the VPN:       141	11.4.3.3. VOICE Caller Statistics:	132
11.4.5.       Function the Stinutation       133         11.4.6.       View the Results       133         11.5.       Further readings       136         11.6.       Exercises       136         11.7.       Lab Report       136         12.       Laboratory - Firewalls and VPN (Network Security and Virtual Private Networks)       137         12.1.       Objective       137         12.2.       Overview       137         12.3.       Prelab Activities       137         12.4.       Create a New Project       137         12.4.2.       Create and Configure the Network       138         12.4.2.       Create and Configure the Network       138         12.4.2.       Coreate and Configure the Network       138         12.4.2.       Conso the Statistics       139         12.4.4.       The Firewall Scenario       139         12.4.5.       Firewall Scenario       140         12.4.6.       The Firewall VPN       141         12.4.6.       Configure the VPN:       141<	11.4.4. Configure the Simulation	133
11.4.5.       View the Results       135         11.5.       Further readings       136         11.6.       Exercises       136         11.7.       Lab Report       136         12.       Laboratory - Firewalls and VPN (Network Security and Virtual Private Networks)       137         12.1.       Objective       137         12.2.       Overview       137         12.3.       Prelab Activities       137         12.4.       Procedure       137         12.4.1.       Create and Configure the Network       138         12.4.2.1.       Initialize the Network:       138         12.4.2.2.       Configure the Nodes:       138         12.4.2.1.       Initialize the Network:       138         12.4.2.2.       Configure the Nodes:       138         12.4.3.       Choose the Statistics       139         12.4.4.       The Firewall Scenario       139         12.4.5.       Firewalls and VPN       140         12.4.6.       The Firewall VPN Scenario       141         12.4.6.1.       Configure the VPN:       141         12.4.6.2.       Simulating Encryption:       142         12.4.7.       Run the Simulation       143	11.4.5. Run the Deculte	100
11.5.       Further readings       136         11.6.       Exercises       136         11.7.       Lab Report       136         12.       Laboratory - Firewalls and VPN (Network Security and Virtual Private Networks)       137         12.       Dojective       137         12.1.       Objective       137         12.2.       Overview       137         12.3.       Prelab Activities       137         12.4.       Procedure       137         12.4.       Create and Configure the Network       138         12.4.2.       Create and Configure the Network       138         12.4.2.1.       Initialize the Network:       138         12.4.2.2.       Configure the Nodes:       138         12.4.2.3.       Choose the Statistics       139         12.4.4.       The Firewall Scenario       139         12.4.5.       Firewalls and VPN       140         12.4.6.       The Firewall VPN Scenario       141         12.4.6.       The Firewall VPN Scenario       142         12.4.7.       Run the Simulation       142         12.4.8.       View the Results       143         12.4.9.       Further readings       145	11.4.0. VIEW INE RESULTS	133
11.0.       Exercises       136         11.7.       Lab Report.       136         12.       Laboratory - Firewalls and VPN (Network Security and Virtual Private Networks)       137         12.1.       Objective.       137         12.2.       Overview.       137         12.3.       Prelab Activities       137         12.4.       Procedure       137         12.4.1.       Create and Configure the Network.       138         12.4.2.       Create and Configure the Network.       138         12.4.2.1.       Initialize the Network:       138         12.4.2.2.       Configure the Nodes:       138         12.4.3.       Choose the Statistics       139         12.4.4.       The Firewall Scenario       139         12.4.5.       Firewall Scenario       141         12.4.6.       The Firewall VPN Scenario       141         12.4.6.       The Firewall VPN Scenario       141         12.4.6.2.       Simulating Encryption:       142         12.4.7.       Run the Simulation       143         12.4.8.       View the Results       143         12.4.9.       Further readings       145         12.4.7.       Run the Simulation	11.5. Further readings	130
11.7.       Laboratory - Firewalls and VPN (Network Security and Virtual Private Networks)       137         12.       Laboratory - Firewalls and VPN (Network Security and Virtual Private Networks)       137         12.1.       Objective       137         12.2.       Overview       137         12.3.       Prelab Activities       137         12.4.       Procedure       137         12.4.1.       Create a New Project       137         12.4.2.       Create and Configure the Network       138         12.4.2.       Create and Configure the Network       138         12.4.2.2.       Configure the Nodes:       138         12.4.3.       Choose the Statistics       139         12.4.4.       The Firewall Scenario       139         12.4.5.       Firewalls and VPN       140         12.4.6.       The Firewall VPN Scenario       141         12.4.6.       The Firewall VPN Scenario       141         12.4.6.1.       Configure the VPN:       141         12.4.6.2.       Simulation       143         12.4.5.       Further readings       143         12.4.6.       Net we Results       143         12.4.6.       Simulation       144         12.	11.7 Lab Papart	120
12.1.       Objective	12 Laboratory Eirowalls and V/DN (Network Security and Virtual Private Networks)	127
12.1.       Objective       137         12.2.       Overview       137         12.3.       Prelab Activities       137         12.4.       Procedure       137         12.4.1.       Create a New Project       137         12.4.2.       Create and Configure the Network       138         12.4.2.       Create and Configure the Network       138         12.4.2.       Create and Configure the Network       138         12.4.2.       Configure the Nodes:       138         12.4.2.       Configure the Nodes:       138         12.4.2.2.       Configure the Nodes:       138         12.4.3.       Choose the Statistics       139         12.4.4.       The Firewall Scenario       139         12.4.5.       Firewall Scenario       140         12.4.6.       The Firewall VPN Scenario       140         12.4.6.       The Firewall VPN Scenario       141         12.4.6.1.       Configure the VPN:       141         12.4.6.2.       Simulation       143         12.4.7.       Run the Simulation       143         12.4.8.       View the Results       143         12.5.       Further readings       145	12. Laboratory - Firewails and VFN (Network Security and Virtual Filvate Networks)	127
12.2.       Overview       137         12.3.       Prelab Activities       137         12.4.       Procedure       137         12.4.1.       Create a New Project       137         12.4.2.       Create and Configure the Network       138         12.4.2.       Create and Configure the Network       138         12.4.2.       Configure the Nodes:       138         12.4.2.       Configure the Nodes:       138         12.4.3.       Choose the Statistics       139         12.4.4.       The Firewall Scenario       139         12.4.5.       Firewall Scenario       140         12.4.6.       The Firewall VPN Scenario       141         12.4.6.       Configure the VPN:       141         12.4.6.       Simulating Encryption:       142         12.4.7.       Run the Simulation       143         12.4.8.       View the Results       143         12.5.       Further readings       145         12.6.       Exercises       145         12.7.       Lab Report       146         13.       Laboratory - Applications (Network Application Performance Analysis)       147         13.1.       Objective       147 <tr< td=""><td>12.1. Objective</td><td>127</td></tr<>	12.1. Objective	127
12.4.       Procedure       137         12.4.       Create a New Project       137         12.4.1.       Create and Configure the Network       138         12.4.2.       Create and Configure the Network       138         12.4.2.1.       Initialize the Network:       138         12.4.2.2.       Configure the Nodes:       138         12.4.3.       Choose the Statistics       139         12.4.4.       The Firewall Scenario       139         12.4.5.       Firewalls and VPN       140         12.4.6.       The Firewall Scenario       141         12.4.6.       The Firewall VPN Scenario       141         12.4.6.       The Firewall VPN Scenario       141         12.4.6.       Simulating Encryption:       142         12.4.7.       Run the Simulation       143         12.4.8.       View the Results       143         12.5.       Further readings       145         12.6.       Exercises       145         12.6.       Exercises       145         12.7.       Lab Report       146         13.       Laboratory - Applications (Network Application Performance Analysis)       147         13.1.       Objective       147 <td>12.2. Overview</td> <td>137</td>	12.2. Overview	137
12.4.       Indecenter       137         12.4.1.       Create a New Project       137         12.4.2.       Create and Configure the Network       138         12.4.2.1.       Initialize the Network:       138         12.4.2.2.       Configure the Nodes:       138         12.4.2.3.       Choose the Statistics       139         12.4.4.       The Firewall Scenario       139         12.4.5.       Firewalls and VPN       140         12.4.6.       The Firewall Scenario       141         12.4.6.       The Firewall VPN Scenario       141         12.4.6.       The Firewall VPN Scenario       141         12.4.6.       The Firewall VPN Scenario       141         12.4.6.       Simulating Encryption:       142         12.4.7.       Run the Simulation       143         12.4.8.       View the Results       143         12.5.       Further readings       145         12.6.       Exercises       145         12.6.       Exercises       145         12.7.       Lab Report       146         13.       Laboratory - Applications (Network Application Performance Analysis)       147         13.1.       Objective       147	12.5. Fleidd Activities	137
12.4.1.       Oreate and Configure the Network       138         12.4.2.       Create and Configure the Network       138         12.4.2.1.       Initialize the Network:       138         12.4.2.2.       Configure the Nodes:       138         12.4.3.       Choose the Statistics       139         12.4.4.       The Firewall Scenario       139         12.4.5.       Firewalls and VPN       140         12.4.6.       The Firewall VPN Scenario       141         12.4.6.1.       Configure the VPN:       141         12.4.6.2.       Simulating Encryption:       142         12.4.7.       Run the Simulation       143         12.4.8.       View the Results       143         12.5.       Further readings       145         12.6.       Exercises       145         12.6.       Exercises       145         12.6.       Exercises       145         12.7.       Lab Report       146         13.       Laboratory - Applications (Network Application Performance Analysis)       147         13.2.       Overview       147         13.3.       Prelab Activities       147         13.4.       Procedure       148	12.4. Trocedure	137
12.4.2.1       Initialize the Network:       138         12.4.2.1       Initialize the Network:       138         12.4.2.2       Configure the Nodes:       138         12.4.3       Choose the Statistics       139         12.4.4       The Firewall Scenario       139         12.4.5       Firewalls and VPN       140         12.4.6       The Firewall VPN Scenario       141         12.4.6.1       Configure the VPN:       141         12.4.6.2       Simulating Encryption:       142         12.4.7       Run the Simulation       143         12.4.8       View the Results       143         12.4.8       View the Results       143         12.5       Further readings       145         12.6       Exercises       145         12.7       Lab Report       146         13       Laboratory - Applications (Network Application Performance Analysis)       147         13.2       Overview       147         13.3       Prelab Activities       147         13.4       Procedure       148         13.4.1       Open the Application Characterization Environment       148	12.4.1. Create and Configure the Network	138
12.4.2.1.       Initialize the Nodes:       138         12.4.2.2.       Configure the Nodes:       138         12.4.3.       Choose the Statistics       139         12.4.4.       The Firewall Scenario       139         12.4.5.       Firewall Scenario       140         12.4.6.       The Firewall VPN Scenario       141         12.4.6.       The Firewall VPN Scenario       141         12.4.6.1.       Configure the VPN:       141         12.4.6.2.       Simulating Encryption:       142         12.4.7.       Run the Simulation       143         12.4.8.       View the Results       143         12.5.       Further readings       145         12.6.       Exercises       145         12.6.       Exercises       145         12.6.       Exercises       145         12.7.       Lab Report       146         13.       Laboratory - Applications (Network Application Performance Analysis)       147         13.2.       Overview       147         13.3.       Prelab Activities       147         13.4.       Procedure       148         13.4.1.       Open the Application Characterization Environment       148	12.4.2.1 Initialize the Network $12.4.2.1$	138
12.4.3.Choose the Statistics13912.4.4.The Firewall Scenario13912.4.5.Firewalls and VPN14012.4.6.The Firewall VPN Scenario14112.4.6.1.Configure the VPN:14112.4.6.2.Simulating Encryption:14212.4.7.Run the Simulation14312.4.8.View the Results14312.5.Further readings14512.6.Exercises14512.7.Lab Report14613.Laboratory - Applications (Network Application Performance Analysis)14713.1.Objective14713.2.Overview14713.4.Procedure14813.4.1.Open the Application Characterization Environment148	12.4.2.2 Configure the Nodes:	138
12.4.3.       The Firewall Scenario	12/13 Choose the Statistics	130
12.4.5.Firewalls and VPN	12.4.0. The Firewall Scenario	130
12.4.6.The Firewall VPN Scenario.14112.4.6.Configure the VPN:14112.4.6.1.Configure the VPN:14112.4.6.2.Simulating Encryption:14212.4.7.Run the Simulation14312.4.8.View the Results14312.5.Further readings14512.6.Exercises14512.7.Lab Report14613.Laboratory - Applications (Network Application Performance Analysis)14713.1.Objective14713.2.Overview14713.3.Prelab Activities14713.4.Procedure14813.4.1.Open the Application Characterization Environment148	12.4.5 Firewalls and VPN	140
12.4.6.1.Configure the VPN:14112.4.6.2.Simulating Encryption:14212.4.7.Run the Simulation14312.4.8.View the Results14312.5.Further readings14512.6.Exercises14512.7.Lab Report14613.Laboratory - Applications (Network Application Performance Analysis)14713.1.Objective14713.2.Overview14713.3.Prelab Activities14713.4.1.Open the Application Characterization Environment148	12.4.6 The Firewall VPN Scenario	141
12.4.6.2.Simulating Encryption:14212.4.7.Run the Simulation14312.4.8.View the Results14312.5.Further readings14512.6.Exercises14512.7.Lab Report14613.Laboratory - Applications (Network Application Performance Analysis)14713.1.Objective14713.2.Overview14713.3.Prelab Activities14713.4.Procedure14813.4.1.Open the Application Characterization Environment148	12.4.6.1 Configure the VPN	141
12.4.7.Run the Simulation14312.4.8.View the Results14312.5.Further readings14512.6.Exercises14512.7.Lab Report14613.Laboratory - Applications (Network Application Performance Analysis)14713.1.Objective14713.2.Overview14713.3.Prelab Activities14713.4.Procedure14813.4.1.Open the Application Characterization Environment148	12.4.6.2 Simulating Encryption:	142
12.4.8.View the Results	1247 Bun the Simulation	143
12.5.Further readings14512.6.Exercises14512.7.Lab Report14613.Laboratory - Applications (Network Application Performance Analysis)14713.1.Objective14713.2.Overview14713.3.Prelab Activities14713.4.Procedure14813.4.1.Open the Application Characterization Environment148	12.4.8. View the Besults	143
12.6.Exercises14512.7.Lab Report14613.Laboratory - Applications (Network Application Performance Analysis)14713.1.Objective14713.2.Overview14713.3.Prelab Activities14713.4.Procedure14813.4.1.Open the Application Characterization Environment148	12.5 Further readings	145
12.7.Lab Report.14613.Laboratory - Applications (Network Application Performance Analysis)14713.1.Objective.14713.2.Overview.14713.3.Prelab Activities14713.4.Procedure14813.4.1.Open the Application Characterization Environment148	12.6. Exercises	145
13. Laboratory - Applications (Network Application Performance Analysis)14713.1. Objective14713.2. Overview14713.3. Prelab Activities14713.4. Procedure14813.4.1. Open the Application Characterization Environment148	12.7. Lab Report	146
13.1.Objective	13. Laboratory - Applications (Network Application Performance Analysis)	147
13.2.Overview	13.1. Objective	147
13.3.Prelab Activities14713.4.Procedure14813.4.1.Open the Application Characterization Environment148	13.2. Overview	147
13.4.Procedure	13.3. Prelab Activities	147
13.4.1. Open the Application Characterization Environment	13.4. Procedure	148
	13.4.1. Open the Application Characterization Environment	148

13.4.2.	Visualize the Application	1	48
13.4.3.	Analyze with AppDoctor	1	50
13.4.4.	Examine the Statistics	1	53
13.4.5.	Ideal TCP Window Size	1	55
13.4.6.	Impact of Network Bandwidth	1	56
13.4.7.	Deploy an Application	1	57
13.4.7.1.	Run the Simulation and View the Results:	1	59
13.5. Furt	her readings	1	60
13.6. Exe	rcises	1	60
13.7. Lab	Report	1	61
14. Laboratory	y - Wireless Local Area Network (Medium Access Control for Wirelessly		
Connecte	d Stations)	1	62
14.1. Obje	ective	1	62
14.2. Ove		1	62
14.3. Prel	ab Activities	1	63
14.4. Proc		1	63
14.4.1.	Create a New Project	1	63
14.4.2.	Create and Configure the Network	1	63
14.4.2.1.	Configure the wireless nodes:	1	64
14.4.2.2.	I raffic Generation Parameters:	1	64
14.4.3.	Choose the Statistics	1	65
14.4.4.	Configure the Simulation	1	66
14.4.5.	Duplicate the Scenario	1	66
14.4.5.1.	The DCF_Frag Scenario:	1	66
14.4.5.2	The DCF_PCF Scenario:	1	6/
14.4.5.3.	Ine DCF_PCF_Frag Scenario:	1	6/
14.4.6.		1	68
14.4.7.	View the Results	1	68 74
14.5. Furt	ner readings	1	/
14.0. EXE	ICISES	1	71
14./. Lab	Repoil	I	/ 1
15. Laboratory		1	72
15 1 Obic		1	72
15.1. Obje		1	72
15.2. Ove	ab Activitios	1	72
15.0. The		1	72
15 4 1	Create a New Project	1	72
15.4.1	Create and Configure the Network	1	73
15 4 2 1	Initialize the Network	1	73
15422	Configure the Applications:	1	74
15423	Configure the Profiles	1	74
15424	Configure the Applications in the Server and Clients	1	75
15425	Configure the Trajectory	1	75
15.4.3.	Configure the Simulation	1	76
15.4.4.	Choose the Statistics	1	78
1545	Duplicate the Scenario	1	78
15.4.6	Run the Simulation	1	79
15.4.7	View the Results	1	79
15.5 Furt	her readings	1	82
15.6. Exe	rcises	1	82
15.7. Lab	Report	1	82
	-		

#### NETWORK SIMULATION EXPERIMENTS MANUAL

Prepared by Professor Hmad Aboelela, University of Massachusetts/Dartmouth



 $\mathsf{A} \Longrightarrow \mathsf{S} \, \mathsf{Y} \, \mathsf{S} \, \mathsf{T} \, \mathsf{E} \, \mathsf{M} \, \mathsf{S} \Longrightarrow \mathsf{A} \, \mathsf{P} \, \mathsf{P} \, \mathsf{R} \, \mathsf{O} \, \mathsf{A} \, \mathsf{C} \, \mathsf{H}$ 

#### LARRY L. PETERSON AND BRUCE S. DAVIE

# NETWORK SIMULATION

# EXPERIMENTS MANUAL

## Prepared by Emad Aboelela, Ph.D.

University of Massachusetts Dartmouth

## NETWORK SIMULATION EXPERIMENTS MANUAL

### Second Edition



ELSEVIER

AMSTERDAM • BOSTON • HEIDELBERG • LONDON • NEW YORK • OXFORD PARIS • SAN DIEGO • SAN FRANCISCO • SINGAPORE • SYDNEY • TOKYO

Morgan Kaufmann is an imprint of Elsevier



MORGAN KAUFHANN PUBLISHERS

Acquisitions Editor	Rick Adams
Publishing Services Manager	George Morrison
Senior Production Kditor	Paul Gottchrer
Editorial Assistant	Gregory Chalson
Cover Design	Eric DeCicco
Interior Printer	Maple-Vail Book Manufacturing Group
Cover Printer	Phoenix Color Corp.

Morgan Kaufmann Publishers is an imprint of Elsevier.

30 Corporate Drive, Suite 4(K). Burlington. MA 01803. USA

This book is printed on acid-free paper.

© 2008 by Elsevier Inc. All rights reserved.

Designations used by companies to distinguish their products are often claimed as trademarks or registered trademarks. In all instances in which Morgan Kaufmann Publishers is aware of a claim, the product names appear in initial capital or all capital letters. Readers, however, should contact the appropriate companies for more complete information regarding trademarks and registration.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means - electronic, mechanical, photocopying, scanning, or otherwise - without prior written permission of the publisher.

Permissions may be sought directly from Elsevier's Science & Technology Rights Department in Oxford, UK: phone: (+44) 1865 843830. fax: (+44) 1865 853333, E-mail: permissions@elsevier.com. You may also complete your request online via the Elsevier homepage (<u>http://elsevier.com</u>), by selecting "Support & Contact" then "Copyright and Permission" and then "Obtaining Permissions."

#### Library of Congress Cataloging-in-Publication Data

Application submitted

ISBN: 978-0-12-373974-2

For information on all Morgan Kaufmann publications visit our Web site at <u>www.mkp.com</u> or <u>www.books.elsevier.com</u>

Printed in The United States of America 09 10  $11 \Rightarrow 5432$ 

Working together to grow libraries in developing countries

www.dievier.com | www.bookaid.org | www.sabrc.org

# Contents

#### Laboratory - Introduction (Basics of OPNET IT Guru Academic Edition) 2 0.

#### 0.1. Objective

This lab teaches you the basics of using OPNET IT Guru Academic Edition. OPNET IT Guru Academic Edition enables students to better understand the core concepts of networking and equips them to effectively troubleshoot and manage real-world network infrastructures.

> In this lab, you will learn the basics of the OPNET IT Guru Academic Edition software. You will learn how to setup and run OPNET IT Guru Academic Edition. You will become familiar with some of its capabilities by running some tutorials.

#### 0.3. Prelab Activities

Read Chapter 1 from "Computer Networks: A Systems Approach", 4th Edition.

Go to www.net-seal.net/animations.php and play the following animation:

- No Network. •
- 1. Laboratory - *Ethernet* (A *Direct Link Network* with Media Access Control) 6

#### 1.1. Objective

This lab is designed to demonstrate the operation of the **Ethernet** network. The simulation in this lab will help you examine the performance of the Ethernet network under different scenarios.

> In this lab you will set up an Ethernet with thirty nodes connected via a coaxial link in a *bus topology*. The coaxial link is operating at a data rate of 10 Mbps. You will study how the throughput of the network is affected by the network load as well as the size of the packets.

#### 1.3. Prelab Activities

Read section 2.6 from "Computer Networks: A Systems Approach", 4" Edition.

Go to *www.net-seal.net/animations.php* and play the following animation:

Hub.

#### 2. Laboratory - Token Ring (A Shared-Media Network with Media Access Control) 17

#### 2.1. Objective

This lab is designed to demonstrate the implementation of a **token ring** network. The simulation in this lab will help you examine the performance of the token ring network under different scenarios.

#### 2.3. Prelab Activities

In this lab, you will set up a token ring network with 14 nodes connected in a star topology. The links you will use operate at a data rate of 4 Mbps. You will study how the utilization and delay of the network are affected by the network load as well as the token holding time THT.

Read section 2.7 from "Computer Networks: A Systems Approach", 4th Edition.

#### Laboratory - Switched LANs (A Set of Local Area Networks Interconnected 3. by Switches) 32

#### 3.1. Objective

This lab is designed to demonstrate the implementation of switched local area networks. The simulation in this lab will help you examine the performance of different implementations of local network simulation experiments manual.doc utorak, 28. rujan 2010 1 area networks connected by *switches* and *hubs*.

In this lab you will set up switched LANs using two different *switching devices*: *hubs* and *switches*. A hub forwards the packet that arrives on any of its inputs on all the outputs regardless of the destination of the packet. On the other hand, a switch forwards incoming packets to one or more outputs depending on the destination(s) of the packets. You will study how the *throughput* and *collision* of packets in a switched network are affected by the *configuration of the network* and the *types of switching devices* that are used.

#### 3.3. Prelab Activities

Read section 3.1 from "Computer Networks: A Systems Approach", 4th Edition.

Go to *www.net-seal.net/animations.php* and play the following animations:

- <u>Hub</u>.
- <u>Switch</u>.
- <u>Switched Network With No Server</u>.
- <u>Switched Network With Server</u>
- Laboratory *Network Design* (Planning a Network with Different Users, Hosts, and Services)
   42

#### 4.1. Objective

The objective of this lab is to demonstrate the basics of **designing a network**, taking into consideration the *users*, *services*, and *locations of the hosts*.

In this lab you will design a network for a company that has four departments: Research, Engineering, E-Commerce, and Sales. You will utilize a LAN model that allows you to simulate multiple clients and servers in one simulation object. This model dramatically reduces both the amount of configuration work you need to perform and the amount of memory needed to execute the simulation. You will be able to define a profile that specifies the pattern of applications employed by the users of each department in the company. By the end of this lab, you will be able to study how different design decisions can affect the performance of the network.

#### 4.3. Prelab Activities

• Read section 3.2 from "Computer Networks: A Systems Approach", 4th Edition.

Go to <u>www.net-seal.net/animations.php</u> and play the following animations:

• Adding Switches.

#### 5. Laboratory - ATM: *Asynchronous Transfer Mode* (A Connection-Oriented, Cell-Switching Technology) 51

#### 5.1. Objective

The objective of this lab is to examine the effect of **ATM** adaptation layers and service classes on the performance of the network.

In this lab you will set up an *ATM network* that carries three applications: *Voice*, *Email*, and *FTP*. You will study how the choice of the adaptation layer as well as the service classes can affect the performance of the applications.

#### 5.3. Prelab Activities

• Read section 3.3 from "Computer Networks: A Systems Approach", 4th Edition.

#### Laboratory - RIP: *Routing Information Protocol* (A Routing Protocol Based on the Distance-Vector Algorithm) 65

#### 6.1. Objective

The objective of this lab is to configure and analyze the performance of the **Routing Information Protocol** (RIP) model.

In this lab you will set up a network that utilizes RIP as its *routing protocol*. You will analyze the *routing tables* generated in the *routers*, and you will observe how RIP is affected by *link failures*. You will also utilize the ICMP (Internet Control Message Protocol) to create *echo reply messages* (i.e., *ping*) to analyze the created routes.

#### 6.3. Prelab Activities

• Read sections 4.1.5, 4.1.7, and 4.2.2 from *"Computer Networks: A Systems Approach"*, 4th *Edition.* 

Go to <u>www.net-seal.net/animations.php</u> and play the following animations:

- The Address Resolution Protocol (ARP). <u>Example1</u>, <u>Example2</u>, <u>Example3</u>.
- <u>ARP with Multiple Networks</u>.
- Routing and Forwarding.
- Laboratory OSPF: *Open Shortest Path First* (A Routing Protocol Based on the Link-State Algorithm) 76

#### 7.1. Objective

The objective of this lab is to configure and analyze the performance of the **Open Shortest Path First** (OSPF) routing protocol.

In this lab, you will set up a network that utilizes OSPF as its *routing protocol*. You will analyze the *routing tables* generated in the routers and will observe how the resulting routes are affected by assigning areas and enabling load balancing.

#### 7.3. Prelab Activities

 Read sections 4.2.3 and 4.2.4 from "Computer Networks: A Systems Approach". 4th Edition.

Go to *www.net-seal.net/animations.php* and play the following animation:

- Routing and forwarding.
- 8. Laboratory BGP: *Border Gateway Protocol* (An Interdomain Routing Protocol) 86

#### 8.1. Objective

The objective of this lab is to simulate and study the basic features of an interdomain routing protocol called **Border Gateway Protocol** (BGP).

In this lab you will set up a network with *three different ASs* (Autonomous Systems). RIP will be used as the intradomain routing protocol and BGP as the interdomain one. You will analyze the *routing tables* generated in the *routers* as well as the effect of applying a simple policy.

#### 8.3. Prelab Activities

• Read section 4.3 from "Computer Networks: A Systems Approach", 4th Edition.

Go to *www.net-seal.net/animations.php* and play the following animation:

• IP Subnets.

- 9. Laboratory TCP: *Transmission Control Protocol* (A Reliable, Connection-Oriented, Byte-Stream Service) 98
- 9.1. Objective
- This lab is designed to demonstrate the congestion control algorithms implemented by the **Transmission Control Protocol** (TCP). The lab provides a number of scenarios to simulate these algorithms. You will compare the performance of the algorithms through the analysis of the simulation results.

In this lab you will set up a network that utilizes TCP as its *end-to-end transmission* protocol and analyze the size of the *congestion window* with different mechanisms.

- 9.3. Prelab Activities
  - Read sections 5.1 and 5.2 from "Computer Networks: A Systems Approach", 4th Edition.

Go to *www.net-seal.net/animations.php* and play the following animations:

- <u>TCP Connections</u>.
- <u>TCP Multiplexing</u>.
- <u>TCP Buffering and Sequencing</u>.
- <u>User Datagram Protocol (UDP)</u>.
- 10. Laboratory *Queuing Disciplines* (Order of Packet Transmission and Dropping) 109

#### 10.1. Objective

The objective of this lab is to examine the effect of different **queuing disciplines** on *packet delivery* and *delay* for *different services*.

In this lab you will set up a network that carries three applications: *FTP*, *Video*, and *VoIP*. You will study how the choice of the *queuing discipline* in the routers can affect the performance of the applications and the utilization of the network resources.

10.3. Prelab Activities

• Read section 6.2 from "Computer Networks: A Systems Approach", 4th Edition.

Go to *www.net-seal.net/animations.php* and play the following animations:

- <u>Switch Congestion</u>.
- <u>IP Fragmentation</u>.
- 11. Laboratory RSVP: *Resource Reservation Protocol* (Providing QoS by Reserving Resources in the Network) 121

#### 11.1. Objective

The objective of this lab is to study the **Resource Reservation Protocol** (RSVP) as a part of the *Integrated Services approach* to providing *Quality of Service* (QoS) to individual applications or flows.

In this tab you will set up a network that carries *real-time applications* and that utilizes RSVP to provide QoS to one of these applications. You will study how RSVP contributes to the performance of the application that makes use of it.

#### 11.3. Prelab Activities

Read section 6.5 from "Computer Networks: A Systems Approach", 4th Edition.

Go to *www.net-seal.net/animations.php* and play the following animation:

• <u>TCP Flow Control</u>.

## 12. Laboratory - *Firewalls* and *Virtual Private Networks* (VPN and Network Security) 137

#### 12.1. Objective

The objective of this lab is to study the role of **firewalls** and Virtual Private Networks VPNs) in providing **security** to shared public networks such as the Internet.

In this lab you will set up a network where servers are accessed over the Internet by customers who have different privileges. You will study how firewalls and VPNs can provide *security* to the information in the servers while maintaining access for customers with the appropriate privilege.

#### 12.3. Prelab Activities

Read section 4.5.3 from "Computer Networks: A Systems Approach", 4th Edition.
 Firewalls

#### 13. Laboratory - Applications (Network Application Performance Analysis) 147

#### 13.1. Objective

The objective of this lab is to analyze the performance of an Internet application protocol and its relation to the underlying network protocols. In addition, this lab reviews some of the topics covered in previous labs.

In this lab you will analyze the performance of an FTP application. You will analyze the *probable bottlenecks* for the application scenario under investigation. You will also study the sensitivity of the application to different network conditions such as *bandwidth* and *packet loss*. The trace was captured on a real network, which is shown in the figure below, and already imported into ACE. The FTP application runs on that network; the client connects to the server over a 768 Kbps Frame Relay circuit with 36 ms of latency. The FTP application downloads a 1 MB file in 37 seconds. Normally the download time for a file this size should be about 11 seconds.

#### 13.3. Prelab Activities

 Read sections 9.1.1 and 9.1.3 from "Computer Networks: A Systems Approach" 4th Edition.

Go to *www.net-seal.net/animations.php* and play the following animations:

- Internet Access.
- Email Protocols

## 14. Laboratory - *Wireless Local Area* Network (Medium Access Control for Wirelessly Connected Stations) 161

#### 14.1. Objective

This lab addresses the **Medium Access Control** (MAC) sublayer of the **IEEE 802.11 standard** for WLAN (wireless local area network). Different options of this standard are studied in this lab. The performance of these options is analyzed under different scenarios.

#### 14.3. Prelab Activities

- Read section 2.8.2 from "Computer Networks: A Systems Approach", 4th Edition.
- Laboratory *Mobile Wireless Network* (A Wireless Local Area Network with Mobile Stations) 173

#### 15.1. Objective

This lab simulates mobility in wireless local area network. The effect of mobility on the TCP

performance is studied. In addition, the lab studies how the request to send (RTS) and clear to send (CTS) frames are utilized in avoiding the hidden node problem usually induced by mobility in WLAN.

In this lab we will simulate a wireless LAN with *mobile workstations* and *server*. The workstations will run an FTP application to upload files to the server. We will study the *effect of node mobility* on the performance of the TCP connection for the *FTP session*. We will study also the role of the *request to send* (RTS) and *clear to send* (CTS) frames in avoiding the *hidden node problem* usually induced by mobility in wireless LAN.

#### 15.3. Prelab Activities

- Read sections 2.8.2 and 4.2.5 from *"Computer Networks: A Systems Approach"* 4th *Edition.* 
  - Wireless Network and Multiple Access with Collision Avoidance

1										
	2.6 2.7	3.1 3.2	4.3	5.1 5.2	6.2 6.5					
	202	3.3	445					011		
	2.8.2		4.1.5					9.1.1		
			4.1.7					9.1.3		
			4.2.2							
			4.2.3							
			4.2.4							
			4.2.5							
			4.5.3							
	1									
	2.6									
			2.7	'						
	2.8.2									

<del>2.8.2</del> 3.1 3.2 3.3 4.1.5 4.1.7 4.2.2 4.2.3 4.2.4 4.2.5 4.3 4.5.3 5.1 5.2 6.2 6.5 9.1.1 9.1.3

### Preface

Welcome to the Network Simulation Experiments Manual, 2<sup>nd</sup> Edition. As networking systems have become more complex and expensive, hands-on experiments based on networking simulation have become essential for teaching the key computer networking topics to students and professionals. The simulation approach is highly useful because it provides a virtual environment for a variety of desirable features such as modeling a network based on specified criteria and analyzing its performance under different scenarios.

This manual has 15 laboratory experiments that cover a variety of networking designs and protocols. The experiments in this manual do not require programming skills as a prerequisite. They are generic and can be easily expanded to utilize new technologies and networking standards. With the free easy-to-install software, the OPNET IT Guru Academic Edition, networking students and professionals can implement the experiments from the convenience of their homes or workplaces. The manual is suitable for a single-semester course on computer networking at the undergraduate or beginning graduate level. Professors can pick the experiments that arc appropriate to their class.

The new materials in the  $2^{nd}$  edition of the manual are:

- A new **Prelab Activities** section in every laboratory assignment. This section includes recommended readings from the textbook as well as references to animations from the Net-SEAL project (www.net-seal.net)<sup>1</sup>. These activities are intended to reinforce the student's understanding of the concepts related to the topics covered in the laboratory.
- Two new laboratory experiments to cover wireless networking protocols.
- One new laboratory experiment to cover the Border Gateway Protocol (BGP).
- A new component to address the ICMP protocol has been added to the RIP lab.
- A new component to address the effect of encryption has been added to the VPN lab.

**OPNET IT Guru Academic Edition** provides a virtual environment for modeling, analyzing, and predicting the performance of IT infrastructures, including applications, servers, and networking technologies. Based on OPNET's award-winning IT Guru product, Academic Edition is designed to complement specific lab exercises that teach fundamental networking concepts. The commercial version of IT Guru has broader capabilities designed for the enterprise II environment, documentation, and professional support. OPNET software is used by thousands of commercial and government organizations worldwide, and by over 500 universities. For more information, visit www.opnet.com. OPNET and IT Guru are trademarks of OPNET Technologies, Inc.

I would like to extend my appreciation to Professor Larry Peterson and Dr. Bruce Davie for giving me the opportunity to associate the laboratory experiments of this manual with their valuable book. I want to thank the folks at Morgan Kaufmann who have helped to bring this project to life. Many thank to the reviewers from academia and OPNET, who read through the various drafts of the experiments and provided me with extremely valuable feedback. My gratitude to the Net-SEAL project team, with special appreciation to Neal Charbonneau for the superb job he did in the project. I want to thank my family for their consideration and enthusiastic assurance throughout the development of this project. Last, but not least, I want to thank you for choosing the manual. I welcome your emails to report bug or to suggest improvements.

Emad Aboclela, Ph.D. eaboclela@umassd.edu University of Massachusetts Dartmouth July 2007.

<sup>&</sup>lt;sup>1</sup> The materials in the <u>www.ncl-scal.net</u> website are based upon work supported by the National Science Foundation under Grant No. DUF-0536388. Any opinions, findings and conclusions or recommendations expressed in this website are those of the Net-SEAL project team and do not necessarily reflect the views of the National Science Foundation (NSF). network simulation experiments manual.doc utorak, 28. rujan 2010

#### 0. Laboratory - Introduction (Basics of OPNET IT Guru Academic Edition)

#### 0.1. *Objective*

This lab teaches you the basics of using OPNET IT Guru Academic Edition. OPNET IT Guru Academic Edition enables students to better understand the core concepts of networking and equips them to effectively <u>troubleshoot</u> and manage real-world network infrastructures.

#### 0.2. Overview

OPNET's IT Guru provides a Virtual Network Environment that models the behavior of your entire network, including its routers, switches, protocols, servers, and individual applications. By working in the Virtual Network Environment, IT managers, network and system planners, and operations, staff are empowered to diagnose difficult problems more effectively, validate changes before they are implemented, and plan for future scenarios including growth and failure.

OPNET's **Application Characterization** Environment (ACE) module for IT Guru enables enterprises to identify the root cause of end-to-end application performance problems and to solve them cost-effectively by understanding the impact of changes.

In this lab, you will learn the basics of the **OPNET IT Guru Academic Edition** software. You will learn how to setup and run **OPNET IT Guru Academic Edition**. You will become familiar with some of its capabilities by running some tutorials.

The labs in this manual are implemented with **OPNET IT Guru Academic Edition** release 9.1.A (Build 1997). If you want to download the software, please visit the following site to register with OPNET technology:

www.opnet.com/university\_program/itguru\_academic\_edition/

http://www.opnet.com/itguru-academic/registration.html

Recommended System Configuration, Platforms, and Software:

- 1.5 GHz processor or better
- 512 MB 2 GB RAM
- 1 GB disk space
- Display: 1024 x 768 or higher resolution, 256 or more colors
- Adobe Acrobat reader.
- The English language version of the following operating systems are supported:
  - Microsoft Windows NT (Service Pack 3.5, or 6a)
  - Windows 2000 Professional (Service Pack 1, 2, and 4 are supported but not required)

Windows XP (Service Pack 1 is required; Service Pack 2 is supported but not required.)

#### 0.3. Prelab Activities

- Read Chapter 1 from "Computer Networks: A Systems Approach", 4th Edition.
   Go to <u>www.net-seal.net/animations.php</u> and play the following animation:
  - <u>No Network</u>.

#### 0.4.1. Start OPNET IT Guru Academic Edition

To start OPNET IT Guru Academic Edition:

- 1. Click on Start  $\Rightarrow$  Programs  $\Rightarrow$  OPNET IT Guru Academic Edition x.x  $\Rightarrow$  OPNET IT Guru Academic Edition, where x.x is the software version (e.g., 9.1)
- 2. Read the Restricted Use Agreement and if you agree, click I have read this SOFTWARE AGREEMENT and I understand and accept the terms and conditions described herein.

Now you should see the starting window of **OPNET IT Guru Academic Edition** as shown:



#### 0.4.2. Check the OPNET Preferences

The OPNET Preferences let you display and edit environment attributes, which control program operations. In this lab you will check three of these attributes.

- 1. After starting OPNET, from the Edit menu, choose Preferences.
- 2. The list of environment attributes is sorted alphabetically according to name. You can locate attributes faster by typing any part of the attribute's name in the **Find** field.
- 3. Check the value of the **license\_server** attribute. It has the name of the License Server's host. If IT Guru is getting its license from the local host (i.e., the computer on which the software was installed), the value of **license\_server** should be **localhost** as shown in the following figure.

Eind				
Name	Value	Source	Group	-
license_port	port_a	default	Licensing	
license_server	-> localhost	default	Licensing	
license_server_standalone	TRUE	changed	Licensing	
license_server_standalone_diagnose	FALSE	default	Licensing	
license_username	<null></null>	default	Licensing	
load_image	<null></null>	default	GUI	
manage_licenses	FALSE	default	GUI	
mark_nondefault_attrs	FALSE	default	GUI	
mark_nondefault_attrs.changed_color		default	GUI	
mark_nondefault_attrs.intended_color	#BFBFFF	default	GUI	
* mem_clear	0	default	Development	
* mem_optimize	TRUE	default	Development	
* mem_shred	FALSE	default	Development	
* mem_track	FALSE	default	Development	
* mem_track_object	<null></null>	default	Development	
mod_dirs 🔶		els, C:\D env. file	File	
* model_name	<null></null>	default	GUI	
movo dolta	10	dofault	CI II	

- 4. Set the **license\_server\_standalone** attribute to TRUE. This attribute specifies whether the program acts as its own license server.
- 5. A model directory is a directory that contains OPNET model files. If the directory is listed in the mod\_dirs environment attribute, then OPNET programs will use the models in that directory. Check the value of the mod\_dirs attribute. The first directory in the list is where your own models will be saved. In the future you might need to access that directory to back up, copy, or move your models. IT Guru saves numerous files for every single project you create.
- 6. Click **OK** to close the dialog box.

#### 0.4.3. Run the Introduction Tutorial

Now you will run the introductory tutorial that teaches you the basics of using OPNET IT Guru.

- 1. From the Help menu, select Tutorial.
- 2. Go over the Introduction lesson from the list of Basic Lessons.

#### 0.4.4. Run the Small Internetworks Tutorial

In this tutorial you will learn how to use OPNET IT Guru features to build and analyze network models.

- 1. From the Help menu, select Tutorial.
- 2. Carry out the <u>Small Internetworks</u> tutorial from the list of *Basic Lessons*.

