

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

FEASIBILITY STUDY OF VOIP INTEGRATION INTO THE MYSEA ENVIRONMENT

by

Lily Tse

September 2005

Thesis Advisor: Co-advisor: Cynthia E. Irvine Thuy D. Nguyen

Approved for public release; distribution is unlimited

REPORT DOCUMENTATION PAGE Form Approved				l OMB No. 0704-0188		
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.						
1. AGENCY USE ONLY (Leave	blank)	2. REPORT DATE September 2005	3. REP	PORT TY	PE AND DATE Master's Thes	
 4. TITLE AND SUBTITLE: Fe MYSEA Environment 6. AUTHOR(S) Lily Tse 	easibili	ty Study of VoIP Integ	gration ir	nto the	5. FUNDING N	IUMBERS
7. PERFORMING ORGANIZAT Naval Postgraduate School Monterey, CA 93943-5000	TION N	AME(S) AND ADDRES	S(ES)		8. PERFORMI ORGANIZATI NUMBER	
				ING/MONITORING EPORT NUMBER		
11. SUPPLEMENTARY NOTES policy or position of the Departmer				hose of t	he author and do	not reflect the official
12a. DISTRIBUTION / AVAILABILITY STATEMENT 12b. DISTRIBUTION CODE Approved for public release; distribution is unlimited. 12b. DISTRIBUTION CODE						
13. ABSTRACT (maximum 200 words) Voice over Internet Protocol (VoIP) is becoming popular due to its low cost and the management advantages it offers over traditional PSTN phone systems. VoIP is widely implemented with H.323 and Session Initiation Protocol (SIP) standards. However, both protocols are poorly designed for networks with common security solutions such as firewalls and Network Address Translation (NAT). This project is a feasibility study of SIP-based VoIP integration into the Monterey Security Architecture (MYSEA), a multilevel secure environment that uses NAT as a security mechanism. A gathering of comparative studies on VoIP protocols was performed to guide the selection of SIP as the test protocol. A set of experiments was devised and conducted using SIP-based softphones for this study. The insights gained from the experiment provide useful insights to the MYSEA project concerning VoIP security.						
14. SUBJECT TERMS Voice over Internet Protocol, H.323, Session Initiation Protocol, Network 15. NUMBER OF Address Translation, Monterey Security Architecture PAGES 204						
16. P			16. PRICE CODE			
17. SECURITY CLASSIFICATION OF REPORT Unclassified NSN 7540-01-280-5500		CURITY SIFICATION OF THIS	G C	BSTRA	ICATION OF CT classified	20. LIMITATION OF ABSTRACT UL lard Form 298 (Rev. 2-89)

Prescribed by ANSI Std. 239-18

Approved for public release; distribution is unlimited

FEASIBILITY STUDY OF VOIP INTEGRATION INTO THE MYSEA ENVIRONMENT

Lily Tse Civilian, Naval Postgraduate School B.S., University of California, Davis, 2003

Submitted in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE

from the

NAVAL POSTGRADUATE SCHOOL September 2005

Author: Lily Tse

Approved by:

Cynthia E. Irvine Thesis Advisor

Thuy D. Nguyen Co-Advisor

Peter J. Denning Chairman, Department of Computer Science

ABSTRACT

Voice over Internet Protocol (VoIP) is becoming popular due to its low cost and the management advantages it offers over traditional PSTN phone systems. VoIP is widely implemented with H.323 and Session Initiation Protocol (SIP) standards. However, both protocols are poorly designed for networks with common security solutions such as firewalls and Network Address Translation (NAT).

This project is a feasibility study of SIP-based VoIP integration into the Monterey Security Architecture (MYSEA), a multilevel secure environment that uses NAT as a security mechanism. A gathering of comparative studies on VoIP protocols was performed to guide the selection of SIP as the test protocol. A set of experiments was devised and conducted using SIP-based softphones for this study. The insights gained from the experiments provide useful insights to the MYSEA project concerning VoIP security.