#### 0.5. Further readings

- OPNET <u>Standard Network Applications</u>: From the **Protocols** menu, select **Applications**  $\Rightarrow$  **Model Usage Guide**  $\Rightarrow$  <u>Standard Network Applications</u>.
- From the **Help** menu, select **Tutorial**. ⇒ Carry out the <u>Troubleshooting Tutorial</u> <u>Simulations</u> tutorial from the list of *Basic Lessons*.

#### 0.6. Exercises

1) In the project you created for the Small Internetworks tutorial, add a new scenario as a duplicate of the first\_floor scenario. Name the new scenario expansion2. In the expansion2 scenario expand the network the same way as in the expansion scenario but with 30 nodes in the second floor instead of 15 nodes. Run the simulation and compare the load and delay graphs of this new scenario with the corresponding graphs of the first\_floor and expansion scenarios.

#### 0.7. Lab Report

The laboratory report of this lab (and also all the following labs in this manual) should include the following items/sections:

- 2) A cover page with your name, course information, lab number and title, and date of submission.
- 3) A summary of the addressed topic and objectives of the lab.
- 4) Implementation: a brief description of the process you followed in conducting the implementation of the lab scenarios.
- 5) Results obtained throughout the lab implementation, the analysis of these results, and a comparison of these results with your expectations.
- 6) Answers to the given exercises at the end of the lab. If an answer incorporates new graphs, analysis of these graphs should be included here.
- 7) A conclusion that includes what you learned, difficulties you faced, and any suggested extensions/improvements to the lab.

## 1. Laboratory - Ethernet (A Direct Link Network with Media Access Control)

#### 1.1. Objective

This lab is designed to demonstrate the operation of the Ethernet network. The simulation in this lab will help you examine the performance of the Ethernet network under different scenarios.

#### 1.2. Overview

The Ethernet is a working example of the more general Carrier Sense, Multiple Access with Collision Detect (CSMA/CD) local area network technology. The Ethernet is a multiple-access network, meaning that a set of nodes sends and receives frames over a shared link. The "carrier sense" in CSMA/CD means that all the nodes can distinguish between an idle and a busy link. The "collision detect" means that a node listens as it transmits and can therefore detect when a frame it is transmitting has interfered (collided) with a frame transmitted by another node. The Ethernet is said to be a 1-persistent protocol because an adaptor with a frame to send transmits with probability 1 whenever a busy line goes idle.

In this lab you will set up an Ethernet with thirty nodes connected via a coaxial link in a bus topology. The coaxial link is operating at a data rate of 10 Mbps. You will study how the throughput of the network is affected by the network load as well as the size of the packets.

#### 1.3. Prelab Activities

- Read section 2.6 from *"Computer Networks: A Systems Approach"*, 4" Edition.
  - Go to *www.net-seal.net/animations.php* and play the following animation:
  - <u>Hub</u>.

#### 1.4. Procedure

#### 1.4.1. Create a New Project

To create a new project for the Ethernet network:

- 1. Start **OPNET IT Guru Academic Edition**  $\Rightarrow$  Choose **New** from the **File** menu.
- 2. Select **Project** ⇒ Click **OK** ⇒ Name the project **<your initials>\_Ethernet**, and the scenario **Coax** ⇒ Click **OK**.
- In the Startup Wizard: Initial Topology dialog box, make sure that Create Empty Scenario is selected ⇒ Click Next ⇒ Choose Office from the Network Scale list ⇒ Click Next ⇒ Assign 200 to X Span and keep Y Span as 100 ⇒ Click Next twice ⇒ Click OK.
- 4. Close the *Object Palette* dialog box.



#### 1.4.2. Create the Network

To create our coaxial Ethernet network:

- 1. To create the network configuration, select **Topology**  $\Rightarrow$  **Rapid Configuration**. From the drop-down menu choose **Bus** and Click **OK**.
- 2. Click the **Select Models** button in the *Rapid Configuration* dialog box. From the *Model List* drop-down menu choose **ethcoax** and Click **OK**.
- 3. In the Rapid Configuration dialog box, set the following eight values.

Rapid Configuration: Bus	×
MODELS Node Model ethcoax_station	Number 30 Tap Model eth_tap
PLACEMENT	
● <u>H</u> orizontal	<u>⊆</u> vertical
✓ Top of bus	Left of bus
Bottom of bus	Right of bus
Head of bus	Size
X 20 Y 50	Bus 170 Tap 20
Select Models.	<u>C</u> ancel <u>O</u> K

#### 4. Click OK.

The **eth\_tap** is an Ethernet bus tap that connects a node with the bus.

The eth\_coax is an Ethernet bus that can connects nodes with bus receivers and transmitters via taps.



5. To configure the coaxial bus, right-click on the horizontal link  $\Rightarrow$  Select **Advanced Edit Attributes** from the menu:

6		
	🛣 (bus_0) Attributes	
	Attribute	Value
	Attribute	value
af <u>e E</u> naaf	Image: Provide the second s	bus_0
	? – model	eth_coax
+ +	? - color	eth_coax
1	⑦ – financial cost	Edit
	Ine style	solid
, <u> </u>	? - symbol	none
Letter a	① L thickness	1

- a. Click on the **value** of the **model** attribute ⇒ Select **Edit** from the drop-down menu ⇒ Choose the **eth\_coax\_adv** model.
- b. Assign the value **0.05** to the **delay** attribute (propagation delay in sec/m).
- c. Assign 5 to the thickness attribute.
- d. Click OK.

A higher delay is used here as an alternative to generating higher traffic which would require much longer simulation time.

Thickness specifies the thickness of the line used to "draw" the bus link.

🛣 (bus_0) Attributes	
Attribute	Value
⑦ ⊢ name	bus_0
	eth_coax_adv
⑦ - ber	0,0
⑦ – channel count	1
⑦ – closure model	dbu_closure
⑦ – coll model	dbu_coll
	RGB000
⑦ – condition	enabled
① - cost	0,0
① – data rate	10.000.000
① - delay	0,05 🔶
Pecc model	dbu_ecc
Perror model	dbu_error
⑦ – financial cost	0.00
⑦ – line style	solid
Packet formats	ethernet
Propdel model	dbu_propdel
⑦ – symbol	none
(?) – thickness	5
(?) – txdel model	dbu_txdel
(?) ∟userid	
Redefine Path Extended Attrs.	
Apply Changes to Selected Ubjects	I✓ A <u>d</u> vanced
Eind Next	<u>C</u> ancel <u>O</u> K

- 6. Now you have created the network. It should look like the illustration below.
- 7. Make sure to save your project.



#### 1.4.3. Configure the Network Nodes

To configure the traffic generated by the nodes:

- 1. Right-click on any of the 30 nodes  $\Rightarrow$  Select Similar Nodes. Now all nodes in the network are selected.
- 2. Right-click on any of the 30 nodes  $\Rightarrow$  Edit Attributes.
- 3. Check the **Apply Changes to Selected Objects** check box. This is <u>important to</u> <u>avoid reconfiguring each node individually</u>.
- 4. Expand the **Traffic Generation Parameters** hierarchy:
  - a. Change the value of the ON State Time to exponential(100) ⇒ Change the value of the OFF State Time to exponential(0). (*Note*: <u>Packets are generated only in the ON state</u>.)
- 5. Expand the Packet Generation Arguments hierarchy:
  - a. Change the value of the Packet Size attribute to constant(1024).
  - b. Right-click on the **Interarrival Time** attribute and choose **Promote Attribute to Higher Level.** This allows us to assign multiple values to the **Interarrival Time** attribute and hence to test the network performance under different loads.

🛣 (node_12) Attributes	
Type: station	
Attribute	Value
⑦ rame	node_12
model	ethcoax_station
⑦	()
⑦	constant (5.0)
⑦ – ON State Time (seconds)	exponential (100)
OFF State Time (seconds)	exponential (0)
Packet Generation Arguments	()
Interarrival Time (seconds)	promoted
Packet Size (bytes)	constant (1024)
Optimized Control Size (bytes)	No Segmentation
Optimized Stop Time (seconds)	Never
Traffic Generation Parameters [0].Packet	. promoted
Apply Changes to Selected Objects	☐ A <u>d</u> vanced
Eind Next	<u>Cancel</u>

- 6. Click OK to return back to the Project Editor.
- 7. Make sure to save your project.

The argument of the exponential distribution is the mean of the interval between successive events. In the exponential distribution the probability of occurrence of the next event by a given name is not at all dependent upon the time of occurrence of the last event of the elapsed time since that event.

The interarrival time is the time between successive packet generations in the "ON" state.

#### 1.4.4. Configure the Simulation

To examine the network performance under different loads, you need to run the simulation *several times* by changing the *load* into the *network*. There is an easy way to do that. Recall that we promoted the Interarrival Time attribute for package generation. Here we will assign different values to that attribute:

1. Click on the Configure/Run Simulation button:  $23 \Rightarrow$  Make sure that the **Common** tab is chosen  $\Rightarrow$  Assign 15 seconds to the **Duration**.

	🛣 Configure Simu	lation: MN_Ethe	rnet-Coax	
0	Common Gobal Attrib	outes Object Attribute	es Reports SLAs Animation Profiling Advance	d Environment Files
1	Duration:	15	second(s)	
	Seed:	128		
	Values per statistic:	100		
	Update interval:	100000	Events	
	Enable simulation	log		
		-		
	<u> </u>		Help	<u>Cancel</u> <u>D</u> K

2. Click on the Object Attributes tab.

- 3. Click on the **Add** button. The *Add Attribute* dialog box should appear filled with the promoted attributes of all nodes in the network (if you do not see the attributes in the list, close the whole project and reopen it). You need to add the **Interarrival Time** attribute for all nodes. To do that:
  - a. Click on the first attribute in the list (Office Network.node\_0.Traffic Generation.)  $\Rightarrow$  Click the Wildcard button  $\Rightarrow$  Click on node\_0 and choose the asterisk (\*) from the drop-down menu  $\Rightarrow$  Click OK.

Attribute: scenario			
🔣 Find Wildcard			×
Office Network . node_0 . Traffic Ge	meration Parameters [0] .	Packet Generation Arguments [0]	. Interarrival Time
		<u> </u>	el <u>O</u> K
Office Network.node_15.Traffic Gen Office Network.node_16.Traffic Gen Office Network.node_17.Traffic Gen	eration Parameter eration Parameter	View Props Values	

b. A new attribute is now generated containing the asterisk (the second one in the list), and you need to add it by clicking on the corresponding cell under the **Add?** column.

🛣 Ada	l Attribute: scenario	$\times$
Add?	Unresolved Attributes	
add	Office Network.node_0.Traffic Generation Parameters Office Network.*.Traffic Generation Parameters [0].Pa Office Network.node_1.Traffic Generation Parameters Office Network.node_10.Traffic Generation Parameter Office Network.node_11.Traffic Generation Parameter Office Network.node_12.Traffic Generation Parameter Office Network.node_13.Traffic Generation Parameter Office Network.node_14.Traffic Generation Parameter Office Network.node_15.Traffic Generation Parameter Office Network.node_16.Traffic Generation Parameter Office Network.node_17.Traffic Generation Parameter Office Network.node_17.Traffic Generation Parameter	
	Office Network.node_19.Traffic Generation Parameter	-
	Expand Cancel OK	

- c. The Add Attribute dialog box should look like the shown one  $\Rightarrow$  Click **OK**.
- 4. Now you should see the **Office Network.\*.Traffic Generation Parameter** ... in the list of simulation object attributes. Click on that attribute to select it. ⇒ Click the **Values** button of the dialog box.
- Add the following nine values. (Note: To add the first value, double-click on the first cell in the Value column ⇒ Type "exponential (2)" into the textbox and hit Enter ⇒ Repeat this for all nine values.)

🛣 Attribute: Of	fice	Network.*.Traffic Generation Parame	$\times$	
Enter one or more values:				
Value	Limit	Step		
exponential (2)				
exponential (1)				
exponential (0.5)				
exponential (0.25)				
exponential (0.1)				
exponential (0.05)				
exponential (0.035)				
exponential (0.03)				
exponential (0.02)				
			-	
View Props	<u>D</u> ele	te <u>C</u> ancel <u>O</u> K		

6. Click **OK**. Now look at the upper-right comer of the *Simulation Configuration* dialog box and make sure that the *Number of runs in set* is 9.

🗄 Configure Simulation: eha_Ethernet-Coax					
Common Global Attributes Object Attributes Reports       SLAs       Animation       Profiling       Advanced       Envirc       Image: State St					
Attribute	Value				<u> </u>
Office Network.*.Tr exponential (2), exponential (1), exponential (0.5), exponential (0.25), exponen					
Add	E <u>x</u> pand	De <u>l</u> ete	<u>U</u> pdate	<u>V</u> iew Props	Values
<u>R</u> un		<u>H</u> elp		<u>C</u> ancel	<u>о</u> к

- 7. For each simulation of the nine runs, we need the simulator to save a "scalar" value that represents the "average" load in the network and to save another scalar value that represents the average throughput of the network. To save these scalars we need to configure the simulator to save them in a file. Click on the **Advanced** tab in the *Configure Simulation* dialog box.
- 8. Assign <your initials>\_Ethernet\_Coax to the Scalar file text field.

🔣 Configure	e Simulation: eha_Ethernet-Coax
Common	àlobal Attributes Object Attributes Reports SLAs Animation Profilin Advanced Envirc 🕙 🕨
Network:	eha_Ethernet-Coax
Probe file:	eha_Ethernet-Coax
Vector file:	eha_Ethernet-Coax
Scalar file:	eha_Ethernet_Coax
Simulation	program: op_runsim 👤
Command-I	line options
Record a da	ate/time in results: none 🔽 Date: Time:
<u>R</u> un	<u>H</u> elp <u>C</u> ancel <u>O</u> K

9. Click OK and then save your project.

#### 1.4.5. Choose the Statistics

To choose the statistics to be collected during the simulation:

- 1. Right-click anywhere in the project workspace (but not on one of the nodes or links) and select **Choose individual Statistics** from the pop-up menu ⇒ Expand the **Global Statistics** hierarchy.
  - a. Expand the **Traffic Sink** hierarchy ⇒ Click the check box next to Traffic Received **(packets/sec)** (make sure you select the statistic with units of packets/sec),
  - b. Expand the **Traffic Source** hierarchy ⇒ Click the check box next to Traffic Sent (packets/sec).
  - c. Click OK.

🔀 Choose Results		
Global Statistics  Global Statistics  Find-to-End Delay (seconds)  Traffic Received (bits)  Traffic Received (bits/sec)  Traffic Received (packets)  Traffic Source  Traffic Sent (bits)  Traffic Sent (bits/sec)  Traffic Sent (packets)  Traffic Sen		*
	<u>C</u> ancel	<u>K</u>

A probe represents a request by the user to collect a particular piece of data about a simulation.

- 2. Now to collect the average of the above statistics as a scalar value by the end of each simulation run:
  - a. Select Choose Statistics (Advanced) from the Simulation menu.
  - b. The **Traffic Sent** and **Traffic Received** probes should appear under the **Global Statistic Probes**.
  - c. Right-click on Traffic Received probe  $\Rightarrow$  Edit Attributes. Set the scalar data attribute to enabled  $\Rightarrow$  Set the scalar type attribute to time average  $\Rightarrow$  Compare to the following figure and Click OK.

📧 (pb0) Attributes			
Attribute	Value		
⑦ ⊢name	pb0		
⑦ ⊢draw style	linear		
⑦ ⊢group	Traffic Sink		
⑦ ⊢statistic	Traffic Received (packets/sec)		
⑦ ⊢ordinate label			
⑦ ⊢vector data	enabled		
⑦ ⊢vector start	0.0		
⑦ ⊢vector stop	infinity		
⑦ ⊢scalar data	enabled		
⑦ ⊢scalar type	time average 🖌 🗕		
⑦ ⊢scalar start	0.0		
Apply Changes to Selected Ol	ojects		
Eind Next	<u>C</u> ancel <u>O</u> K		

- d. Repeat the previous step with the Traffic Sent probe.
- e. Select **save** from the **File** menu in the *Probe Model* window and then close that window.
- f. Now you are back to the *Project Editor*. Make sure to save your project.

#### 1.4.6. Run the Simulation

To run the simulation:

- 1. Click on the **Configure/Run Simulation** button:  $\bigcirc$  .  $\Rightarrow$  Make sure that 15 **second(s)** (not hours) is assigned to the **Duration**  $\Rightarrow$  Click **Run.** Depending on the speed of your processor, this may take several minutes to complete.
- Now the simulator is completing nine runs, one for each traffic generation inter-arrival time (representing the load into the network). Notice that each successive run takes longer to complete because the traffic intensity is increasing.

Kimulation Sequence: MN_Ethernet-Coa	x	$\times$
Simulation runs to go: 0	osed Time: — Estimated	Remaining Time: —
Running: Coax	Us. Es	stimating
		15 / 15 sim seconds
Simulation Speed Messages Memory Usage Memo	ry Stats Profiling	1
Beginning simulation at 11:29:56 uto lis 05 2	2010	
Simulation Completed - Collating Results. Events: Total (330), Average Speed (0 eve Time: Elapsed (0 sec.), Simulated (15 sec. Beginning simulation at 11:29:57 uto lis 05 2 Simulation Completed - Collating Results. Events: Total (330), Average Speed (0 eve Time: Elapsed (0 sec.), Simulated (15 sec.	ents/sec.) ) 2010 ents/sec.) )	•
Simulated Time: 15s. Events: 330 Speed: Average: 0 events/sec. Current: 0 events/s	sec.	Update
Save output when stopping simulation		
Pause Resume Stop Run	Stop Sequen	ice <u>C</u> lose

3. After the nine simulation runs, complete, click Close.
4. Save your project.



When you rerun the simulation, OPNET IT Guru will "append" the new results to the results already in the scalar file. To avoid that, delete the scalar file *before* you start a new run. (*Note:* Deleting the scalar file after a run will result in losing the collected results from that run.)

Go to the File menu ⇒ Select Model Files ⇒ Delete Model Files ⇒ Select (.os):
 Output Scalars ⇒ Select the scalar file to be deleted; in this lab it is <your initials>\_Ethernet\_Coax ⇒ Confirm the deletion by clicking OK ⇒ Click Close.

#### 1.4.7. View the Results

To view and analyze the results:

- 1. Select View Results (Advanced) from the Results menu. Now the Analysis Configuration tool is open.
- 2. Recall that we saved the average results in a scalar file. To load this file, select Load Output Scalar File from the File menu  $\Rightarrow$  Select <your initials>\_ Ethernet-Coax from the pop-up menu.
- 3. Select Create Scalar Panel from the Panels menu ⇒ Assign Traffic Source.Traffic Sent(packets/sec).average to Horizontal ⇒ Assign Traffic Sink.Traffic Received(packets/sec).average to Vertical ⇒ Click OK.

🛣 Select Scalar Panel Data		
Horizontal:	Traffic Source.T	raffic Sent (r 💌
Vertical:	Traffic Sink.Traf	fic Receivec 💌
	<u>C</u> ancel	<u>0</u> K

4. The resulting graph should resemble the one below:



Note: Check ordinate scale!

# 1.5. Further readings

• OPNET <u>Ethernet Model Description</u>: From the **Protocols** menu, select **Ethernet** ⇒ <u>Model Usage Guide</u>.

# 1.6. Exercises

- 1) Explain the graph we received in the simulation that shows the relationship between the received (throughput) and sent (load) packets. Why does the throughput drop when the load is either very low or very high?
- 2) Create three duplicates of the simulation scenario implemented in this tab. Name these scenarios Coax\_Q2a, Coax\_Q2b, and Coax\_Q2c. Set the Interarrival Time attribute of the *Packet Generation Arguments* for all nodes (make sure to check Apply Changes to Selected Objects while editing the attribute) in the new scenarios as follows:
  - Coax\_Q2a scenario: exponential(0.1)
  - Coax\_Q2b scenario: exponential(0.05)
  - Coax\_Q2c scenario: exponential(0.025)
- 3) In all the above new scenarios, open the *Configure Simulation* dialog box and from the *Object Attributes* delete the multiple-value attribute (the only attribute shown in the list).
- 4) Choose the following statistic for node 0: Ethcoax → Collision Count. Make sure that the following global statistic is chosen: Global Statistics → Traffic Sink → Traffic Received (packet/sec). (Refer to the Choose the Statistics section in the lab.)
- 5) Run the simulation for all three new scenarios. Get two graphs: one to compare node 0's collision counts in these three scenarios and the other graph to compare the received traffic from the three scenarios. Explain the graphs and comment on the results. (*Note*: To compare results you need to select **Compare Results** from the **Results** menu after the simulation run is done.)
- 6) To study the effect of the number of stations on Ethernet segment performance, create a duplicate of the Coax\_Q2c scenario, which you created in Exercise 2. Name the new scenario Coax\_Q3. In the new scenario, remove the network simulation experiments manual.doc

odd-numbered nodes, a total of 15 nodes (node 1, node 3, ..., and node 29). Run the simulation for the new scenario. Create a graph that compares node 0's collision counts in scenarios **Coax\_Q2c** and **Coax\_Q3**. Explain the graph and comment on the results.

7) In the simulation a packet size of 1024 bytes is used (*Note:* Each Ethernet packet can contain up to 1500 bytes of data). To study the effect of the packet size on the throughput of the created Ethernet network, create a duplicate of the Coax\_Q2c scenario, which you created in Exercise 2. Name the new scenario Coax\_Q4. In the new scenario use a packet size of 512 bytes (for all nodes). For both Coax\_Q2c and Coax\_Q4 scenarios, choose the following global statistic: Global Statistics → Traffic Sink → Traffic Received (bits/sec) Rerun the simulation of Coax\_Q2c and Coax\_Q4 scenarios. Create a graph that compares the throughput as packets/sec and another graph that compares the throughput as bits/sec in Coax\_Q2c and Coax\_Q4 scenarios. Explain the graphs and comment on the results.

## 1.7. Lab Report

Prepare a report that follows the guidelines explained in Lab 0. The report should include the answers to the above exercises as well as the graphs you generated from the simulation scenarios. Discuss the results you obtained and compare these results with your expectations. Mention any anomalies or unexplained behaviors.

# 2. Laboratory - Token Ring (A Shared-Media Network with Media Access Control)

# 2.1. Objective

This lab is designed to demonstrate the implementation of a token ring network. The simulation in this lab will help you examine the performance of the token ring network under different scenarios.

## 2.2. Overview

A token ring network consists of a set of nodes connected in a ring. The ring is a single shared medium. The token ring technology involves a distributed algorithm that controls when each node is allowed to transmit. All nodes see all frames. The destination node, which is identified in the frame header, saves a copy of the frame as the frame flows past the node. With a ring topology, any link or node failure would render the whole network useless. This problem can be solved by using a star topology where nodes are connected to a token ring hub. The hub acts as a relay, known as a multi-station access unit (MSAU). MSAUs are almost always used because of the need for robustness and ease of node addition and removal.

The "token," which is just a special sequence of bits, circulates around the ring; each node receives and then forwards the token. When a node that has a frame to transmit sees the token, it takes the token off the ring and instead inserts its frame into the ring. When the frame makes its way back around to the sender, this node strips its frame off the ring and reinserts the token. The *token holding time* (THT) is the time a given node is allowed to hold the token. From its definition, the THT has an effect on the utilization and fairness of the network, where utilization is the measure of the bandwidth used versus that available on the given ring.

In this lab, you will set up a token ring network with 14 nodes connected in a star topology. The links you will use operate at a data rate of 4 Mbps. You will study how the utilization and delay of the network are affected by the network load as well as the *token holding time* THT.

# 2.3. Prelab Activities

Read section 2.7 from "Computer Networks: A Systems Approach", 4th Edition.

# 2.4. Procedure

## 2.4.1. Create a New Project

To create a new project for the token ring network:

- 1. Start **OPNET IT Guru Academic Edition**  $\Rightarrow$  Choose **New** from the **File** menu.
- 2. Select **Project** and Click **OK** ⇒ Name the project **<your initials>\_Token**, and the scenario **Balanced** ⇒ Click **OK**.
- 3. In the *Startup Wizard: Initial Topology* dialog box, make sure that **Create Empty Scenario** is selected ⇒ Click **Next** ⇒ Choose **Office** for the Network scale ⇒ Click **Next** three times ⇒ Click **OK**.
- 4. Close the **Object Palette** and then save your project.

### 2.4.2. Create the Network

To create our token ring network:

- 1. Select **Topology**  $\Rightarrow$  **Rapid Configuration**. From the drop-down menu choose **Star** and Click **OK**.
- 2. Click the **Select Models** button in the *Rapid Configuration* dialog box. From the *Model List* drop-down menu choose **token\_ring** and Click **OK**.
- 3. In the Rapid Configuration dialog box, set the following six values and Click OK.

Rapid Configuration: Star	×
MODELS Center Node Model tr32_hub Periphery Node Model tr_station	Number 14
PLACEMENT Center X 50 Y 50 Select Models	Radius 35

The **tr.32\_hub** node model is a token ring hub supporting up to 32 connections at 4 or 16 Mbps. The hub forwards an arriving packet to the next output port. There is no queuing of packets in the hub itself as the processing time is considered to be zero.

The TR4 link connects two token ring devices to form a ring at 4 Mbps.

4. You have now created the network, and it should look like the following:



5. Make sure to save your project.

#### 2.4.3. Configure the Network Nodes

Here you will configure the **THT** of the nodes as well as the traffic generated by them. To configure the **THT** of the nodes, you need to use the **tr\_station\_adv** model for the nodes instead of the current one, **tr\_station**.

- 1. Right-click on any of the 14 nodes.  $\Rightarrow$  Select Similar Nodes. Now all nodes in the network are selected.
- 2. Right-click on any of the 14 nodes  $\Rightarrow$  Edit Attributes.
  - a. Check the **Apply Changes to Selected Objects** check box. This is important to avoid reconfiguring each node individually.

The following figure shows the attributes we will change in steps 3 to 6:

🛣 (node_0) Attributes	
Attribute	Value
⑦ ⊢name	node_0
⑦ ⊢model	tr_station_adv 🔶
⑦ ⊢Highest Destination Addre	Maximum Dest Address
⑦ ⊢Lowest Destination Address	Minimum Dest Address
⑦ ⊡ Token Ring Parameters	()
⑦ ⊢Address	Auto Assigned
⑦ ⊢Hop Propagation Delay (	3.3E-006
⑦ ⊢Operational Mode	Switched
Promiscuous Mode	Disabled
⑦ ⊢Ring ID	Auto Assigned
⑦ ⊢Spawn Station Offset	0
⑦ ⊢Stack Modification Time	5E-006
⑦ ⊢Station Latency (bits)	4
THT Duration (seconds)	promoted 🔶
⑦ ⊡ Traffic Generation Parame	()
⑦ ⊢Start Time (seconds)	constant (5.0)
⑦ ⊢ON State Time (seconds)	exponential (100.0)
⑦ ⊢OFF State Time (second	exponential (0.0)
Packet Generation Argu	()
⑦ ⊢Interarrival Time (seco	exponential (0.025)
Packet Size (bytes)	exponential (1024)
	<b>&gt;</b>
Apply Changes to Selected Obj	ects ← Advanced
Eind Next	<u>C</u> ancel <u>O</u> K

The **THT** (*Token Holding Time*) specifies the maximum amount of time a token ring MAC (*Media Access Control*) may use the token before releasing it.

The interarrival time is the time between successive packet generations in the "ON" state.

- 3. Click on the model value: **tr\_station** and select **Edit** from the drop-down menu. Now select **tr\_station\_adv** from the extended drop-down menu.
- 4. To test the network under different THT values, you need to "promote" the THT parameter. This allows us to assign multiple values to the THT attribute.
  - a. Expand the Token Ring Parameters hierarchy.

- b. Right-click on the THT Duration attribute.  $\Rightarrow$  Choose Promote Attribute to Higher Level.
- 5. Expand the **Traffic Generation Parameters** hierarchy. ⇒ Assign **exponential(100)** to the ON State Time attribute ⇒ Assign **exponential(0)** to the OFF State Time attribute. (*Note:* Packets are generated only in the "ON" state.)
- 6. Expand the **Packet Generation Arguments** hierarchy. ⇒ Assign **exponential(0.025)** to the **Interarrival Time** attribute.
- 7. Click OK to return back to the Project Editor.
- 8. Make sure to save your project.

#### 2.4.4. Configure the Simulation

To examine the network performance under different THTs, you need to run the simulation several times by changing THT with every run of the simulation. There is an easy way to do that. Recall that we promoted the THT Duration attribute. Here we will assign different values to that attribute:

- 1. Click on the **Configure/Run Simulation** button:
- 2. Make sure that the **Common** tab is chosen.  $\Rightarrow$  Assign 5 minutes to the **Duration**.

🗄 Configure Simulation: eha_Token-Balanced					
Common Global Attrib	outes Object	Attributes Reports SLAs Anin	nation Profiling Advan	ced Envire	
Duration:	5	minute(s)			
Seed:	128	$\checkmark$			
Values per statistic:	100				
Update interval:	100000	Events			
Enable simulation lo	ю				
Run		<u>H</u> elp	<u>C</u> ancel	<u>O</u> K	

- 3. Click on the **Object Attributes** tab.  $\Rightarrow$  Click the **Add** button.
- 4. As shown in the following *Add Attribute* dialog box, you need to add the **THT Duration** attribute for all nodes. To do that:
  - a. Add the unresolved attribute: **Office Network.\*.Token Ring Parameters[0].THT Duration** by clicking on the corresponding cell under the **Add?** column ⇒ Click **OK**.



5. Now you should see the Office Network.\*.Token Ring Parameters[0].THT. Duration in the list of simulation object attributes (widen the "Attribute" column to see the full name of the attribute). Click on that attribute  $\Rightarrow$  Click the Values button, as shown below.

Configure Simulation: eha_Token-Balanced						
Common Global	Common Global Attributes Object Attributes Reports SLAs Animation Profiling Advanced Envirc					
Use de <u>f</u> ault val	✓Use default values for unresolved attributes			Number of runs in set: 1		
Save vector file	e for each run in s	et	S <u>i</u> mula	ation set info		
Attribute			Value		<u> </u>	
Office Network.*.	.Token Ring Parar	neters [0].THT D	uration			
		1	0			
Add	E <u>x</u> pand	Delete	<u>U</u> pdate	<u>V</u> iew Props	Values	
Run		<u>H</u> elp		<u>C</u> ancel	<u>О</u> К	

6. Add the following six values. (Note: To add the first value, double-click on the first cell in the **Value** column  $\Rightarrow$  Type "0.01" into the textbox and hit enter. Repeat this for all six values.)

🟽 Attribute: Office Network.*.Token Ring Parameters [0].T 🔀			
Enter one or more values:			
Value Limit Step			
0.01			
0.02			
0.04			
0.08			
0.16			
0.32			
View Props         Delete         Cancel         OK			

7. Click **OK**. Now look at the upper-right comer of the *Simulation Configuration* dialog box and make sure that the *Number of runs in set* is 6.

🗄 Configure Simulation: eha_Token-Balanced					
Common Globa Use default va Save vector fi Attribute Office Network	I Attributes Object alues for unresolver le for each run in s *.Token Ring Paran	Attributes d attributes et neters [0].THT D	ts SLAs Animati Numbe Simul Value uration 0.01, 0.0	on Profiling Advan er of runs in set: 6 ation set info 2, 0.04, 0.08, 0.16, 0	Ced Envire
Add     Expand     Delete     Update     View Props     Values					
Run		<u>H</u> elp		Cancel	<u> </u>

- 8. For each of the six simulation runs we need the simulator to save "scalar" values that represent the "average" values of the collected statistics. To save these scalars we need to configure the simulator to save them in a file. Click on the **Advanced** tab in the *Configure Simulation* dialog box.
- 9. Assign <your initials>\_Token\_Balanced to the *Scalar file* text field.

🔣 Configure Sin	nulation: eha_Tok	en-Balanced			
Common Globa	al Attributes Object	Attributes Repor	rts SLAs Animation	Profiling	
Network: eha	_Token-Balanced				<u></u>
Probe file: eha	a_Token-Balanced				¥
Vector file: eha	_Token-Balanced				
Scalar file: eha	_Token_Balanced	←			
Simulation prog	ram: op_runsim	•			
Command-line	options				
Record a date/t	ime in results: non	e 🗾 Date	ə:	Time:	
Run		Help		Cancel	ОК
		Tob		Ganoor	<u></u>

10. Click **OK** and then save your project.

#### 2.4.5. Choose the Statistics

To choose the statistics to be collected during the simulation:

- 1. Right-click anywhere in the project workspace (but not on a node or link) and select **Choose Individual Statistics** from the pop-up menu.
  - a. Expand the Global Statistics hierarchy:
    - Expand the Traffic Sink hierarchy.  $\Rightarrow$  Click the check box next to Traffic Received (packets/sec).
    - Expand the Traffic Source hierarchy.  $\Rightarrow$  Click the check box next to Traffic Sent (packets/sec).
  - b. Expand the Node Statistics hierarchy:

- Expand the Token Ring hierarchy.  $\Rightarrow$  Click the check box next to Utilization.
- c. Click OK.

The utilization is a measure of the bandwidth used versus that available on the given ring.

- 2. Now we want to collect the average of the above statistics as a scalar value by the end of each simulation run.
  - a. Select Choose Statistics (Advanced) from the Simulation menu.
  - b. The **Traffic Sent** and **Traffic Received** probes should appear under the **Global Statistic Probes**. The **Utilization** probe should appear under the **Node Statistics Probes**.
  - c. Right-click on Traffic Received probe.  $\Rightarrow$  Edit Attributes. Set the scalar data attribute to enabled.  $\Rightarrow$  Set the scalar type attribute to time average.  $\Rightarrow$  Compare to the following figure and Click OK.

🔀 (pb0) Attribi	utes		×
Attribute		Value	
⑦ ⊢name		рb0	
⑦ ⊢draw style	9	linear	
⑦ ⊢group		Traffic Sink	
⑦ ⊢statistic		Traffic Received (packets/sec)	
⑦ ⊢ordinate la	abel		
⑦ ⊢vector dat	a	enabled	
⑦ ⊢vector sta	rt	0.0	
⑦ ⊢vector sto	р	infinity	
⑦ ⊢scalar dat	a	enabled	
⑦ ⊢scalar typ	e	time average 🛛 🗲 🗕	
⑦ ⊢scalar sta	rt	0.0	
⑦ ⊢scalar sto	р	infinity	•
Apply Chang	es to Selected O	bjects	
	Eind Next	<u>C</u> ancel <u>O</u> K	

d. Repeat the previous step with the Traffic Sent and Utilization probes.

A probe represents a request by the user to collect a particular piece of data about a simulation.

- 3. Since we need to analyze the effect of THT on the network performance, THT must be added as an "input" statistic to be recorded by the simulation. To do that:
  - a. Select **Create Attribute Probe** from the **Objects** menu. Now a new attribute is created under the **Attribute Probes** hierarchy as shown.
  - b. Right-click on the new attribute probe and select Choose Attributed Object from the pop-up menu. ⇒ Expand the Office Network hierarchy. ⇒ Click on node\_0 (actually you can pick any other node) ⇒ Click OK.

🕿 Probe Model: eha_Token-Balanced [Subnet: top.Office Network] 📃 🗖 🔀
File Edit Objects Windows Help
Global Statistic Probes
- collect Name Group.Statistic
- bb0 Traffic Sink.Traffic Received (packets/sec)
Listing pb1 Traffic Source.Traffic Sent (packets/sec)
□ Probes
- collect Name Group.Statistic Object
🗠 🖾 🗤 pb2 Token Ring.Utilization top.*.*
由 Link Statistic Probes
🕀 🐹 Demand Statistic Probes
🕀 Coupled Node Statistic Probes
白  Attribute Probes
– Name Attribute Object
pb3 Office Network.node_0
Automatic Animation Probes

c. Right-click again on the new attribute probe and select **Edit Attributes** from the pop-up menu. ⇒ Assign the **Token Ring Parameter[0].THT Duration** value to the "**attribute**" Attribute, as shown in the figure. ⇒ Click **OK**.

🔣 (pb3) Attributes		
Attribute	Value	
⑦ ⊢ name	pb3	
⑦ ⊢object	Office Network.node_0	
⑦ ⊢attribute	Token Ring Parameters [0].THT Duration	
Apply Changes to Selected Ol	bjects	
Eind Next	<u>C</u> ancel <u>O</u> K	

- 4. Select save from the **File** menu in the *Probe Model* window and then **Close** the window.
- 5. Now you are back to the *Project Editor*. Make sure to save your project.

#### 2.4.6. Duplicate the Scenario

The token ring network scenario we just implemented is *balanced*: the distribution of the generated traffic in all nodes is the same. To compare performance, you will create an "unbalanced" scenario as follows:

- 1. Select **Duplicate Scenario** from the **Scenarios** menu and give it the name **Unbalanced**  $\Rightarrow$  Click **OK**.
- Select node\_0 and node\_7 by shift-clicking on both nodes. ⇒ Right-click on one of these two selected nodes and select Edit Attributes ⇒ Expand the Traffic Generation Parameters hierarchy ⇒ Expand the Packet Generation Arguments hierarchy ⇒ Change the value of the Interarrival Time attribute to exponential(0.005) as shown. Make sure to check the Apply Changes to Selected Objects box before you Click OK.

🔣 (node_0) Attributes			
Type: station			
Attribute	Value 🔺		
⑦ ⊢name	node_0		
⑦ ⊢model	tr_station_adv		
⑦ ⊢Highest Destination Address	Maximum Dest Address		
	Minimum Dest Address		
⑦	()		
Traffic Generation Parameters	()		
⑦ ⊢Start Time (seconds)	constant (5.0)		
ON State Time (seconds)	exponential (100.0)		
③ FOFF State Time (seconds)	exponential (0.0)		
Packet Generation Arguments	()		
⑦ ⊢Interarrival Time (seconds)	exponential (0.005) <		
⑦ ⊢Packet Size (bytes)	exponential (1024)		
▲ 10 · · · · · · · · · · · · · · · · · ·			
✓Apply Changes to Selected Objects	← A <u>d</u> vanced		
<u>Eind Next</u>	<u>C</u> ancel <u>O</u> K		

- Select all nodes except node\_0 and node\_7 ⇒ Right-click on one of the selected nodes and select Edit Attributes. ⇒ Change the value of the Interarrival Time attribute to exponential(0.075) as in the previous step. Make sure to check the Apply Changes to Selected Objects box before you Click OK
- 4. Click anywhere in the workspace to unselect objects.
- 6. Click OK and then save your project.

#### 2.4.7. Run the Simulation

To run the simulation for both scenarios simultaneously:

- 1. Go to the Scenarios menu.  $\Rightarrow$  Select Manage Scenarios.
- 2. Change the values under the **Results** column to <**collect**> (or <**recollect**>) for both scenarios. Compare to the following figure.

<b>₩</b> M	🗄 Manage Scenarios 📃 🗖 🔀					
Pro	Project Name: eha Token					
#	Scenario Name	Saved	Results	Sim Duration	Time Units 🔺	
1	Balanced	saved	<collect></collect>	5.0	minute(s)	
2	Unbalanced	saved	<collect></collect>	5.0	minute(s)	
	Y					
[	Delete Discard Results Collect Results Cancel OK					

- 3. Click **OK** to run the simulations. Depending on the speed of your processor, this may take several minutes to complete.
- 4. After the simulation completes the 12 runs, 6 for each scenario, click Close.

5. Save your project.

When you rerun the simulation, OPNET IT Guru will "**append**" the new results to the results already in the scalar file. To avoid that, delete the scalar file before you start a new run.

- Go to the File menu ⇒ Select Model Files ⇒ Delete Model Files ⇒ From the list, choose other model types ⇒ Select (.os): Output Scalars ⇒ Select the scalar file to be deleted; in this tab they are:
  - <your initials>\_Token\_Balanced and
  - $\circ$  <your initials>\_Token\_Unbalanced.  $\Rightarrow$  Click Close.

#### 2.4.8. View the Results

To view and analyze the results.

- 1. Select View Results (Advanced) from the Results menu. Now the Analysis Configuration tool is open.
- Recall that we saved the average results in two scalar files, one for each scenario. To load the scalar file for the Balanced scenario, select Load Output Scalar File from the File menu ⇒ Select <your initials>\_Token\_Balanced from the pop-up menu.
- 3. Select Create Scalar Panel from the Panels menu ⇒ Select the scalar panel data as shown in the following dialog box: THT for Horizontal and Utilization for Vertical (*Note*: If any of the data is missing, make sure that you carried out steps <u>2.c</u> and <u>2.d</u> in the *Choose the Statistics* section.)

<table-of-contents> Select Scalar Panel Data 🛛 🔀</table-of-contents>			
Horizontal:	Office Network.node		
Vertical:	top.Office Network.n		
	<u>C</u> ancel <u>O</u> K		

- 4. Click OK.
- 5. To change the title of the graph, right-click on the graph area and choose **Edit Graph Properties**.  $\Rightarrow$  Change the **Custom Title** to **Balanced Utilization** as shown.

🛠 Graph #1 of Panel #1						
top.Office Net	top.Office Network.node_14.Token Ring.Utilizatic					
Custom Title:	Balanced Utilization	n 🔶				
File:		S <u>h</u> ow				
Report:		Sho <u>w</u>				
Object:		Show				
Statistic:		Show				
Annotation:		Show				
Parameter:		Show				
Draw Style:	linear 💌	Set Color				
Vertical Min:	0.974916	<u>F</u> ull Scale				
Vertical Max:	0.989051	Legend				
Height (pixels):	308	Set Color				
Show Confidence Interval						
<u>A</u> pply Ca <u>n</u> cel <u>O</u> K						

6. Click **OK**. The resulting graph should resemble the one shown below. Do not close the graph and continue with the following step.