TABLE OF CONTENTS

I.	INT	RODUCT	ION	1
	А.	MOTI	VATION	1
	В.	PURP (OSE OF STUDY	1
	C.	ORGA	NIZATION OF PAPER	1
II.	BAC	KGROU	ND	3
	А.	INTRO	DUCTION	3
		1.	Advantages of VoIP	3
			a. Efficient Use of Bandwidth	3
			b. Reduction or Possibly Elimination of Long Distance and	
			Phone Charges	4
			c. Convergence of Voice and Data Networks	
			d. Advanced Features	
		2.	Disadvantages of VoIP	
			a. Quality of Voice	
			b. Security	
			c. Availability	5
			d. 911	5
	В.	VOIP	OVERVIEW	5
		1.	VoIP Phone Overview	6
	C.	VOIP S	SERVICES	7
		1.	Encoding	8
		2.	Transport	8
		3.	Gateway Control	8
	D.	VOIP	PROTOCOLS	8
		1.	H.323	9
		2.	Session Initiation Protocol	9
		3.	MGCP	9
		4.	Megaco/H.248	10
	Е.	VOIP	CHALLENGES	10
		1.	Quality of Service	10
		2.	Security	10
	F.			
		1.	netfilter/iptables	13
		2.	SIP with NAT	13
	G.	MYSE	A OVERVIEW	14
	H.	SUMM	[ARY	15
III.	TEC	HNICAL	COMPARISON BETWEEN H.323 AND SIP	17
	А.		AND SIP OVERVIEW	
		1.	Background	17
		2.	Architecture	18

		3. Components	19
		4. Call Setup	
		a. H.323	20
		<i>b. SIP</i>	21
		5. Services	
	В.	H.323 AND SIP COMPARISON	
		1. Simplicity and Flexibility	
		a. Protocol Specification	
		b. Message Encoding	
		c. Protocol Interactions	24
		d. Applications	25
		2. Extensibility	
		a. Extensible Mechanisms	25
		b. Backward-Compatibility	26
		c. Interoperability	26
		3. Scalability	
		a. Protocol Design	26
		b. Servers	27
		c. Conferencing	27
		4. Security	
		a. H.323 Security - H.235	27
		b. SIP Security	28
		c. Security Comparison	28
		5. Conclusion	
	C.	SUMMARY	
IV.	TES	TING	
	A.	TEST METHODOLOGY	
	B .	TEST DESCRIPTION	
		1. Test 1: No NAT VoIP Configuration	
		2. Test 2: Single NAT VoIP Configuration	
		3. Test 3: Double NAT VoIP Configuration	
		4. Test 4: Extended Double NAT VoIP Configuration	
		5. Test 5: Extended Double NAT VoIP Configuration	on with
		Simultaneous VoIP Sessions	
		6. Test 6: MYSEA Configuration	
	C.	PROBLEMS ENCOUNTERED	
	D.	TEST RESULT	
	Е.	SUMMARY	
v.	ттт.	URE WORK AND CONCLUSIONS	13
v .	гот A.	FUTURE WORK	
	Α.		
		 Routing in MLS Server VoIP Conversations Initiated from the Internet 	
	B.	2. VolP Conversations initiated from the internet	
APP	ENDIX	XA. A SURVEY OF VOIP HARDPHONES AND SOFTPHONE	545

А.	HARDPHONES	45
В.	SOFTPHONES	46
APPENDIX I	B. TEST 1: NO NAT VOIP DEMONSTRATION USING SJPHO	ONE47
	C. TEST 2: SINGLE NAT VOIP DEMONSTRATION U	
	D. TEST 3: DOUBLE NAT VOIP DEMONSTRATION U	
	E. TEST 4: EXTENDED DOUBLE NAT VOIP DEMONSTRA G SJPHONE	
SIMU	F. TEST 5: EXTENDED DOUBLE NAT VOIP LTANEOUS VOIP SESSIONS DEMONSTRATION U	USING
APPENDIX (G. TEST 6: MYSEA VOIP CONFIGURATION	129
LIST OF RE	FERENCES	179
INITIAL DIS	STRIBUTION LIST	181