🔣 itgu	ru		
9900	Balanced Utilization		
.9875			
.9850			
.9825			
.9800			
.9775			
.9750	1		
.9725	 		
	0 0.2	0.4	
	Office Network.node_0.Token Ring Parameters [0].THT Duration		

- 7. To compare with the **Unbalanced** scenario, load its scalar file, select **Load Output Scalar File** from the **File** menu ⇒ Select **<your initials>\_Token\_ Unbalanced** from the pop-up menu.
- 8. Select **Create Scalar Panel** from the **Panels** menu Select the scalar panel data as in <u>step 3</u>.
- 9. Click  $OK \Rightarrow$  Change the graph title to **Unbalanced** as in <u>step 5</u>  $\Rightarrow$  Click OK. The resulting graph should resemble the one shown below. Do not close this graph or the previous one and continue with the following step.



10. To combine the above two graphs on a single graph, select **Create Vector Panel** from the **Panels** menu. ⇒ Click on the **Display Panel Graphs** tab. ⇒ Select both **Balanced** and **Unbalanced** statistics. ⇒ Choose **Overlaid Statistics** from the drop-down menu in the right-bottom area of the dialog box as shown.



11. Click Show and the resulting graph should resemble the one shown below.



- 12. Repeat the same process to check the effect of the **THT** on **Traffic Received** for both scenarios. Assign the appropriate titles to the graphs.
- 13. The resulting graph, which combines the **Traffic Received** statistic for both the **Balanced** and **Unbalanced** scenarios, should resemble the following one:



# 2.5. Further readings

 OPNET <u>Token Ring Model Description</u> From the **Protocols** menu, select **Token** Ring ⇒ <u>Model Usage Guide</u>.

# 2.6. Exercises

- 1) Why does the utilization increase with higher THT values?
- 2) Create a duplicate scenario of the Balanced scenario. Name the new scenario Q2\_HalfLoad. In the Q2\_HalfLoad scenario, decrease the load into the network (i.e., load from all nodes in the network) by half and repeat the simulation. Compare the utilization and traffic received in the Q2\_HalfLoad scenario with those of the Balanced scenario.

Hints:

- Decreasing the load from a node by half can be done by doubling the "Interarrival Time" of the node's Packet Generation Arguments.
- Do not forget to assign a separate "scalar file" for the new scenario.
- 3) Create a duplicate scenario of the Balanced scenario. Name the new scenario Q3\_OneNode. In the Q3\_OneNode scenario, reconfigure the network so that node\_0 generates a traffic load that is equivalent to the traffic load generated by all nodes in the Balanced scenario combined. The rest of the nodes, node\_1 to node\_13, generate no traffic. Compare the utilization and traffic received in Q3 OneNode scenario with those of the Balanced scenario.

Hints:

- One way to configure a node so that it does not generate traffic is to set its Start Time (it is one of the Traffic Generation Parameters) to the special value Never.
- Do not forget to assign a separate "scalar file" for the new scenario.

#### 2.7. Lab Report

Prepare a report that follows the guidelines explained in Lab 0. The report should include the answers to the above exercises as well as the graphs you generated from the simulation scenarios. Discuss the results you obtained and compare these results with your expectations. Mention any anomalies or unexplained behaviors.

# 3. Laboratory - Switched LANs (A Set of Local Area Networks Interconnected by Switches)

# 3.1. Objective

This lab is designed to demonstrate the implementation of switched local area networks. The simulation in this lab will help you examine the performance of different implementations of local area networks connected by switches and hubs.

## 3.2. Overview

There is a limit to how many hosts can be attached to a single network and to the size of a geographic area that a single network can serve. Computer networks use switches to enable the communication between one host and another, even when no direct connection exists between those hosts. A switch is a device with several inputs and outputs leading to and from the hosts that the switch interconnects. The core job of a switch is to take packets that arrive on an input and forward (or switch) them to the right output so that they will reach their appropriate destination.

A key problem that a switch must deal with is the finite bandwidth of its outputs. If packets destined for a certain output arrive at a switch and their arrival rate exceeds the capacity of that output, then we have a problem of contention. In this case, the switch will queue, or buffer packets until the contention subsides. If the contention lasts too long, however, the switch will run out of buffer space and be forced to discard packets. When packets are discarded too frequently, the switch is said to be congested.

In this lab you will set up switched LANs using two different switching devices: hubs and switches. A hub forwards the packet that arrives on any of its inputs on all the outputs regardless of the destination of the packet. On the other hand, a switch forwards incoming packets to one or more outputs depending on the destination(s) of the packets. You will study how the throughput and collision of packets in a switched network are affected by the configuration of the network and the types of switching devices that are used.

# 3.3. Prelab Activities

Read section 3.1 from "Computer Networks: A Systems Approach", 4th Edition.

Go to *www.net-seal.net/animations.php* and play the following animations:

- <u>Switch</u>.
- <u>Switched Network With No Server</u>.
- <u>Switched Network With Server</u>.

# 3.4. Procedure

## 3.4.1. Create a New Project

- 1. Start the OPNET IT Guru Academic Edition  $\Rightarrow$  Choose New from the File menu.
- 2. Select Project and Click  $OK \Rightarrow$  Name the project **<your initials>**SwitchedLAN, and the scenario OnlyHub  $\Rightarrow$  Click OK.
- In the Startup Wizard: Initial Topology dialog box, make sure that Create Empty Scenario is selected. ⇒ Click Next ⇒ Choose Office from the Network Scale list ⇒ Click Next three times ⇒ Click OK.

4. Close the Object Palette dialog box.

## 3.4.2. Create the Network

To create our switched LAN:

- 1. Select Topology  $\Rightarrow$  Rapid Configuration. From the drop-down menu choose Star and Click OK.
- 2. Click the Select Models button in the Rapid Configuration dialog box. From the Model List drop-down menu choose ethernet and Click OK.
- In the Rapid Configuration dialog box, set the following five values: Center Node Model = ethernet16\_hub, Periphery Node Model = ethernet\_station, Link Model = 10BaseT, Number = 16, Y = 50, and Radius = 42 ⇒ Click OK.

The prefix Ethernet16 indicates that the device support up to 16 Ethernet connections.

Rapid Configuration: Star	×
MODELS Center Node Model ethernet16_hub Periphery Node Model ethernet_station	Number 16
PLACEMENT Center X 50 Y 50 Select Models	Radius 42

The **10BaseT** link represents an Ethernet connection operating at 10 Mbps.

- 1. Right-click on node\_16, which is the hub  $\Rightarrow$  Edit Attributes  $\Rightarrow$  Change the name attribute to Hub1 and Click OK.
- 2. Now that you have created the network, it should look like the following one.
- 3. Make sure to save your project.



#### 3.4.3. Configure the Network Nodes

Here you will configure the traffic generated by the stations.

- 1. Right-click on any of the 16 stations (node\_0 to node\_15)  $\Rightarrow$  Select Similar Nodes. Now all stations in the network are selected.
- 2. Right-click on any of the 16 stations  $\Rightarrow$  **Edit** Attributes.
  - a. Check the **Apply Changes to Selected Objects** check box. This is important to avoid reconfiguring each node individually.
- 3. Expand the hierarchies of the Traffic Generation Parameters attribute and the Packet Generation Arguments attribute  $\Rightarrow$  Set the following four values:
- 4. Click OK to close the attribute editing window(s).
- 5. Save your project.

🗄 (node_0) Attributes 📃 🗖 🔀					
Type: station					
Attribute	Value 🔺				
⑦ ⊢ name	node_0				
⑦ ⊢model	ethernet_station				
⑦ ⊡ Traffic Generation Parameters	()				
⑦ ⊢Start Time (seconds)	constant (5.0)				
⑦ ├ON State Time (seconds)	exponential (100.0)				
⑦ ├OFF State Time (seconds)	exponential (0.0)				
Packet Generation Arguments	()				
Interarrival Time (seconds)	exponential (0.02)				
⑦ ⊢Packet Size (bytes)	constant (1500)				
③ LSegmentation Size (bytes)	No Segmentation				
•					
Apply Changes to Selected Objects					
Eind Next	<u>C</u> ancel <u>O</u> K				

#### 3.4.4. Choose Statistics

To choose the statistics to be collected during the simulation:

- 1. Right-click anywhere in the project workspace and select Choose Individual Statistics from the pop-up menu.
- 2. In the Choose Results dialog box, choose the following four statistics:

The Ethernet Delay represents the end to end delay of all packets received by all the stations.

Traffic Received (in packets/sec) by the traffic sinks across all nodes.

Traffic Sent (in packets/sec) by the traffic sources across all nodes.

Collision Count is the total number of collisions encountered by the hub during packet transmissions.



#### 3. Click OK.

#### 3.4.5. Configure the Simulation

Here we need to configure the duration of the simulation:

- 1. Click on the Configure/Run Simulation button:
- 2. Set the duration to be 2.0 minutes.
- 3. Click OK.

#### 3.4.6. Duplicate the Scenario

The network we just created utilizes only one hub to connect the 16 stations. We need to create another network that utilizes a switch and see how this will affect the performance of the network. To do that we will create a duplicate of the current network:

- 1. Select **Duplicate Scenario** from the **Scenarios** menu and give it the name **HubAndSwitch**  $\Rightarrow$  Click **OK**.
- 2. Open the **Object Palette** by clicking on Make sure that **Ethernet** is selected in the pull-down menu on the object palette.
- 3. We need to place the shown hub and switch in the new scenario.



- To add the Hub, click its icon in the object palette ⇒ Move your mouse to the workspace ⇒ Click to drop the hub at a location you select. Right-click to indicate you are done deploying hub objects.
- 5. Similarly, add the Switch and then close the Object Palette.
- 6. Right-click on the new hub  $\Rightarrow$  Edit Attributes  $\Rightarrow$  Change the name attribute to Hub2 and Click OK.
- 7. Right-click on the switch **Edit Attributes**  $\Rightarrow$  Change the **name** attribute to **Switch** and Click **OK**.
- 8. Reconfigure the network of the **HubAndSwitch** scenario so that it looks like the following one.



#### Hints:

- b. To remove a link, select it and choose **Cut** from the **Edit** menu (or simply hit the **Delete** key). You can select multiple links and delete all of them at once.
- c. To add a new link, use the **10BaseT** link available in the **Object Palette**.
- 9. Save your project.

#### 3.4.7. Run the Simulation

To run the simulation for both scenarios simultaneously:

- 1. Select Manage Scenarios from the Scenarios menu.
- 2. Change the values under the **Results** column to **<collect>** (or **<recollect>**) for both scenarios. Compare to the following figure.

\star Ma	🕷 Manage Scenarios 📃 🗖 🔀					
Proj	ect Name: eha Swite	che	Ļ			
#	Scenario Name	Saved	Results	Sim Duration	Time Units	
1	OnlyHub	saved	<collect></collect>	2.0	minute(s)	
2	HubAndSwitch	saved	<collect></collect>	2.0	minute(s)	
					<b>_</b>	
D	elete Discard <u>R</u> est	ults <u>C</u> ol	lect Results		C <u>a</u> ncel <u>O</u> K	

- 3. Click **OK** to run the two simulations. Depending on the speed of your processor, this may take several minutes to complete.
- 4. After the two simulation runs complete, one for each scenario, click **Close**.
- 5. Save your project.

#### 3.4.8. View the Results

To view and analyze the results:

- 1. Select **Compare Results** from the **Results** menu.
- 2. Change the **drop-down** menu in the lower-right part of the *Compare Results* dialog box from **As Is** to **time\_average**, as shown.

🔣 Compare Results		
Discrete Event Graphs Displayed Panel Graphs		
Global Statistics	Show Preview	
Hub2 H node_0	Overlaid Statistics 💽 All S	Scenarios 💌
	time_average	
Results Generated: 17:11:32 Mar 18 2003	Unselect Add	Show
		Close

**time\_average** is the average value over time of the values generated during the collection windows. This average is performed assuming a "sample-and-hold" behavior of the data set (i.e., each value is weighted by the amount of time following update and the sum of all the weighted values is divided by the width of the collection window). For example, suppose you have a 1-second bucket in which 10 values have been generated. The first 7 values were generated between 0 and 0.3 seconds, the 8<sup>th</sup> value at 0.4 seconds, the 9<sup>th</sup> value at 0.6 seconds, and the 10<sup>th</sup> at 0.99 seconds. Because the last 3 values have higher durations, they are weighted more heavily in calculating the **time average**.

3. Select the **Traffic Sent (packets/sec)** statistic and click **Show.** The resulting graph should resemble the one below. As you can see, the traffic sent in both scenarios is almost identical.



Select the **Traffic Received (packets/sec)** statistic and click **Show**. The resulting graph should resemble the one below. As you see, the traffic received with the second scenario, **HubAndSwitch**, is higher than that of the **OnlyHub** scenario.



4. Select the **Delay (sec)** statistic and click **Show**. The resulting graph should resemble the one below. (Note: Result may vary slightly due to different node placement.)



- 5. Select the Collision Count statistic for Hub1 and click Show.
- On the resulting graph right-click anywhere on the graph area ⇒ Choose Add Statistic ⇒ Expand the hierarchies as shown below ⇒ Select the Collision Count statistic for Hub2⇒ Change As Is to time\_average ⇒ Click Add.

🛣 View Results		
Discrete Event Graphs Displayed Panel Gra	phs	
Graph Output Files	Show Preview	
Global Statistics	1,000	
	800	
Object Statistics	400	
Hub1	200	
Ethernet	0	
the node_0 the node_1 the node_1	0 100	200
□ node_10	Stacked Statistics	ime (sec)
	time_average	
	Unselect Add	Show
		<u>C</u> lose

7. The resulting graph should resemble the one below.



8. Save your project.

## 3.5. Further readings

 OPNET <u>Building Network Topologies</u>: From the **Protocols** menu, select Methodologies ⇒ <u>Building Network Topologies</u>.

# 3.6. Exercises

1) Explain why adding a switch makes the network perform better in terms of throughput and delay.

- 2) We analyzed the collision counts of the hubs. Can you analyze the collision count of the "Switch"? Explain your answer.
- 3) Create two new scenarios. The first one is the same as the OnlyHub scenario but replace the hub with a switch. The second new scenario is the same as the HubAndSwitch scenario but replace both hubs with two switches, remove the old switch, and connect the two switches you just added together with a 10BaseT link. Compare the performance of the four scenarios in terms of delay, throughput, and collision count. Analyze the results. Note: To replace a hub with a switch, right-click on the hub and assign ethernet16\_switch to its model attribute.

# 3.7. Lab Report

Prepare a report that follows the guidelines explained in Lab 0. The report should include the answers to the above exercises as well as the graphs you generated from the simulation scenarios. Discuss the results you obtained and compare these results with your expectations. Mention any anomalies or unexplained behaviors.

# 4. Laboratory - Network Design (Planning a Network with Different Users, Hosts, and Services)

# 4.1. Objective

The objective of this lab is to demonstrate the basics of designing a network, taking into consideration the users, services, and locations of the hosts.

## 4.2. Overview

Optimizing the design of a network is a major issue. Simulations are usually used to analyze the conceptual design of the network. The initial conceptual design is usually refined several times until a final decision is made to implement the design. The objective is to have a design that maximizes the network performance, taking into consideration the cost constraints and the required services to be offered to different types of users. After the network has been implemented, network optimization should be performed periodically throughout the lifetime of the network to ensure maximum performance of the network and to monitor the utilization of the network resources.

In this lab you will design a network for a company that has four departments: Research, Engineering, E-Commerce, and Sales. You will utilize a LAN model that allows you to simulate multiple clients and servers in one simulation object. This model dramatically reduces both the amount of configuration work you need to perform and the amount of memory needed to execute the simulation. You will be able to define a profile that specifies the pattern of applications employed by the users of each department in the company. By the end of this lab, you will be able to study how different design decisions can affect the performance of the network.

## 4.3. Prelab Activities

Read section 3.2 from "Computer Networks: A Systems Approach", 4th Edition.

Go to *www.net-seal.net/animations.php* and play the following animations:

Adding Switches.

## 4.4. Procedure

#### 4.4.1. Create a New Project

- 1. Start **OPNET IT Guru Academic Edition**  $\Rightarrow$  Choose **New** from the **File** menu.
- 2. Select **Project** and Click **OK** ⇒ Name the project **<your initials>\_NetDesig**, and the scenario **SimpleNetwork** ⇒ Click **OK**.
- 3. In the Startup Wizard Initial Topology dialog box, make sure that Create Empty Scenario is selected ⇒ Click Next ⇒ Choose Campus from the Network Scale list ⇒ Click Next ⇒ Choose Miles from the Size drop-down menu and assign 1 for both X Span and Y Span ⇒ Click Next twice ⇒ Click OK.

# 4.4.2. Create and Configure the Network

#### *4.4.2.1. Initialize the Network:*

1. The *Object Palette* dialog box should be now on the top of your project space. If

it is not there, open it by clicking . Make sure that the internet\_toolbox is selected from the pull-down menu on the object palette.

- 2. Add to the project workspace the following objects from the palette: **Application Config, Profile Config,** and a **subnet**.
  - a. To add an object from palette, click its icon on the object palette.  $\Rightarrow$  Move your mouse to the workspace.  $\Rightarrow$  Left click to place the object. Right-click when finished. The workplace should contain the following three objects:





Application Config is used to specify application that will be used to configure user's profiles.

**Profile Config** describes the activity patterns of a user or group of users in terms of the applications used over a period of time. You must define the applications using the **Application Config** object between using this object

#### 4.4.2.2. Configure the Services:

- Right-click on the Application Config node ⇒ Edit Attributes Change the name attribute to Applications ⇒ Change the Application Definitions attribute to Default ⇒ Click OK.
- 2. Right-click on the **Profile Config node**  $\Rightarrow$  **Edit Attributes**  $\Rightarrow$  Change the **name** attribute to **Profiles**  $\Rightarrow$  Change the **Profile Configuration** attribute to **Sample Profiles**  $\Rightarrow$  Click **OK**.
- 3. **Sample Profiles** provides patterns of applications employed by users such as engineers, researchers, salespeople, and multimedia users.

#### 4.4.2.3. Configure a Subnet:

- 1. Right-click on the **subnet** node  $\Rightarrow$  **Edit Attributes**  $\Rightarrow$  Change the **name** attribute to **Engineering** and Click **OK**.
- 2. Double-click on the **Engineering** node. You get an empty workspace, indicating that the subnet contains no objects.
- 3. Open the object palette and make sure it is still set to internet\_toolbox.
- 4. Add the following items to the subnet workspace: **10BaseT LAN**, **ethernet16\_Switch**, and a **10BaseT** link to connect the LAN with the Switch  $\Rightarrow$  Close the palette.

- 5. Right-click on the **10BaseT LAN** node  $\Rightarrow$  **Edit Attributes**  $\Rightarrow$  Change the **name** attribute to LAN Observe that the **Number of Workstations** attribute has a value of 10 Click in the **Value** column for the **Application: Supported Profiles** attribute, and select **Edit**. You should get a table in which you should do the following:
  - a. Set the number of **rows** to **1**.
  - b. Set the **Profile Name** to **Engineer**. *Note:* **Engineer** is one of the "sample" profiles provided within the **Profile Config** object.
  - c. Click OK twice.

The object we just created is equivalent to a 10-workstation star topology LAN. The traffic generated from the users of this LAN resembles that generated by "engineers."

- 6. Rename the ethernet16\_Switch to Switch.
- 7. The subnet should look like the shown one.
- 8. Save your project.



- 4.4.2.4. Configure All Departments:
  - 1. Now you have completed the configuration of the Engineering department subnet. To go back to the main project space, click the **Go to the higher level**

button.

The subnets of the other departments in the company should be similar to the engineering one except for the supported profiles.

- Make three copies of the Engineering subnet we just created: Click on the Engineering node ⇒ From the Edit menu, select Copy. From the Edit menu, select Paste three times, placing the subnet in the workspace after each, to create the new subnets.
- 3. Rename (right-click on the subnet and select Set **Name**) and arrange the subnets as shown bellow:



4. Double-click the Research node ⇒ Edit the attributes of its LAN ⇒ Edit the value of the Application: Supported Profiles attribute. ⇒ Change the value of the Profile Name from Engineer to Researcher ⇒ Click OK twice ⇒ Go to the

higher level by clicking the 😈 button.

- 5. Repeat step 4 with the **Sales** node and assign to its **Profile Name** the profile **Sales Person**.
- 6. Repeat step 4 with the **E-commerce** node and assign to its **Profile Name** the profile **E-commerce Customer.**
- 7. Save your project.
- 4.4.2.5. Configure the Servers:

Now we need to implement a subnet that contains the servers. The servers have to support the applications defined in the profiles we deployed. You can double-check those applications by editing the attributes of our **Profile** node. Inspect each row under the **Applications** hierarchy, which in turn, is under the **Profile Configuration** hierarchy. You will see that we need servers that support the following applications: Web browsing, Email, Telnet, File Transfer, Database, and File Print.

- 1. Open the **Object Palette** and add a new **subnet**  $\Rightarrow$  Rename the new subnet to **Servers**  $\Rightarrow$  Double-click the **Servers** node to enter its workspace.
- 2. From the **Object Palette**, add three **ethernet\_servers**, one **ethernet16\_switch** and three **10BaseT** links to connect the servers with the switch.
- 3. Close the **Object Palette**.
- 4. Rename the servers and the switch as follows:



- 5. Right-click on each one of the above servers and **Edit** the value of the **Application: Supported Services** attribute.
  - i. For the *Web Server* add four rows to support the following services: **Web Browsing (Light HTTP1.1) Web Browsing (Heavy HTTP1.1), Email (Light),** and **Telnet Session (Light)**.
  - ii. For the *File Server* add two rows to support the following services: **File Transfer (Light)** and **File Print (Light)**.
  - iii. For the *Database Server* add one row to support the following service: **Database Access (Light)**.
- 6. Go back to the project space by clicking the **Go to the higher level W** button.
- 7. Save your project.
- 4.4.2.6. Connect the Subnets:

Now all subnets are ready to be connected together.

1. Open the **Object Palette** and add four **100BaseT** links to connect the subnets of the departments to the Servers subnet.

As you create each link, make sure that it is configured to connect the "switches" in both subnets to each other. Do this by choosing them from the drop-down menus as follows:

🛣 Select Nodes		
node a	Engineering.Switch	•
node b	Servers.Server Switch	•
	<u>C</u> ancel <u>O</u> K	

- 2. Close the **Object Palette**.
- 3. Now your network should resemble the following one:



4. Save your project.

#### 4.4.2.7. Choose the Statistics

To test the performance of our network we will collect one of the many available statistics as follows:

- 1. Right-click anywhere in the project workspace and select **Choose Individual Statistics** from the pop-up menu.
- 2. In the *Choose Results* dialog box, choose the following statistic:

🔣 Choose Results		
Global Statistics ACE Cache Custom Application Custom Application DB Entry DB Query Email Ethernet Ftp Object Response Time (se Page Response Time (se Traffic Received (bytes/sec) Traffic Sent (bytes/sec) Traffic Sent (packets/sec) Traffic Sent (packets/sec) IP	econds) conds) <del>&lt;</del> ec) ec) ;/sec)	
	<u>C</u> ancel	<u>0</u> K

Page Response Time is the required time to retrieve the entire page.

3. Click OK.

### 4.4.3. Configure the Simulation

Here we need to configure the duration of the simulation:

- 1. Click on the **Configure/Run Simulation** dutton.
- 2. Set the duration to be **30.0 minutes**.
- 3. Press OK.

#### 4.4.4. Duplicate the Scenario

In the network we just created we assumed that there is no background traffic already in the links. In real networks, the links usually have some existing background traffic. We will create a duplicate of the **SimpleNetwork** scenario but with background utilization in the **100BaseT** links.

- 1. Select **Duplicate Scenario** from the **Scenarios** menu and give it the name **BusyNetwork** ⇒ Click **OK**.
- 2. Select all the **100BaseT** links simultaneously (click on all of them while holding the **Shift** key) ⇒ Right-click on anyone of them ⇒ **Edit Attributes** ⇒ Check the **Apply Changes to Selected Objects** check box.
- 3. Expand the hierarchy of the **Background Utilization** attribute  $\Rightarrow$  Expand the **row 0** hierarchy  $\Rightarrow$  Assign **99** to the **background utilization (%)** as shown below.

butes 📃 🗆 🔀
Value
E-Commerce <-> Servers
100BaseT
E-Commerce.Switch.Ethernet (P1)
Servers.Server Switch.Ethernet (P12)
()
1
0.0
99
A < B
100.000.000
ts
<u>C</u> ancel <u>O</u> K

#### 4. Click OK.

Link utilization is the percentage of the used link bandwidth.

## 4.4.5. Run the Simulation

To run the simulation for both scenarios simultaneously:

- 1. Go to the Scenarios menu  $\Rightarrow$  Select Manage Scenarios.
- 2. Change the values under the **Results** column to **<collect>** (or **<recollect>**) for both scenarios. Compare to the following figure.

<b>₩</b> M	anage Scenarios								
Project Name: eha NetDesi									
#	Scenario Name	Saved	Results	Sim Duration	Time Units	<b>A</b>			
1	SimpleNetwork	saved	<collect></collect>	30	minute(s)				
2	BusyNetwork	saved	<collect></collect>	30	minute(s)				
						-			
[	Delete Discard Res	sults <u>C</u> ol	lect Results		C <u>a</u> ncel	<u></u> K			

- 3. Click **OK** to run the two simulations. Depending on the speed of your processor, this may take several seconds to complete.
- 4. After the two simulation runs complete (one for each scenario), click Close.
- 5. Save your project.

#### 4.4.6. View the Results

To view and analyze the results:

- 1. Select **Compare Results** from the **Results** menu.
- 2. Change the drop-down menu in the lower-right part of the *Compare Results* dialog box from **As Is** to **time\_average** as shown.

🔣 Compare Results			
Discrete Event Graphs Displayed Panel Graphs			
	Show Preview		
Page Response Time (seconds)	0.04		
⊡	0.02		
	0.01		
	0.00		
	0	1000	2000 time (sec)
	Overlaid Statistics	▼ All Scena	arios 💌
× •	time_average		<b>•</b>
Results Generated: 19:54:26 Mar 18 2003	Unselect	Add	Show
			<u>C</u> lose

3. Select the **Page Response Time (seconds)** statistic and click **Show**. The resulting graph should resemble the one below. (Note: Results may vary slightly due to different node placement.)


# 4.5. Further readings

OPNET <u>Configuring Applications and Profiles</u>: From the **Protocols** menu, select **Applications**  $\Rightarrow$  **Model Usage Guide**  $\Rightarrow$  Configuring Applications and Profiles.

# 4.6. *Exercises*

- 1) Analyze the result we obtained regarding the HTTP page response time. Collect four other statistics, of your choice, and rerun the simulation of the *Simple* and the *Busy* network scenarios. Get the graphs that compare the collected statistics. Comment on these results.
- In the BusyNetwork scenario, study the utilization% of the CPUs in the servers (Right-click on each server and select Choose Individual Statistics ⇒ CPU ⇒ Utilization).
- 3) Create a new scenario as a duplicate of the BusyNetwork scenario. Name the new scenario Q3\_OneServer. Replace the three servers with only one server that supports all required services. Study the utilization% of that server's CPU. Compare this utilization with the three CPU utilizations you obtained in the previous exercise.
- 4) Create a new scenario as a duplicate of the BusyNetwork scenario. Name the new scenario Q4\_FasterNetwork. In the Q4\_FasterNetwork scenario, replace all 100BaseT links in the network with 10Gbps Ethernet links and replace all 10BaseT links with 100BaseT links. Study how increasing the bandwidth of the links affects the performance of the network in the new scenario (e.g., compare the HTTP page response time in the new scenario with that of the BusyNetwork).

# 4.7. Lab Report

Prepare a report that follows the guidelines explained in Lab 0. The report should include the answers to the above exercises as well as the graphs you generated from the simulation scenarios. Discuss the results you obtained and compare these results with your expectations. Mention any anomalies or unexplained behaviors.

# 5. Laboratory - ATM (A Connection-Oriented, Cell-Switching Technology)

# 5.1. *Objective*

The objective of this lab is to examine the effect of ATM adaptation layers and service classes on the performance of the network.

## 5.2. Overview

Asynchronous Transfer Mode (ATM) is a connection-oriented, packet-switched technology. The packets that are switched in an ATM network are of a fixed length, 53 bytes, and are called *cells*. The cell size has a particular effect on carrying voice traffic effectively. The ATM Adaptation Layer (AAL) sits between ATM and the variable-length packet protocols that might use ATM, such as IP. The AAL header contains the information needed by the destination to reassemble the individual cells back into the original message. Because ATM was designed to support all sorts of services, including voice, video, and data, it was felt that different services would have different AAL needs. AAL1 and AAL2 were designed to support applications, like voice, that require guaranteed bit rates. AAL3/4 and AAL5 provide support for packet data running over ATM.

ATM provides QoS capabilities through its five service classes: CBR, VBR-rt VBR-nrt, ABR, and UBR. With CBR (constant bit rate), sources transmit stream traffic at a fixed rate. CBR is well-suited for voice traffic that usually requires circuit switching. Therefore, CBR is very important to telephone companies. UBR, unspecified bit rate, is ATM's best-effort service. There is one small difference between UBR and the best-effort model. Because ATM always requires a signaling phase before data is sent, UBR allows the source to specify a maximum rate at which it will send. Switches may make use of this information to decide whether to admit or reject the new VC (virtual circuit).

In this lab you will set up an ATM network that carries three applications: Voice, Email, and FTP. You will study how the choice of the adaptation layer as well as the service classes can affect the performance of the applications.

# 5.3. Prelab Activities

Read section 3.3 from "Computer Networks: A Systems Approach", 4th Edition.

# 5.4. Procedure

# 5.4.1. Create a New Project

- 1. Start **OPNET IT Guru Academic Edition**  $\Rightarrow$  Choose **New** from the **File** menu.
- 2. Select **Project** and Click **OK** ⇒ Name the project **<your initials>\_ATM**, and the scenario **CBR\_UBR** ⇒ Click **OK**.
- 3. In the Startup Wizard: Initial Topology dialog box, make sure that Create Empty Scenario is selected ⇒ Click Next ⇒ Select Choose From Maps from the Network Scale list ⇒ Click Next ⇒ Choose USA from the maps ⇒ Click Next ⇒ From the Select Technologies list, include the atm\_advanced Model Family as shown in the following figure ⇒ Click Next ⇒ Click OK.

Startup Wizard: Select Tech	nologies	×
Select the technologies you will use in	Model Family	Include?
your network.	3Com	No
	ACE	No
	applications	No
	Ascend	No
	atm	No
	atm_advanced	Yes
	atm_lane	No 👻
	Quit Back	Next

## 5.4.2. Create and Configure the Network

#### 5.4.3. Initialize the Network:

- 1. The *Object Palette* dialog box should now be on the top of your project workspace. If it is not there, open it by clicking . Make sure that **atm advanced** is selected from the pull-down menu on the object palette.
- 2. Add to the project work space the following objects from the palette: **Application Config**, **Profile Config**, two **atm8\_crossconn\_adv** switches, and a **subnet**.
  - b. To add an object from a palette, click its icon in the object palette ⇒ Move your mouse to the workspace and click to place the object ⇒ Right-click to get out of "object creation mode."
- 3. Close the *Object Palette* dialog box and rename (right-click on the node  $\Rightarrow$  Set **Name**) the objects you added as shown and then save your project:



#### 5.4.3.1. Configure the Applications:

- 1. Right-click on the Applications node  $\Rightarrow$  Edit Attributes Expand the Application Definitions attribute and set rows to 3  $\Rightarrow$  Name the rows: FTP, EMAIL, and VOICE.
  - i. Go to the FTP row  $\Rightarrow$  Expand the Description hierarchy  $\Rightarrow$  Assign High Load to FTP.

- ii. Go to the EMAIL row  $\Rightarrow$  Expand the Description hierarchy  $\Rightarrow$  Assign High Load to Email.
- iii. Go to the VOICE row  $\Rightarrow$  Expand the Description hierarchy  $\Rightarrow$  Assign PCM Quality Speech to Voice.

<table-of-contents> (Applications) Attributes</table-of-contents>	
Type: Utilities	
Attribute	Value
⑦ ⊡ Application Definitions	()
⑦ ⊢rows	3 🔶
⊞ row 0	FTP,()
⊞ row 1	EMAIL,()
⊡ row 2	
⑦ ⊢Name	VOICE
②	()
⑦ ⊢Custom	Off
⑦ - Database	Off
⑦ ⊢Email	Off
⑦ ⊢Ftp	Off
⑦ ⊢Http	Off
⑦ ⊢Print	Off
Remote Login	Off
Instantiation     Instantiation	Off
	PCM Quality Speech < 🗾
Apply Changes to Selected O	bjects Advanced
Eind Next	<u>Cancel</u> <u>O</u> K

2. Click OK and then save your project

**PCM** stands for Pulse Code Modulation. It is a procedure used to digitize speech before transmitting it over the network.

#### 5.4.3.2. Configure the Profiles:

- 1. Right-click on the **Profiles** node  $\Rightarrow$  **Edit Attributes**, Expand the **Profile Configuration** attribute and set **rows** to **3**.
  - i. Name and set the attributes of row 0 as shown:

🔀 (Profiles) Attributes	
Type: Utilities	
Attribute	Value
⑦ ⊢name	Profiles
⑦ ⊢model	Profile Config
⑦ ⊡ Profile Configuration	()
⑦ ⊢rows	3
⊟row 0	
(1) Profile Name	FTP_P
⑦ / □ Applications	()
⑦ ⊢rows	1
⊡ row 0	
HName	FTP
Start Time Offset (seconds)	exponential (5)
Ouration (seconds)	End of Profile
⑦	Once at Start Time
Operation Mode	Simultaneous
③ Start Time (seconds)	uniform (100,110)
③ Fouration (seconds)	End of Simulation
⑦	Once at Start Time
Apply Changes to Selected Objects	☐A <u>d</u> vanced
<u>Eind Next</u>	<u>C</u> ancel <u>O</u> K

ii. Name and set the attributes of row 1 as shown:

₩	(Profiles) Attributes	
Т	vpe: Utilities	
Γ	Attribute	Value
	⊡row 1	
?	) ⊢Profile Name	EMAIL_P
2	○ □ Applications	()
?	) ⊢rows	1
	⊡ row 0	
?	) ⊢Name	EMAIL
?	Start Time Offset (seconds)	exponential (5)
2	→ Duration (seconds)	End of Profile
2	D	Once at Start Time
2	Operation Mode	Simultaneous
0	Start Time (seconds)	uniform (100,110)
0	→ Duration (seconds)	End of Simulation
2		Once at Start Time
Γ	Apply Changes to Selected Objects	Advanced
	<u>F</u> ind Next	<u>Cancel</u> <u>O</u> K

iii. Name and set the attributes of row 2 as shown. (Note: To set the Duration to exponential(60), you will need to assign "Not Used" to the "Special Value") ⇒ Close the Object Palette dialog box.

₩	(Profiles) Attributes	
ту	/pe: Utilities	
Г	Attribute	Value
	⊡row 2	
?	Profile Name	VOICE_P
?	○ □ Applications	()
?	) ⊢rows	1
	⊡ row 0	
?	) ⊢Name	VOICE
?	Start Time Offset (seconds)	exponential (5)
?	Duration (seconds)	exponential (60)
?		Unlimited
?	Operation Mode	Simultaneous
?	Start Time (seconds)	uniform (100,110)
?	→ → Duration (seconds)	End of Simulation
?		Once at Start Time
Γ	Apply Changes to Selected Objects	Advanced
	Eind Next	<u>Cancel</u> <u>O</u> K

- 5.4.3.3. Configure the NorthEast Subnet:
  - 1. Double-click on the **NorthEast** subnet node. You get an empty workspace, indicating that the subnet contains no objects.
  - 2. Open the object palette and make sure that **atm\_advanced** is selected from the pull-down menu on the object palette ...
  - 3. Add the following items to the subnet workspace one **atm8crossconn\_adv** switch one **atm\_uni\_server\_adv**, four **atm\_uni\_client\_adv**, and connect them with bidirectional **atm\_adv** links ⇒ Close the palette ⇒ Rename the objects as shown.



Hint: To edit the attributes of multiple of multiple nodes in the single operation, select all nodes simultaneously using shift and left-click, then **Edit Attributes** of one of the nodes, and select **Apply Changes to Selected Objects**.

- 4. Change the data rate attribute for all links to DS1.
- 5. For both NE\_Voice1 and NE\_Voice2, set the following attributes:
  - i. Set ATM Application Parameters to CBR only.

- ii. Expand the ATM Parameters hierarchy  $\Rightarrow$  Set Queue Configuration to CBR only.
- iii. Expand the Application: Supported Profiles hierarchy  $\Rightarrow$  Set rows to 1  $\Rightarrow$ Expand the row 0 hierarchy  $\Rightarrow$  Set Profile Name to VOICE P.
- iv. Application: Supported Services  $\Rightarrow$  Edit its value  $\Rightarrow$  Set rows to 1  $\Rightarrow$  Set Name of the added row to VOICE  $\Rightarrow$  Click OK.
- v. Expand the Application: Transport Protocol hierarchy  $\Rightarrow$  Voice Transport = AAL2.

**Client Address** is the Transport Adaptation Layer (TPAL) address of the node. This value must be unique for each node. The **TPAL model** suite presents a basic, uniform interface between applications and transport layer models. All interactions with a remote application through TPAL are organized into session. A session is a single conversation between two applications through a transport protocol.

- 6. For NE Voice1, select Edit Attributes  $\Rightarrow$  Edit the value of the Client Address attribute and write down NE Voice1.
- 7. For NE\_Voice2, select Edit Attributes  $\Rightarrow$  Edit the value of the Client Address attribute and write down NE Voice2.
- 8. Configure the NE DataServer as follows:
  - Application: Supported Services  $\Rightarrow$  Edit its value  $\Rightarrow$  Set rows to 2  $\Rightarrow$  Set i. Name of the added rows to: **EMAIL** and **FTP**  $\Rightarrow$  Click **OK**.
  - ii. Expand the Application: Transport Protocol Specification hierarchy  $\Rightarrow$  Voice Transport = AAL2.
  - iii. Edit the value of the Server Address attribute and write down NE DataServer.

The queue configuration specifies a one-to-one mapping between output port queues and the QoS that they support. A specific queue may be configured to support a specific QoS.

- 9. For both NE\_Data1 and NE\_Data2, set the following attributes:
  - Expand the ATM Parameters hierarchy  $\Rightarrow$  Set Queue Configuration to i. UBR.
  - ii. Expand the Application: Supported Profiles hierarchy  $\Rightarrow$  Set rows to  $2 \Rightarrow$ Set Profile Name to FTP P (for row 0) and to EMAIL P (for row 1).
- 10. For NE\_Data1, select Edit Attributes  $\Rightarrow$  Edit the value of the Client Address attribute and write down NE Data1.
- 11. For NE Data2 select Edit Attributes  $\Rightarrow$  Edit the value of the Client Address attribute and write down NE Data2.
- 12. Save your project.
- 5.4.3.4. Add Remaining Subnets:
  - 1. Now you completed the configuration of the NorthEast subnet. To go back to the

project space, click the **Go to the higher level W** button.

The subnets of the other regions should be similar to the NorthEast one except for the names and server addresses.

- 2. Make three copies of the subnet we just created.
- 3. Rename (right-click on the node  $\Rightarrow$  Set **Name**) the subnets and connect them to the switches with bidirectional atm adv links as shown. (Note: You will be asked network simulation experiments manual.doc utorak, 28. rujan 2010 57

to pick the node inside the subnet to be connected to the link. Make sure to choose the "switch" inside each subnet to be connected.)



- 4. Change the **data rate** for all links to **DS1**.
- 5. Select and double-click each of the new subnets (total four subnets) and change the **names**, **server address**, and **server address** of the nodes inside these subnets as appropriate (e.g., replace NE with SW for the *SouthWest* subnet).

Hint: To do step 6, you can right-click on any voice station and choice **Edit Similar Nodes**. This brings up a table in which each node occupies one row and attributes are shown in the columns. Follow the same procedure with similar steps in this lab.

- 6. For all **voice** stations in all subnets (total of eight stations), edit the value of the **Application: Destination Preferences** attribute as follows:
  - i. Set rows to  $1 \Rightarrow$  Set Symbolic Name to Voice Destination  $\Rightarrow$  Click on (...) under the Actual Name column  $\Rightarrow$  Set rows to  $6 \Rightarrow$  For each row choose a voice station that is not in the current subnet. The following figure shows the actual names for one of the **voice** stations in the *NorthEast* subnet:

👫 (Actual Name)	Table			
Name	Sel	ection Weight		
SE_Voice1	10			
SE_Voice2	10			
NW_Voice1	10			
NW_Voice2	10			
SW_Voice1	10			
SW_Voice2	10			-
6 Rows	Delete	Insert	Duplicate	Mov
D <u>e</u> tails	Promote	<u>C</u> an	cel Oł	2

- 7. For all **data** stations in all subnets (total of eight stations), configure the **Application: Destination Preferences** attribute as follows:
  - ii. Set rows to  $2 \Rightarrow$  Set Symbolic Name to FTP Server for the one row and Email Server for the other row  $\Rightarrow$  For each symbolic name (i.e., FTP Server

and Email Server), click on (.) under the **Actual Name** column  $\Rightarrow$  Set **rows** to  $\mathbf{3} \Rightarrow$  For each row choose a data server that is not in the current subnet The following figure shows the actual names for one of the **data** stations in the *NorthEast* subnet:

🚼 (Actual Name)	Table				
Name	<u></u>	Selecti	on Weight		
SE_DataServer		10			
SW_DataServer		10			
WW_DataServer		10			
					<b>T</b>
•					Þ
3 Rows	<u>D</u> elete		Insert	D <u>u</u> plica	ate <u>M</u> ov
D <u>e</u> tails	Promote	;	<u>C</u> anc	el	OK

Hint: To do step 8 in a single operation, you can use the right-click menu on any switch to **Select Similar Nodes**, then **Edit Attributes**, and check **Apply Changes to Selected Objects**. This feature does work, even across objects in different subnets.