LIST OF FIGURES

Figure 1.	MYSEA Network Architecture [From Ref. 8]	15
Figure 2.	H.323 Protocol Stack [From Ref. 9]	
Figure 3.	SIP Protocol Stack [From Ref. 9]	
Figure 4.	Simple H.323 Call Setup	
Figure 5.	Simple SIP Call Setup	22
Figure 6.	Test 1: Physical and Logical Network Topology	32
Figure 7.	Test 2: Physical Network Topology (with and without firewall)	33
Figure 8.	Test 2: Logical Network Topology (with firewall)	34
Figure 9.	Test 3: Physical Network Topology	
Figure 10.	Test 3: Logical Network Topology	35
Figure 11.	Test 4: Physical Network Topology	36
Figure 12.	Test 4: Logical Network Topology	37
Figure 13.	Test 5: Physical Network Topology	38
Figure 14.	Test 5: Logical Network Topology	
Figure 15.	Test 6: Physical Network Topology	39
Figure 16.	Test 6: Logical Network Topology	40
Figure 17.	Test 1: Packet Capture on Client A	49
Figure 18.	Test 1: Packet Capture on Client B	50
Figure 19.	Test 2: Packet Capture on Client A (without firewall)	58
Figure 20.	Test 2: Packet Capture on Client B (without firewall)	59
Figure 21.	Test 2: Packet Capture on eth0 of NAT (without firewall)	60
Figure 22.	Test 2: Packet Capture on eth1 of NAT (without firewall)	61
Figure 23.	Test 2: Packet Capture on Client A (with firewall)	64
Figure 24.	Test 2: Packet Capture on Client B (with firewall)	65
Figure 25.	Test 2: Packet Capture on eth0 of NAT (with firewall)	66
Figure 26.	Test 2: Packet Capture on eth1 of NAT (with firewall)	67
Figure 27.	Test 3: Packet Capture on Client A	
Figure 28.	Test 3: Packet Capture on Client B	76
Figure 29.	Test 3: Packet Capture on eth0 of NAT 1	77
Figure 30.	Test 3: Packet Capture on eth1 of NAT 1	
Figure 31.	Test 3: Packet Capture on eth0 of NAT 2	
Figure 32.	Test 3: Packet Capture on eth1 of NAT 2	80
Figure 33.	Test 4: Packet Capture on Client A (Client B Calls Client A)	90
Figure 34.	Test 4: Packet Capture on Client B (Client B Calls Client A)	91
Figure 35.	Test 4: Packet Capture on eth1 of NAT 1 (Client B Calls Client A)	93
Figure 36.	Test 4: Packet Capture on eth0 of NAT 2 (Client B Calls Client A)	94
Figure 37.	Test 4: Packet Capture on eth1 of NAT 2 (Client B Calls Client A)	95
Figure 38.	Test 4: Packet Capture on Client A (Client C Calls Client A)	97
Figure 39.	Test 4: Packet Capture on Client C (Client C Calls Client A)	98
Figure 40.	Test 4: Packet Capture on eth0 of NAT 1 (Client C Calls Client A)	99
Figure 41.	Test 4: Packet Capture on eth1 of NAT 1 (Client C Calls Client A)	100

Figure 42.	Test 4: Packet Capture on eth0 of NAT 3 (Client C Calls Client A)101
Figure 43.	Test 4: Packet Capture on eth1 of NAT 3 (Client C Calls Client A)102
Figure 44.	Test 5: Packet Capture on Client A
Figure 45.	Test 5: Packet Capture on Client C
Figure 46.	Test 5: Packet Capture on eth0 of NAT 2
Figure 47.	Test 5: Packet Capture on eth1 of NAT 2
Figure 48.	Test 5: Packet Capture on eth0 of Router
Figure 49.	Test 5: Packet Capture on eth1 of Router
Figure 50.	Test 5: Packet Capture on eth2 of Router
Figure 51.	Test 5: Packet Capture on Client B
Figure 52.	Test 5: Packet Capture on Client D
Figure 53.	Test 5: Packet Capture on eth0 of NAT 3123
Figure 54.	Test 5: Packet Capture on eth1 of NAT 3124
Figure 55.	Test 5: Packet Capture on eth0 of NAT 1125
Figure 56.	Test 5: Packet Capture on eth1 of NAT 1126
Figure 57.	Test 6: Scenario 1 Packet Capture on Router (pinged from NAT 2), Part 1.137
Figure 58.	Test 6: Scenario 1 Packet Capture on Router (pinged from NAT 2), Part 2.138
Figure 59.	Test 6: Scenario 1 Packet Capture on NAT 1 (pinged from NAT 2)139
Figure 60.	Test 6: Scenario 1 Packet Capture on Router (pinged from Router), Part 1141
Figure 61.	Test 6: Scenario 1 Packet Capture on Router (pinged from Router), Part 2142
Figure 62.	Test 6: Scenario 1 Packet Capture on NAT 1 (pinged from Router)143
Figure 63.	Test 6: Scenario 2 Packet Capture on Router (pinged from NAT 2)148
Figure 64.	Test 6: Scenario 2 Packet Capture on NAT 1 (pinged from NAT 2), Part 1.149
Figure 65.	Test 6: Scenario 2 Packet Capture on NAT 1 (pinged from NAT 2), Part 2.150
Figure 66.	Test 6: Scenario 2 Packet Capture on NAT 1 (pinged from NAT 2), Part 3.151
Figure 67.	Test 6: Scenario 2 Packet Capture on NAT 1 (pinged from NAT 2), Part 4.152
Figure 68.	Test 6: Scenario 2 Packet Capture on Router (pinged from Router)154
Figure 69.	Test 6: Scenario 2 Packet Capture on NAT 1 (pinged from Router)155
Figure 70.	Test 6: Scenario 3 Packet Capture on Router (pinged from NAT 2)160
Figure 71.	Test 6: Scenario 3 Packet Capture on NAT 1 (pinged from NAT 2), Part 1.161
Figure 72.	Test 6: Scenario 3 Packet Capture on NAT 1 (pinged from NAT 2), Part 2.162
Figure 73.	Test 6: Scenario 3 Packet Capture on NAT 1 (pinged from NAT 2), Part 3.163
Figure 74.	Test 6: Scenario 3 Packet Capture on Router (pinged from Router)165
Figure 75.	Test 6: Scenario 3 Packet Capture on NAT 1 (pinged from Router)
Figure 76.	Test 6: Scenario 4 Packet Capture on Router (pinged from NAT 2), Part 1 .171
Figure 77.	Test 6: Scenario 4 Packet Capture on Router (pinged from NAT 2), Part 2.172
Figure 78.	Test 6: Scenario 4 Packet Capture on NAT 1 (pinged from NAT 2)
Figure 79.	Test 6: Scenario 4 Packet Capture on Router (pinged from Router), Part 1.175
Figure 80.	Test 6: Scenario 4 Packet Capture on Router (pinged from Router), Part 2.176
Figure 81.	Test 6: Scenario 4 Packet Capture on NAT 1 (pinged from Router)177

LIST OF TABLES

Hardphones	7
VoIP Protocols	9
SIP and H.323 components [From Ref. 9]	19
Basic Call Control Features	23
H.235 Security Profiles	
SIP Security Features	29
Summary of Hardphones	
Summary of Softphones	46
Test 6: Test Scenario Configurations	129
Test 6: Ping Operations	130
Test 6: Scenario 1 Result	136
Test 6: Scenario 2 Result	147
Test 6: Scenario 3 Result	159
Test 6: Scenario 4 Result	170
	VoIP Protocols SIP and H.323 components [From Ref. 9] Basic Call Control Features H.235 Security Profiles SIP Security Features Summary of Hardphones Summary of Softphones Test 6: Test Scenario Configurations Test 6: Ping Operations Test 6: Scenario 1 Result Test 6: Scenario 2 Result Test 6: Scenario 3 Result

ACRONYMS AND ABBREVIATIONS

AP	Access Point
ASN.1	Abstract Syntax Notation One
ATA	Analog Telephone Adapter
BES	Back End Service
CODEC	Coder-Decoder
DNAT	Destination Network Address Translation
DoD	Department of Defense
DoS	Denial of Service
GSM	Global System for Mobile Communication
IANA IETF IP IPsec IPv4 IPv6 ITU-T	Internet Assigned Numbers Authority Internet Engineering Task Force Internet Protocol Internet Protocol Security Internet Protocol version 4 Internet Protocol version 6 International Telecommunications Union – Telecommunications Standards Committee
LAN	Local Area Network
MEGACO	Media Gateway Control
MIME	Multipurpose Internet Mail Extensions
MGCP	Media Gateway Control Protocol
MCU	Multipoint Control Unit
MYSEA	Monterey Security Architecture
NAT	Network Address Translation
NIST	National Institute of Standards and Technology
PBX	Public Branch Exchange
PDA	Personal Digital Assistant
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RTCP	Real-time Control Protocol
RTP	Real-time Transport Protocol