8. For all **switches** in the network (total of six switches) configure the **Max\_Avail\_BW** of the CBR queue to be 100%, as shown bellow, and the **Min\_Guaran\_BW** to be 20%.

₩	(CW_Switch) Attributes	
Т	ype: switch	
Γ	Attribute	Value
2	) ⊢name	CW_Switch
?	) ⊢model	atm8_crossconn_adv
2	ATM Parameters	()
?	Address	Auto Assigned
?	☐ Queue Configuration	()
?	) - rows	5
	⊡ row 0	
?	Category	CBR
2	Queue Parameters	()
2	) ⊢Type	Class Based
?	→ → Max_Avail_BW (%Link BW)	100% <
?	→ → Min_Guaran_BW (%Link BW)	20% 🔶 🗌
?	→ Oversubscription (%Min_Guaran_BW)	100%
•	Apply Changes to Selected Objects 🔫 ——	Advanced
Γ	Eind Next	<u>C</u> ancel <u>O</u> K

**Max\_Avail\_BW** is the maximum bandwidth allocated to this queue. Calls will be admitted into this queue only if they are within the maximum available bandwidth requirement.

9. Save your project.

#### 5.4.4. Choose the Statistics

To test the performance of the applications defined in the network, we will collect some of the available statistics as follows:

1. Right-click anywhere in the project workspace and select **Choose Individual Statistics** from the pop-up menu.

network simulation experiments manual.doc

2. In the *Choose Results* dialog box, choose the following statistics:



3. Click OK.

# 5.4.5. Configure the Simulation

Here we need to configure the duration of the simulation:

- 1. Click on the **Configure/Run Simulation** button:
- 2. Set the duration to be **10.0 minutes**.
- 3. Click **OK**. We will be running the simulation later.

#### 5.4.6. Duplicate the Scenario

In the network we just created, we used the CBR service class for the Voice application and the UBR service class for the FTP and Email applications. To analyze the effect of such different classes of services, we will create another scenario that is similar to the **CBR\_UBR** scenario we just created but it uses only one class of service, UBR, for all applications. In addition, to test the effect of the ATM adaptation layer, in the new scenario we will use AAL5 for the Voice application rather than AAL2.

1. Select **Duplicate Scenario** from the **Scenarios** menu and give it the name  $UBR\_UBR \Rightarrow Click OK$ 

- 2. For all **voice** stations in all subnets, reconfigure them as follows. (Check the note below for a faster way to carry out this step.)
  - i. Set ATM Application Parameters to UBR only.
  - ii. ATM Parameters  $\Rightarrow$  Set Queue Configuration to UBR.
  - iii. Application: Transport Protocol  $\Rightarrow$  Set Voice Transport to AAL5.
- 3. Save your project.

*Note:* One easy way to carry out step 2 above is through the network browser as:

- Select Show Network Browser from the View menu.
- Select **Nodes** from the drop-down menu, and check the **Only Selected** check box as shown in the following figure.
- Write **voice** in the find field and click **Enter**.
- In the network browser you should see a list of all **voice** stations selected.
- Right-click on any of the voice stations in the list, select Edit Attributes, and check Apply Changes to Selected Objects.
- Carry out the configuration changes in step 2 above.
- To hide the network browser, deselect **Show Network Browser** from the **View** menu.



#### 5.4.7. Run the Simulation

To run the simulation for both scenarios simultaneously:

- 1. Go to the Scenarios menu  $\Rightarrow$  Select Manage Scenarios.
- 2. Change the values under the **Results** column to <**collect**> (or <**recollect**>) for both scenarios. Compare to the following figure.

<b>*</b> M	anage Scenarios					
Proj	ect Name: eha ATM		J			
#	Scenario Name	Saved	Results	Sim Duration	Time Units	<b>A</b>
1	CBR_UBR	saved	<collect></collect>	10	minute(s)	
2	UBR_UBR	saved	<collect></collect>	10	minute(s)	
						-
	Delete Discard Res	ults <u>C</u> ol	lect Results		C <u>a</u> ncel	<u>0</u> K

- 3. Click **OK** to run the two simulations. Depending on the speed of your processor, this may take several minutes to complete.
- 4. After the two simulation runs complete, one for each scenario, click **Close**.
- 5. Save your project.

## 5.4.8. View the Results

To view and analyze the results:

- 1. Select **Compare Results** from the **Results** menu.
- 2. Change the **drop-down** menu in the right-lower part of the *Compare Results* dialog box from **As Is** to **time\_average** as shown.

🔛 Compare Results			
Discrete Event Graphs Displayed Panel Graphs			
Global Statistics	Show Preview		
	0.0002		
Packet End-to-End Delay (sec)	0.0001		
Packet Delay Variation	0.0000		
	0	400	800
	Overlaid Statistics	▼ All Scenar	time (sec)
	lume_average		
Results Generated: 04:48:28 Mar 19 2003	Unselect	Add	Show
			<u>C</u> lose

3. Select the voice **Packet Delay Variation** statistic and click **Show**. The resulting graph should resemble the one below. (Note: Result may vary slightly due to different node placement.)



# 5.5. Further readings

 OPNET <u>ATM Model Description</u>: From the **Protocols** menu, select **ATM** ⇒ <u>Model</u> <u>Usage Guide</u>.

# 5.6. Exercises

- Analyze the result we obtained regarding the voice Packet Delay Variation time. Obtain the graphs that compare the Voice packet end-to-end delay the Email download response time, and the FTP download response time for both scenarios. Comment on the results.
- 2) Create another scenario as a duplicate of the CBR\_UBR scenario Name the new scenario Q2\_CBR\_ABR. In the new scenario you should use the ABR class of service for data, i.e., the FTP and Email applications in the data stations. Compare the performance of the CBR\_ABR scenario with that of the CBR\_UBR scenario.

#### Hints:

- To set ABR class of service to a node, assign ABR Only to its ATM Application Parameters attribute and ABR only (Per VC Queue) to its Queue Configuration (one of the ATM Parameters).
- For all **switches** in the network (total of 6 switches), configure the **Max\_Avail\_BW** of the **ABR** queue to be 100% and the **Min\_Guaran\_BW** to be 20%.
- 3) Edit the FTP application defined in the Applications node so that its File Size is twice the current size (i.e., make it 100000 bytes instead of 50000 bytes). Edit the EMAIL application defined in the Applications node so that its File Size is five times the current size (i.e., make it 10000 bytes instead of 2000 bytes). Study how this affects the voice application performance in both the CBR\_UBR and UBR\_UBR scenarios. (*Hint.* to answer this exercise, you might need to create duplicates of the CBR\_UBR and UBR\_UBR scenarios. Name the new scenarios Q3\_CBR\_UBR and Q3\_UBR\_UBR respectively).

# 5.7. Lab Report

Prepare a report that follows the guidelines explained in Lab 0. The report should include the answers to the above exercises as well as the graphs you generated from the simulation scenarios. Discuss the results you obtained and compare these results with your expectations. Mention any anomalies or unexplained behaviors.

# 6. Laboratory - RIP: Routing Information Protocol (A Routing Protocol Based on the Distance-Vector Algorithm)

# 6.1. Objective

The objective of this lab is to configure and analyze the performance of the Routing Information Protocol (RIP) model.

# 6.2. Overview

A router in the network needs to be able to look at a packet's destination address and then determines which one of the output ports is the best choice to get the packet to that address. The router makes this decision by consulting a forwarding table. The fundamental problem of routing is: How do routers acquire the information in their forwarding tables?

Routing algorithms are required to build the routing tables and hence forwarding tables. The basic problem of routing is to find the lowest-cost path between any two nodes, where the cost of a path equals the sum of the costs of all the edges that make up the path. Routing is achieved in most practical networks by running routing protocols among the nodes. The protocols provide a distributed, dynamic way to solve the problem of finding the lowest-cost path in the presence of link and node failures and changing edge costs.

One of the main classes of routing algorithms is the distance-vector algorithm. Each node constructs a vector containing the distances (costs) to all other nodes and distributes that vector to its immediate neighbors RIP is the canonical example of a routing protocol built on the distance-vector algorithm. Routers running RIP send their advertisements regularly (e.g., every 30 seconds). A router also sends an update message whenever a triggered update from another router causes it to change its routing table.

The Internet Control Message Protocol (ICMP) can be utilized to analyze the performance of the created routes. It can be used to model traffic between routers without the need of running applications in an end node.

In this lab you will set up a network that utilizes RIP as its routing protocol. You will analyze the routing tables generated in the routers, and you will observe how RIP is affected by link failures. You will also utilize the ICMP to create echo reply messages (i.e., ping) to analyze the created routes.

# 6.3. Prelab Activities

Read sections 4.1.5, 4.1.7, and 4.2.2 from *"Computer Networks: A Systems Approach"*, 4th *Edition.* 

Go to <u>www.net-seal.net/animations.php</u> and play the following animations:

- The Address Resolution Protocol (ARP). <u>Example1</u>, <u>Example2</u>, <u>Example3</u>.
- <u>ARP with Multiple Networks</u>.
- Routing and Forwarding.

# 6.4. Procedure

# 6.4.1. Create a New Project

1. Start **OPNET IT Guru Academic Edition**  $\Rightarrow$  Choose **New** from the **File** menu.

- 2. Select **Project** and Click **OK** ⇒ Name the project **<your initials>\_RIP**, and the scenario **NO\_Failure** ⇒ Click **OK**.
- 3. In the *Startup Wizard: Initial Topology* dialog box, make sure that **Create Empty** Scenario is selected ⇒ Click Next ⇒ Select Campus from the *Network Scale* list ⇒ Click Next three times ⇒ Click OK.

# 6.4.2. Create and Configure the Network

## 6.4.2.1. Initialize the Network:

1. The *Object Palette* dialog box should now be on top of your project workspace.

If it is not there, open it by clicking . Make sure that the internet\_toolbox is selected from the pull-down menu on the object palette.

- 2. Add to the project workspace the following objects from the palette: one ethernet4\_slip8\_gtwy router and two 100BaseT\_LAN objects.
  - a. To add an object from a palette, click its icon in the object palette  $\Rightarrow$  Move your mouse to the workspace  $\Rightarrow$  Click to place the object  $\Rightarrow$  Right-click to stop creating objects of that type.
- Use bidirectional 100BaseT links to connect the objects you just added as in the following figure. Also, rename the objects as shown (right-click on the node ⇒ Set Name).
- 4. Close the *Object Palette* dialog box.
- 5. Save your project.

The **ethernet4\_slip8\_gtwy** node model represents an IP based gateway supporting four Ethernet hub interfaces and eight serial line interfaces. IP packets arriving on any interface are routed to the appropriate output interface based on their destination IP address. The Routing Information Protocol (RIP) or the Open Shortest Path First (OSPF) protocol may be used to dynamically and automatically create the gateway's routing tables and select routes in an adaptive manner.



# 6.4.2.2. Configure the Router:

- 1. Right-click on **Router1** ⇒ **Edit Attributes** ⇒ Expand the **IP Routing Parameters** hierarchy and set the following:
  - i. **Routing Table Export = Once at End of Simulation.** This asks the router to export its routing table at the end of the simulation to the *simulation log*.
- 2. Click **OK** and then save your project.

# 6.4.2.3. Add the Remaining LANs:

1. Highlight or select simultaneously (using shift and left-click) all five objects that you currently have in the project workspace (one router, two LANs, and two links). You can click-and-drag a box around the objects to do this.

- 2. Press Ctri+C to copy the selected objects and then press Ctri+V to paste them.
- 3. Repeat step 2 three times to generate three new copies of the objects and arrange them in a way similar to the following figure. Rename all objects as shown.
- 4. Connect routers, as shown, using PPP\_DS3 links.



The **PPP\_DS3** link has a data rate of 44.736 Mbps.

# 6.4.3. Choose the Statistics

To test the performance of the RIP protocol, we will collect the following statistics:

- 1. Right-click anywhere in the project workspace and select **Choose Individual Statistics** from the pop-up menu.
- 2. In the *Choose Results* dialog box, check the following statistics:
  - a. Global Statistics  $\Rightarrow$  RIP  $\Rightarrow$  Traffic Sent (bits/sec).
  - b. Global Statistics  $\Rightarrow$  RIP  $\Rightarrow$  Traffic Received (bits/sec).
  - c. Nodes Statistics  $\Rightarrow$  Route Table  $\Rightarrow$  Total Number of Updates.
- 3. Click **OK** and then save your project.

**RIP traffic** is the total amount of RIP update traffic (in bits) sent/received per second by all the nodes using RIP as the routing protocol in the IP interfaces in the node.

**Total Number of Updates** is the number of times the routing table at this node gets updated (e.g., due to a new route addition, an existing route deletion, and/or a next hop update).

# 6.4.4. Configure the Simulation

Here we need to configure some of the simulation parameters:



- 2. Set the duration to be **10.0 minutes**.
- 3. Click on the **Global Attributes** tab and change the following attributes:
  - a. **IP Dynamic Routing Protocol = RIP.** This sets the RIP protocol to be the routing protocol of all routers in the network.
  - b. IP Interface Addressing Mode = Auto Addressed/Export.
  - c. RIP Sim Efficiency = Disabled. If this attribute is enabled, RIP will stop after the "RIP Stop Time" But we need the RIP to keep updating the routing table in case there is any change in the network (as we will see in the second scenario).
- 4. Click **OK** and then save the project.

Configure Simulation: eha_RIP-NO_Failu	re 📃 🗖 🔀
Common Global Attributes Object Attributes	Reports SLAs Animation Profiling Advanced Envirc
Attribute	Value
IP Dynamic Routing Protocol	RIP 🔶
IP Interface Addressing Mode	Auto Addressed/Export
IP Routing Table Export/Import	Not Used
LDP Discovery End Time	250
LDP Discovery Start Time	100
LSP Signaling Protocol	RSVP
OSPF Sim Efficiency	Enabled
OSPF Stop Time	260
RIP Sim Efficiency	Disabled
RIP Stop Time	65
RSVP Sim Efficiency	Enabled
Details Reset Value	
<u>R</u> un <u>H</u> el	p <u>C</u> ancel <u>O</u> K

**Auto Addressed** means that all IP interfaces are assigned IP addresses automatically during simulations. The class of address (e.g., A, B, or C) is determined based on the number of hosts in the designed network. Subnet masks assigned to these interfaces are the default subnet masks for that class.

**Export** causes the auto-assigned IP interface to a file (name of the file is <net\_name> ip\_address.gdf and gets saved in the primary model directory).

#### 6.4.5. The Ping Scenario

In this scenario we will utilize the ping model to print the list of traversed nodes while the ICMP request message is sent to the destination and the ICMP response is received from the destination. Traversed routes are logged in the simulation log file

•••

- 1. Select **Duplicate Scenario** from the **Scenarios** menu and name it **ICMP\_Ping**  $\Rightarrow$  Click **OK**.
- 2. Select both **Router1** and **Router3** simultaneously (click on both of them while holding the Shift key)  $\Rightarrow$  Select the **Protocols** menu  $\Rightarrow$  **IP**  $\Rightarrow$  **Demands**  $\Rightarrow$  **Configure Ping Traffic on Selected Nodes**.
- 3. Change the Pattern attribute to Record Route as shown  $\Rightarrow$  Click **OK**.

This operation will con	figure exchange	of ICMP Ping messages with the folk
Ping Traffic Details		Direction
Start Time (sec)	100.0	●Full Mesh
Pattern>	Record R	
Name	Record Route	CFrom Router1
Interval (sec)	1.00	Cramba ha
Packet Size (bytes)	64	· From  Router3
Count (packets)	5	
Record Route	Enabled V	

Notice that a *Ping Parameter* node will be added to the project space. In addition the ping demand is created between *Rotuer1* and *Router3* as a dotted line.

#### 6.4.6. The Failure Scenario

The routers in the network we created will build their routing tables with no need to update these tables further because we didn't simulate any node or link failures. In this scenario we will simulate failures so that we can compare the behavior of the routers in both cases.

- 1. Select **Duplicate Scenario** from the **Scenarios** menu and name it **Failure**  $\Rightarrow$  Click **OK**.
- 2. Open *Object Palette* by clicking  $\square$ . Select the **Utilities** palette from the drop-down menu  $\Rightarrow$  Add a **Failure Recovery** object to your workspace and name it **Failure** as shown  $\Rightarrow$  Close the *Object Palette* dialog box.



3. Right-click on the Failure object  $\Rightarrow$  Edit Attributes  $\Rightarrow$  Expand the Link Failure/Recovery Specification hierarchy  $\Rightarrow$  Set rows to 1  $\Rightarrow$  Set the attributes of the added row, row 0, as follows:

🛣 (Failure) Attributes	
Type: Utilities	
Attribute	Value
⑦ ⊢name	Failure
⑦ ⊢model	Failure Recovery
⑦ ⊢Failure/Recovery Modeling	Enabled
⑦ □ Link Failure/Recovery Specification	()
⑦ ⊢rows	1
⊡ row 0	
③ FName	Campus Network.Router1 <-> Router2
⑦ ⊢Time	200
③ Status	Fail
⑦ ⊢Link Failure/Recovery Specification	NOT USED
Apply Changes to Selected Objects	Advanced
Eind Next	<u>C</u> ancel <u>O</u> K

- 4. This will "fail" the link between Router1 and Router2 200 seconds into the simulation.
- 5. Click OK and then save the project.

# 6.4.7. Run the Simulation

To run the simulation for both scenarios simultaneously: network simulation experiments manual.doc

- 1. Go to the Scenarios menu  $\Rightarrow$  Select Manage Scenarios.
- 2. Change the values under the **Results** column to <**collect**> (or <**recollect**>) for the three scenarios. Compare to the following figure.

<b>*</b> M	anage Scenarios					
Proj	ect Name: eha RIP	_	↓ I			
#	Scenario Name	Saved	Results	Sim Duration	Time Units	
1	NO_Failure	saved	<collect></collect>	10	minute(s)	
2	Failure	saved	<collect></collect>	10	minute(s)	
						<b>_</b>
Ē	Discard <u>R</u> esu	ılts <u>C</u> ol	lect Results		C <u>a</u> ncel	<u>О</u> К

- 3. Click **OK** to run the three simulations. Depending on the speed of your processor, this may take several seconds to complete.
- 4. After the three simulation runs complete, one for each scenario, click  $Close \Rightarrow$  Save your project.

#### 6.4.8. View the Results

- 6.4.8.1. Compare the Number of Updates:
  - 1. Select **Compare Results** from the **Results** menu.
  - 2. Change the drop-down menu in the right-lower part of the *Compare Results* dialog box to **Stacked Statistics** and **Select Scenarios** as shown.

🛨 Compare Results			
Discrete Event Graphs Displayed Panel Graphs			
Global Statistics	Show Preview		
	20		
	20		
Boute Table			
Total Number of Updates	0	1	/
Router2	0	400	800
由 Router3			time (sec)
⊡ Router4	Stacked Statistics	✓ All Scena	rios 💌
	As Is		<b>_</b>
Results Generated: 13:13:25 Mar 19 2003	Unselect	Add	Show
			Close

- 3. Select the **Total Number of Updates** statistic for **Router1** and click **Show**  $\Rightarrow$  Select the **NO\_Failure** and **Failure** scenarios in the **Select Scenarios** dialog box.
- 4. You should get two graphs, one for each scenario. Right-click on each graph and select **Draw Style**  $\Rightarrow$  **Bar**.
- 5. The resulting graphs should resemble the following (you can zoom in on the graphs by clicking-and-dragging a box over the region of interest):



#### 6.4.8.2. Obtain the IP Addresses of the Interface:

Before checking the contents of the routing tables, we need to determine the IP address information for all interfaces in the current network. Recall that these IP addresses are assigned automatically during simulation, and we set the global attribute IP Interface Addressing Mode to export this information to a file.

- From the File menu choose Model Files ⇒ Refresh Model Directories. This causes OPNET IT Guru to search the model directories and update its list of files.
- From the File menu choose Open ⇒ From the drop-down menu choose Generic Data File ⇒ Select the <your initials>\_RIP-NO\_Failure-ip\_addresses file (the other file created from the Failure scenario should contain the same information) ⇒ Click OK.

🖁 Open
Generic Data File
eha_NetDesign-SimpleNetwork-stp_info
eha_RIP-Failure-ip_addresses
eha_RIP-NO_Failure-ip_addresses
eha_SwitchedLAN-HubAndSwitch-stp_info
<u>C</u> ancel <u>O</u> K

3. The following is a part of the gdf file content. It shows the IP addresses assigned to the interfaces of Router1 in our network. For example the interface of Router1 that is connected to Net11 has the IP address 192.0.0.1 (Note: Your result may vary due to different nodes placement.) The Subnet Mask associated with that interface indicates that the address of the sub-network, to which the interface is connected, is 192.0.0.0 (i.e., the logical AND of the interface IP address and the subnet mask).

Node Name: Campus Iface Name	Network.Router1	IP Address	Subnet Mask	Connected Link
IF0 IF1 IF10 IF11 Loopback	0 1 10 11 12	192.0.0.1 192.0.1.1 192.0.2.1 192.0.3.1 192.0.4.1	255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0	Campus Network.Net11 <-> Router1 Campus Network.Net10 <-> Router1 Campus Network.Router1 <-> Router2 Campus Network.Router4 <-> Router1 Not connected to any link.

4. Print out the layout of the network you implemented in this lab. On this layout, from the information included in the gdf file, write down the IP addresses associated with Router1 as well as the addresses assigned to each sub-network as shown in the following two figures (Note: Your IP addresses may vary due to different nodes placement.)



#### 6.4.8.3. Getting the Ping Report:

- 1. To check the content of the ping report for **Router1**:
  - i. Go to the ICMP\_Ping scenario  $\Rightarrow$  Go to the **Results** menu  $\Rightarrow$  Open Simulation Log  $\Rightarrow$  Click on the field PING REPORT for "Campus Network Router1". The report should resemble the following one:

```
PING REPORT for "Campus Network.Router1" (192.0.4.1)
DETAILS:
  Received ICMP echo reply packet for a request packet sent to the following node:
    IP Address: 192.0.4.1
    Node Name : Campus Network.Router1
PERFORMANCE :
  Based on the first ICMP echo request packet
(i.e., a "ping" packet) sent to the above
  node, the following metrics were computed:
    1. Response Time: 0.00028 seconds
    2. List of traversed IP interfaces:
        IP Address
                            Hop Delay
                                             Node Name
         192.0.7.2
                            0.00000
                                            Campus Network.Router3
                            0.00005
          192.0.2.2
                                            Campus Network.Router2
         192.0.4.1
                                            Campus Network.Router1
         192.0.2.1
192.0.7.1
                            0.00002
                                            Campus Network.Router1
                             0.00005
                                            Campus Network.Router2
                            0.00006
         192.0.7.2
                                            Campus Network.Router3
  Note that the IP addresses shown above represent
the address of the output interface on which the
  IP datagram was routed from the corresponding
  nodes to the next node enroute to its destination
  and back.
```

#### 6.4.8.4. Compare the Routing Tables Content:

- 1. To check the content of the routing tables in **Router1** for the **Failure** and **NO\_Failure** scenarios:
  - i. Go to the **Results** menu.  $\Rightarrow$  Open **Simulation** Log  $\Rightarrow$  Expand the hierarchy on the left as shown below.  $\Rightarrow$  Click on the field **COMMON** ROUTE TABLE.

🕞 Simulation Log 🔺	Time	Event	Node	Category	Message
☐ Categories	600	20847	Campus Network.Router1	Results	COMMON ROUTE TABLE snapshot for:   ()
	600	20851	Campus Network.Router2	Results	COMMON ROUTE TABLE snapshot for:   ()
	600	20855	Campus Network.Router3	Results	COMMON ROUTE TABLE snapshot for:   ()
- Route Ta	600	20859	Campus Network.Router4	Results	COMMON ROUTE TABLE snapshot for:   ()
Houto Fu					

 Carry out the previous step for the Failure and NO\_Failure scenarios. The following are partial contents of Router1's routing table for both scenarios (Note: Your results may vary due to different nodes placement):

Routing table of Router1 (NO Failure scenario):

Router name: Ca at time: 60	Router name: Campus Network.Router1 at time: 600.00 seconds					
ROUTE TABLE conte	nts:					
Dest. Address	Subnet Mask	Next Hop	Interface Name	Metric	Protocol	
$192.0.0.0 \\ 192.0.1.0 \\ 192.0.2.0 \\ 192.0.3.0 \\ 192.0.4.0 \\ 192.0.5.0 \\ 192.0.5.0 \\ 192.0.6.0 \\ 192.0.7.0 \\ 192.0.8.0 \\ 192.0.11.0 \\ 192.0.11.0 \\ 192.0.13.0 \\ 192.0.15.0 \\ 192.0.9.0 \\ 192.0.10.0 \\ 192.0.12.0 \\ 192.0.0.0 \\ 192.0.0.0 \\ 192$	255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0	192.0.0.1 $192.0.1.1$ $192.0.2.1$ $192.0.3.1$ $192.0.2.2$ $192.0.2.2$ $192.0.2.2$ $192.0.2.2$ $192.0.3.2$ $192.0.3.2$ $192.0.3.2$ $192.0.3.2$ $192.0.3.2$ $192.0.3.2$ $192.0.3.2$ $192.0.2.2$ $192.0.2.2$ $192.0.2.2$ $192.0.2.2$	IF0 IF1 IF10 IF11 Loopback IF10 IF10 IF10 IF11 IF11 IF11 IF11 IF11	0 0 0 1 1 1 1 1 1 1 2 2 2	Direct Direct Direct RIP RIP RIP RIP RIP RIP RIP RIP RIP RIP	

Loopback interface allows a client and a server on the same host to communicate with each other using TCP/IP.

Routing table of Router1 (Failure scenario):

Router name: Campus Network.Router1 at time: 600.00 seconds					
ROUTE TABLE conter	nts:				
Dest. Address	Subnet Mask	Next Hop	Interface Name	Metric	Protocol
$192.0.0.0 \\ 192.0.1.0 \\ 192.0.2.0 \\ 192.0.3.0 \\ 192.0.4.0 \\ 192.0.11.0 \\ 192.0.13.0 \\ 192.0.13.0 \\ 192.0.15.0 \\ 192.0.5.0 \\ 192.0.5.0 \\ 192.0.6.0 \\ 192.0.7.0 \\ 192.0.8.0 \\ 192.0.9.0 \\ 192.0.10.0 \\ 192.0.12.0 \\ 192.0.0 \\ 192.0.0.0 \\ 192.0.0.0 \\ 192.0.0.0 \\ 192.0.0.0 \\ 192.0.0.0 \\ 192.0.0.0$	255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0	192.0.0.1 $192.0.2.1$ $192.0.3.1$ $192.0.3.2$	IF0 IF1 IF10 IF11 Loopback IF11 IF11 IF11 IF11 IF11 IF11 IF11 IF1	0 0 0 1 1 1 3 3 2 3 2 2 2 2	Direct Direct Direct Direct RIP RIP RIP RIP RIP RIP RIP RIP RIP RIP

# 6.5. Further readings

- RIP: IETF RFC number 2453 (www.ietf.org/rfc.html)
- ICMP. IETF RFC number 792 (www.ietf.org/rfc.html).

# 6.6. *Exercises*

- 1) Obtain and analyze the graphs that compare the sent RIP traffic for the **Failure** and **NO\_Failure** scenarios. Make sure to change the draw style for the graphs to **Bar**.
- 2) Describe and explain the effect of the failure of the link connecting **Router1** to **Router2** on the routing tables of **Router1**.
- 3) Create another scenario as a duplicate of the Failure scenario. Name the new scenario Q3\_Recover. In this new scenario have the link connecting Router1 to Router2 recover after 400 seconds (make sure to keep the failure that occurs at the 200<sup>th</sup> second). Generate and analyze the graph that shows the effect of this network simulation experiments manual.doc
  Utorak, 28. rujan 2010
  75

recovery on the **Total Number of Updates** in the routing table of **Router1**. Check the contents of **Router1's** routing table. Compare this table with the corresponding routing tables generated in the **NO\_Failure** and **Failure** scenarios.

4) Change the Ping packet size to 5000 bytes (*Hint:* Edit the attributes of the Ping Parameters node). Run the simulation to generate a new Ping report. What is the effect of the new size on the ICMP packet response time?

# 6.7. Lab Report

Prepare a report that follows the guidelines explained in Lab 0. The report should include the answers to the above exercises as well as the graphs you generated from the simulation scenarios. Discuss the results you obtained and compare these results with your expectations. Mention any anomalies or unexplained behaviors.

# 7. Laboratory - OSPF: Open Shortest Path First (A Routing Protocol Based on the Link-State Algorithm)

# 7.1. Objective

The objective of this lab is to configure and analyze the performance of the Open Shortest Path First (OSPF) routing protocol.

# 7.2. Overview

In Lab 6 we discussed RIP, which is the canonical example of a routing protocol built on the distance-vector algorithm. Each node constructs a vector containing the distances (costs) to all other nodes and distributes that vector to its immediate neighbors. Link-state routing is the second major class of intra-domain routing protocol. The basic idea behind link-state protocols is very simple: Every node knows how to reach its directly connected neighbors, and if we make sure that the totality of this knowledge is disseminated to every node, then every node will have enough knowledge of the network to build a complete map of the network.

Once a given node has a complete map for the topology of the network, it is able to decide the best route to each destination. Calculating those routes is based on a well-known algorithm from graph theory - Dijkstra's shortest-path algorithm.

OSPF introduces another layer of hierarchy into routing by allowing a domain to be partitioned into areas. This means that a router within a domain does not necessarily need to know how to reach every network within that domain – it may be sufficient for it to know how to get to the right area. Thus, there is a reduction in the amount of information that must be transmitted to and stored in each node. In addition, OSPF allows multiple routes to the same destination to be assigned the same cost and will cause traffic to be distributed evenly over those routers.

In this lab, you will set up a network that utilizes OSPF as its routing protocol. You will analyze the routing tables generated in the routers and will observe how the resulting routes are affected by assigning areas and enabling load balancing.

# 7.3. Prelab Activities

• Read sections 4.2.3 and 4.2.4 from *"Computer Networks: A Systems Approach",* 4th *Edition.* 

Go to *www.net-seal.net/animations.php* and play the following animation:

• Routing and forwarding.

# 7.4. Procedure

# 7.4.1. Create a New Project

- 1. Start **OPNET IT Guru Academic Edition**  $\Rightarrow$  Choose **New** from the **File** menu.
- 2. Select **Project** and Click **OK** ⇒ Name the project **<your initials>\_OSPF**, and the scenario **No\_Areas** ⇒ Click **OK**.
- 3. In the *Startup Wizard: Initial Topology* dialog box, make sure that **Create Empty Scenario** is selected ⇒ Click **Next** ⇒ Select **Campus** from the *Network Scale* list ⇒ Click **Next** three times ⇒ Click **OK**.

# 7.4.2. Create and Configure the Network

## 7.4.2.1. Initialize the Network:

1. The Object Palette dialog box should now be on top of your project workspace.

If it is not there, open it by clicking . Select the **routers** item from the pull-down menu on the object palette.

- a. Add to the project workspace eight routers of type **slip8\_gtwy**. To add an object from a palette, click its icon in the object palette. ⇒ Move your mouse to the workspace and click to place the object. ⇒ You can keep on left-clicking to create additional objects. Right-click when you are finished placing the last object.
- 2. Switch the palette configuration so it contains the **internet\_toolbox**. Use bidirectional **PPP\_DS3** links to connect the routers. Rename the routers as shown below.



3. Close the *Object Palette* and then save your project.

The **slip8\_gtwy** node model represents an IP based gateway supporting up to eight serial line interfaces at a selectable data rate. The RIP or OSPF protocols may be used to automatically any dynamically create the gateway's routes in an adaptive manner.

The **PPP\_DS3** link has a data of 44.736 Mbps.

#### 7.4.2.2. Configure the Link Costs:

1. We need to assign link costs to match the following graph:



2. Like many popular commercial routers, OPNET router models support a parameter called a *reference bandwidth* to calculate the actual cost, as follows:

# Cost = (Reference bandwidth)/(Link bandwidth)

where the default value of the *reference bandwidth* is 1,000,000 Kbps.

- 3. For example, to assign a cost of 5 to a link, assign a bandwidth of 200,000 Kbps to that link. Note that this is not the actual bandwidth of the link in the sense of transmission speed, but merely a parameter used to configure link costs.
- 4. To assign the costs to the links of our network, do the following:
  - i. Select all links in your network that correspond to the links with a cost of 5 in the above graph by shift-clicking on them.
  - ii. Select the Protocols menu  $\Rightarrow$  IP  $\Rightarrow$  Routing  $\Rightarrow$  Configure Interface Metric Information.
  - iii. Assign 200,000 to the Bandwidth (Kbps) field  $\Rightarrow$  Check the Interfaces across selected links radio button, as shown  $\Rightarrow$  Click OK.

🖁 Configure Interface Metric Infor						
This operation will configure the specified bandwidth and delay on all/selected link interfaces.						
Bandwidth (Kbps):	200000					
Delay (10 * usecs):	secs): Not Used					
Apply the above speci	fication to subinterfaces					
Apply the above specification	ation to:					
All connected interfaces						
Interfaces across selected links						
	<u>Cancel</u>	]				

- 5. Repeat step 4 for all links with a cost of 10 but assign 100,000 Kbps to the **Bandwidth (Kbps)** field.
- 6. Repeat step 4 for all links with a cost of 20 but assign 50,000 Kbps to the **Bandwidth (Kbps)** field.
- 7. Save your project.

# 7.4.2.3. Configure the Traffic Demands:

- 1. Select both **RouterA** and **RouterC** by shift-clicking on them.
  - Select the Protocols menu ⇒ IP ⇒ Demands ⇒ Create Traffic Demands ⇒ Check the From RouterA radio button as shown ⇒ Keep the color as blue ⇒ Click Create. Now you should see a blue-dotted line representing the traffic demand between RouterA and RouterC.

Reate Traffic Demands	
Direction <u>Eull Mesh</u> From RouterA	Intensity Packets/sec: 100 Bits/sec: 1000
CFrom RouterC	Duration (secs): 3600
Color: Description: Represents IP Tra	affic Flows
Characterize Demands	<u>C</u> ancel C <u>r</u> eate

2. Select both RouterB and RouterH by shift-clicking on them.

i. Select the **Protocols** menu  $\Rightarrow$  **IP**  $\Rightarrow$  **Demands**  $\Rightarrow$  **Create Traffic Demands**  $\Rightarrow$  Check the **From RouterB** radio button  $\Rightarrow$  Change the color to **red**  $\Rightarrow$  Click **OK**  $\Rightarrow$  Click **Create**.

Now you can see the lines representing the traffic demands as shown.



- 3. To hide these lines: Select the View menu  $\Rightarrow$  Select **Demand Objects**  $\Rightarrow$  Select **Hide All**.
- 4. Save your project.
- 7.4.2.4. Configure the Routing Protocol and Addresses:
  - 1. Select the **Protocols** menu  $\Rightarrow$  **IP**  $\Rightarrow$  **Routing**  $\Rightarrow$  **Configure Routing Protocols**.
  - 2. Check the **OSPF** check box  $\Rightarrow$  Uncheck the **RIP** check box  $\Rightarrow$  Uncheck the **Visualize Routing Domains** check box, as shown:

🛣 Routing Protocol Configura 🔀					
Choose from the following routing protocols. This operation will overwrite the existing configuration on selected IP interfaces.					
None ▼O <u>S</u> PF <del>←</del>					
Apply the above selection to subinterfaces					
All interfaces (including loopback)					
<ul> <li>Injeriaces across selected links</li> </ul>					
Visualize Routing Domains					
<u>C</u> ancel <u>OK</u>					

- 3. Click OK.
- Select RouterA and RouterB only ⇒ Select the Protocols menu ⇒ IP ⇒ Routing ⇒ Select Export Routing Table for Selected Routers ⇒ Click OK on the Status Confirm dialog box.

Auto-Assign IP Addresses assigns a unique IP address to connected IP interfaces whose IP address is currently set to auto-assigned. It does not change the value of manually set IP address.

# 7.4.3. Configure the Simulation

Here we need to configure some of the simulation parameters:

- 1. Click on and the *Configure Simulation* window should appear.
- 2. Set the duration to be **10.0 minutes**.
- 3. Click **OK** and then save your project.

## 7.4.4. Duplicate the Scenario

In the network we just created, all routers belong to one level of hierarchy (i.e., one area). Also, we didn't enforce load balancing for any routes. Two new scenarios will be created. The first new scenario will define two new areas in addition to the backbone area. The second one will be configured to balance the load for the traffic demands between **RouterB** and **RouterH**.

## 7.4.4.1. The Areas Scenario:

- 1. Select **Duplicate Scenario** from the **Scenarios** menu and give it the name **Areas**  $\Rightarrow$  Click **OK**.
- 2. Area 0.0.0.1:
  - i. Select the three links that connect RouterA, RouterB, and RouterC by shift-clicking on them ⇒ Select the Protocols menu OSPF ⇒ Configure Areas ⇒ Assign the value 0.0.0.1 to the Area Identifier, as shown ⇒ Click OK.

🔀 OSPF Area Confi	guration			
This operation will configure Area IDs on the connected interfaces for the selected links:				
Area Identifier: 0.0.0.1				
	<u>C</u> ancel	<u>O</u> K		

- ii. Right-click on RouterC  $\Rightarrow$  Edit Attributes  $\Rightarrow$  Expand the OSPF Parameters hierarchy  $\Rightarrow$  Expand the Loopback Interfaces hierarchy  $\Rightarrow$  Expand the row0 hierarchy  $\Rightarrow$  Assign 0.0.0.1 to the value of the Area ID attribute  $\Rightarrow$  Click OK.
- 3. Area 0.0.0.2
  - i. Click somewhere in the project workspace to disable the selected links and then repeat step 2-i for the three links that connect RouterF, RouterG, and RouterH but assign the value 0.0.0.2 to their Area Identifier.
- 4. To visualize the areas we just created, select the **Protocols** menu  $\Rightarrow$  **OSPF**  $\Rightarrow$  **Visualize Areas**  $\Rightarrow$  Click **OK**. The network should look like the following one with different colors assigned to each area (you may get different colors though).

Loopback interface allows a client and a server on the same host to communicate with each other using TCP/IP.

Note:

- The area you did not configure is the backbone area and its **Area Identifier =** 0.0.0.0.
- The figure shows the links with a thickness of 3.



- 7.4.4.2. The Balanced Scenario:
  - 1. Under the Scenarios menu, Switch to Scenario  $\Rightarrow$  Select No\_Areas.
  - 2. Select **Duplicate Scenario** from the **Scenarios** menu, and give it the name **Balanced**  $\Rightarrow$  Click **OK**.
  - 3. In the new scenario, select both **RouterB** and **RouterH** by shift-clicking on them.
  - Select the Protocols menu ⇒ IP ⇒ Routing ⇒ Configure Load Balancing Options ⇒ Make sure that the option is Packet-Based and the radio button Selected Routers is selected as shown ⇒ Click OK.



5. Save your project.

OPNET provides two types of IP load balancing.

With **Destination Based**, load balancing is done on a per destination basis. The route chosen from the source router to the destination network is the same for all packets.

With **Packet Based**, load balancing is done on a per packet basis. The route chosen from the source router to the destination network is determined for every individual packet.

#### 7.4.5. Run the Simulation

To run the simulation for the three scenarios simultaneously:

- 1. Go to the Scenarios menu  $\Rightarrow$  Select Manage Scenarios.
- 2. Click on the row of each scenario and click the **Collect Results** button. This should change the values under the **Results** column to <**collect**> as shown.

* Manage Scenarios					
Project Name: eha OSPF					
#	Scenario Name	Saved	Results	Sim Duration	Time Units
1	NO_Areas	saved	<collect></collect>	10	minute(s)
2	Areas	saved	<collect></collect>	10	minute(s)
3	Balanced	saved	<collect></collect>	10	minute(s)
					<b>•</b>
Delete Discard Results Collect Results Cancel OK					

- 3. Click **OK** to run the three simulations. Depending on the speed of your processor, this may take several seconds to complete.
- 4. After the three simulation runs complete, one for each scenario, click **Close** and then save your project.

## 7.4.6. View the Results

- 7.4.6.1. The No\_Areas Scenario:
  - 1. Go back to the No\_Areas scenario.
  - 2. To display the route for the traffic demand between RouterA and RouterC: Select the Protocols menu ⇒ IP ⇒ Demands ⇒ Display Routes for Configured Demands. ⇒ Expand the hierarchies as shown and select RouterA → RouterC ⇒ Go to the Display column and pick Yes ⇒ Click Close.



3. The resulting route will appear on the network as shown:



4. Repeat step 2 to show the route for the traffic demand between **RouterB** and **RouterH**. The route is as shown below. (Note: Depending on the order in which you created the network topology, the other "equal-cost" path can be used, that is, the *RouterB-RouterA-RouterD-RouterF-RouterH* path).

network simulation experiments manual.doc utorak, 28. rujan 2010



- 7.4.6.2. The Areas Scenario:
  - 1. Go to scenario Areas.
  - 2. Display the route for the traffic demand between **RouterA** and **RouterC**. The route is as shown:



3. Save your project.

#### 7.4.6.3. The Balanced Scenario:

- 1. Go to scenario Balanced
- 2. Display the route for the traffic demand between **RouterB** and **RouterH**. The route is as shown:



3. Save your project.

# 7.5. Further readings

- 1. OPNET <u>OSPF Model Description</u>: From the **Protocols** menu, select **OSPF**  $\Rightarrow$  <u>Model</u> <u>Usage Guide</u>.
- 2. OSPF: IETF RFC number 2328 (www.ietf.org/rfc.html).