SDP SIP S/MIME SNAT SS7	Session Description Protocol Session Initiation Protocol Secure/ Multipurpose Internet Mail Extensions Source Network Address Translation Signaling System 7
ТСР	Transmission Control Protocol
UDP	User Datagram Protocol
VoIP	Voice over Internet Protocol
WAN WEP WLAN	Wide Area Network Wired Equivalent Privacy Wireless Local Area Network

ACKNOWLEDGMENTS

I would like to thank my thesis advisors, Cynthia Irvine and Thuy Nguyen, for their support and guidance throughout the thesis process. I would also like to thank Jean Khosalim and Phil Hopfner for lending me a helpful hand during testing.

This material is based upon work supported by the National Science Foundation under Grant No. DUE-0114018 and the Office of Naval Research. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author and do not necessarily reflect the views of the National Science Foundation or the Office of Naval Research.

I. INTRODUCTION

A. MOTIVATION

Voice over Internet Protocol (VoIP) is becoming a popular technology. Currently, three million households use VoIP. It is estimated that the number will increase to twenty-seven million by the end of 2009 [1]. Furthermore, companies and public-sector organizations are expected to invest over nine hundred million dollars into the VoIP technology in 2005, an increase of more than two hundred million dollars compared to last year [2]. This indicates that VoIP continues to grow in popularity and remains a promising telecommunication technology that will gradually replace traditional PSTN phone systems.

Integration of VoIP capabilities into the existing MYSEA architecture is highly desirable for both economical and management reasons. Deploying VoIP greatly reduces the cost of making long distance calls from the MLS LAN to an external network such as the Internet. Management of telephone systems in the MLS LAN will also be simplified with the use of VoIP as rewiring phones for nomadic users is no longer needed. Thus, extending MYSEA to include VoIP is beneficial.

B. PURPOSE OF STUDY

This study is a preliminary step in integrating VoIP capabilities into the existing MYSEA architecture. The objective is to determine the feasibility of this integration. The current MYSEA environment has a number of NAT components that may make the integration of VoIP into the MLS environment difficult if not impossible. A set of experiments were devised and conducted to test if VoIP works with the NAT components in MYSEA.

C. ORGANIZATION OF PAPER

This paper is organized into five chapters and six appendices. A brief introduction is provided in Chapter I. Chapter II provides the background information related to this research study. A technical comparison between two popular VoIP protocols, H.323 and SIP, is presented in Chapter III. One of the two protocols will be selected for testing purposes. Chapter IV describes the test plan used to confirm the

feasibility of integrating VoIP capabilities into MYSEA. The problems encountered and results from each test are also discussed in this chapter. The last chapter or Chapter V talks about future work and conclusion.

Six appendices are also included in this paper. Appendix A has surveys of hard and softphones. Appendices B through F contain descriptions, instructions, and results of tests described in Chapter IV.

II. BACKGROUND

This chapter presents background information pertaining to this thesis study. It includes a high-level technical overview of the current VoIP technology. Finally, the MYSEA architecture is described in the last section.

A. INTRODUCTION

The traditional phone system has been evolving since the first voice transmission in 1876 using a ring-down circuit. Today, phone systems no longer run on an analog network, instead they use a digital network known as the Public Switched Telephone Network (PSTN). The PSTN greatly reduces the amount of noise inflicted by analog voice amplification during transmission and provides number of services, such as call waiting, call forwarding, three-way calling, call blocking, etc. Despite the benefits obtained from the PSTN, there are drawbacks to the system that motivated the VoIP solution.

1. Advantages of VoIP

VoIP has many advantages over the traditional PSTN phone systems. These include the efficient use of bandwidth, reduction or possible elimination of long distance and phone charges, convergence of the voice and data networks, and advanced features. Some of them will be discussed further below.

a. Efficient Use of Bandwidth

Bandwidth is a key performance measure of a network. It defines how many bits can be transmitted every second, which means the more bandwidth available, the more data can be sent in a given period of time.