# 7.6. Exercises

- 1) Explain why, for the same pair of routers, the **Areas** and **Balanced** scenarios result in different routes than those observed in the **No\_Areas** scenario.
- 2) Using the simulation log, examine the generated routing table in **RouterA** for each one of the three scenarios. Explain the values assigned to the *Metric* column of each route.

Hints:

Refer to the *View Results* section in Lab 6 for information about examining the routing tables. You will need to set the global attribute **IP Interface Addressing Mode** to the value **Auto Addressed/Export** and rerun the simulation.

To determine the IP address information for all interfaces, you need to open the *Generic Data File* that contains the IP addresses and associated with the scenarios.

3) OPNET allows you to examine the link-state database that is used by each router to build the directed graph of the network. Examine this database for **RouterA** in the **No\_Areas** scenario. Show how **RouterA** utilizes this database to create a map for the topology of the network and draw this map (This is the map that will be used later by the router to create its routing table.)

Hints:

- To export the link-state database of a router, Edit the attributes of the router and set the Link State Database Export parameter (one of the OSPF Parameters, under Processes) to Once at End of Simulation.
- You will need to set the global attribute IP Interface Addressing Mode to the value Auto Addressed/Export. This will allow you to check the automatically assigned IP addresses to the interfaces of the network. (Refer to the notes of exercise 2 above.)
- After rerunning the simulation, you can check the link-state database by opening the simulation log (from the **Results** menu). The link-state database is available in **Classes** ⇒ **OSPF** ⇒ **LSDB\_Export**.
- 4) Create another scenario as a duplicate of the No\_Areas scenario Name the new scenario Q4\_No\_Areas\_Failure. In this new scenario simulate a failure of the link connecting RouterD and RotuerE. Have this failure start after 100 seconds. Read the simulation. Show how that link failure affects the content of the link-state database and routing table of RouterA. (You will need to disable the global attribute OSPF Sim Efficiency. This will allow OSPF to update the routing table if there is any change in the network.)
- 5) For both **No\_Areas** and **Q4\_No\_Areas\_Failure** scenario, collect the **Traffic Sent** (bits/sec) statistic (one of the Global Statistics under OSPF). Rerun the simulation for these two scenarios and obtain the graph that compares the

OSPF's Traffic Sent (bits/sec) in both scenarios. Comment on the obtained graph.

*Note*: A stub network only carries local traffic (i.e., packets to and from local hosts). Even if it has paths to more than one other network, it does not carry traffic for other networks (RFC 1983).

# 7.7. Lab Report

Prepare a report that follows the guidelines explained in Lab 0. The report should include the answers to the above exercises as well as the graphs you generated from the simulation scenarios. Discuss the results you obtained and compare these results with your expectations. Mention any anomalies or unexplained behaviors.
# 8. Laboratory - Border Gateway Protocol (BGP) (An Interdomain Routing Protocol)

# 8.1. Objective

The objective of this lab is to simulate and study the basic features of an interdomain routing protocol called Border Gateway Protocol (BGP).

## 8.2. Overview

The Internet is organized as a set of routing domains. Each routing domain is called an autonomous system (AS). Each AS is controlled by a single administrative entity (e.g., an AS of a single service provider). Each AS has a unique 16-bit identification number. This number is assigned by a central authority. An AS employs its own *intradomain* routing protocol (e.g., RIP or OSPF). Different ASs establish routes among each other through *interdomain* routing protocols. The border gateway protocol (BGP) is one of the major interdomain routing protocols.

The main goal of BGP is to find any path to the destination that is loop-free. This is different from the common goal of intradomain routing protocols, which is to find an optimal route to the destination based on a specific link metric. The routers that connect different ASs are called border gateways. The task of the border gateways is to forward packets between ASs. Each AS has also at least one BGP speaker BGP speakers exchange reachability information among ASs.

BGP advertises the complete path to the destination AS as an enumerated list. This way routing loops can be avoided. A BGP speaker can also apply some policies such as balancing the load over the neighboring ASs. If a BGP speaker has a choice of several different routes to a destination, it will advertise the best one according to its own local policies. BGP is defined to run on top of TCP and hence BGP speakers do not need to worry about acknowledging received information or retransmission of sent information.

In this lab you will set up a network with three different ASs. RIP will be used as the intradomain routing protocol and BGP as the interdomain one. You will analyze the routing tables generated in the routers as well as the effect of applying a simple policy.

## 8.3. Prelab Activities

• Read section 4.3 from "Computer Networks: A Systems Approach", 4th Edition.

Go to *www.net-seal.net/animations.php* and play the following animation:

IP Subnets

# 8.4. Procedure

## 8.4.1. Create a New Project

- 1. Start **OPNET IT Guru Academic Edition**  $\Rightarrow$  Choose **New** from the **File** menu.
- 2. Select **Project** and Click **OK** ⇒ Name the project **<your initials>\_BGP**, and the scenario **No\_BGP** ⇒ Click **OK**.
- 3. In the *Startup Wizard: Initial Topology* dialog box, make sure that **Create Empty Scenario** is selected ⇒ Click **Next** ⇒ Select **Campus** from the *Network Scale* list ⇒ Click **Next** three times ⇒ Click **OK**.

## 8.4.2. Create and Configure the Network

### 8.4.2.1. Initialize the Network:

1. The *Object Palette* dialog box should now be on top of your project workspace.

If it is not there, open it by clicking . Make sure that the internet\_toolbox is selected from the pull-down menu on the object palette.

- 2. Add to the project workspace the following objects from the palette: six ethernet4\_slip8\_gtwy routers and two 100BaseT\_LAN objects.
  - a. To add an object from a palette, click its icon in the object palette  $\Rightarrow$  Move your mouse to the workspace  $\Rightarrow$  Click to place the object  $\Rightarrow$  Right-click to stop creating objects of that type.
- 3. Use bidirectional PPP\_DS3 links to connect the routers you just added as in the following figure. Also, rename the network objects as shown (right-click on the node ⇒ Set Name).
- 4. Use a bidirectional **100BaseT** link to connect **LAN\_West** to **Router1** and another **100BaseT** link to connect **LAN\_East** to **Router6** as in the following figure.
- 5. Close the Object Palette dialog box.
- 6. Save your project.



The **ethernet4\_slip8\_gtwy** node model represents an IP based gateway supporting four Ethernet hub interfaces and eight serial line interfaces. IP packets arriving on any interface are routed to the appropriate output interface based on their destination IP address.

#### 8.4.2.2. Routers Configuration:

- 1. Highlight or select simultaneously (using shift- and left-click) all six routers  $\Rightarrow$ Right-click on any router  $\Rightarrow$  Edit Attributes.  $\Rightarrow$  Check the Apply Changes to Selected Objects check box.
- 2. Expand the BGP Parameters hierarchy and set the following:
  - i. Redistribution  $\rightarrow$  Routing Protocols  $\rightarrow$  RIP  $\rightarrow$  Redistribute w/ Default.

- 3. Expand the IP Routing Parameters hierarchy and set the following:
  - i. Routing Table Export = Once at End of Simulation. This asks the router to export its routing table at the end of the simulation to the *simulation log*.
- 4. Expand the RIP Parameters hierarchy and set the following:
  - i. Redistribution  $\rightarrow$  Routing Protocols  $\rightarrow$  Directly Connected  $\rightarrow$  Redistribute w/ Default.
- 5. Click **OK** and then save your project.

Redistribute w/ Default allows router to have a route to a destination that belongs to another Autonomous System.

- 8.4.2.3. Application Configuration:
  - Right-click on LAN\_West ⇒ Edit Attributes ⇒ Assign All to Application: Supported Services ⇒ Assign West\_Server to the LAN Server Name attribute as shown ⇒ Click OK.

Notice that two objects for *Applications* and *Profiles* will be added automatically to the project.

Type: LAN		
Attribute	Value	
⑦ ⊢ name	LAN_West	
	100BaseT	LAN
Application: ACE Tier Configuration	Unspecifie	d
Application: Destination Preferences	None	•
	None	
Application: Supported Profiles	None	
Application: Supported Services	All	←
	None	
	Single Proc	cessor
	()	
	()	
①	None	68
LAN Server Name	West_Serv	ver 🔶 🚽
Image: Provide the second s	10	-
Apply Changes to Selected Objects		Advanced
Find Next (	ancel	OK

- 2. Right-click on LAN\_East  $\Rightarrow$  Edit Attributes:
  - i. Expand the Application: Supported Profiles hierarchy  $\Rightarrow$  Set rows to  $1 \Rightarrow$  Expand the row 0 hierarchy  $\Rightarrow$  Set Profile Name to E-commerce Customer.
  - ii. Edit the Application: Destination Preferences attribute as follows:

Set rows to  $1 \Rightarrow$  Set Symbolic Name to HTTP Server  $\Rightarrow$  Edit Actual Name  $\Rightarrow$  Set rows to  $1 \Rightarrow$  In the new row, assign West\_Server to the Name column.

3. Click **OK** three times and then save your project.

## 8.4.3. Configure the Simulation

Here we need to configure some of the simulation parameters:



- 2. Set the duration to be **10.0 minutes**.
- 3. Click on the **Global Attributes** tab and make sure that the following attributes are assigned as follows:
  - a. IP Interface Addressing Mode = Auto Addressed/Export.
  - b. IP Routing Table Export/Import = Export.
  - c. **RIP Sim Efficiency = Disabled**. If the attribute is enabled, RIP will stop after the "RIP Stop Time". But we need the RIP to keep updating the routing table in case there is any change in the network.
- 4. Click **OK** and then save the project.

+ Configure Simulation: tmp_BGP-NO_Policies						
Common Global Attributes Object A	ttributes Reports State Animation Rectiling Advancer					
Attnbute	Value					
IP Dynamic Routing Protocol	Default					
IP Interface Addressing Mode	Auto Addressed/Export	•				
IP Routing Table Export/Import	Export					
LDP Discovery End Time	250					
LDP Discovery Start Time	100					
LSP Signaling Protocol	RSVP					
OSPF Sim Efficiency	Enabled					
OSPF Stop Time	260					
RIP Sim Efficiency	Disabled					
RIP Stop Time	65					
RSVP Sim Efficiency	Enabled					
Tracer Packet Redundancy	Fnahled					
Dolais Read Value						
Bun	Help Qancel QK					

Auto Addressed means that all IP interfaces are assigned. IP addresses automatically during simulation. The class of address (e.g., A, B, or C) is determined based on the number of hosts in the designed network. Subnet masks assigned to these interfaces are the default subnet masks for that class.

**Export** causes the auto assigned IP interface to be exported to a file (name of the file is <net\_name>ip\_addresses.gdf and gets saved in the primary model directory).

#### 8.4.4. Choose the Statistics

- 1. Right-click on LAN\_East and select Choose Individual Statistics from the pop-up menu ⇒ From the Client HTTP hierarchy choose the Traffic Received (bytes/sec) statistic ⇒ Click OK.
- Right-click on the link that connects Router2 to Router3 and select Choose Individual Statistics from the pop-up menu ⇒ From the point-to-point hierarchy choose the "Throughput (bits/sec) →" statistic ⇒ Click OK.

*Note*: If the name of the link is "**Router3** <-> **Router2**" then you will need to choose the ''**Throughput (bits/sec)** ←" statistic instead.

3. Right-click on the link that connects **Router2** to **Router4** and select **Choose Individual Statistics** from the pop-up menu ⇒ From the **point-to-point** hierarchy choose the **"Throughput (bits/sec)** →" statistic ⇒ Click **OK**. *Note*: If the name of the link is "**Router4** <-> **Router2**" then you will need to choose the "**Throughput (bits/sec)** ←" statistic instead.

4. Save your project.

## 8.4.5. Router Interfaces and IP Addresses

Before setting up the routers to use BGP, we need to get the information of the routers' interfaces along with the IP addresses associated to these interfaces. Recall that these IP addresses are assigned automatically during simulation, and we set the global attribute IP Interface Addressing Mode to export this information to a file.

- 1. First we need to run the simulation. Click on  $\bigotimes$  and the *Configure Simulation* window should appear  $\Rightarrow$  Click on **Run**.
- 2. After the simulation run completes click Close.
- 3. From the **File** menu choose **Model Files** ⇒ **Refresh Model Directories**. This causes OPNET IT Guru to search the model directories and update its list of files.
- From the File menu choose Open. ⇒ From the drop-down menu choose Generic Data File ⇒ Select the <your initials>\_BGP-No\_BGP-ip\_addresses file ⇒ Click OK.

The file that contains all the information about router interfaces and their IP addresses will open. Table 1 shows the interface number and IP addresses between the six routers in our projects. For example **Router1** is connected to **Router2** through interface (IF) 11, which is assigned 192.0.1.1 as its IP address. A router is connected to itself by a Loop-back interface as shown. Create a similar table for your project but note that your result may vary due to different nodes placement.

Routers	1	2	3	4	5	6
1	IF: 12	IF: 11				
I	IP: 192.0.2.1	IP: 192.0.1.1				
2	IF: 10	IF: 12	IF:11	IF:4		
2	IP: 192.0.1.2	IP: 192.0.8.1	IP: 192.0.4.2	IP: 192.0.7.1		
2		IF: 10	IF: 12	IF: 11	IF: 4	
5		IP: 192.0.4.1	IP: 192.0.6.1	IP: 192.0.5.1	IP: 192.0.3.1	
1		IF: 10	IF: 11	IF: 12	IF 4	
4		IP: 192.0.7.2	IP: 192.0.5.2	IP: 192.010.1	IP: 192.0.9.1	
5			IF: 10	IF: 11	IF: 12	IF: 4
5			IP: 192.0.3.2	IP: 192.0.9.2	IP: 192.0.12.1	IP: 1920.11.1
6					IF: 10	IF: 12
0					IP: 192.0.11.2	IP: 192.0.14.1

Table 1: Interfaces that connect the routers and their assigned IP addresses.

## 8.4.6. Creating the BGP Scenario

In the network we just created, all routers belong to the same autonomous system. We will divide the network into three autonomous systems and utilize BGP to route packets among these systems.

1. Select **Duplicate Scenario** from the **Scenarios** menu and name it **BGP\_Simple**  $\Rightarrow$  Click **OK**.

- 2. Highlight or select simultaneously (using shift and left-click) Router1 and Router2  $\Rightarrow$  Right-click on Router1  $\Rightarrow$  Edit Attributes  $\Rightarrow$  Check the Apply Changes to Selected Objects check box.
- 3. Expand the IP Routing Parameters hierarchy and set the Autonomous System Number to 12 ⇒ Click OK.
- 4. Repeat steps 2 and 3 above for routers **Router3** and **Router4**. Assign their **Autonomous System Number** to **34**.
- 5. Repeat steps 2 and 3 above for routers **Router5** and **Router6**. Assign their **Autonomous System Number** to **56**.

The following figure shows the created autonomous systems. The figure shows also the interfaces that connect routers across different autonomous systems. There interfaces are taken from Table 1 above (note: the interface numbers in your project may vary). The next step is to disable the RIP protocol on the shown interfaces.



6. Right-click on Router2 ⇒ Edit Attributes ⇒ Expand the IP Routing Parameters hierarchy ⇒ Expand the Interface Information hierarchy ⇒ Expand row 4 hierarchy. ⇒ Click on the values of the Routing Protocol(s) attribute ⇒ Disable RIP as shown ⇒ Click OK twice.

Ati	tribute intow 4 EName	Value	
•	F Status F Address	\star Select Dynai	mic Ro 🗙
	<ul> <li>F Subnet Mask</li> <li>Secondary Address</li> <li>Subinterface Inform</li> <li>Routing Protocol(s)</li> <li>HMTU (bytes)</li> <li>Metric Information</li> <li>QoS Information</li> </ul>	Routing Protocol RIP IGRP OSPF EIGRP IS-IS	Status  Disabled Disabled Disabled Disabled Disabled Disabled Visabled Disabled
© ©	Huiticast Mode	<u>C</u> ar	ncel <u>Q</u> K

- 7. Repeat step 6 above for all other interfaces that connect routers across autonomous systems (i.e., All the eight inter-domain interfaces shown above).
- 8. Save your project.

### 8.4.7. Configuring the BGP Neighbor Information

If you try to run the simulation of the **BGP\_Simple** scenario, you will receive hundreds of errors! This is because there is no routing protocol running between the inter-domain routers. Therefore, no routing tables are created to deliver packets among autonomous systems. The solution is to utilize BGP by defining the neighbors of inter-domain routers. Table 2 shows the neighbors of the routers that will run BGP. Neighbors are defined by their interface IP address and the AS number. For each router in Table 2 carry out the following step:

 Right-click on the router ⇒ Edit Attributes ⇒ Expand the BGP Parameters hierarchy ⇒ Expand the Neighbor Information hierarchy ⇒ Assign to the rows attribute the value 1 for Router1 and Router6. For all other routers, assign the value 3 to the rows attribute ⇒ Utilize Table 2 to assign the corresponding values to the IP Address, Remote AS, and Update Source attributes for each of the added rows.

*Note:* the values to be assigned to the **IP Address** attribute have to match the values you will collect in your Table 1.

2. Save your project.

Routers	BGP Parameters $\Rightarrow$ Neighbor Information				
nouters	row 0	row 1	row 2		
	IP Address: 192.0.8.1				
Router1	Remote AS: 12				
	Update Source: Loopback				
	IP Address 192.0.4.1	IP Address: 192.0.7.2	IP Address: 192.0.2.1		
Router2	Remote AS: 34	Remote AS: 34	Remote AS: 12		
	Update Source Not Used	Update Source Not Used	Update Source: Loopback		

Table 2: Neighbors' info f	for inter-domain routers.
----------------------------	---------------------------

Routers	BGP Parameters $\Rightarrow$ Neighbor Information				
nouters	row 0	row 1	row 2		
	IP Address 192.0.4.2	IP Address: 192.0.3.2	IP Address: 192.0.10.1		
Router3	Remote AS: 12	Remote AS: 56	Remote AS: 34		
	Update Source Not Used	Update Source: Not Used	Update Source: Loopback		
	IP Address: 192.0.7.1	IP Address: 192 0.9.2	IP Address: 192.0.6.1		
Router4	Remote AS: 12	Remote AS: 56	Remote AS: 34		
	Update Source: Not Used	Update Source: Not Used	Update Source: Loopback		
	IP Address: 192.0.3.1	IP Address: 192.0.9.1	IP Address 192.0.14.1		
Router5	Remote AS: 34	Remote AS: 34	Remote AS: 56		
	Update Source: Not Used	Update Source: Not Used_	Update Source: Loopback		
	IP Address: 192.0.12.1				
Router6	Remote AS: 56				
	Update Source: Loopback				

### 8.4.8. Creating the BGP with Policy Scenario

BGP allows for routing policies that can be enforced using route maps. We will utilize this feature to configure **Router2** to redirect its load on the two egress links of its autonomous system.

- First make sure that your project is in the BGP\_Simple scenario. Select Duplicate Scenario from the Scenarios menu and name it BGP\_Policy ⇒ Click OK.
- 2. Right-click on Router2 ⇒ Edit Attributes ⇒ Expand the IP Routing Parameters hierarchy ⇒ Expand the Route Map Configuration hierarchy. ⇒ Set the attributes as shown in the following figure.

The purpose of the created route map is to reduce the degree of preference of the "route to AS 56" to the value 10 (Note: the normal value is "99", which is calculated as 100 - number of AS that should be crossed to reach the destination).

• (F	(Router2) Attributes					
Туре	router					
At	tribute	Value		<b>A</b>		
٢	Route Map Configuration	(				
٢	rows	1	←			
	⊡row 0					
•	- Map Label	Route Map 1				
1	Map Configuration	()				
٢	rows	1	←			
	⊡ row 0					
1	⊢ Term	10				
٢	Match Info	()				
1	Frows	1	←			
	— row 0					
1	-Match Prop	AS Path	←			
1	-Match Con	Contains	←			
1	LMatch Value	56				
٢	⊟ Set Info	()				
•	Frows	1	←			
	row 0					
0	- Set Attribute	Local Preference	←			
1	- Set Operati	Set As [=]	←			
1	L Set Value	10	←			
0	L Action	Permit				
٢	L Next Map Label	Not Used		•		
Ар	ply Changes to Selected Obj	ects		Advanced		
	Eind Next		Cancel	QK		

The next step is to assign the above route map to the link connecting **Router2** to **Router3**. This way traffic from **Router2** to AS 56 will be preferred to go through **Router4** instead.

- 3. Right-click on **Router2** ⇒ **Edit Attributes** ⇒ Expand the **BGP Parameters** hierarchy ⇒ Expand the **Neighbor Information** hierarchy ⇒ Expand the row that has the IP address of **Router3** interface (it is **row 0** in my project) ⇒ Expand the **Routing Policies** hierarchy ⇒ Set its attribute as shown in the following figure.
- 4. Click OK and save your project.

Type:	router		
Att	ribute	Value	•
۰ - ۱	name	Router2	
⊕ ⊦r	model	ethernet4_slip8_gtwy	
	BGP Parameters	()	
•	Status	Enabled	
0	- Start Time	constant (70)	
•	Neighbor Information	()	
•	Frows	3	
	⊡row 0		
1	- IP Address	192.0.4.1	
۲	-Remote AS	34	
0	EBGP Multihop Sett.	No EBGP Multihop	
1	Timers	()	
•	Hext Hop Self	Default	
•	- Update Source	Not Used	
0	Prefix Limit	No Max Limit	
•	- Weight	100	
1	- Send-Community	Disabled	
1	Routing Policies	()	
0	Frows	1	
	⊡ row 0		
1	-Route Map	Route Map 1	
1	L Applicable Direc.	. In 🔶	-
4			
App	bly Changes to Selected Ob	jects	Advanced
	Eind Novt	Cancel	Or

#### 8.4.9. Run the Simulation

To run the simulation for the three scenarios simultaneously:

- 1. Go to the Scenarios menu  $\Rightarrow$  Select Manage Scenarios.
- 2. Change the values under the **Results** column to <**collect**> (or <**recollect**>) for the three scenarios. Compare to the following figure.

[+]/	Manage Scenarios				
Proj	ect Name eha BGP	-	Ļ		
#	Scenario Name	Saved	Results	Sim Duration	Time Units 🔺
1	No_BGP	saved	<collect></collect>	10	minute(s)
2	BGP_Simple	saved	<coliect></coliect>	10	minute(s)
3	BGP_Policy	unsaved	<collect></collect>	10	minute(s) 🔹
1	Delete Discard Results	a di segara s			Cancel QK

- 3. Click **OK** to run the three simulations. Depending on the speed of your processor, this may take several minutes to complete.
- 4. After the three simulation runs complete, one for each scenario, click Close.  $\Rightarrow$  Save your project.

#### 8.4.10. View the Results

#### 8.4.10.1. Compare the Routing Tables Content:

- 1. To check the content of the routing tables in **Router2** for both scenarios:
  - Go to the Results menu ⇒ Open Simulation Log ⇒ Expand the hierarchy on the left as shown below ⇒ Click on the field COMMON ROUTE TABLE in the row corresponds to Router2.

Simulation Log	Node	Category	Message
Categories	Campus Network Router1	Results	COMMON ROUTE TABLE snapshot for   (
Classes	Campus Network Router3	Results	COMMON ROUTE TABLE snapshot for   (
	Campus Network Router2	Results	COMMON ROUTE TABLE snapshot for   (
D IP	Campus Network Router4	Results	COMMON ROUTE TABLE snapshot for   (
Route T	Campus Network Router5	Results	COMMON ROUTE TABLE snapshot for   (
THOULD IN	Campus Network Router6	Results	COMMON ROUTE TABLE snapshot for   (

2. Carry out the previous step for scenario **No\_BGP** and scenario **BGP\_Simple**. The following are partial contents of **Router2**'s routing table for both scenarios (Note: Your results may vary due to different nodes placement):

Routing table of **Router2** for the **No\_BGP** scenario.

Dest. Address	Subnet Mask	Next Hop	Interface Name	Metric	Protocol
103.0.3.0		163.6.7.1	xc.4	0	63
	233.233.233.0	192.0.7.1	1F4 TC10	0	Direct
192.0.4.0	255 255 255 0	192 0 4 2	TF11	0	Direct
192.0.8.0	255.255.255.0	192.0.8.1	Loopback	Ŏ	Direct
192.0.0.0	255.255.255.0	192.0.1.1	IF 10	1	RIP
192.0.2.0	255.255.255.0	192.0.1.1	IF10	1	RIP
192.0.5.0	255.255.255.0	192.0.7.2	IF4	1	RIP
192.0.9.0	255.255.255.0	192.0.7.2	114	1	RIP
		192.0.7.2	11-4	1	-KIP
192 0 5 0	255 255 255 0	192.0.4.1	1011	1	RTP RTP
192.0.11.0	255.255.255.0	192.0.4.1	îriî	2 2	RIP
192.0.12.0	255.255.255.0	192.0.4.1	IFII	2	RIP
192.0.13.0	255.255.255.0	192.0.4.1	IF11	ः <u>३</u>	RIP
192.0.14.0	255.255.255.0	192.0.4.1	IF11	3	RIP

Routing table of Router2 for the BGP\_Simple scenario:

Dest. Address	Subnet Mask	Next Hop	Interface Name	Metric	Protocol
the system of the second site of the site of the second site of the se	ine del se natione ner de period de se se ner sed part. A	n an	na an a	law and no low day law	in the off on the set in the "
192.0.1.0	255.255.255.0	192.0.1.2	IF10	ò	Direct
192.0.8.0	255.255.255.0	192.0.8.1	Loopback	0	Direct
192.0.7.0	255.255.255.0	192.0.7.1	IF4	0	Direct
192.0.4.0	255.255.255.0	192.0.4.2	IF11	0	Direct
192.0.0.0	255.255.255.0	192.0.1.1	1110	1	RIP
192.0.2.0	255.255.255.0	192.0.1.1	1F10	1	RIP
192.0.10.0	255.255.255.0	192.0.7.2	IF4	0	BGP
192.0.5.0	255.255.255.0	192.0.4.1	IF11	0	8GP
192.0.6.0	255.255.255.0	192.0.4.1	IF11	0	BGP
192.0.9.0	255.255.255.0	192.0.4.1	IF11	2	8GP
192.0.3.0	255.255.255.0	192.0.4.1	IF11	2	8GP
192.0.11.0	255.255.255.0	192.0.4.1	IF11	0	8GP
192.0.12.0	255.255.255.0	192.0.4.1	IF 11	0	BGP
192.0.13.0	255.255.255.0	192.0.4.1	IF11	0	BGP
192.0.14.0	255.255.255.0	192.0.4.1	IF11	0	BGP

- 8.4.10.2. Compare the load in the network:
  - 1. Select **Compare Results** from the **Results** menu.
  - 2. Change the drop-down menu in the right-lower part of the **Compare Results** dialog box from **As Is** to **time\_average** as shown.

Discrete Event Graphs Displayed Panel Graphs	5
Global Statistics Object Statistics Campus Network Client Http Traffic Received (bytes/sec) <e- Router2 &lt;-&gt; Router3 [0] Client Http Router2 &lt;-&gt; Router3 [0] Router2 &lt;-&gt; Router4 [0]</e- 	Show Preview
point-to-point     throughput (bits/sec) ->	Overlaid Statistics   All Scenarios

3. Select and show the graphs of the following statistics: **Traffic Received** in **LAN\_East**, throughput in the **Router2-Router3** link, and throughput in the **Router2-Router4** link. The resulting graphs should resemble the graphs below.





# 8.5. Further readings

- A Border Gateway Protocol 4 (BGP-4): <u>IETF RFC number 1771</u> (<u>www.ietf.org/rfc.html</u>).
- Application of the Border Gateway Protocol in the Internet: <u>IETF RFC number 1772</u> (www.ietf.org/rfc.html).
- BGP4 Protocol Analysis: <u>IETF RFC number 1774 (www.ietf.org/rfc.html</u>).

## 8.6. Exercises

- 1) Obtain and analyze the routing table for **Router5** in the project before and after applying **BGP**.
- 2) Analyze the graphs that show the throughput in both **Router2-Router3** link and **Router2-Router4** link. Explain the effect of applying the routing policy on these throughputs.
- 3) Create another scenario as a duplicate of the BGP\_Simple scenario. Name the new scenario BGP\_OSPF\_RIP. In this new scenario change the intra-domain routing protocol in AS 56 to be OSPF instead of RIP. Run the new scenario and check the contents of Router5's routing table. Analyze the content of this table.

# 8.7. Lab Report

Prepare a report that follows the guidelines explained in Lab 0. The report should include the answers to the above exercises as well as the graphs you generated from the simulation scenarios. Discuss the results you obtained and compare these results with your expectations. Mention any anomalies or unexplained behaviors.

# 9. Laboratory - TCP: Transmission Control Protocol (A Reliable, Connection-Oriented, Byte-Stream Service)

# 9.1. Objective

This lab is designed to demonstrate the congestion control algorithms implemented by the Transmission Control Protocol (TCP). The lab provides a number of scenarios to simulate these algorithms. You will compare the performance of the algorithms through the analysis of the simulation results.

### 9.2. Overview

The Internet's TCP guarantees the reliable, in-order delivery of a stream of bytes. It includes a flow-control mechanism for the byte streams that allows the receiver to limit how much data the sender can transmit at a given time. In addition, TCP implements a highly tuned congestion-control mechanism. The idea of this mechanism is to throttle how fast TCP sends data to keep the sender from overloading the network

The idea of TCP congestion control is for each source to determine how much capacity is available in the network, so that it knows how many packets it can safely have in transit. It maintains a state variable for each connection, called the *congestion window*, which is used by the source to limit how much data the source is allowed to have in transit at a given time. TCP uses a mechanism, called *additive increase/multiplicative decrease*, that decreases the congestion window when the level of congestion goes up and increases the congestion window when the level of congestion goes down. TCP interprets timeouts as a sign of congestion. Each time a timeout occurs, the source sets the congestion window to half of its previous value. This halving corresponds to the *multiplicative decrease* part of the mechanism. The congestion window is not allowed to fall below the size of a single packet (the TCP maximum segment size, or MSS). Every time the source successfully sends a congestion window; this is the *additive increase* part of the mechanism.

TCP uses a mechanism called *slow start* to increase the congestion window "rapidly" from a cold start in TCP connections. It increases the congestion window exponentially, rather than linearly. Finally, TCP utilizes a mechanism called *fast retransmit and fast recovery*. Fast retransmit is a heuristic that sometimes triggers the retransmission of a dropped packet sooner than the regular timeout mechanism

In this lab you will set up a network that utilizes TCP as its end-to-end transmission protocol and analyze the size of the congestion window with different mechanisms.

## 9.3. Prelab Activities

 Read sections 5.1 and 5.2 from "Computer Networks: A Systems Approach", 4th Edition.

Go to *www.net-seal.net/animations.php* and play the following animations:

- <u>TCP Connections</u>.
- <u>TCP Multiplexing</u>.
- <u>TCP Buffering and Sequencing</u>.
- User Datagram Protocol (UDP).

# 9.4. Procedure

## 9.4.1. Create a New Project

- 1. Start OPNET IT Guru Academic Edition  $\Rightarrow$  Choose New from the File menu.
- 2. Select Project and Click OK ⇒ Name the project **<your initials>**\_TCP, and the scenario No\_Drop ⇒ Click OK.
- In the Startup Wizard: Initial Topology dialog box, make sure that Create Empty Scenario is selected ⇒ Click Next - ⇒ Select Choose From Maps from the Network Scale list ⇒ Click Next ⇒ Choose USA from the Map List ⇒ Click Next twice ⇒ Click OK.

## 9.4.2. Create and Configure the Network

- 9.4.2.1. Initialize the Network:
  - 1. The *Object Palette* dialog box should now be on the top of your project space. If it is not there, open it by clicking . Make sure that the internet\_toolbox item is selected from the pull-down menu on the object palette.
  - 2. Add to the project workspace the following objects from the palette: Application Config, Profile Config, an ip32\_Cloud, and two subnets.
    - a. To add an object from a palette, click its icon in the object palette  $\Rightarrow$  Move your mouse to the workspace  $\Rightarrow$  Click to drop the object in the desired location  $\Rightarrow$  Right-click to finish creating objects of that type.
  - 3. Close the palette.
  - 4. Rename the objects you added as shown and then save your project:



The **ip32\_cloud** node model represents an IP cloud supporting up to 32 serial line interfaces at a selectable data rate through which IP traffic can be modeled. IP packets arriving on any cloud interface are routed to the appropriate output interface based on their destination IP address. The RIP or OSFP protocol may be used to automatically and dynamically create the cloud's routing tables and select routes in an adaptive manner. This cloud requests a fixed amount of time to route each packet, as determined by the **Packet Latency** attribute of the node.

#### 9.4.2.2. Configure the Applications:

- Right-click on the Applications node ⇒ Edit Attributes ⇒ Expand the Application Definitions attribute and set rows to 1 ⇒ Expand the new row ⇒ Name the row FTP\_Application.
  - i. Expand the **Description** hierarchy. ⇒ Edit the **FTP** row as shown (you will need to set the **Special Value** to **Not Used** while editing the shown attributes):

👪 (Ftp) Table		🟽 "Inter-Request Time" Specification 🔀		
Attribute	Value			
Command Mix (Get/Total)	100%	Distribution Name:> constant		
Inter-Request Time (secon File Size (bytes)	constant (3600)	Mean Outcome: -> 3600		
Symbolic Server Name	FTP Server	Second Argument: Not Used		
Type of Service	Best Effort (0)			
RSVP Parameters	None	Special Value: ->> Not Used 🗾		
Back-End Custom Applicati	Not Used			
<u>D</u> etails <u>P</u> romot	е <u>О</u> К	Help Cancel OK		

2. Click OK twice and then save your project.

## 9.4.2.3. Configure the Profiles:

- 1. Right-click on the Profiles node  $\Rightarrow$  **Edit** Attributes  $\Rightarrow$  Expand the Profile Configuration attribute and set rows to 1.
  - i. Name and set the attributes of **row 0** as shown  $\Rightarrow$  Click **OK**.

(Profiles) Attributes	
Type: Utilities	
Attribute	Value
⑦ ⊢ name	Profiles
⑦ ⊢model	Profile Config
⑦	()
⑦ ⊢rows	1
⑦ - Profile Name	FTP_Profile
⑦ / □ Applications	()
⑦ ⊢rows	1
⊡ row 0	
	FTP_Application
O +Start Time Offset	. constant (5)
Duration (second	. End of Profile
⑦	Once at Start Time
⑦ ├ Operation Mode	Serial (Ordered)
③ Start Time (seconds)	constant (100)
② Fouration (seconds)	End of Simulation
⑦	Once at Start Time
Apply Changes to Selected O	hjects Advanced
Eind Next	<u>C</u> ancel <u>O</u> K

network simulation experiments manual.doc

- 9.4.2.4. Configure the West Subnet:
  - 1. Double-click on the West subnet node. You get an empty workspace, indicating that the subnet contains no objects.
  - 2. Open the object palette and make sure that the internet\_toolbox item is selected from the pull-down menu.
  - Add the following items to the subnet workspace: one ethernet\_server, one ethernet4\_slip8\_gtwy router, and connect them with a bidirectional 100\_BaseT link ⇒ Close the palette ⇒ Rename the objects as shown.



The **ethernet4\_slip8\_gtwy** mode model represents an IP-based gateway supporting four Ethernet hub interfaces and eight serial line interfaces.

- 1. Right-click on the Server\_West node  $\Rightarrow$  Edit Attributes:
  - i. Edit Application: Supported Services  $\Rightarrow$  Set rows to  $1 \Rightarrow$  Set Name to FTPApplication  $\Rightarrow$  Click OK.
  - ii. Edit the value of the Server Address attribute and write down Server\_West.
  - iii. Expand the TCP Parameters hierarchy  $\Rightarrow$  Set both Fast Retransmit and Fast Recovery to Disabled.
- 2. Click OK and then save your project.

Now, you have completed the configuration of the **West** subnet. To go back to the top level of the project, click the **Go to next higher level** button.

- 9.4.2.5. Configure the East Subnet:
  - 1. Double-click on the East subnet node. You get an empty workspace, indicating that the subnet contains no objects.
  - 2. Open the object palette and make sure that the internet\_toolbox item is selected from the pull-down menu.
  - 3. Add the following items to the subnet workspace: one ethernet\_wkstn, one ethernet4\_slip8\_gtwy router, and connect them with a bidirectional 100\_BaseT link ⇒ Close the palette ⇒ Rename the objects as shown.



- 4. Right-click on the Client\_East node  $\Rightarrow$  **Edit** Attributes:
  - i. Expand the Application: Supported Profiles hierarchy  $\Rightarrow$  Set rows to 1  $\Rightarrow$  Expand the row 0 hierarchy  $\Rightarrow$  Set Profile Name to FTP\_Profile.
  - ii. Assign Client\_ East to the Client Address attributes.

iii. Edit the Application: Destination Preferences attribute as follows:

Set rows to  $1 \Rightarrow$  Set Symbolic Name to FTP Server  $\Rightarrow$  Edit Actual Name  $\Rightarrow$  Set rows to  $1 \Rightarrow$  In the new row, assign Server\_West to the Name column.

- 5. Click OK three times and then save your project.
- 6. You have now completed the configuration of the East subnet. To go back to the project space, click the **Go to next higher level** button.
- 9.4.2.6. Connect the Subnets to the IP Cloud:
  - 1. Open the object palette
  - 2. Using two PPP\_DS3 bidirectional links connect the East subnet to the IP Cloud and the West subnet to the IP Cloud.
  - 3. A pop-up dialog box will appear asking you what to connect the subnet to the IP Cloud with. Make sure to select the "routers."



4. Close the palette.

#### 9.4.3. Choose the Statistics

- 1. Right-click on **Server\_West** in the **West** subnet and select **Choose Individual Statistics** from the pop-up menu.
- 2. In the **Choose Results** dialog box, choose the following statistic:
- 3. TCP Connection  $\Rightarrow$  Congestion Window Size (bytes) and Sent Segment Sequence Number.
- Right-click on the Congestion Window Size (bytes) statistic ⇒ Choose Change Collection Mode ⇒ In the dialog box check Advanced ⇒ From the drop-down menu assign all values to Capture mode as shown ⇒ Click OK.

🛠 Congestion Window Si			
Capture mode	all values		
€Every	seconds		
CEvery	values		
C <u>T</u> otal of	values		
Bucket mode	max value		
<b>I</b> <u>R</u> eset			
Advanced			
	<u>C</u> ancel <u>OK</u>		

OPNET provides the following capture modes:

- All values collects every data point from a statistic.
- **Sample** collects the data according to a user specified time interval or sample count. For example, if the time interval is 10, data is sampled and recorded every 10<sup>th</sup> second. If the sample count is 10, every 10<sup>th</sup> data points is recorded. All other data points are discarded.
- **Bucket** collects all of the points over the time interval or sample count into a "data busket" and generates a result from each bucket. This is the default mode.
  - 5. Right-click on the Sent Segment Sequence Number statistic ⇒ Choose Change Collection Mode ⇒ In the dialog box check Advanced ⇒ From the drop-down menu, assign all values to Capture mode.
  - 6. Click OK twice and then save your project.
  - 7. Click the Go to next higher level 😻 button.

#### 9.4.4. Configure the Simulation

Here we need to configure the duration of the simulation:

- 1. Click on and the Configure Simulation window should appear.
- 2. Set the duration to be 10.0 minutes.
- 3. Click OK and then save your project.

#### 9.4.5. Duplicate the Scenario

In the network we just created we assumed a perfect network with no discarded packets. Also, we disabled the fast retransmit and fast recovery techniques in TCP. To analyze the effects of discarded packets and those congestion-control techniques, we will create two additional scenarios.

- 1. Select **Duplicate Scenario** from the **Scenarios** menu and give it the name **Drop\_NoFast** ⇒ Click **OK**.
- 2. In the new scenario, right-click on the IP Cloud  $\Rightarrow$  Edit Attributes  $\Rightarrow$  Assign 0.05% to the Packet Discard Ratio attribute.
- 3. Click **OK** and then save your project.
- 4. While you are still in the **Drop\_NoFast** scenario, select **Duplicate Scenario** from the **Scenarios** menu and give it the name **Drop\_Fast**.

- 5. In the Drop\_Fast scenario, right-click on Server\_West, which is inside the West subnet ⇒ Edit Attributes ⇒ Expand the TCP Parameters hierarchy ⇒ Enable the Fast Retransmit attribute ⇒ Assign Reno to the Fast Recovery attribute.
- 6. Click **OK** and then save your project.

With **fast transmit**, TCP performs a retransmission of what appears to be the missing segment for a retransmission timer to expire. After fast retransmit sends what appears to be the missing segment, congestion advance but not slow start is performed. This is the **fast recovery** algorithm. The fast retransmit and fast recovery algorithms are usually implemented together (RFC 2001).

### 9.4.6. Run the Simulation

To run the simulation for the three scenarios simultaneously:

- 1. Go to the Scenarios menu  $\Rightarrow$  Select Manage Scenarios.
- 2. Change the values under the **Results** column to **<collect>** (or **<recollect>**) for the three scenarios. Compare to the following figure.

<b>*</b> M	* Manage Scenarios						
Pro	Project Name: eha TCP						
#	Scenario Name	Saved	Results	Sim Duration	Time Units		
1	NO_Drop	saved	<collect></collect>	10	minute(s)		
2	Drop_NoFast	saved	<collect></collect>	10	minute(s)		
3	Drop_Fast	saved	<collect></collect>	10	minute(s)		
						•	
	Delete         Discard Results         Cancel         OK						

- 3. Click **OK** to run the three simulations. Depending on the speed of your processor, this may take several minutes to complete.
- 4. After the three simulation runs complete, one for each scenario, click  $Close \Rightarrow$  Save your project.

## 9.4.7. View the Results

To view and analyze the results.

- 1. Switch to the **Drop\_NoFast** scenario (the second one) and choose **View Results** from the **Results** menu.
- 2. Fully expand the **Object Statistics** hierarchy and select the following two results: **Congestion Window Size (bytes)** and **Sent Segment Sequence Number**.

To switch to a scenario, choose Switch to Scenario from the Scenarios menu or just press Ctrl+<scenario number>

View Results			
Discrete Event Graphs Displayed Panel Graphs			
Global Statistics	Show Preview		
Diject Statistics			
En West	40,000,000		
Congestion Window Size (byte	U	400	time (sec)
Jent Segment Sequence Num	Stacked Statistics	This Scena	ario 💌
<b>↓</b>	As Is		-
Results Generated: 00:37:21 Mar 20 2003	Unselect	Add	Show
			<u>C</u> lose

3. Click **Show**. The resulting graphs should resemble the ones below.



- 4. To zoom in on the details in the graph, click and drag your mouse to draw a rectangle, as shown above.
- 5. The graph should be redrawn to resemble the following one:



- 6. Notice the **Segment Sequence Number** is almost flat with every drop in the congestion window.
- 7. Close the View Results dialog box and select **Compare Results** from the **Result** menu.
- 8. Fully expand the **Object Statistics** hierarchy as shown and select the following result: **Sent Segment Sequence Number**.

Tompare Results	
Discrete Event Graphs Displayed Panel Graphs  Global Statistics  Choose From Maps Network  West  Server_West  Congestion Window Size (bytes)  Sent Segment Sequence Number  Overlaid Statistics  All Scenarios  As Is  Results Generated: 00:37:21 Mar 20 2003 Unselect  Add	800 time (sec)
	<u>C</u> lose

9. Click **Show**. After zooming in, the resulting graph should resemble the one below.



# 9.5. Further readings

- OPNET <u>TCP Model Description</u>: From the **Protocols** menu, select **TCP** ⇒ <u>Model</u> <u>Usage Guide</u>.
- Transmission Control Protocol: <u>IETF RFC number 793</u> (www.ietf.org/rfc.html).

# 9.6. Exercises

- 1) Why does the **Segment Sequence Number** remain unchanged (indicated by a horizontal line in the graphs) with every drop in the congestion window?
- 2) Analyze the graph that compares the Segment Sequence numbers of the three scenarios. Why does the Drop\_NoFast scenario have the slowest growth in sequence numbers?
- In the Drop\_NoFast scenario, obtain the overlaid graph that compares Sent Segment Sequence Number with Received Segment ACK Number for Server\_West. Explain the graph.

#### Hint:

Make sure to assign **all values** to the **Capture mode** of the **Received Segment ACK Number** statistic.

4) Create another scenario as a duplicate of the Drop\_Fast scenario. Name the new scenario Q4\_Drop\_Fast\_Buffer. In the new scenario, edit the attributes of the Client\_East node and assign 65535 to its Receiver Buffer (bytes) attribute (one of the TCP Parameters). Generate a graph that shows how the Congestion Window Size (bytes) of Server\_West gets affected by the increase in the receiver buffer (compare the congestion window size graph from the Drop\_Fast

scenario with the corresponding graph from the Q4\_Drop\_Fast\_Buffer scenario.)

# 9.7. Lab Report

Prepare a report that follows the guidelines explained in Lab 0. The report should include the answers to the above exercises as well as the graphs you generated from the simulation scenarios. Discuss the results you obtained and compare these results with your expectations. Mention any anomalies or unexplained behaviors.

# 10. Laboratory - Queuing Disciplines (Order of Packet Transmission and Dropping)

## 10.1. *Objective*

The objective of this lab is to examine the effect of different queuing disciplines on packet delivery and delay for different services.

## 10.2. Overview

As part of the resource allocation mechanisms, each router must implement some queuing discipline that governs how packets are buffered while waiting to be transmitted. Various queuing disciplines can be used to control which packets get transmitted (bandwidth allocation) and which packets get dropped (buffer space). The queuing discipline also affects the latency experienced by a packet, by determining how long a packet waits to be transmitted. Examples of the common queuing disciplines are first-in-first-out (FIFO) queuing, priority queuing (PQ), and weighted-fair queuing (WFQ).

The idea of FIFO queuing is that the first packet that arrives at a router is the first packet to be transmitted. Given that the amount of buffer space at each router is finite, if a packet arrives and the queue (buffer space) is full, then the router discards (drops) that packet. This is done without regard to which flow the packet belongs to or how important the packet is.

**PQ** is a simple variation of the basic FIFO queuing. The idea is to mark each packet with a priority; the mark could be carried, for example, in the IP Type of Service (ToS) field. The routers then implement multiple FIFO queues, one for each priority class. Within each priority, packets are still managed in a FIFO manner. This queuing discipline allows high-priority packets to cut to the front of the line.

The idea of the fair queuing (FQ) discipline is to maintain a separate queue for each flow currently being handled by the router. The router then services these queues in a round-robin manner. WFQ allows a weight to be assigned to each flow (queue). This weight effectively controls the percentage of the link's bandwidth each flow will get. We could use ToS bits in the IP header to identify that weight.

In this lab you will set up a network that carries three applications: FTP, Video, and VoIP. You will study how the choice of the queuing discipline in the routers can affect the performance of the applications and the utilization of the network resources.

# 10.3. *Prelab Activities*

• Read section 6.2 from "Computer Networks: A Systems Approach", 4th Edition.

Go to *www.net-seal.net/animations.php* and play the following animations:

- Switch Congestion.
- <u>IP Fragmentation</u>.
- 10.4. *Procedure*

# 10.4.1. Create a New Project

1. Start **OPNET IT Guru Academic Edition**  $\Rightarrow$  Choose **New** from the **File** menu.

- 2. Select **Project** and Click **OK** ⇒ Name the project **<your initials>\_Queues**, and the scenario **FIFO** ⇒ Click **OK**.
- 3. In the *Startup Wizard: Initial Topology* dialog box, make sure that **Create Empty Scenario** is selected ⇒ Click **Next** ⇒ Select **Campus** from the *Network Scale* list ⇒ Click **Next** three times ⇒ Click **OK**.

# 10.4.2. Create and Configure the Network

- 10.4.2.1. Initialize the Network:
  - 1. The *Object Palette* dialog box should be now on the top of your project space. If it is not there, open it by clicking . Make sure that the **internet\_toolbox** item is selected from the pull-down menu on the object palette.
  - 2. Add to the project workspace the following objects from the palette: Application Config, Profile Config, QoS Attribute Config, five ethernet\_wkstn, one ethernet\_server, and two ethernet4\_slip8\_gtwy routers.
  - 3. Connect both routers together with a bidirectional **PPP\_DS1** link.
  - 4. Connect the workstations and the server to the routers using bidirectional **10Base\_T** links as shown.
  - 5. Rename the objects you added as shown and then save your project.



The **QoS Attribute Config** node defines attribute configuration details for protocols supported at the IP layer. These specifications can be referenced by the individual nodes using symbolic names. It defines different queuing profiles such as FIFO, WFQ, priority queuing, custom queuing, MWRR, MDRR, and DWRR.

# 10.4.2.2. Configure the Applications:

- 1. Right-click on the Applications node ⇒ Edit Attributes ⇒ Expand the Application Definitions hierarchy ⇒ Set rows to 3 ⇒ Name the rows: FTP Application, Video Application, and VoIP Application.
  - i. Go to the FTP Application row ⇒ Expand the Description hierarchy ⇒ Assign High Load to Ftp ⇒ Click on the High Load value and choose Edit from the drop-down menu ⇒ Assign Constant(10) to Inter-Request Time ⇒ Assign Constant(1000000) to File Size. Keep the Type of Service (ToS) as Best Effort (0).

- ii. Go to the Video Application row ⇒ Expand the Description hierarchy ⇒ Assign Low Resolution Video to Video Conferencing ⇒ Click on the Low Resolution Video value and choose Edit ⇒ Edit the value of the Type of Service field (the Configure TOS/DSCP window appears) ⇒ From the drop-down menu, assign Streaming Multimedia (4) to ToS ⇒ Click OK twice.
- iii. Go to the VoIP Application row  $\Rightarrow$  Expand the **Description** hierarchy  $\Rightarrow$  Assign **PCM Quality Speech** to Voice. If you edit it, you can see that the ToS assigned to it is **Interactive Voice (6)**.
- 2. Click OK and then save your project.

🖁 (Applications) Attributes				
Type: Utilities				
Attribute	Value			
⑦ ⊢ name	Applications			
⑦ ⊢model	Application Config			
⑦	None			
②	()			
⑦ ⊢rows	3			
⊞ row 0	FTP Application,()			
⊞røw 1	Video Application,()			
Frow 2				
⑦ / ⊢Name	VoIP Application			
⑦	()			
⑦ ⊢Custom	Off			
⑦ + Database	Off			
⑦ ⊢Email	Off			
⑦ ⊢Ftp	Off			
⑦ ⊢Http	Off			
Print	Off			
PRemote Login	Off			
Video Conferencing	Off			
③ LVoice	PCM Quality Speech			
⑦ ⊞ Voice Encoder Schemes	All Schemes			
Apply Changes to Selected Objects				
Eind Next	<u>Cancel</u> <u>O</u> K			

**Type of Service** (ToS) is assigned to the IP packets. It represents a session attribute that allows packets to be provided the appropriate service in the IP queues.

Best-effort delivery means that delivery of a packet is attempted but is not guaranteed.

PCM (Pulse Code Modulation) is a procedure used to digitize speech before transmitting it over the network.

#### 10.4.2.3. Configure the Profiles:

- 1. Right-click on the **Profiles** node  $\Rightarrow$  **Edit** Attributes  $\Rightarrow$  Expand the **Profile Configuration** hierarchy  $\Rightarrow$  Set rows to 3.
  - i. Name and set the attributes of row 0 as shown:

署 (Profiles) Attributes				
Type: Utilities				
Attribute	Value			
⑦ ⊢name	Profiles			
⑦ ⊢model	Profile Config			
⑦	()			
⑦ ⊢rows	3			
⊡ row Ø				
Profile Name	FTP Profile			
②	()			
⑦ / ⊢rows	1			
⊡ row 0				
⑦ ⊢Name	FTP Application			
③ Start Time Offset	. constant (5)			
Duration (second	. End of Profile			
⑦	Once at Start Time			
Operation Mode	Simultaneous			
③ Start Time (seconds)	constant (100)			
③ PQuration (seconds)	End of Simulation			
⑦	Once at Start Time			
Apply Changes to Selected Objects				
Eind Next	<u>C</u> ancel <u>O</u> K			

ii. Name and set the attributes of row 1 as shown:

*	🗄 (Profiles) Attributes			
Ту	pe: Utilities			
	Attribute	Value		
	⊡row 1			
?	Profile Name	Video Profile		
?	Applications	()		
?	Frows	1		
	⊡ row 0			
?	Name	Video Application		
?	Start Time Offset	constant (5)		
?	Duration (second	End of Profile		
?		Once at Start Time		
?	-Operation Mode	Simultaneous		
?	⊢Start Time (seconds)	constant (100)		
?	⊢Duration (seconds)	End of Simulation		
?		Once at Start Time	-	
	Apply Changes to Selected Ol	ojects A	<u>d</u> vanced	
	<u>F</u> ind Next	<u>C</u> ancel <u>C</u>	<u>v</u> K	

iii. Name and set the attributes of row 2 as shown:

₩	🔀 (Profiles) Attributes				
ту	rpe: Utilities				
	Attribute	Value			
	🗆 row 2				
?	Profile Name	VoIP Profile			
?	□ Applications	()			
?	⊳ ⊢rows	1			
	⊡ row 0				
2	Name	VoIP Application			
?	Start Time Offset.	constant (5)			
?	Duration (second.	End of Profile			
2		Once at Start Time			
?	⊢Operation Mode	Simultaneous			
?	Start Time (seconds)	constant (100)			
2	Duration (seconds)	End of Simulation			
?		Once at Start Time			
Γ	Apply Changes to Selected O	bjects A <u>d</u> vanced			
	Eind Next	<u>Cancel</u> <u>O</u> K			

- 2. Click OK and then save your project.
- 10.4.2.4. Configure the Queues:

We will keep the default queuing profiles that are defined in our **Queues** object. It is recommended that you check out the configuration of the FIFO, PQ, and WFQ profiles.

- 10.4.2.5. Configure the Workstations and Servers:
  - Right-click on the FTP Client ⇒ Edit Attributes ⇒ Expand the Application: Supported Profiles hierarchy ⇒ Set rows to 1 ⇒ Set Profile Name to FTP Profile ⇒ Click OK.
  - Right-click on the Video Client ⇒ Edit Attributes ⇒ Expand the Application: Supported Profiles hierarchy ⇒ Set rows to 1 ⇒ Set Profile Name to Video Profile ⇒ Click OK.
  - 3. Right-click on the VoIP West  $\Rightarrow$  Edit Attributes.
    - i. Expand the Application: Supported Profiles hierarchy  $\Rightarrow$  Set rows to  $1 \Rightarrow$  Set Profile Name to VoIP Profile.
    - ii. Edit the Application: Supported Services value  $\Rightarrow$  Set rows to 1  $\Rightarrow$  Set Service Name to VoIP Application  $\Rightarrow$  Click OK twice.
  - 4. Right-click on the VoIP East  $\Rightarrow$  Edit Attributes.
    - i. Expand the Application: Supported Profiles hierarchy  $\Rightarrow$  Set rows to  $1 \Rightarrow$  Set Profile Name to VoIP Profile.
    - ii. Edit the Application: Supported Services value  $\Rightarrow$  Set rows to 1  $\Rightarrow$  Set Service Name to VoIP Application  $\Rightarrow$  Click OK twice.
  - Right-click on the FTP Server ⇒ Edit Attributes ⇒ Edit the Application: Supported Services value ⇒ Set rows to 1 ⇒ Set Service Name to FTP Application ⇒ Click OK twice.

- 6. Right-click on the Video Server ⇒ Edit Attributes ⇒ Edit the Application: Supported Services value ⇒ Set rows to 1 ⇒ Set Service Name to Video ⇒ Click OK twice.
- 7. Save your project.
- 10.4.2.6. Configure the Routers:
  - 1. Click on the link connecting the **East** and **West** routers to select it.  $\Rightarrow$  From the **Protocols** menu choose IP  $\rightarrow$  QoS  $\rightarrow$  Configure QoS.
  - 2. Make sure the selected items are as shown in the following *QoS Configuration* dialog box  $\Rightarrow$  Click **OK**.

🛠 QoS Configuration 📃 🗖 🔀					
This operation will overwrite the existing QoS configuration on IP interfaces.					
QoS Scheme:	FIFO				
QoS Profile:	FIFO Profile				
Apply the above selection to subinterfaces					
Apply the above selection to: CAll connected interfaces Interfaces across selected link(s) CInterfaces on selected router(s)					
Visualize QoS Configuration					
	<u>C</u> ancel <u>O</u> K				

*Note:* Since the **Visualize QoS Configuration** radio button is checked, the link is colored based on the QoS scheme used (blue for FIFO).

3. Save your project.

# 10.4.3. Choose the Statistics

To test the performance of the applications defined in the network, we will collect some of the available statistics as follows:

- 1. Right-click anywhere in the project workspace and select **Choose Individual Statistics** from the pop-up menu.
- 2. In the *Choose Results* dialog box, select the following global statistics:



3. Click **OK** and then save your project.

**Traffic Dropped**. The number of IP diagrams dropped by all nodes in the network across all IP interfaces. The reason for dropping an IP datagram can be any one of the following:

- Insufficient space in the queue
- Maximum number of bops exceeded by an IP datagram.
- On nonrouting nodes, a local router interface was not found to be used as the next hop.
- On routing nodes, the route table lookup failed to yield a route to the destination.

#### 10.4.4. Configure the Simulation

Here we need to configure the duration of the simulation.

- 1. Click on and the *Configure Simulation* window should appear.
- 2. Set the duration to be **150 seconds**.

3. Click **OK** and then save your project.

#### 10.4.5. Duplicate the Scenario

In the network we just created, we used the FIFO queuing discipline in the routers. To analyze the effect of different queuing disciplines, we will create two more scenarios to test the **PQ** and **WFQ** disciplines.

- A. Select **Duplicate Scenario** from the **Scenarios** menu and give it the name  $PQ \Rightarrow$  Click OK.
  - 1. Click on the link connecting the East and West routers to select it ⇒ From the Protocols menu choose IP → QoS → Configure QoS.
  - 2. Make sure the selected items are as shown in the following *QoS Configuration* dialog box  $\Rightarrow$  Click **OK**.

🔣 QoS Configu	iration 📃 🗖 🔀				
This operation will overwrite the existing QoS configuration on IP interfaces.					
QoS Scheme:	Priority Queuing				
QoS Profile:	ToS Based				
Apply the above selection to subinterfaces					
Apply the above selection to: Call connected interfaces (Call connected interfaces)					
CInterfaces on selected router(s)					
Visualize QoS Configuration					
<u>_</u>	2ancel <u>O</u> K				

*Note:* Since the Visualize QoS Configuration radio button is checked, the link is colored based on the QoS scheme used (orange for priority queuing).

- 3. Save your project.
- B. Select **Duplicate Scenario** from the **Scenarios** menu and give it the name  $WFQ \Rightarrow Click OK$ .
  - 1. Click on the link connecting the **East** and **West** routers to select it  $\Rightarrow$  From the **Protocols** menu choose IP  $\rightarrow$  QoS  $\rightarrow$  Configure QoS.
  - 2. Make sure the selected items are as shown in the following *QoS Configuration* dialog box  $\Rightarrow$  Click **OK**.

QoS Configuration     QoS Configuration     This operation will overwrite the existing     QoS configuration on IP interfaces.					
QoS Scheme:	WFQ				
QoS Profile:	ToS Based				
Apply the above selection to subinterfaces					
Apply the above selection to: Call connected interfaces Interfaces across selected link(s) Interfaces on selected router(s)					
Visualize QoS Configuration					
<u>C</u>	ancel <u>O</u> K				

*Note.* Since the Visualize QoS Configuration radio button is checked the link is colored based on the QoS scheme used (green for WFQ).

3. Save your project.

#### 10.4.6. Run the Simulation

To run the simulation for the three scenarios simultaneously:

- 1. Go to the Scenarios menu  $\Rightarrow$  Select Manage Scenarios.
- 2. Change the values under the **Results** column to <**collect**> (or <**recollect**>) for the three scenarios. Compare to the following figure.

🗶 M	anage Scenarios					×		
Project Name: eha Queues								
#	Scenario Name	Saved	Results	Sim Duration	Time Units			
1	FIFO	saved	<collect></collect>	150	second(s)			
2	PQ	saved	<collect></collect>	150	second(s)			
3	WFQ	saved	<collect></collect>	150	second(s)			
						-		
D	elete Discard <u>R</u> es	ults <u>C</u> ol	lect Results		C <u>a</u> ncel <u>O</u> K			

- 3. Click **OK** to run the three simulations. Depending on the speed of your processor, this may take several minutes to complete.
- 4. After the simulation completes the three runs, one for each scenario, click **Close**.
- 5. Save your project.

*Note:* Actual results will vary slightly based on the actual node positioning in the project.

## 10.4.7. View the Results

To view and analyze the results:

- 1. Select **Compare Results** from the **Results** menu.
- 2. Select the IP **Traffic Dropped** statistic and click **Show.** The resulting graph should resemble the one below. *Note:* The shown graph is the result of zooming into the region of interest on the original graph.



3. Create the graph for Video Conferencing Traffic Received:



4. Create the graph for Voice Traffic Received:



5. Create graphs for Voice Packet End-to-end Delay and Voice Packet Delay Variation (Note: the trace for WFQ is not shown on the following graphs because it is overlapped by the trace of PQ.)



# 10.5. Further readings

• The Differentiated Services Field: IETF RFC number 2474 (www.ietf.org/rfc.html).

# 10.6. Exercises

1) Analyze the graphs we obtained and verify the overlap of the Voice Packet End-to-end Delay and Voice Packet Delay Variation graphs. Compare the three queuing disciplines and explain their effect on the performance of the three applications.

- 2) In the implemented project, edit the **Queues** object and check the profiles assigned to the **FIFO**, **PQ**, and **WFQ** disciplines. For each profile answer the following questions:
  - a. How many queues are associated with each discipline?
  - b. In this lab, we used **ToS** to identify the priority and weight for the **PQ** and **WFQ** disciplines respectively. What are the other parameters that can be used to identify the priority and weight?
  - c. In PQ, how are queues configured to serve different ToS values?
  - d. In WFQ, how are queues configured to serve different ToS values?
- 3) For all scenarios, choose the "queuing delay ←" statistic for the link that connects East Router and West Router. Rerun the simulation and generate the graph that compares that queuing delay for all queuing disciplines (scenarios). Analyze this graph.

Hint:

#### 10.7. Lab Report

Prepare a report that follows the guidelines explained in Lab 0. The report should include the answers to the above exercises as well as the graphs you generated from the simulation scenarios. Discuss the results you obtained and compare these results with your expectations. Mention any anomalies or unexplained behaviors.

# 11. Laboratory - RSVP: Resource Reservation Protocol (Providing QoS by Reserving Resources in the Network)

## 11.1. Objective

The objective of this lab is to study the Resource Reservation Protocol (RSVP) as a part of the Integrated Services approach to providing Quality of Service (QoS) to individual applications or flows.

## 11.2. Overview

For many years, packet-switched networks have offered the promise of supporting multimedia applications, that is, those that combine audio, video, and data. Audio and video applications are examples of *real-time* applications. In the best-effort model, the network tries to deliver your data but makes no promises and leaves the "cleanup operation" to the edges. This model is not sufficient for real-time applications. What we need is a new service model - one in which applications that need better assurances can request such service from the network. The network may then respond by providing an assurance that it will do better or perhaps by saying that it cannot promise anything better at the moment. A network that can provide different levels of service is often said to support QoS.

Two approaches have been developed to provide a range of QoS: Integrated Services and Differentiated Services. The Resource Reservation Protocol follows the Integrated Services approach, whereby QoS is provided to individual applications or flows. The Differentiated Services approach provides QoS to large classes of data or aggregated traffic.

While connection-oriented networks have always needed some sort of setup protocol to establish the necessary virtual circuit state in the routers, connectionless networks like the Internet have had no such protocols. One of the key assumptions underlying RSVP is that it should not detract from the robustness that we find in the Internet. Therefore, RSVP uses the idea of *soft state* in the routers. Soft state - in contrast to the *hard state* found in connection-oriented networks–does not need to be explicitly deleted when it is no longer needed instead, it times out after some fairly short period if it is not periodically refreshed. RSVP adopts the *receiver-oriented* approach - the receivers keep track of their own resource requirements, and they periodically send refresh messages to keep the soft state in place.

In this tab you will set up a network that carries real-time applications and that utilizes RSVP to provide QoS to one of these applications. You will study how RSVP contributes to the performance of the application that makes use of it.

# 11.3. *Prelab Activities*

• Read section 6.5 from "Computer Networks: A Systems Approach", 4th Edition.

Go to *www.net-seal.net/animations.php* and play the following animation:

<u>TCP Flow Control</u>.

# 11.4. *Procedure*

## 11.4.1. Create the Project

1. Start **OPNET IT Guru Academic Edition**  $\Rightarrow$  Choose **Open** from the **File** menu.
- 2. Select the project you created in Lab 9: **<your initials>\_Queues**  $\Rightarrow$  Click **OK**.
- 3. From the File menu, choose Save As  $\Rightarrow$  Rename the project to <your initiate>\_RSVP  $\Rightarrow$  Click OK.
- 4. From the Scenarios menu, choose Manage Scenarios ⇒ Click on FIFO ⇒ Click Delete ⇒ Click on PQ ⇒ Click Delete.

🛣 Ma	🚼 Manage Scenarios							
Proj	ect Name: eha RSVF	2						
#	Scenario Name	Saved	Results	Sim Duration	Time Units			
1	FIFO 🔶	saved	out of date	150	second(s)			
2	PQ 🔶	saved	out of date	150	second(s)			
3	WFQ	saved	up to date	150	second(s)			
	K					•		
<u>D</u>	Delete Discard Results Collect Results Cancel OK							

- 5. Click on WFQ and rename it to  $QoS_RSVP \Rightarrow Click OK$ .
- 6. Make sure that you have only the **QoS\_RSVP** scenario in your project. The following figure shows one way to check for the available scenarios in the project.

🗶 P	roject:	eha_R	SVP Scenar	io: QoS_RS	VP [Sub	onet: top.	Can	npus Netw	ork]		
File	Edit	View	Scenarios	Topology	Traffic	Protocols	s S	imulation	Results	Windows	Help
Application		New Sce Duplicat Manage	enario e Scenario Scenarios	Ctrl+ . Ctrl+	Shift+N Shift+D					A	
		Previous Next Sce	Scenario enario	Ctrl+ Ctrl+	Up Down						
		DEFINITION	Switch T	o Scenario			•	QoS_RSV	P Ctrl+1		
	Application		Scenario	Componen	ts	I					

7. Save your project.

The idea of the **FQ** (fair queuing) discipline is to maintain a separate queue for each flow currently being handled by the router. The router then service these queue in a round robin manner.

**WFQ** allows a weight to be assigned to each flow (queue). This weight effectively controls the percentage of the link's bandwidth each flow will get. We could use the ToS (Type of Service) field in the IP header to identify that weight.

# 11.4.2. Configure the Network

#### 11.4.2.1. Add More VoIP Nodes:

In this project we will set up the two VoIP nodes so that one will always be the *Caller* party and the other will be the *Called* party. In addition, we will add two new VoIP *Caller* and *Called* nodes. These new nodes will utilize RSVP to reserve their required resources through the network.

- Right-click on the VoIP East node ⇒ Edit Attributes. ⇒ Rename the node to Voice Called ⇒ Assign None to the Application: Supported Profiles attribute ⇒ Assign Voice Called to the Client Address attribute ⇒ Click OK.
- 2. Right-click on the VoIP West node  $\Rightarrow$  Edit Attributes.
  - i. Rename the node to **Voice Caller**.
  - ii. Assign None to the Application: Supported Services attribute.
  - iii. Edit the value of the Application: Destination Preferences attribute  $\Rightarrow$  Set Rows to 1  $\Rightarrow$  Assign Voice Destination to the Symbolic Name of the new row  $\Rightarrow$  Edit the Actual Name attribute  $\Rightarrow$  Set Rows to 1  $\Rightarrow$  Assign Voice Called to the Name attribute of the new row as shown.
  - iv. Click **OK** three times.

Attribute	Value Voice Caller ethernet_wkstn Unspecified	Symbolic Nam Voice Destinat	e	Actual Name		
<ul> <li>♥ Application: Supported Profiles</li> <li>♥ Application: Supported Services</li> <li>♥ Application: Transport Protocol Spe</li> <li>♥ CPU Background Utilization</li> <li>♥ CPU Resource Parameters</li> </ul>	() None . D∉ Nc <mark>I (Actual N</mark> Si	ame) Table	*			
<ul> <li>Client Address</li> <li>IP Host Parameters</li> <li>IP Processing Information</li> <li>Apply Changes to Selected Objects</li> </ul>	AL Name ( Voice Calle De	d	Selection We	eight	×	OK

- Click on the Voice Called node to select it ⇒ From the Edit menu, select Copy ⇒ From the Edit menu, select Paste (alternatively, use the standard keyboard shortcuts, Ctrl-C and Ctrl-V).
  - i. Locate the new node somewhere below the Voice Called node on the screen  $\Rightarrow$  Connect the new node to the East Router using a 10BaseT link.
  - ii. Right-click on the new node  $\Rightarrow$  Edit Attributes.
  - iii. Click on the **ethernet\_wkstn** value of the **model** attribute  $\Rightarrow$  Select **Edit**  $\Rightarrow$  Select the **ethernet\_wkstn\_adv** model.
  - iv. Rename it to Voice\_RSVP Called  $\Rightarrow$  Assign Voice\_RSVP Called to its Client Address attribute.
  - v. Click OK.
- 4. Copy and paste the Voice Caller node.
  - i. Locate the new node somewhere below the Voice Caller node  $\Rightarrow$  Connect the new node to the West Router using a 10BaseT link.

- ii. Right-click on the new node  $\Rightarrow$  Edit Attributes.
- iii. Click on the ethernet\_wkstn value of the model attribute  $\Rightarrow$  Select Edit  $\Rightarrow$  Select the ethernet\_wkstn\_adv model.
- iv. Rename it to Voice\_RSVP Caller.
- v. Edit the Application: Destination Preferences attribute ⇒ Open the Actual Name table by clicking in the value field of Actual Name ⇒ Assign Voice\_RSVP Called to the Name attribute (this is to replace the current value, which is Voice Called).
- vi. Click OK three times.
- 5. Rename the **Queues** node in the project to **QoS**. Your project should look like the following diagram.
- 6. Save your project.



11.4.2.2. Define the Data Flow:

Here, we will define the data flow characteristics of the voice traffic in the network. The sender's RSVP module periodically sends RSVP Path messages, that uses the data flow characteristics to describe the traffic generated by the sender. When the receiver's RSVP module receives the Path message, the receiver host application checks the characteristics of the requested data flow and decides if resources should be reserved. Once a decision is made to request network resource reservation, the host application sends a request to the local RSVP module to assist in the reservation setup. The receiver's RSVP module then carries the request as Resv messages to all nodes along the reverse data path to the sender.

The flow is defined by its required bandwidth and buffer size. Bandwidth is set to be the *token bucket rate* in the flow specification of the Path and Resv messages. The buffer size represents the amount of the application "bursty" data to be buffered. It

specifies the *token bucket size* that will be set in the Path or Resv messages for the session.

- 2. Right-click on the **QoS** node  $\Rightarrow$  **Edit Attributes**.
  - i. Expand the **RSVP Flow Specification** hierarchy and its **row 0** hierarchy ⇒ Set **Name** to **RSVP\_Flow** ⇒ Assign **50,000** to the **Bandwidth (bytes/sec)** attribute ⇒ Assign **10,000** to the **Buffer Size (bytes)** attribute.
  - ii. Expand the RSVP Profiles hierarchy and its row 0 hierarchy  $\Rightarrow$  Set Profile Name to RSVP\_Profile.
  - iii. Click **OK** and then save your project.

🖁 (QoS) Attributes	
Type: Utilities	
Attribute	Value
⑦ ⊢name	QoS
⑦ ⊢model	QoS Attribute Config
⑦ ⊞ CAR Profiles	Default
⑦ ⊞ Custom Queuing Profiles	Standard Schemes
⑦ ⊞ FIFO Profiles	Standard Schemes
⑦ ⊞ MWRR / MDRR / DWR	Standard Schemes
⑦ ⊞ Priority Queuing Profiles	Standard Schemes
⑦ ⊟ RSVP Flow Specification	()
⑦ ⊢rows	1
row 0	
⑦	RSVP_Flow
⑦ ⊢Bandwidth (bytes/se	. 50,000
Image: Buffer Size (bytes)	10,000
RSVP Profiles     RSVP ProfILe     RSVP Pr	()
⑦ ↓rows	1 / -
⑦ ⊢Profile Name	RSVP_Profile
Image: Threshold (bytes/sec)	None 👻
Apply Changes to Selected C	Dbjects Advanced
Eind Next	<u>Cancel</u> <u>O</u> K

11.4.2.3. Configure the Application:

Here we will create a VoIP application that utilizes the RSVP flow specifications we configured.

- Right-click on the Applications node ⇒ Edit Attributes ⇒ Expand the Application Definitions hierarchy ⇒ Set rows to 4 (to add a fourth row to the Application Definitions attribute).
  - i. Name and set the attributes of row 3 as shown:

<b>æ (</b>	👪 (Applications) Attributes					
Ту	pe: Utilities					
	Attribute		Value	<b>_</b>		
0		on Definitions	()			
?	rows		4	←		
	<b>∃</b> row 0		FTP Application,()			
	+ row 1		Video Application,()			
	± row 2		VoIP Application,()			
	⊡ row 3					
?	⊢Name	)	VoIP_RSVP	←		
?	Desc	ription	()			
?	-Cus	stom	Off			
?	Database		Off			
?	⊢Em	ail	Off			
0	⊢Ftp		Off			
?	⊢Htt	р	Off			
?	⊢Prir	nt	Off			
?	Rer	note Login	Off			
?	⊢Vid	eo Conferencing	Off			
?	L <b>_</b> Voi	ce	PCM Quality Speech			
?	<b>∃Voice</b> End	coder Schemes	All Schemes	-		
	Apply Chang	es to Selected O	bjects	Advanced		
		Eind Next	Cancel	<u>О</u> К		

ii. Click on the **PCM Quality Speech** value (shown above)  $\Rightarrow$  Select **Edit**  $\Rightarrow$  Edit the value of the **RSVP Parameters** attribute  $\Rightarrow$  Assign the following values (recall that we defined the **RSVP\_Flow** in the QoS node)  $\Rightarrow$  Click **OK** three times.

	(RSVP Parameters) Table	
	Attribute	Value
	RSVP Status	Enabled
(	Outbound Flow	RSVP_Flow
	hobound Flow	RSVP_Flow
		<b>_</b>
	Details Promote	<u>Cancel</u>

Note that the characteristics of the **Outbound Flow** are carried in the Path messages to be sent from sender to receiver, and the characteristics of the **Inbound Flow** parameters are carried in the Resv messages to be sent from the receiver to the sender.

#### 11.4.2.4. Configure the Profile:

1. Right-click on the **Profiles** node  $\Rightarrow$  **Edit** Attributes  $\Rightarrow$  Expand the **Profile Configuration** hierarchy  $\Rightarrow$  Set rows to 4 (to add a fourth row to the **Profile Configuration** attribute)  $\Rightarrow$  Name and set the attributes of row 3 as shown:

<b>* (</b>	🖁 (Profiles) Attributes						
Тур	pe: Utilities						
	Attribute	Value					
?	Frows	4 🔶					
	⊡row 0	FTP Profile,(),Simultaneous,c					
	⊡row 1	Video Profile,(),Simultaneous					
	row 2	VoIP Profile,(),Simultaneous,					
	⊡row 3						
?	Profile Name	VoIP_RSVP Profile					
0	Applications	()					
?	Frows	1					
	⊡row 0						
?	⊢Name	VoIP_RSVP					
?	⊢Start Time Offset (seconds)	constant (5)					
?	⊢Duration (seconds)	End of Profile					
?	田 Repeatability	Once at Start Time					
?	Operation Mode	Simultaneous					
?	Start Time (seconds)	constant (100)					
?	Duration (seconds)	End of Simulation					
?	⊞ Repeatability	Once at Start Time					
4							
F	Apply Changes to Selected Objects	Advanced					
	<u>F</u> ind Next	<u>C</u> ancel <u>O</u> K					

2. Click **OK** and then save your project.

# 11.4.2.5. Configure the Interfaces:

OPNET IT Guru supports RSVP on a per-interface basis; RSVP can be enabled or disabled for each node's interface.

1. Simultaneously select (shift + left-click) the following three links:



2. From the **Protocols** menu, select **RSVP**  $\Rightarrow$  Select **Configure Interface Status**  $\Rightarrow$  Make the selections shown below in the configuration dialog box  $\Rightarrow$  Click **OK** and then save your project.

🛪 Configure RS 📘 🗖 🔀								
This operation will enable/disable RSVP protocol status across connected interfaces for all/selected links.								
Status: CDisable								
Apply the above selection to:								
<u>C</u> ancel <u>O</u> K								

The above process enables RSVP on all interfaces along the path between the two Voice parties that need to utilize RSVP.

11.4.2.6. Configure the Hosts and Routers:

In OPNET IT Guru, the RSVP process runs only in IP-enabled nodes. The advanced versions (**\*\_adv**) of those node models must be used, as we did already, to configure RSVP-related parameters. In addition, the RSVP model in OPNET IT Guru requires either WFQ or custom queuing schemes.

- 1. Right-click on the Voice\_RSVP Caller node  $\Rightarrow$  Edit Attributes.
  - i. Expand the Application: Supported Profiles hierarchy and its row 0 hierarchy ⇒ Assign VoIP\_RSVP Profile to the Profile Name attribute.
  - ii. Expand the **Application: RSVP Parameters** hierarchy ⇒ Expand its **Voice** hierarchy ⇒ Enable the **RSVP Status** ⇒ Expand the **Profile List** hierarchy ⇒ Assign to the **Profile attribute** of **row 0** the value **RSVP Profile**.

Type: workstation							
Attribute	Value 🔺						
⑦ ⊡Voice	()						
⑦ ⊢RSVP Status	Enabled 🔶 🖊 🔤						
Profile List	()						
⑦ ⊢rows	1						
⊡ row 0							
⑦ └Profile	RSVP_Profile < 🚽						
•							

iii. Expand the IP Host Parameters hierarchy  $\Rightarrow$  Expand its Interface Information hierarchy  $\Rightarrow$  Expand the QoS Information hierarchy  $\Rightarrow$  Assign WFQ to the Queuing Scheme attribute  $\Rightarrow$  Assign ToS Based to the Queuing Profile attribute  $\Rightarrow$  Assign RSVP Enabled to the RSVP Info attribute.

Type: workstation						
Attribute	Value					
⑦ ⊡ IP Host Parameters	()					
Interface Information	()					
⑦ ⊢Name	IF0					
⑦ ⊢Address	Auto Assigned					
⑦ ⊢Subnet Mask	Auto Assigned					
⑦ ⊢MTU (bytes)	Ethernet					
⑦ ⊢Compression Information	None					
⑦ ⊢Multicast Mode	Disabled					
②	()					
⑦ ⊢Incoming CAR Profile	None					
⑦ ⊢Outgoing CAR Profile	None					
⑦ ⊢Buffer Size (Bytes)	1MBytes					
Processing Rate	Link Speed					
③ RSVP Info	RSVP Enabled					
① ( ⊢Queuing Scheme	WFQ					
② Queuing Profile	ToS Based					

**Type of service** (ToS) is assigned to the IP packets. It represents a session attribute that allows packets to be provided the appropriate service in the IP queues.

iv. Expand the RSVP Protocol Parameters hierarchy  $\Rightarrow$  Expand the Interface Information hierarchy. (You should notice that the word *Enabled* is listed in the summary line. When you expand it, you will see that it is the value of RSVP Status. If *Enabled* is not listed, go back to the *Configure the Interfaces* steps.)  $\Rightarrow$  Expand the hierarchy of the row of that interface  $\Rightarrow$  Assign 75% to both the Maximum Reservable BW and Maximum Bandwidth Per Flow attributes as shown:

Attribute	Value
Interface Information	()
Frows	1
⊡ row 0	
Name	
③ FRSVP Status	Enabled
⑦ ( + Maximum Reservable BW	75%
Maximum Bandwidth Per Flow	75%
⑦	None 🗸

#### v. Click **OK**.

Maximum Reservable BW specifies the percentage of the bandwidth of the connected link that RSVP can reserve on the interface.

Maximum Bandwidth Per Flow specifies the amount of reservable bandwidth that can be allocated to a single flow.

- 2. Right-click on the Voice\_RSVP Called node  $\Rightarrow$  Edit Attributes.
  - i. Edit the Application: Supported Services attribute. The Application: Supported Services Table will popup ⇒ In that table, replace the VoIP Application with VoIP\_RSVP and Click OK.
  - ii. Expand the Application: RSVP Parameters hierarchy ⇒ Expand its Voice hierarchy. ⇒ Enable the RSVP Status ⇒ Expand the Profile List hierarchy ⇒ Edit the value of the Profile attribute of row 0 and enter RSVP\_Profile.

- iii. Expand the IP Host Parameters hierarchy  $\Rightarrow$  Expand its Interface Information hierarchy  $\Rightarrow$  Expand the QoS Information hierarchy  $\Rightarrow$  Assign WFQ to the Queuing Scheme attribute  $\Rightarrow$  Assign ToS Based to the Queuing Profile attribute  $\Rightarrow$  Assign RSVP Enabled to the RSVP Info attribute.
- iv. Expand the **RSVP Protocol Parameters** hierarchy ⇒ Expand the **Interface Information** hierarchy. (You should notice that the **RSVP Status** of the interface that is connected to the router is *Enabled*. If not, go back to the *Configure the Interfaces* steps.) ⇒ Expand the hierarchy of the row of that interface ⇒ Assign **75%** to both **Maximum Reservable BW** and **Maximum Bandwidth Per Flow** attributes.
- v. Click OK.
- 3. Right-click on the East Router node  $\Rightarrow$  Edit Attributes.
  - i. Click on the **Ethernet4\_slip8\_gtwy** value of the **model** attribute.  $\Rightarrow$  Select **Edit**  $\Rightarrow$  Select the **Ethernet4\_slip8\_gtwy\_adv** model.
  - ii. Expand the **RSVP Protocol Parameters** hierarchy ⇒ Expand the Interface Information hierarchy. (You should notice that the **RSVP Status** of two interfaces, which are connected to the **West Router** and the **Voice\_RSVP** Called node, are *Enabled*. If not, go back to the *Configure the Interfaces* steps.) ⇒ Expand the hierarchies of the rows of these two interfaces ⇒ Assign 75% to both Maximum Reservable BW and Maximum Bandwidth Per Flow attributes.
  - iii. Expand the IP Routing Parameters hierarchy  $\Rightarrow$  Expand the Interface Information hierarchy  $\Rightarrow$  Expand the hierarchies of the rows of the same two interfaces you configured in the previous step (step ii)  $\Rightarrow$  Expand the QoS Information hierarchy for both  $\Rightarrow$  Set Queuing Scheme to WFQ and Queuing Profile to ToS Based for both.
  - iv. Click OK.
- 4. Right-click on the West Router node  $\Rightarrow$  Edit Attributes.
  - i. Click on the Ethernet4\_slip8\_gtwy value of the model attribute  $\Rightarrow$  Select Edit  $\Rightarrow$  Select the Ethernet4\_slip8\_gtwy\_adv model.
  - ii. Expand the **RSVP Protocol Parameters** hierarchy ⇒ Expand the **Interface Information** hierarchy. (You should notice that the **RSVP Status** of two interfaces, which are connected to the **East Router** and the **Voice\_RSVP Caller** node, are *Enabled.* If not, go back to the *Configure the Interfaces* steps.) ⇒ Expand the hierarchies of the rows of these two interfaces ⇒ Assign **75%** to both **Maximum Reservable BW** and **Maximum Bandwidth Per Flow** attributes.
  - iii. Expand the IP Routing Parameters hierarchy  $\Rightarrow$  Expand the Interface Information hierarchy  $\Rightarrow$  Expand the hierarchies of the rows of the same two interfaces you configured in the previous step (step ii)  $\Rightarrow$  Expand the QoS Information hierarchy for both  $\Rightarrow$  Set Queuing Scheme to WFQ and Queuing Profile to ToS Based for both.
  - iv. Click OK.

# **11.4.3.** Choose the Statistics

We will select statistics from three different nodes:

- 11.4.3.1. Voice\_RSVP Caller Statistics:
  - 1. Right-click on the Voice\_RSVP Caller node and select Choose Individual Statistics from the pop-up menu.
  - 2. Expand the RSVP hierarchy and select Number of Path States.
  - 3. Right-click on the Number of Path States statistic  $\Rightarrow$  Select Change Draw Style from the pop-up menu  $\Rightarrow$  Choose bar chart.
  - Right-click on the Number of Path States statistic ⇒ Select Change Collection Mode from the pop-up menu ⇒ Check the Advanced checkbox ⇒ From the Capture mode drop-down menu, select all values, as shown ⇒ Click OK.

<table-of-contents></table-of-contents>	1	🔣 Number o	of Path Stat	tes
(Bucket Mode) Sample Frequency:	1	Capture mode	all values	•
CEvery seconds	<u>8</u>	CEvery		seconds
CEvery values		CEyery		values
● Iotal of default values		€ <u>⊺</u> otal of	default 💌	values
Reset		Bucket mode	max value	<b>*</b>
Advanced		Reset		
Cancel OK		Advanced		18
		<u>C</u> a	ancel	OK

- 5. Expand the Voice Calling Party hierarchy and select the following statistics: Packet Delay Variation and Packet End-to-End Delay (sec).
- 6. Click OK.

Packet Delay Variation is the variance among end-to-end delays for voice packets received by this node.Packet End-to-End Delay for a voice packet is measured from the time it is created to the time it is received.

#### 11.4.3.2. Voice\_RSVP Called Statistics:

- 1. Right-click on the Voice\_RSVP Called node and select Choose Individual Statistics from the pop-up menu.
- 2. Expand the **RSVP** hierarchy and select **Number of Resv States**.
- 3. Right-click on the Number of Resv States statistic  $\Rightarrow$  Select Change Draw Style from the pop-up menu  $\Rightarrow$  Choose bar chart.
- Right-click on the Number of Resv States statistic ⇒ Select Change Collection Mode from the pop-up menu ⇒ Check the Advanced checkbox ⇒ From the Capture mode drop-down menu, select all values ⇒ Click OK.
- 5. Click OK.

# 11.4.3.3. Voice Caller Statistics:

- 1. Right-click on the **Voice Caller** node and select **Choose Individual Statistics** from the pop-up menu.
- 2. Expand the Voice Calling Party hierarchy and select the following statistics: Packet Delay Variation and Packet End-to-End Delay (sec).
- 3. Click OK.

# 11.4.4. Configure the Simulation

Here, we need to configure the duration of the simulation:

- 1. Click on and the *Configure Simulation* window should appear.
- 2. Make sure that the duration is set to 150 seconds.
- 3. Click on the **Global Attributes** tab and make sure that the following attribute is enabled:
  - a. **RSVP Sim Efficiency = Enabled.** This decreases the simulation time and memory requirements by not sending refresh messages (i.e., Path and Resv refreshes).
- 4. Click **OK** and then save your project.

#### 11.4.5. Run the Simulation

To run the simulation:

- 1. Click on and then click the **Run** button. Depending on the speed of your processor, this may take several minutes to complete.
- 2. After the simulation completes, click Close.
- 3. Save your project.

#### 11.4.6. View the Results

To view and analyze the results:

- 1. Select View Results from the Results menu.
- 2. As shown in the following figure, choose the **Packet End\_to\_End Delay** for both the **Voice Caller** and **Voice\_RSVP Caller** nodes. Choose **Overlaid Statistics** and **time\_average**.



3. Click **Show** to get the following graph. (*Note*: To zoom in on the graph, click and drag your mouse to draw a rectangle around the area of interest and release the mouse button.)



 Similarly, you can get the following graph that compares the Packet Delay Variation for both the Voice Caller and Voice\_RSVP Caller nodes. (*Note*: Make sure to "unselect" the statistics you chose for the previous graph.)



5. Finally, prepare the graph that displays the number of Path and Resv states by selecting the following statistics. Make sure to select **Stacked Statistics** and **As Is** as shown.

🐨 View Results			
Discrete Event Graphs Displayed Panel Graphs Campus Network Coice Caller Voice_RSVP Called RSVP Number of Resv States Noice_RSVP Caller RSVP Number of Path States	Show Preview	105	time (sec)
	As Is		•
Results Generated: 14:43:48 Mar 20 2003	Unselect	Add	Show
			<u>C</u> lose

6. Right-click on the resulting graph and choose Edit Panel Properties ⇒ Change the assigned values to the Horizontal Min and Horizontal Max fields as shown (your graph might require a slightly different range):

<table-of-contents> Panel Operat</table-of-contents>	ions 🛛 🔀
Panel Title:	
	Show Panel <u>T</u> itle
Panel	Coordinates Set Color
Horizontal Label:	time (sec)
Horizontal Min:	104.999s 룾 🗕
Horizontal Max:	105.072s 🗲 🗕
	<u>F</u> ull Scale
Set All Draw S	bar chart
Др	ply <u>C</u> ancel <u>O</u> K

7. Click **OK**. The resulting graph should resemble the one below.



# 11.5. *Further readings*

 OPNET <u>RSVP Model Description</u>: From the **Protocols** menu, select **RSVP** ⇒ <u>Model</u> <u>Usage Guide</u>.

# 11.6. Exercises

- 1) Analyze the graphs we obtained in this lab. Show the effect of RSVP on the Voice application and explain the obtained numbers of Path and Resv states.
- 2) How does the data rate of the link connecting the East and West routers affect the performance (e.g., Packet End-to-End Delay) of the Voice and Video Conference applications? To answer this question, create a new scenario as a duplicate of the QoS\_RSVP scenario. Name the new scenario Q2\_HighRate. In the Q2\_HighRate scenario replace the current PPP\_DS1 link (data rate 1.544 Mbps) with a PPP\_DS3 link (data rate 44.736 Mbps).

# 11.7. Lab Report

Prepare a report that follows the guidelines explained in Lab 0. The report should include the answers to the above exercises as well as the graphs you generated from the simulation scenarios. Discuss the results you obtained and compare these results with your expectations. Mention any anomalies or unexplained behaviors.

# 12. Laboratory - Firewalls and VPN (Network Security and Virtual Private Networks)

# 12.1. *Objective*

The objective of this lab is to study the role of firewalls and Virtual Private Networks VPNs) in providing security to shared public networks such as the Internet.

### 12.2. Overview

Computer networks are typically a shared resource used by many applications for many different purposes. Sometimes the data transmitted between application processes is confidential, and the application users would prefer that others not be able to read it.

A firewall is a specially programmed router that sits between a site and the rest of the network. It is a router in the sense that it is connected to two or more physical networks and it forwards packets from one network to another, but it also fitters the packets that flow through it. A firewall allows the system administrator to implement a security policy in one centralized place. File-based firewalls are the simplest and most widely deployed type of firewall. They are configured with a table of addresses that characterize the packets they will and will not forward.

A VPN is an example of providing a controlled connectivity over a public network such as the Internet. VPNs utilize a concept called an *IP tunnel* - a virtual point-to-point link between a pair of nodes that are actually separated by an arbitrary number of networks. The virtual link is created within the router at the entrance to the tunnel by providing it with the IP address of the router at the far end of the tunnel. Whenever the router at the entrance of the tunnel wants to send a packet over this virtual link, it encapsulates the packet inside an IP datagram. The destination address in the IP header is the address of the router at the far end of the tunnel, white the source address is that of the encapsulating router.

In this lab you will set up a network where servers are accessed over the Internet by customers who have different privileges. You will study how firewalls and VPNs can provide security to the information in the servers while maintaining access for customers with the appropriate privilege.

- 12.3. *Prelab Activities* 
  - Read section 4.5.3 from "Computer Networks: A Systems Approach", 4th Edition.
     Firewalls
- 12.4. *Procedure*

#### 12.4.1. Create a New Project

- 1. Start **OPNET IT Guru Academic Edition**  $\Rightarrow$  Choose **New** from the **File** menu.
- 2. Select **Project** and Click **OK** ⇒ Name the project **<your initials>\_VPN**, and the scenario **NoFirewall** ⇒ Click **OK**.
- 3. Click Quit on the Startup Wizard.
- 4. To remove the world background map, select the View menu  $\Rightarrow$  Background  $\Rightarrow$ Set Border Map  $\Rightarrow$  Select NONE from the drop-down menu  $\Rightarrow$  Click OK.

# 12.4.2. Create and Configure the Network

### 12.4.2.1. Initialize the Network:

- 1. Open the **Object Palette** dialog box by clicking **S**. Make sure that the **internet\_toolbox** item is selected from the pull-down menu on the object palette.
- 2. Add the following objects, from the palette, to the project workspace (see figure below for placement): Application Config, Profile Config, an ip32\_cloud, one ppp\_server, three ethernet4\_slip8\_gtwy routers, and two ppp\_wkstn hosts.
  - a. To add an object from a palette, click its icon in the object palette. ⇒ Move your mouse to the workspace and click where you want to place the object.
     ⇒ Right-click to indicate you are done creating objects of this type.
- 3. Rename the objects you added and connect them using **PPP\_DS1** links, as shown below:



#### 4. Save your project.

The **ppp\_server** and **ppp\_wkstn** support one underlying SLIP (Serial Line Internet Protocol) connection at a selectable data rate.

**PPP\_DS1** connects two nodes running PPP. Its data rate is 1.344 Mbps.

# 12.4.2.2. Configure the Nodes:

- 1. Right-click on the **Applications** node  $\Rightarrow$  **Edit Attributes**  $\Rightarrow$  Assign **Default** to the **Application Definitions** attribute  $\Rightarrow$  Click **OK**.
- 2. Right-click on the **Profiles** node  $\Rightarrow$  **Edit Attributes**  $\Rightarrow$  Assign **Sample Profiles** to the **Profile Configuration** attribute  $\Rightarrow$  Click **OK**.
- 3. Right-click on the Server node  $\Rightarrow$  Edit Attributes  $\Rightarrow$  Assign All to the Application: Supported Services attribute  $\Rightarrow$  Click OK.
- 4. Right-click on the Sales A node  $\Rightarrow$  Select Similar Nodes (make sure that both Sales A and Sales B are selected).
  - i. Right-click on the Sales A node  $\Rightarrow$  Edit Attributes  $\Rightarrow$  Check the Apply Changes to Selected Objects check-box.
  - ii. Expand the Application: Supported Profiles attribute  $\Rightarrow$  Set rows to  $1 \Rightarrow$ Expand the row 0 hierarchy  $\Rightarrow$  Profile Name = Sales Person (this is one of the "sample profiles" we configured in the Profiles node).

- iii. Click OK.
- 5. Save your project.

Several examples application configurations are available under the Default setting. For example, "Web Browsing (Heavy HTTP1.1)" indicates a Web browsing application performing heavy browsing using HTTP1.1. protocol.

# 12.4.3. Choose the Statistics

- 1. Right-click anywhere in the project workspace and select **Choose Individual Statistics** from the pop-up menu.
- 2. In the *Choose Results* dialog, check the following statistics:
  - i. Global Statistics  $\Rightarrow$  DB Query  $\Rightarrow$  Response Time (sec).
  - ii. Global Statistics  $\Rightarrow$  HTTP  $\Rightarrow$  Page Response Time (seconds).
- 3. Click OK.
- 4. Right-click on the **Sales A** node and select **Choose Individual Statistics** from the pop-up menu.
- 5. In the *Choose Results* dialog, check the following statistics:
  - i. Client DB  $\Rightarrow$  Traffic Received (bytes/sec).
  - ii. Client Http  $\Rightarrow$  Traffic Received (bytes/sec).
- 6. Click OK.
- 7. Right-click on the **Sales B** node and select **Choose Individual Statistics** from the pop-up menu.
- 8. In the *Choose Results* dialog, check the following statistics:
  - i. Client DB  $\Rightarrow$  Traffic Received (bytes/sec).
  - ii. Client Http  $\Rightarrow$  Traffic Received (bytes/sec).
- 9. Click **OK** and then save your project.

DQ Query Response Time is measured from the time when the database query application sends a request to the server to the time it receives a response packet.

HTTP Page Response Time specifies the time required to retrieve the entire page with all the contained inline objects.

#### 12.4.4. The Firewall Scenario

In the network we just created, the **Sales Person** profile allows both sales sites to access applications such as Database Access, Email, and Web Browsing from the server (check the **Profile Configuration** of the **Profiles** node) Assume that we need to protect the database in the server from external access, including the sales people. One way to do that is to replace **Router C** with a firewall as follows:

- 1. Select **Duplicate Scenario** from the **Scenarios** menu and name it **Firewall**  $\Rightarrow$  Click **OK**.
- 2. In the new scenario, right-click on **Router C**  $\Rightarrow$  **Edit Attributes**.
- 3. Assign ethernet2\_slip8\_firewall to the model attribute.
- Expand the hierarchy of the Proxy Server Information attribute ⇒ Expand the row 1, which is for the Database application, hierarchy ⇒ Assign No to the Proxy Server Deployed attribute as shown:

<table-of-contents> (Router C) Attributes</table-of-contents>	
Type: router	
Attribute	Value
⑦ ⊢name	Router C
⑦ ⊢model	ethernet2_slip8_firewall
⑦	None
⑦	Single Processor
⑦	()
⑦	Not Configured
⑦	Default
⑦	()
⑦	Default
⑦	()
⑦	()
⑦	()
⑦	None
⑦	()
Proxy Server Information	()
Frows	10
row 0	Custom Application, Yes, constant (
⊡row 1	
Application	Database
Proxy Server Deployed	No 🔶
① Latency (secs)	exponential (0.00005)
row 2	Email,Yes,No Latency
Apply Changes to Selected Object	ts Advanced
	<u>C</u> ancel <u>O</u> K

#### 5. Click **OK** and then save your project.

**Proxy Server Information** is a table defining the configuration of the firewall. Each roe indicates whether a proxy server exists for a certain application and the amount of additional delay that will be introduced to each forwarded packet of that application by the proxy server.

# 12.4.5. Firewalls and VPN

Our **Firewall** configuration does not allow database-related traffic to pass through the firewall (it filters such packets out). This way, the databases in the server are protected from external access. Your **Firewall** scenario should look like the following figure.



# 12.4.6. The Firewall VPN Scenario

In the **Firewall** scenario, we protected the databases in the server from "any" external access using a firewall router. Assume that we want to allow the people in the **Sales A** site to have access to the databases in the server. Since the firewall fitters all database-related traffic regardless of the source of the traffic, we need to consider the VPN solution. A virtual tunnel can be used by **Sales A** to send database requests to the server. The firewall will not filter the traffic created by **Sales A** because the IP packets in the tunnel will be encapsulated inside an IP datagram.

- 1. While you are in the **Firewall** scenario, select **Duplicate Scenario** from the **Scenarios** menu and give it the name **Firewall\_VPN** ⇒ Click **OK**.
- 2. Remove the link between Router C and the Server.
- 3. Open the *Object Palette* dialog box by clicking **N**. Make sure that the **internet\_toolbox** is selected from the pull-down menu on the object palette.
  - i. Add to the project workspace one **ethernet4\_slip8\_gtwy** and one **IP VPN Config** (see the figure below for placement).
  - ii. From the *Object Palette*, use two **PPP\_DS1** links to connect the new router to **Router C** (the firewall) and to the **Server**, as shown below.
  - iii. Close the Object Palette dialog box.
- 4. Rename the IP VPN Config object to VPN.
- 5. Rename the new router to **Router D** as shown:



The **ethernet4\_slip8\_gtwy** node model represents an IP based gateway supporting four Ethernet hub interfaces and eight serial line interfaces: IP packets arriving on any interface are routed to the appropriate output interface based on their destination IP address. The Routing Interface Protocol (RIP) or the Open Shortest Path First (OSPF) protocol may be used to dynamically and automatically create the gateway's routing tables and select routers in an adaptive manner.

12.4.6.1. Configure the VPN:

- 1. Right-click on the VPN node  $\Rightarrow$  Edit Attributes.
  - i. Expand the VPN Configuration hierarchy  $\Rightarrow$  Set rows to 1  $\Rightarrow$  Expand row 0 hierarchy  $\Rightarrow$  Edit the value of Tunnel Source Name and enter Router A  $\Rightarrow$  Edit the value of Tunnel Destination Name and enter Router D.

- ii. Expand the **Remote Client List** hierarchy  $\Rightarrow$  Set rows to  $1 \Rightarrow$  Expand row 0 hierarchy  $\Rightarrow$  Edit the value of Client Node Name and enter Sales A.
- iii. Click **OK** and then save your project.

🔀 (VPN) Attributes	
Type: Utilities	
Attribute	Value
⑦ _ name	VPN
⑦ ⊢model	IP VPN Config
PN Configuration	()
⑦ ⊢rows	1
⊡ row 0	
Tunnel Source Name	Router A
Tunnel Destination Name	Router D
①	None
Operation Mode	Compulsory
Remote Client List	()
⑦ ⊢rows	1
i row 0	
Client Node Name	Sales A < 🗕
	~
•	
Apply Changes to Selected Objects	Advanced
<u><u> </u></u>	<u>C</u> ancel <u>O</u> K

#### 12.4.6.2. Simulating Encryption:

A virtual tunnel between **Sales A** and the **Server** does not guarantee security for the contents of the transferred database packets. If the contents of these packets are confidential, encryption of these packets will be needed. In OPNET AE, the effect of packets encryption can be simulated by the available compression function. Two of the available compression schemes are the Per-Interface Compression and the Per-Virtual Circuit Compression as shown. Once you edit the Compression Information attribute of an interface, OPNET adds the IP Config node to the project.

Type: workstation		
Attribute	Value	
Client Address	Auto Assigned	88
IP Host Parameters	()	
Interface Information	()	
Interview Provide America Ameri America America Ame	IFO	1000
Address	Auto Assigned	1
Subnet Mask	Auto Assigned	
MTU (bytes)	IP	
Compression Inform	natNone	
Hulticast Mode N	one	
QoS Information D	efault TCP/IP Header Compression	
EDescription	efault Per-Interface Compression	
	nage Compression	1883
Passive RIP Routin Te	elnet App. Compression	-
Apply Changes to Selected	Objects Advan	nced
Find Next	Cancel OK	1

Per-Interface Compression compresses the entire packet (including the headers). This means the packet is decompressed and compressed at each hop on the route Per-Virtual Circuit Compression compresses the packet payload only. Therefore, compression and decompression take place only at the end nodes. One of the exercises by the end of this lab will ask you to create a new scenario to utilize the compression function.

# 12.4.7. Run the Simulation

To run the simulation for the three scenarios simultaneously:

- 1. Go to the Scenarios menu  $\Rightarrow$  Select Manage Scenarios.
- Change the values under the **Results** column to <collect> (or <recollect>) for the three scenarios. Keep the default value of the Sim Duration (1 hour). Compare to the following figure.

🛣 Ma	anage Scenarios					
Proje	ct Name: eha_VPN		1			
#	Scenario Name	Saved	Results	Sim Duration	Time Units	
1	NoFirewall	saved	<collect></collect>	1.0	hour(s)	
2	Firewall	saved	<collect></collect>	1.0	hour(s)	
3	Firewall_VPN	saved	<collect></collect>	1.0	hour(s)	
						•
D	elete Discard <u>R</u> esults <u>C</u> o	llect Resu	ults	0	Cancel <u>O</u> K	

- 3. Click **OK** to run the three simulations. Depending on the speed of your processor, this may take several minutes to complete.
- 4. After the three simulation runs complete, one for each scenario, click  $Close \Rightarrow$  Save your project.

#### 12.4.8. View the Results

To view and analyze the results:

- 1. Select **Compare Results** from the **Results** menu.
- 2. Expand the **Sales A** hierarchy  $\Rightarrow$  Expand the **Client DB** hierarchy  $\Rightarrow$  Select the **Traffic Received** statistic.
- 3. Change the drop-down menu in the middle-lower part of the **Compare Results** dialog box from **As\_Is** to **time\_average** as shown.

Compare Results		
Compare Results Discrete Event Graphs Displayed Panel Graph Global Statistics DB Query HTTP Object Statistics Sales A Client DB Client Http Sales B Results Generated: 01:13:07 Mar 21 2003	show Preview 20 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	 4000 ime (sec) ✓ Show
		Close

4. Press **Show** and the resulting graph should look similar to the following figure. Your graph may not match exactly due to node placement.



5. Create a graph similar to the previous one, but for Sales B:



6. Create two graphs similar to the previous ones to depict the **Traffic Received** by the **Client Http** for **Sales A** and **Sales B**.



Note: Results may vary slightly due to different node placement.

# 12.5. Further readings

- <u>The Impact of Internet Link Capacity on Application Performance</u>: From the **Protocols** menu, select **Methodologies** ⇒ <u>Capacity Planning</u>.
- <u>Virtual Private Networks Management</u>: <u>IETF RFC number 2685</u> (www.ietf.org/rfc.html).
- 12.6. Exercises
  - 1) From the obtained graphs, explain the effect of the firewall, as well as the configured VPN, on the database traffic requested by **Sales A** and **Sales B**.
  - 2) Compare the graphs that show the received HTTP traffic with those that show the received database traffic.

- 3) Generate and analyze the graph(s) that show the effect of the firewall, as well as the configured VPN, on the response time (delay) of the HTTP pages and database queries.
- 4) In the Firewall\_VPN scenario we configured the VPN node so that no traffic from Sales A is blocked by the firewall. Create a duplicate of the Firewall\_VPN scenario and name the new scenario Q4\_DB\_Web. In the Q4\_DB\_Web scenario we want to configure the network so that:
  - a. The databases in the server can be accessed only by the people in the Sales A site.
  - b. The web sites in the server can be accessed only by the people in the **Sales B** site.

Include in your report the diagram of the new network configuration including any changes you made to the attributes of the existing or added nodes. Generate the graphs of the DB traffic received and the HTTP traffic received for both **Sales A** and **Sales B** to show that the new network meets the above requirements.

5) Create a duplicate of the Firewall\_VPN scenario and name the new scenario Q5\_Compression. In the new scenario simulate packet encryption between Sales A and the Server by allowing Per-Virtual Circuit Compression in both nodes. As encryption takes more time than compression, edit the attributes of the Per-Virtual Circuit Compression row (row 3) in the IP Config node. Assign 3E-006 and 1E-006 to Compression Delay and Decompression Delay respectively. Study the effect of compression on the DB Query response time between Sales A and the Server.

# 12.7. Lab Report

Prepare a report that follows the guidelines explained in Lab 0. The report should include the answers to the above exercises as well as the graphs you generated from the simulation scenarios. Discuss the results you obtained and compare these results with your expectations. Mention any anomalies or unexplained behaviors.

# 13. Laboratory - Applications (Network Application Performance Analysis)

# 13.1. *Objective*

The objective of this lab is to analyze the performance of an Internet application protocol and its relation to the underlying network protocols. In addition, this lab reviews some of the topics covered in previous labs.

#### 13.2. Overview

Network applications are part network protocol (in the sense that they exchange messages with their peers on other machines) and part traditional application program (in the sense that they interact with the users).

OPNET's Application Characterization Environment (ACE) provides powerful visualization and diagnosis capabilities that aid in network application analysis. ACE provides specific information about the root cause of application problems. ACE can also be used to predict application behavior under different scenarios. ACE takes as input a real trace file captured using any protocol analyzer, or using OPNET's capture agents (not included in the Academic Edition).

In this lab you will analyze the performance of an FTP application. You will analyze the probable bottlenecks for the application scenario under investigation. You will also study the sensitivity of the application to different network conditions such as bandwidth and packet loss. The trace was captured on a real network, which is shown in the figure below, and already imported into ACE. The FTP application runs on that network; the client connects to the server over a 768 Kbps Frame Relay circuit with 36 ms of latency. The FTP application downloads a 1 MB file in 37 seconds. Normally the download time for a file this size should be about 11 seconds.



#### 13.3. *Prelab Activities*

 Read sections 9.1.1 and 9.1.3 from "Computer Networks: A Systems Approach" 4th Edition.

Go to *www.net-seal.net/animations.php* and play the following animations:

- Internet Access.
- Email Protocols

# 13.4. Procedure

# 13.4.1. Open the Application Characterization Environment

- 1. Start **OPNET IT Guru Academic Edition**  $\Rightarrow$  Choose **Open** from the **File** menu.
- 2. Select Application Characterization from the pull-down menu.
- 3. Select **FTP\_with\_loss** from the list  $\Rightarrow$  Click **OK**.



# 13.4.2. Visualize the Application

After opening the file, ACE shows the Data Exchange Chart (DEC), depicting the flow of application traffic between tiers. The DEC you see on your screen may or may not show the **FTP Server** tier as the top tier. If it does not, drag the tier label from the bottom to the top, so your screen matches the one shown in the following diagram.



- 1. Select Network Chart Only from the drop-down menu as shown below.
- 2. Differentiate the messages flowing in different directions by selecting  $\textsc{View} \Rightarrow \textsc{Split Groups}.$

The Data Exchange Chart can display the following:

- The Application Chart, which shows the flow of application traffic between nets.
- The Network Chart, which shows the flow of network protocols on application traffic.

Network protocols split packets into segments, add header, and often include mechanisms to ensure reliable data transfer. These network protocol effects can influence application behavior.



To get a better understanding of this traffic, you will zoom in on the transaction. To understand how the Application Chart and Network Chart views differ, you will view both simultaneously.

- 3. Select **Application and Network Charts** from the drop-down menu in the middle of the dialog box.
- 4. To disable the split groups view, select **View**  $\Rightarrow$  **Split Groups**.
- 5. Select View  $\Rightarrow$  Set Visible Time Range  $\Rightarrow$  Set Start Time to 25.2 and End Time to 25.5  $\Rightarrow$  Click OK.
- 6. The Application Message Chart shows a single message flowing from the **FTP Server** to the Client. To show the size, rest the cursor on the message to show the tooltip. **Client Payload** is shown as 8192.



The Network Chart shows that this application message causes many packets to flow over the network. These packets are a mix of large (blue and green) packets from the FTP Server to the Client and small (red) packets from the Client to the FTP Server. As the red color indicates, these packets contain 0 bytes of application data. They are the acknowledgments sent by TCP.

#### 13.4.3. Analyze with AppDoctor

AppDoctor's *Summary of Delays* provides insight into the root cause of the overall application delay.

1. From the AppDoctor menu, select Summary of Delays  $\Rightarrow$  Check the Show Values checkbox.

Notice that the largest contributing factor to the application response time is protocol/congestion. Only about 30 percent of the file download time is caused by the limited bandwidth of the Frame Relay circuit (768 Kbps). Notice also that application delay (processing inside the node) by both the Client and **FTP Server** is a very minor contributing factor to the application response time.

AppDoctor Summary of Delays - FTP_with	_loss 📃 🗖 🔀
	30.5% Client FTP Server
Client FTP Server	68.5%
Delays: Application Propagation	Transmission Protocol / Congestion
✓ <u>S</u> ort Network Delays by Tier Pair ✓ Show <u>V</u> alues	Update Help Close

2. Close the *Summary of Delays* dialog box.

The **Diagnosis** function of AppDoctor should give further insight into the cause of the protocol/congestion delay.

3. From the AppDoctor menu, select Diagnosis.

The diagnosis shows four bottlenecks: transmission delay, protocol/congestion delay, retransmissions, and out of sequence packets. One factor that contributes to protocol/congestion delay is retransmissions. So it is no surprise that here, in the more detailed diagnosis, you see retransmissions listed as a bottleneck. The out of-sequence packets, also listed as a bottleneck, are a side effect of the retransmissions. Correcting that issue will probably also cure the out of sequence packets problem.

🛣 AppDoctor Diagnosis	FTP_wit	h_loss				
Total	FTP Server		Client			
Processing Delay No Bottle	neck	No Bottle	eneck	No Bottleneck		-
<u>.</u>						
	Total		Client <->	FTP Server		
Network Cost of Chattiness	No Bottlen	eck	No Bottlen	eck		
Propagation Delay	No Bottlen	eck	No Bottlen	eck		
Transmission Delay	Bottleneck		Bottleneck	c		
Protocol/Congestion Delay	Bottleneck		Bottleneck	¢		
Connection Resets	No Bottlen	eck	No Bottler	eck	i i i i i i i i i i i i i i i i i i i	2000 200 10 10 10 10 10 10 10 10 10 10 10 10 1
Retransmissions	Bottleneck		Bottleneck	-		Click on the word
Out of Sequence Packets	Bottleneck		Bottleneck bottleneck			bottleneck to see
TCP Windowing (A -> B)	Not Applic	able	No Bottler	eck		the description.
TCP Windowing (A <- B)	Not Applic	able	No Bottler	eck	1	
•						Þ
There are many pack	et retrar	smissi	ons. The	e network ma	v be	▲ <u>V</u> iew Values
heavily congested, or	there m	ay be a	an error-j	orone link.		
						_
Threshold: 3.0%, Va	ue: 4.1%	6 - a lo <sup>,</sup>	wer valu	e is better.		•
				Update	<u>H</u> elp	Close

# 4. Close the Diagnosis Window

AppDoctor also provides summary statistics for the application transaction.

5. From the AppDoctor menu, select Statistics.

Notice that 52 retransmissions occurred during a file transfer composed of 1281 packets, yielding a retransmission rate of 4%.

6. Close the *Statistics window*.

AppDoctor Statistics -	FTP_with_lo	555		
	Total	FTP Server	Client	<b>A</b>
Busy Time (Seconds)	0.247009	0.229835	0.017174	
Processing Delay (Seconds)	0.229954	0.229835	0.000119	
Network Delay (Seconds)	37.050164	Not Applicable	Not Applicable	-
4				
		Total	Client <-> FTP Serv	/er 🔺
Response Time (Seconds)		37.280119	37.280119	
Application Turns		4	4	
Application Messages		241	241	
Application Message Bytes		1,057,043	1,057,043	
Average Application Message	Size (Bytes)	4.386.07	4,386.07	
Network Packets		(1,281)	1,281	
Network Packet Bytes		1,201,409	1,201,409	
Average Network Packet Payl	oad Size (Byte	s) 937.87	937.87	
Propagation Delay (Seconds)		Not Applicab	le 0.036000	
Delay due to Propagation (Se	conds)	0.144000	0.144000	
Transmission Speed (Bits/Se	cond)	Not Applicab	le 768,000	
Delay due to Transmission S	peed (Seconds	s) 11.372422	11.372422	
Protocol/Congestion Delay (S	econds)	25.549357	25.549357	
Max Application Turn Bytes (A	(-> B)	Not Applicab	le 23	
Max Application Turn Bytes (A	<b)< td=""><td>Not Applicab</td><td colspan="2">Not Applicable 1,056,891</td></b)<>	Not Applicab	Not Applicable 1,056,891	
Max Unacknowledged Data (A	A -> B) (Bytes)	Not Applicab	le 10	
Max Unacknowledged Data (A <- B) (Bytes)		Not Applicab	le 8,192	
Retransmissions		52	52	
Out of Sequence Packets		41	41	-
		•	-	
		<u>U</u> pdate	Help Cic	ose

# 13.4.4. Examine the Statistics

To view the actual network throughput, use the Graph Statistics feature.

- 1. From the Data Exchange Chart, select **Graph Statistics** from the **Graph** menu (or click the button: ).
- 2. Select the two Network Throughput statistics that measure Kbits/sec.

🛣 Graph Statistics - FTP_with_loss	
	<b>_</b>
Application Throughput (Kbits/sec): Client to FTP Server	
Application Throughput (Kbits/sec): FTP Server to Client	
Application Throughput (messages/sec): Client to FTP Server	
Application Throughput (messages/sec): FTP Server to Client	
🛛 🖊 🗖 Network Throughput (Kbits/sec): Client to FTP Server	
Network Throughput (Kbits/sec): FTP Server to Client	
Network Throughput (packets/sec): Client to FTP Server	
Network Throughput (packets/sec): FTP Server to Client	
Retransmissions: Client to FTP Server	
Retransmissions: FTP Server to Client	
Out of Seguence Packets: Client to FTP Server	
Out of Sequence Packets: FTP Server to Client	
TCP In-Flight Data (bytes): Client to FTP Server	
TCP In-Flight Data (bytes): FTP Server to Client	
The Connection 1: TCP: Client 1043 <-> FTP Server 21	-
Bucket Width (msec): 1000 Unselect Show	<u>C</u> lose

3. Click Show.



Return to the *Graph Statistics window*. ⇒ Unselect the throughput statistics and select only the two **Retransmissions** statistics ⇒ Change the **Bucket Width** to 100 ms ⇒ Click Show.



ACE divides the entire tasks duration into **buckets** of time and calculate a mean of total value for each interval. The default bucket width is 1000 msec; you can change this value in the Bucket Width (msec) field of the ACE statistic hardware.

# 13.4.5. Ideal TCP Window Size

In TCP, rather having a fixed-size sliding window, the receiver advertises a window size to the sender. This is done using the **AdvertisedWindow** field in the TCP header. The sender is then limited to having no more than a value of **AdvertisedWindow** bytes of unacknowledged data at any given time. The receiver selects a suitable value for **AdvertisedWindow** based on the amount of memory allocated to the connection for the purpose of buffering data. This procedure is called *flow control*, and its idea is to keep the sender from overrunning the receiver's buffer.

In addition, TCP maintains a new state variable for each connection, called **CongestionWindow**, which is used by the source to limit how much data it is allowed

to have in transit at a given time. The congestion window is congestion control's counterpart to flow control's advertised window. It is dynamically sized by TCP in response to the congestion status of the connection.

TCP will send data only if the amount of sent-but-not-yet-acknowledged data is less than the minimum of the congestion window and the advertised window. ACE auto-calculates the optimum window size based on the bandwidth/delay product as follows:

1. Return to the Graph *Statistics window*  $\Rightarrow$  Select the **TCP In-Flight Data (bytes)** FTP Server to Client statistic  $\Rightarrow$  Assign 1000 to the Bucket Width (msec).

# Graph Statistics - FTP_with_loss	
TCP In-Flight Data (bytes): Client to FTP Server TCP In-Flight Data (bytes): FTP Server to Client Connection 1: TCP: Client:1043 <-> FTP Server:21 Connection 2: TCP: FTP Server:20 <-> Client:1060	•
Bucket Width (msec): 1000 - Unselect Show	<u>C</u> lose

Click **Show**. From the graph, the ideal window size calculated by ACE is about 7 2. KB.



3. You can now close all opened graphs (delete the panel when you are asked to do that) and close the Graph Statistics window.

The **bandwidth-delay products** of a connection gives the "volume" of the connection - the number of bits it holds. It corresponds to how many bits the sender must retransmit before the first bit arrives at the receiver.

#### 13.4.6. Impact of Network Bandwidth

ACE **QuickPredict** enables you to study the sensitivity of an application to network conditions such as bandwidth and latency.

1. Click on the **QuickPredict** button:



2. In the *QuickPredict Control* dialog box assign **512 Kbps** to the **Min Bandwidth** field and **10 Mbps** to the **Max Bandwidth** field ⇒ Click the **Update Graph** button.

Redict Control				×
Choose Network Path to Modify	Client <-> F	TP Server		•
X Axis: <u>B</u> andwidth C Lat <u>a</u> Min Bandwidth 512Kbps Ma Choose Values Latency 36ms	<u>e</u> ncy ax Bandwidth	10Mbps	The current graph shows the impact of bandwidth on overall application response time. The X-axis shows varying bandwidths between "Client" and "FTP Server".	
0ms	300ms	[	You can put latency on the X-axis by selecting the "Latency" radio button.	•
	<u>C</u> ompare	Close	Add Curve(s) Update Gra	aph

3. The resulting graph should resemble the following one:



4. Close the graph and the *QuickPredict Control* dialog box.

# 13.4.7. Deploy an Application

OPNET IT Guru can be used to perform predictive studies of applications that are characterized in ACE. ACE uses the trace files to create application fingerprints that characterize the data exchange between tiers. From these fingerprints, a simulation can show how the application will behave under different conditions. For example, the ACE topology wizard can be used to build a network model from the ACE file of this lab, **FTP\_with\_loss** to answer the following question: What will the performance of the FTP application be when deployed to 100 simultaneous users over an IP network?

Follow the following steps to answer the above question:

- 1. From the IT Guru main window, select **File** ⇒ **New** ⇒ Select **Project** from the pull-down menu ⇒ Click **OK**.
- 2. Name the project **<your initials>\_FTP**, and the scenario **ManyUsers**  $\Rightarrow$  Click **OK**.

3. In the *Startup Wizard*, select **Import from ACE**  $\Rightarrow$  Click **Next**.



- 4. The Configure ACE Application dialog box appears.
  - i. Set the Name field to FTP Application.
  - ii. Set the **Repeat** application field to **2**. This field controls how many times a user executes the application per hour.
  - iii. Leave the limit at the default value, Infinite.
  - iv. Click on Add Task  $\Rightarrow$  In the Contained Tasks table, click on the word Specify ...  $\Rightarrow$  Select FTP\_with\_loss from the pull-down menu.
  - v. Click Next

Name:	ETP Application		Specify:
	K		op conj.
Repeat	application 2	times per hour	1. Application name.
using th	ne following limit:	•	2. Application repetition per
	Infinite		User. 3. Maximum number of
	Count = 1		
tained	Tasks:		
itained Task	Tasks: ACE Trace File	Tier Names	Click 'Add Task' to select the
itained Task 1	Tasks: ACE Trace File FTP_with_loss	Tier Names	Click 'Add Task' to select the
ntained Task 1	Tasks: ACE Trace File FTP_with_loss	Tier Names	Click 'Add Task' to select the ACE trace file(s) to be contained
Task	Tasks: ACE Trace File FTP_with_loss	Tier Names 	Click 'Add Task' to select the ACE trace file(s) to be contained as part of this application.
ntained Task 1	Tasks: ACE Trace File FTP_with_loss	Tier Names 	Click 'Add Task' to select the ACE trace file(s) to be contained as part of this application. Note:

- 5. The *Create ACE Topology* dialog box appears. Set **Number of Clients** to **100** and set **Packet Latency** to **40**. Leave all other settings at the default values.
- 6. Click Create.
| LAN Details:       100         Number of Clients:       100         Packet Analyzer:       N/A         Client Location:       Remote         WAN Details:       IP         Technology:       IP         Packet Latency (msec):       40         Packet Loss Ratio (0-100):       0 | Specify parameters to create  | a network topolog                            | y for app | id <b>ati8n</b> Application   |   |
|--|---|--|-----------|---|---|
| based on information obtained  | LAN Details:<br>Number of Clients:<br>Packet Analyzer:<br>Client Location:<br>WAN Details:<br>Technology:<br>Packet Latency (msec): | 100       N/A       Remote       IP       40 |           | <ol> <li>Specify the number of clients<br/>running the application. If more<br/>than one client is specified, a<br/>'LAN' node is used to represent<br/>the clients.</li> <li>Packet Analyzer captures<br/>packets in the simulated<br/>network. It is not selectable if the<br/>number of clients is more than<br/>one.</li> <li>The default client location is</li> </ol> |   |
| Access Bandwidth (Kbps): 1536 from the ACE trace files.  | Access Bandwidth (Kbps)   | 1536   | _         | based on information obtained from the ACE trace files.   | • |

7. Select File  $\Rightarrow$  Save  $\Rightarrow$  Click OK to save the project.

The ACE Wizard creates a topology similar to the one shown. The **Tasks**, **Applications**, and **Profiles** objects have all been configured according to the trace files and the entries you made in the ACE Wizard. You can customize them further.



*<sup>13.4.7.1.</sup> Run the Simulation and View the Results:* Now that the topology is created, you can run the simulation.

- 1. Click on the Configure/Run Simulation action button
- 2. Use the default values. Click **Run.** Depending on the speed of your processor, this may take several minutes to complete.
- 3. Close the dialog box when the simulation completes.  $\Rightarrow$  Save your project.
- 4. Select View Results from the Results menu ⇒ Expand the Custom Application hierarchy ⇒ Select the Application Response Time (sec) statistic.

🛣 View Results				
Discrete Event Graphs Displayed Panel Graphs				1
Global Statistics	Show Pre	eview		
	40			
Application Response Time (sec)				Mon
Diject Statistics	0			
	0		2000	4000
				time (sec)
<b>_</b> 1	Stacked St	atistics	▼ This Sc	enario 💌
	As Is			<b>_</b>
Results Generated: 03:22:11 Mar 21 2003		Unselect	Add	Show
				Close

5. Click **Show**. The resulting, graph should resemble the following:



#### 13.5. *Further readings*

• File Transfer Protocol (FTP): IETF RFC number 959 (www.ietf.org/rfc.html).

# 13.6. Exercises

- 1) Explain why the Client to FTP Server messages are mainly 0-byte messages?
- 2) Utilizing the AppDoctor's Summary of Delays, what is the effect of each of the following upgrades on the FTP download time?
  - a. Server upgrade
  - b. Bandwidth upgrade
  - c. Protocol(s) upgrade

- 3) How do retransmissions contribute to protocol/congestion delay? Explain why "out of sequence" packets are constitute a side effect of retransmissions.
- 4) Which protocol is responsible for the retransmission, IP, TCP, or FTP? Explain.
- 5) In the **Network Throughput** graph, the throughput from the **FTP Server** to the Client has an average value of about 300 Kbps and has a spike to about 500 Kbps. But the Frame Relay circuit has an available bandwidth of 768 Kbps. Explain why the throughput is not close to the available bandwidth.
- 6) Explain how the TCP in-flight data is used as an indicator of the TCP window size and how the bandwidth-delay product of the connection is used as an indicator of the ideal window size.
- 7) Comment on the graph we received that shows the relation between the network bandwidth and the FTP application response time. Why does the response time look unaffected by increasing the bandwidth beyond a specific point?
- 8) In the Deploy an Application section, a network model with multiple users was created based on the ACE file, FTP\_with\_loss. Duplicate the created scenario to create a new one with the name Q8\_ManyUsers\_ExistingTraffic. In this new scenario add an "existing" traffic of 80% load in the network. Examine how the existing traffic affects the FTP application's response time. Note: A simple way to simulate the existing traffic is to apply background utilization traffic of 80% to the link between the Remote Router and the IP Cloud.

#### 13.7. Lab Report

Prepare a report that follows the guidelines explained in Lab 0. The report should include the answers to the above exercises as well as the graphs you generated from the simulation scenarios. Discuss the Results you obtained and compare these results with your expectations. Mention any anomalies or unexplained behaviors.

# 14. Laboratory - Wireless Local Area Network (Medium Access Control for Wirelessly Connected Stations)

#### 14.1. Objective

This lab addresses the MAC (Medium Access Control) sublayer of the IEEE 802.11 standard for WLAN (wireless local area network). Different options of this standard are studied in this lab. The performance of these options is analyzed under different scenarios.

#### 14.2. Overview

The IEEE 802.11 standard provides wireless connectivity to computerized stations that require rapid deployment such as portable computers. The Medium Access Control (MAC) sublayer in the standard includes two fundamental access methods: distributed coordination function (DCF) and the point coordination function (PCF). DCF utilizes the carrier sense multiple access with collision avoidance (CSMA/CA) approach. DCF is implemented in all stations in the wireless local area network (WLAN). PCF is based on polling to determine the station that can transmit next. Stations in an infrastructure network optionally implement the PCF access method.

In addition to the physical CSMA/CA, DCF and PCF utilize virtual carrier-sense mechanism to determine the state of the medium. This virtual mechanism is implemented by means of the network allocation vector (NAV). The NAV provides each station with a prediction of future traffic on the medium. Each station uses NAV as an indicator of time periods during which transmission will not be initiated even if the station senses that the wireless medium is not busy. NAV gets the information about future traffic from management frames and the header of regular frames being exchanged in the network.

With DCF, every station senses the medium before transmitting. The transmitting station defers as long as the medium is busy. After deferral and while the medium is idle, the transmitting station has to wait for a random backoff interval. After the backoff interval and if the medium is still idle, the station initiates data transmission or optionally exchanges RTS (request to send) and CTS (clear to send) frames with the receiving station. The effect of RTS and CTS frames will be studied in the following lab.

With PCF, the access point (AP) in the network acts as a point coordinator (PC). The PC uses polling to determine which station can initiate data transmission. It is optional for the stations in the network to participate in PCF and hence respond to poll received from the PC. Such stations are called CF-Pollable stations. The PCF requires control to be gained of the medium by the PC. To gain such control, the PC utilizes the Beacon management frames to set the network allocation vector (NAV) in the network stations. As the mechanism used to set NAV is based on the DCF, all stations comply with the PC request to set their NAV whether or not they are CF-Pollable. This way the PC can control frame transmissions in the network by generating contention free periods (CFP). The PC and the CF-Pollable stations do not use RTS/CTS in the CFP.

The standard allows for fragmentation of the MAC data units into smaller frames. Fragmentation is favorable in case the wireless channel is not reliable enough to transmit longer frames. Only frames with a length greater than a fragmentation threshold will be fragmented. Each fragment will be sent independently and will be separately acknowledged. During a contention period, all fragments of a single frame will be sent as burst with a single invocation of the DCF medium access procedure. In case of PCF and during a contention free period, fragments are sent individually following the rules of the point coordinator (PC).

- 14.3. *Prelab Activities* 
  - Read section 2.8.2 from "Computer Networks: A Systems Approach", 4th Edition.
- 14.4. *Procedure*

#### 14.4.1. Create a New Project

To create a new project for the Ethernet network:

- 1. Start **OPNET IT Guru Academic Edition**  $\Rightarrow$  Choose **New** from the **File** menu.
- 2. Select Project  $\Rightarrow$  Click OK  $\Rightarrow$  Name the project <your initials>\_WirelessLAN, and the scenario DCF  $\Rightarrow$  Click OK.
- 3. In the *Startup Wizard: Initial Topology* dialog box, make sure that **Create Empty Scenario** is selected ⇒ Click **Next** ⇒ Choose **Office** from the *Network Scale* list and check **Use Metric Units** ⇒ Click **Next** twice ⇒ Click **OK**.

#### 14.4.2. Create and Configure the Network

To create our wireless network:

1. The Object Palette dialog box should be now on the top of your project space. If

it is not there, open it by clicking . Make sure that the wireless\_lan is selected from the pull-down menu on the object palette.

- 2. Add to the project workspace the following objects from the palette: 9 wlan\_station\_adv (fix).
  - a. To add an object from a palette, click its icon in the object palette.  $\Rightarrow$  Move your mouse to the workspace  $\Rightarrow$  Left-click to place the object. Right-click when finished.
- 3. Close the *Object Palette* dialog box ⇒ Arrange the stations in the workspace as shown in the following figure ⇒ Save your project.



- 14.4.2.1. Configure the wireless nodes:
  - 1. Repeat the following for each of the nine nodes:

Right-click on the node  $\Rightarrow$  Edit Attributes  $\Rightarrow$  Assign to the Wireless LAN MAC Address attribute a value equals to the node number (e.g., address 1 is assigned to node\_1)  $\Rightarrow$  Assign to the Destination Address attribute the corresponding value shown in the following table  $\Rightarrow$  Click OK.

 The following figure shows the values assigned to the Destination Address and Wireless LAN MAC Address attributes for node\_1.

Node name	Destination Address	(node 1) Attributes		
node_0	Random	M (node_1) Attributes		
node_1	5	Type: station		Long to contract the second state
node_2	8	Attribute	Value	
node_3	6	⑦ ⊢ name	node_1	
node_4	7	Destination Address	5 -	
node_5	1	Traffic Generation Parame     LWireless LAN MAC Address	s 1	3
node_6	3	Apply Changes to Selected Of	niante	-
node_7	4	Cind Next	Canad	
node_8	2	Eind Next	Gancel	

- 14.4.2.2. Traffic Generation Parameters:
  - Select all the nodes in the network simultaneously except node\_0 (click on all of them while holding the Shift key) ⇒ Right-click on any of the selected nodes (i.e., node\_1 to node\_8) ⇒ Edit Attributes ⇒ Check the Apply Changes to Selected Objects check box.
  - 2. Expand the hierarchies of the Traffic Generation Parameters and the Packet Generation Arguments attributes.  $\Rightarrow$  Edit the attributes to match the values shown in the following figure  $\Rightarrow$  Click OK.

Туре	e: station			
A	Attribute	Value		•
0 E	Traffic Generation Parameters	()		
۲	- Start Time (seconds)	constant (2)	-	23
۲	-ON State Time (seconds)	exponential (4)	-	
1	-OFF State Time (seconds)	exponential (4)		
۲	Packet Generation Arguments	()		
1	Interarrival Time (seconds)	exponential (0.06)		
٢	Packet Size (bytes)	uniform (500, 1500)		
1	L Segmentation Size (bytes)	No Segmentation		88
۲	L Stop Time (seconds)	Never		-
A	pply Changes to Selected Objects	-	Advan	cec
-	Find Next	Cancel	OK	

3. Select all the nodes in the network simultaneously including node\_0  $\Rightarrow$ Right-click on any of the selected nodes  $\Rightarrow$  Edit Attributes  $\Rightarrow$  Check the Apply Changes to Selected Objects check box. 4. Expand the hierarchy of the **Wireless LAN Parameters** attribute ⇒ Assign the value 4608000 to the **Buffer Size (bits)** attribute ⇒ Click **OK**.

Type: station		
Attribute	Value	•
Hong Retry Limit	4	0.3
Access Point Function	onality Disabled	
Channel Settings	()	19.92 19.31
Buffer Size (bits)	4608000 <	00.00
Max Receive Lifetime	e (s 0.5	-
Apply Changes to Selecte	ed Objects 🔶	Advanced
Find Nex	t Cancel	ОК

5. Right-click on node\_0  $\Rightarrow$  Edit Attributes  $\Rightarrow$  Expand the Wireless LAN Parameters hierarchy and set the Access Point Functionality to Enabled.  $\Rightarrow$  Click OK.

**Buffer sizes** specifies the maximum size of the higher layer data buffer limit is reached, the data packets arrived from higher layer will be discarded until some packets are removed from the buffer so that the buffer has some free space to store these new packets.

#### 14.4.3. Choose the Statistics

To test the performance of the network in our DCF scenario, we will collect some of the available statistics as follows:

- 1. Right-click anywhere in the project workspace and select **Choose Individual Statistics** from the pop-up menu.
- 2. In the *Choose Results* dialog box, Expand the **Global Statistics** and **Node Statistics** hierarchies ⇒ choose the following five statistics:



3. Click OK and then save your project.

### 14.4.4. Configure the Simulation

Here we will configure the simulation parameters:

- 3. Click on and the *Configure Simulation* window should appear.
- 4. Set the duration to be **10.0 minutes**.
- 5. Click **OK** and then save your project.

## 14.4.5. Duplicate the Scenario

In the network we just created, we did not utilize many of the features explained in the overview section. By default the distributed coordination function (DCF) method is used for the medium access control (MAC) sublayer. We will create three more scenarios to utilize the features available from the IEEE 802.11 standard. In the **DCF\_Frag** scenario we will allow fragmentation of the MAC data units into smaller frames and test its effect on the network performance. The **DCF\_PCF** scenario utilizes the point coordination function (PCF) method for the medium access control (MAC) sublayer along with the DCF method. Finally, in the **DCF\_PCF\_Frag** scenario we will allow fragmentation of the MAC data and check its effect along with PCF.

## 14.4.5.1. The DCF\_Frag Scenario:

- 1. Select **Duplicate Scenario** from the **Scenarios** menu and give it the name  $DCF\_Frag \Rightarrow Click OK$ .
- Select all the nodes in the DCF\_Frag scenario simultaneously (click on all of them while holding the Shift key) ⇒ Right-click on anyone of them ⇒ Edit Attributes ⇒ Check the Apply Changes to Selected Objects check box.
- 3. Expand the hierarchy of the Wireless LAN Parameters attribute ⇒ Assign the value 256 to the Fragmentation Threshold (bytes) attribute ⇒ Click OK.

+ (node_3) Attributes			
Value			
()			
256 -	-		
jects	Advanced		
Cancel	QK		
	Value () None 256  jects <u>C</u> ancel		

4. Right-click on **node\_0**  $\Rightarrow$  **Edit Attributes**  $\Rightarrow$  Expand the **Wireless LAN Parameters** hierarchy and set the **Access Point Functionality** to **Enabled**.  $\Rightarrow$  Click **OK**.

**Fragmentation Threshold** specifies the fragmentation threshold in bytes. Any data packet received from higher layer with a size greater than this threshold will be divided into fragments, which will be transmitted separately over the radio interface. Regardless of the value of this attribute, if the size of a higher layer packet is larger than the maximum MSDU size allowed the IEEE 802.12 WLAN standard, which is 2304 bytes, then such a packet will not be transmitted by the MAC, and it will be immediately discarded when received.

- 14.4.5.2. The DCF PCF Scenario:
  - 1. Switch to the **DCF** scenario, select **Duplicate Scenario** from the **Scenarios** menu and give it the name **DCF PCF**  $\Rightarrow$  Click **OK**  $\Rightarrow$  Save your project.
  - 2. Select node\_0, node\_1, node\_3, node\_5, and node\_7 in the DCF\_PCF scenario simultaneously (click on these nodes while holding the Shift key)  $\Rightarrow$ Right-click on anyone of the selected nodes  $\Rightarrow$  Edit Attributes.
  - 3. Check Apply Changes to Selected Objects  $\Rightarrow$  Expand the hierarchy of the Wireless LAN Parameters attribute  $\Rightarrow$  Expand the hierarchy of the PCF **Parameters** attribute  $\Rightarrow$  Enable the **PCF Functionality** attribute  $\Rightarrow$  Click **OK**.

(node_1) Attribu	utes	>
Type: station		
Attribute	Value	-
Wireless LAN Parar	meters ()	
Rts Threshold (by)	tes) None	
Fragmentation The Fragmenta	hreshol. None	
Data Rate (bps)	1 Mbps	
Physical Character	eristics Frequency Hopping	
Packet Reception	n-Powe 7.33 E-14	
Short Retry Limit	7	
Long Retry Limit	4	
Access Point Fur	nctionality Disabled	
Channel Settings	()	
Buffer Size (bits)	2048000	
Max Receive Life	time (s 0.5	
Large Packet Pro	cessing Drop	
BSS Identifier	Not Used	
PCF Parameters	()	38
PCF Functional	lity Enabled 🗲	
•	100 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	•
Apply Changes to Sele	ected Objects 🔶	- Advanced
Eind	Next Cancel	QK

- 4. Right-click on node 0  $\Rightarrow$  Edit Attributes  $\Rightarrow$  Expand the Wireless LAN Parameters hierarchy and set the Access Point Functionality to Enabled.
- 5. Click OK and save your project.

To switch to a scenario, choose Switch to Scenario from the Scenarios menu or just press Ctrl+<scenario number>

- 14.4.5.3. The DCF\_PCF\_Frag Scenario:
  - Switch to the DCF Frag scenario, select Duplicate Scenario from the Scenarios 1. menu and give it the name DCF\_PCF\_Frag  $\Rightarrow$  Click OK  $\Rightarrow$  Save your project.
  - Select node 0, node 1, node 3, node 5, and node 7 in the DCF PCF Frag 2. scenario simultaneously (click on these nodes of them white holding the Shift key)  $\Rightarrow$  Right-click on anyone of the selected nodes  $\Rightarrow$  Edit Attributes.
  - 3. Check Apply Changes to Selected Objects  $\Rightarrow$  Expand the hierarchy of the Wireless LAN Parameters attribute  $\Rightarrow$  Expand the hierarchy of the PCF **Parameters** attribute  $\Rightarrow$  Enable the **PCF Functionality** attribute  $\Rightarrow$  Click **OK**.
  - 4. Right-click on node 0.  $\Rightarrow$  Edit Attributes  $\Rightarrow$  Expand the Wireless LAN Parameters hierarchy and set the Access Point Functionality to Enabled. network simulation experiments manual.doc utorak, 28. rujan 2010 167

5. Click OK and save your project.

#### 14.4.6. Run the Simulation

To run the simulation for the four scenarios simultaneously:

- 1. Go to the Scenarios menu  $\Rightarrow$  Select Manage Scenarios
- 2. Click on the row of each scenario and click the **Collect Results** button. This should change the values under the **Results** column to <**collect**> as shown.

Pro	ject Name: Vireless	LAN	Sector Conserve Co		
#	Scenario Name	Saved	Results ¥	Sim Duration	Time Units
1	DCF	saved	<collect></collect>	10	minute(s)
2	DCF_Frag	saved	<collect></collect>	10	minute(s)
3	DCF_PCF	saved	<collect></collect>	10	minute(s)
4	DCF_PCF_Frag	saved	<collect></collect>	10	minute(s)

- 3. Click **OK** to run the four simulations. Depending on the speed of your processor, this may take several seconds to complete.
- 4. After the simulation of the four scenarios complete, click **Close** and then save your project.

#### 14.4.7. View the Results

To view and analyze the Results (*Note:* Actual results will vary slightly based on the actual node positioning in the project):

- 1. Select Compare Results from the Result menu.
- 2. Change the drop-down menu in the lower-right part of the *Compare Results* dialog box from As Is to time\_average ⇒ Select the Delay (sec) statistic from the Wireless LAN hierarchy as shown.

Compare Results				- 🗆 🗙
Discrete Event Graphs Displayed	Panel Graphs	*		
Global Statistics Wireless LAN Load (bits/sec) Throughput (bits/sec) Object Statistics Office Network	300 200 100 0	SW		E00
	Overlaid Stat	istics 💽 All Sc : 🗲	xenarios 🗙	]
Results Generated: 08:36:40 Jul 01	2007	Unselect	Add	Show
				Close

**time\_average** is the average value over time of the values generated during the collection window. This average is performed assuming a "sample and hold" behavior of the data set (i.e., each value is weighted by the amount of time separating it from the following update and the sum of all the weighted values is divided by the width of the collection window),

3. Click **Show** to show the result in a new panel. The resulting graph should resemble the shown one.



**Delay** represents the end-to-end delay of all the packets received by the wireless LAN MACs of all WLAN nodes in the network and forwarded to the higher layer. The delay includes medium access delay at the source MAC, reception of all the fragments individually, and transfer of the frames via AP, if access point functionality is enabled.

4. Go to the *Compare Results* dialog box ⇒ Follow the same procedure to show the graphs of the following statistics from the Wireless LAN hierarchy: Load (bits/sec) and Throughput (bits/sec). The resulting graphs should resemble the following ones.



**Load** represents the total load (in bits/sec) submitted to wireless LAN layers by all other WLAN nodes of the network. The statistic does not include the bits of the higher layer packets that are dropped by WLAN MACs upon arrival and not considered for transmission due to, for example, insufficient space left on the higher layer packet buffer of the MAC.



**Throughput** represents the total number of bits (in bits/sec) forwarded from wireless LAN layers to higher layers in all WLAN nodes of the network.

5. Go to the *Compare Results* dialog box ⇒ Expand the **Object Statistics** hierarchy ⇒ Expand the **Office Network** hierarchy ⇒ Expand the hierarchy of two nodes. One node should have PCF enabled in the DCF\_PCF scenario (e.g., node\_3) and the other node should have PCF disabled (e.g., node\_2) ⇒ Show the result of the **Delay (sec)** statistic for the chosen nodes. The resulting graphs should resemble the following ones.



6. Repeat step 5 above but for the **Retransmission Attempts (packets)** statistic. The resulting graphs should resemble the following ones.



7. Close a graphs and the *Compare Results* dialog box  $\Rightarrow$  Save your project.

#### 14.5. *Further readings*

- ANSI/IEEE Standard 802.11, 1999 Edition: <u>Wireless LAN Medium Access Control</u> (MAC) and Physical Layer (PHY) Specifications.
- 14.6. *Exercises* 
  - 1) Based on the definition of the statistic **Load**, explain why with PCF enabled the load is lower than if DCF is used without PCF.
  - 2) Analyze the graphs that compare the **Delay** and **Throughput** of the four scenarios. What are the effect of utilizing PCF and fragmentation on these two statistics?
  - 3) From the last four graphs, explain how the performance of a node without PCF is affected by having PCF enabled in other nodes in the network.
  - 4) Create two new scenarios as duplicates of the DCF\_PCF scenario. Name the first new scenario DCF\_allPCF and the second new scenario DCF\_twoPCF. In DCF\_allPCF, enable the PCF attribute in all 8 nodes: node\_1 through node\_8 (Note: do not include node\_0 in any of your attribute editing). In DCF\_twoPCF, disable the PCF attribute in node\_3 and node\_5 (this will leave only node\_1 and node\_7 with PCF enabled). Generate the graphs for the Delay, Load, and Throughput statistics and explain how the number of PCF nodes might affect the performance of the wireless network.
  - 5) For all scenarios, select the Media Access Delay statistic from the Global Statistics → Wireless LAN hierarchy. Re-run the simulation for all scenarios. Generate the graph that compares the Media Access Delay statistic of all scenarios. Analyze the graph explaining the effect of PCF, fragmentation, and number of PCF nodes on media access delay.

#### 14.7. Lab Report

Prepare a report that follows the guidelines explained in Lab 0. The report should include the answers to the above exercises as well as the graphs you generated from the simulation scenarios. Discuss the results you obtained and compare these results with your expectations. Mention any anomalies or unexplained behaviors.

# **15.** Laboratory - Mobile Wireless Network (A Wireless Local Area Network with Mobile Stations)

#### 15.1. Objective

This lab simulates mobility in wireless local area network. The effect of mobility on the TCP performance is studied. In addition, the lab studies how the request to send (RTS) and clear to send (CTS) frames are utilized in avoiding the hidden node problem usually induced by mobility in WLAN.

#### 15.2. Overview

One of the requirements of the IEEE 802.11 standard is to handle mobile stations in wireless local area networks. Mobile stations are defined as the stations that access the LAN while in motion. IEEE 802.11 handles station mobility within the MAC sublayer and hence such mobility is hidden from the higher layers in the network. However the disconnection and reconnection events induced by mobility in WLAN significantly affect the performance of higher layer protocols such as TCP. For example TCP interprets disconnection due to mobility as congestion and hence it multiplicatively decreases its congestion window size. After reconnection, TCP takes unnecessary longer time to recover the congestion window to a size that matches the available bandwidth.

IEEE 802.11 utilizes the request to send (RTS) and clear to send (CTS) frames in various circumstances to further minimize collisions. RTS and CTS are especially useful in solving the hidden node problem in WLANs that have mobile stations. Exchanging the RTS and CTS between the sender and the receiver informs nearby stations that a transmission is about to begin. Duration information in RTS/CTS frames are used to set the network allocation vector (NAV) in all stations that are within the reception range of the RTS/CTS frames. This way the problem of a hidden sender can be solved as any station that sees the CTS frame knows that it is close to the receiver, and therefore cannot transmit for the period of time indicated in the NAV. If transmitted data frames are short, sending RTS/CTS frames is not recommended as it adds overhead inefficiency. Therefore, a threshold is defined to use RTS/CTS only on frames longer than a specified length.

In this lab we will simulate a wireless LAN with mobile workstations and server. The workstations will run an FTP application to upload files to the server. We will study the effect of node mobility on the performance of the TCP connection for the FTP session. We will study also the role of the request to send (RTS) and clear to send (CTS) frames in avoiding the hidden node problem usually induced by mobility in wireless LAN.

#### 15.3. *Prelab Activities*

- Read sections 2.8.2 and 4.2.5 from "Computer Networks: A Systems Approach" 4th Edition.
  - Wireless Network and Multiple Access with Collision Avoidance

#### 15.4. *Procedure*

#### 15.4.1. Create a New Project

1. Start **OPNET IT Guru Academic Edition**  $\Rightarrow$  Choose **New** from the **File** menu.

- 2. Select **Project** and Click **OK** ⇒ Name the project **<your initials>\_MobileWLAN** and the scenario **Mobile\_noRTSCTS** ⇒ Click **OK**.
- 3. In the Startup Wizard: Initial Topology dialog box, make sure that Create Empty Scenario is selected ⇒ Click Next ⇒ Select Campus from the Network Scale list ⇒ Click Next ⇒ Make sure that Kilometer is the unit chosen for the Size and then assign 2 and 1 to the X Span and Y Span respectively ⇒ Click Next twice ⇒ Click OK.

#### 15.4.2. Create and Configure the Network

- 15.4.2.1. Initialize the Network:
  - 1. The Object Palette dialog box should now be on the top of your project space. If

it is not there, open it by clicking . Make sure that the wireless\_lan is selected from the pull-down menu on the object palette.

- 2. Add to the project workspace the following objects from the palette: Application Config, Profile Config, two wlan\_wkstn (mob), and one wlan\_server (mob).
  - a. To add an object from a palette, click its icon in the object palette ⇒ Move your mouse to the workspace ⇒ Click to drop the object in the desired location ⇒ Right-click to finish creating objects of that type.
- 3. Close the palette.
- 4. Arrange and rename the objects you added as shown:



- 5. Position the workstations and the server according to the x and y positions shown in the following table:
  - a. To position an object: Right-click on the object  $\Rightarrow$  Advanced Edit Attributes  $\Rightarrow$  Edit the x position and y position attributes.

Node	x position	y position
ClientA	1.25	0.5
FTP_Server	1.5	0.5
ClientB	1.75	0.5

0% for the "Command Mix (Get/Total)" attribute means all the FTP sessions will be only "Serial" from the clients to the server.

#### 15.4.2.2. Configure the Applications:

- Right-click on the Applications node ⇒ Edit Attributes ⇒ Expand the Application Definitions attribute and set rows to 1 ⇒ Expand the new row ⇒ Name the row FTP\_Application.
  - i. Expand the **Description** hierarchy ⇒ Edit the FTP row as shown (you will need to set the **Special Value** to **Not Used** while editing the shown attributes):

(Ftp) Table	- <b>D</b> ×	"Inter-Request	Time" Spec 🗙
Attribute Command Mix (Get/Total) Inter-Request Time (seconds) File Size (bytes) Symbolic Server Name Type of Service RSVP Parameters Back-End Custom Application	Value 0% constant (3600) constant (15000000) FTP Server Best Effort (0) None Not Used	Distribution Name: Mean Outcome: Second Argument: Special Value:	constant       3600       Not Used       Not Used
Details Promote		Help	<u>Cancel</u> <u>QK</u>

2. Click OK twice and then save your project.

#### 15.4.2.3. Configure the Profiles:

- 1. Right-click on the **Profiles** node  $\Rightarrow$  **Edit** Attributes  $\Rightarrow$  Expand the **Profile Configuration** attribute and set rows to 1.
  - i. Name and set the attributes of **row 0** as shown  $\Rightarrow$  Click **OK**.

Type: Utilities			
Attribute	Value		
⑦ ⊢ name	Profiles		
	Profile Config		
Profile Configuration	()		
	1		
jŹrow 0			
⑦ / ⊢Profile Name	FTP_Profile		100
Applications	()		
	1		
⊡row 0			1980
P Hame	FTP_Application		
Start Time Offset	constant (5)	/	
In A Duration (seconds)	End of Profile	/	
Repeatability	Once at Start Time		
Operation Mode	Serial (Ordered)		
Start Time (seconds)	constant (55)		
Duration (seconds)	End of Simulation		
⑦	Once at Start Filme		•
Apply Changes to Selected Obj	ects	No State So	Advanced
Find Next	er anter tors a str	Cancel	ОК

- 15.4.2.4. Configure the Applications in the Server and Clients:
  - 1. Right-click on the **FTP\_Server** node  $\Rightarrow$  **Edit Attributes**:
    - i. Edit the Server Address attribute  $\Rightarrow$  Assign the value FTP\_Server to it.
    - ii. Edit Application: Supported Services  $\Rightarrow$  Set rows to  $1 \Rightarrow$  Set Name to FTP\_Application  $\Rightarrow$  Click OK twice.

Name		Description		<u>.</u>
FTP_Application	1	Supported		
	Name star, s tiget blige, gereiertsgage i d	a dia ang ang ang ang ang ang ang ang ang an	si dar na garan para mala ina na manana da karar	<u>,                                    </u>
				COM AS CONTRACT AND A COMPANY AND A
1				<u> し</u>
1 Rows	;)eete	imsort	Orgalicate	Move ti

- Select both ClientA and ClientB in the network simultaneously (click on both of them while holding the Shift key) ⇒ Right-click on one of them ⇒ Edit Attributes ⇒ Check the Apply Changes to Selected Objects check box:
  - i. Expand the Application: Supported Profiles hierarchy  $\Rightarrow$  Set rows to  $1 \Rightarrow$  Set Profile Name to FTP\_Profile as shown  $\Rightarrow$  Click OK.

+ (Applicatio	on: Supporte	d Profiles)	Table	
Profile Name				<b>A</b>
FTP_Profile				
4				ٽ ب
1 Rows	Delete	Insert	Duplicate	Move Up
Details	Promote		Cancel	OK

ii. Edit the Application: Destination Preferences attribute as follows:

Set rows to  $1 \Rightarrow$  Set Symbolic Name to FTP Server  $\Rightarrow$  Edit Actual Name  $\Rightarrow$  Set rows to  $1 \Rightarrow$  In the new row, assign FTP\_Server to the Name column.

- 3. Click **OK** three times and then save your project.
- 15.4.2.5. Configure the Trajectory:
  - 1. Right-click on ClientA  $\Rightarrow$  Edit Attributes  $\Rightarrow$  Assign trajectory\_1 to the trajectory attribute  $\Rightarrow$  Click OK.
  - 2. A green trajectory will appear on the project workspace. Right-click on that trajectory and select Edit Trajectory.
  - 3. In the Edit Trajectory *Information* dialog box, name the trajectory <your initials>\_left\_trajectory ⇒ Click OK.
  - 4. From the Edit menu, choose Preferences. Check the value of the mod\_dirs attribute. A list of directories will appear. The first directory in the list is where a trajectory file with the name <your initials>\_left\_trajectory.trj is saved. Edit that file using any text editor (e.g., Notepad). Replace all the contents of the file with the info shown in the following figure then save and close the text editor.

Version: 2 Position_Unit: Ki Altitude_Unit: Me Coordinate_Method Altitude_Method: locale: English_U Coordinate_Count:	lometers ters : relative absolute nited States.1252 6				
X Position	Y Position	Altitude	Traverse Time	Wait Time	
0	,0	,0	,0h0m0.00s	,0h2m0.00s	
-0.75	, 0	, 0	,0h0m20.97s	,0h1m0.00s	
-0.75	,0.02	, 0	,0h0m2.24s	,0h0m0.00s	
-1	.0.02	,0	,0h0m6.99s	,0h0m0.00s	
-1	,0.04	.0	,0h0m2.24s	,0h0m30.00s	
0	,0.04	, 0	,0h0m27.96s	,0h0m0.00s	

- 5. Right-click on ClientA ⇒ Edit Attributes ⇒ Assign <your initials>\_left\_trajectory to the trajectory attribute ⇒ Click OK.
- 6. The new trajectory should look exactly like the following one. Right-click on the trajectory and select Edit Trajectory.



7. In the *Edit Trajectory* Information dialog box, verify that the trajectory info matches the values shown in the following figure:

*Note:* that the trajectory makes **ClientA** start moving after 2 minutes from the beginning of the simulation. **ClientA** waits at X Pos 0.5 for 1 minute and at X Pos 0.25 for 20 seconds.

Traj	ectory Name	eha_left_traje	ctory						
#	X Pos (km)	Y Pos (km)	Distance (m)	Altitude	Traverse Time	Ground Speed	Wait Time	Accum Time	
1	0.0	0.0	n/a	0.0	n/a	n/a	0h2m0.00s	0h2m0.00s	
2	-0.75	0.0	750	0.0	0h0m20.97s	80	0h1m0.00s	0h3m20.97s	- 22
3	-0.75	0.02	20	0.0	0h0m2.24s	20	0h0m0.00s	0h3m23.21s	
4	-1.0	0.02	250	0.0	0h0m6.99s	80	0h0m0.00s	0h3m30.20s	22
5	-1.0	0.04	20	0.0	0h0m2 24s	20	0h0m30.00s	0h4m2 44s	
6	00	0.04	1,000	0.0	0h0m27.96s	80	0h0m0.00s	0h4m30.40s	
-0	oordi <u>n</u> ates are	relative to ob	ject's position	12.25	Sale Series	(	Ground speed	is in mi/hr	-
						1	Ntitude is in	neter(s)	-
	Insert	Delete	Redefine	1			Cancel	ОК	2013

#### 8. Click OK and then save your project.

The **trajectory** attribute specifies the name of an ASCII trajectory file that specifies the time and locations that a mobile node will pass through as the simulation progresses.

#### 15.4.3. Configure the Simulation

Here we will configure the simulation parameters:

- 1. Click on and the *Configure Simulation* window should appear.
- 2. Assign **10.0 minutes** to the **Duration** attribute.
- 3. Assign **256** to the **Seed** attribute.
- 4. Click **OK** and then save your project.



The **Seed** attribute is an integer that is used by the simulation's random number generator. Its default value is 128.

#### 15.4.4. Choose the Statistics

To test the performance of our mobile wireless network we will collect some of the available statistics as follows:

- 1. Right-click anywhere in the project workspace and select **Choose Individual Statistics** from the pop-up menu.
- 2. In the *Choose Results* dialog box, Expand the Node Statistics hierarchy  $\Rightarrow$  choose the shown three statistics.
- Right-click on the Congestion Window Size (bytes) statistic ⇒ Choose Change Collection Mode ⇒ In the dialog box check Advanced ⇒ From the drop-down menu, assign all values to Capture mode as shown ⇒ Click OK.

Capture mode	all values 💌
<b>G</b> Every	seconds
CEvery	values
C Lotal of	values
Bucket mode	max value
Reset	
Advanced	
Advanced	Cancel C



- 4. Right-click on the **Traffic Received** (bytes) statistic. ⇒ Choose **Change Collection Mode**. ⇒ In the dialog box check **Advanced**. ⇒ From the drop-down menu, assign **all values** to **Capture mode**.
- 5. Click OK twice and then save your project.

#### 15.4.5. Duplicate the Scenario

We will create one more scenarios to utilize the request to send (RTS) and clear to send (CTS) frames to study their effect on minimizing collisions.

- 1. Select **Duplicate Scenario** from the **Scenarios** menu and give it the name **Mobile\_RTSCTS** ⇒ Click **OK**.
- Select ClientA, FTP\_server, and ClientB simultaneously (click on all of them while holding the Shift key). ⇒ Right-click on anyone of them. ⇒ Edit Attributes ⇒ Check the Apply Changes to Selected Objects check box.
- 3. Expand the hierarchy of the Wireless LAN Parameters attribute. ⇒ Assign the value 256 to the Rts Threshold (bytes) attribute.

Туре	e: server		
A	Attribute	Value	
1	Wireless LAN MAC Address	Auto Assigned	1
00	Wireless LAN Parameters	()	10
۲	Rts Threshold (bytes)	256 🔶	
۲	Fragmentation Threshol	None	100
1	-Data Rate (bps)	1 Mbps	
۲	-Physical Characteristics	Frequency Hopping	1
۲	-Packet Reception-Powe	7.33 E-14	
۲	- Short Retry Limit	7	12
۲	Long Retry Limit	4	-
A	pply Changes to Selected Obj	ects 🔶	Advanced
	Eind Novt	Cancel 1	OK

4. Click **OK** and then save your project.

#### 15.4.6. Run the Simulation

To run the simulation for both scenarios simultaneously:

- 1. Go to the Scenarios menu.  $\Rightarrow$  Select Manage Scenarios.
- 2. Click on the row of each scenario and click the **Collect Results** button. This should change the values under the **Results** column to <**collect**> as shown.

Proj	ect Name:	MobileWLAN		+			
#	Scenari	o Name	Saved	Results	Sim Duration	Time Units	
1	Mobile_n	ORTSCTS	saved	<collect></collect>	10	minute(s)	
2	Mobile_F	RTSCTS	saved	<collect></collect>	10	minute(s)	-1

- 3. Click **OK** to run both simulations. Depending on the speed of your processor, this may take several seconds to complete.
- 4. After the simulation of both scenarios complete, click **Close** and then save your project.

#### 15.4.7. View the Results

To view and analyze the results (*Note:* Actual results will vary slightly based on the actual node positioning in the project):

- 1. Select **Compare Results** from the **Result** menu.
- 2. Select the **Congestion Window Size (bytes)** statistic for **ClientA** from the **TCP Connection** hierarchy as shown.

Discrete Event Graphs Displayed Pan	el Graphs			SCHARE
Global Statistics Object Statistics Campus Network CI ClientA CI TCP Connection	<ul> <li>Show Preview</li> <li>200,000</li> <li>100,000</li> </ul>	4		
Congestion Window Si. Traffic Received (bytes)		40	)	800 time (sec)
Congestion Window St. Traffic Received (bytes)	0 0 0 Overlaid Statistics	400	) arios	800 time (sec)

- 3. Click **Show** to show the result in a new panel.
- 4. Repeat the above steps for the following statistics:
  - a. Congestion Windows of ClientB;
  - b. Load for ClientA and
  - c. Load for ClientB.

The resulting graphs should resemble the following graphs.





- Go back to the *Compare Results* dialog box ⇒ Expand the TCP Connection hierarchy for the FTP server ⇒ Select the Traffic Received (bytes) - Conn 1 statistic ⇒ Select sample\_sum to replace As Is as shown in the following figure ⇒ Click Show.
- 6. Repeat the above step for the Traffic Received (bytes)-Conn 2 statistic.



7. The resulting graphs should resemble the following graphs.



#### 15.5. Further readings

- <u>ANSI/IEEE Standard 802.11, 1999 Edition</u>: <u>Wireless LAN Medium Access Control</u> (MAC) and Physical Layer (PHY) Specifications.
- Transmission Control Protocol: IETF RFC number 793 (www.ietf.org/rfc.html).

#### 15.6. Exercises

- 1) Explain how Load and Congestion Window Size are affected by the mobility of ClientA.
- 2) Explain how enabling RTS/CTS helps in avoiding the hidden node problem and hence explain the effect of RTS/CTS frames on the network performance.
- 3) The graphs show that the server terminates the FTP session with **ClientA** earlier if RTS/CTS is enabled. On the other hand, the server terminates the FTP session with **ClientB** later if RTS/CTS is enabled. Explain why.
- 4) Create a new scenario as a duplicate of the Mobile\_noRTSCTS scenario. Name the new scenario twoMobiles\_noRTSCTS. Create a second new scenario as a duplicate of the Mobile\_RTSCTS scenario. Name the second new scenario twoMobiles\_RTSCTS. In both new scenarios, edit the attribute of the FTP\_Server and assign <your initials>\_left\_trajectory to its trajectory attribute. Run the simulation for all scenarios and create the graphs for the Load (bits/sec), Congestion Window Size (bytes), and Traffic Received (bytes) statistic results as we did in this lab. Analyze the graphs explaining the effect of the server mobility on the network performance.

#### 15.7. Lab Report

Prepare a report that follows the guidelines explained in Lab 0. The report should include the answers to the above exercises as well as the graphs you generated from the simulation scenarios. Discuss the results you obtained and compare these results with your expectations. Mention any anomalies or unexplained behaviors.

#### NETWORK SIMULATION EXPERIMENTS MANUAL

# Prepared by Professor Emad Aboelela, University of Massachusetts/Dartmouth

Networking technologies and concepts are often difficult to explain, even through careful description and well thought out examples. One method for making this information "stick" is to create an environment where networking professionals and students can visualize how networks work by utilizing a software tool that simulates the functions within a network. The tool itself is highly useful in that it provides a virtual environment for an assortment of desirable features such as modeling a network based on specified criteria and predicting its performance.

The *Network Simulation Experiments Manual takes* this instructional tool a step further and provides detailed experiments on core networking topologies for use in this simulation environment. Various scenarios are presented within each topology: Review questions, a lab report, and exercises accompany each assignment as well. The manual also comes with directions for downloading the free and easy-to-install **OPNET IT Guru Academic Edition** software. This software provides a virtual environment for modeling, analyzing, and predicting the performance of IT infrastructures, including applications, servers, and networking technologies.

Prepared by Professor Emad Aboelela of the University of Massachusetts Dartmouth, the experiments in the manual are closely tied to the organization of *Computer Network: A Systems Approach, 4e,* and when used together, serve as a complete tool for understanding how and why computer networks function as they do.

#### **KEY FEATURES**

- Written by an instructor who has used OPNET simulation tools in his classroom for numerous demonstrations and real-world scenarios.
- Software download based on an award-winning product made by OPNET Technologies, Inc., whose software is used by thousands of commercial and government organizations worldwide, and by over 500 universities.
- Useful experimentation for professionals in the workplace who are interested in learning and demonstrating the capability of evaluating different commercial networking products, i.e., Cisco routers.
- Covers the core networking topologies and includes assignments on the ethernet, token rings, ATM, Switched LANs, Network Design, RIP, TCP, Queuing Disciplines, QoS, wireless, etc.

#### About the Author

Dr. Emad Aboelela received his Ph.D. in Computer Engineering from the University of Miami (Florida); M.Sc. and B.Sc. in Computer Science from Alexandria University (Egypt). Before joining the University of Massachusetts Dartmouth he taught at Southern Connecticut State University for two years, and prior to that worked at the University of Miami as a part-time professor and research assistant for five years during which time he received many awards including the Award of Academic Merit.

#### ELSEVIER



MORGAN KAUFMANN PUBLISHERS

#### AN IMPRINT OF ELSEVIER

#### www.mkp.com