PSTN phone system requires a minimum of 64-kbps of dedicated circuit between the two calling devices. The circuit is reserved for the entire duration of the call regardless of whether or not any data is in transmission. Hence, bandwidth is unnecessarily wasted. On the other hand, VoIP uses IP networks that have the flexibility to allocate bandwidth as needed and reserve the unallocated bandwidth for other data. Thus, the use of network bandwidth in VoIP is more efficient.

b. Reduction or Possibly Elimination of Long Distance and Phone Charges

The cost of a long distance call generally depends on two factors: duration and destination of call. Charges can accumulate when an enterprise or individual frequently makes this type of call. VoIP service providers have monthly flat-rate plans that offer unlimited or fixed-number of minutes to make calls, including long distance calls. These plans are much more economical than the traditional charge-by-minute service. Thus will greatly reduce or possibly eliminate the phone and long distance charges for individuals and enterprises that make frequent long distance phone calls.

c. Convergence of Voice and Data Networks

Traditionally, a voice network only transmits voice and a data network only carries data. This is no longer true. Data makes up major traffic on voice networks. Unlike data networks, voice networks are not efficient in carrying data due to its inflexible bandwidth allocation and limited bandwidth. Therefore, most enterprises maintain both networks.

However, in many cases, management and maintenance of two different networks has proved to be cumbersome and costly for enterprises. Upgrading the voice network equipment such as the Public Branch Exchanges (PBX) telephones burdens enterprise budgets. If VoIP is deployed, the voice network will no longer be needed and will leave the enterprise with only the data network.

d. Advanced Features

VoIP provides all the services of a traditional phone system including speed-dial, call waiting, busy signaling, caller-ID, etc. In addition, VoIP can interoperate with services traditional phone systems lack such as video-conferencing, instant messaging, email, click-to-dial, and directory service.

2. Disadvantages of VoIP

While more home users and businesses are in the transition to use VoIP, the technology does have shortcomings. These will be discussed in detail below.

a. Quality of Voice

Voice data traveling across an IP network is highly susceptible to delay and loss due to routing and network latency. Voice in analog form has to be converted and compressed into digital packets before transmission over an IP network. A compression method that aggressively minimizes the size of voice packets will deteriorate the quality of voice. As a result, the quality of voice using VoIP may be worse than that obtained from PSTN due to delay, loss, and compression of the information.

b. Security

In many cases, maintaining separate voice and data networks can be difficult and costly. Convergence of both networks simplifies management and greatly reduces cost. However, convergence leads to security problems. Voice will be vulnerable to the same attacks as other data traveling across an IP network. Attacks include interception, modification, spoofing, man-in-the-middle attacks and denial of service.

c. Availability

Making a VoIP call requires a connection to an IP network through properly configured network devices that are dependent on a stable electrical power supply. Power outage and connection problems will prevent an individual from making or receiving a VoIP call.

d. 911

Currently, none of the VoIP protocols provide information regarding the caller's physical location to the emergency operator. When the caller dials 911, there is no guarantee the call will be routed to the nearest 911 police station. At the same time, the 911 operator has no way of identifying the location of the caller.

B. VOIP OVERVIEW

VoIP uses IP or a packet-switched network as the data transmission vehicle. A VoIP system digitizes voice using an audio codec, divides the digitized voice into packets, and sends the packets over an IP network to the destination. All packets are routed without a guarantee that they will travel the same path. Unlike a PSTN call, no dedicated circuit is ever created for a VoIP call.

The exact process required to set up a VoIP call is dependent on the VoIP protocol. Two types of protocols are necessary to complete a VoIP call: signaling and media transport. A signaling protocol has the responsibility of establishing a session

between the call participants. A media transport protocol specifies the rules and formats of the actual voice packets. Currently, the Real Time Protocol is commonly used as the media transport protocol in VoIP. However, there is a wider variety of signaling protocols. VoIP protocols will be further discussed later in this chapter.

For PSTN systems, a phone number consisting of digits is used to locate a phone. A phone number in VoIP can be a regular PSTN phone number, an address, or an alias. The "phone number" ultimately is translated to a 32-bit or 128-bit IP address depending on whether IPv4 or IPv6 is used. Every VoIP signaling protocol must provide address resolution capability.

There are four general VoIP communication modes. They are Phone-to-Phone, Phone-to-PC, PC-to-Phone, and PC-to-PC.¹ Voice transmission is carried by both PSTN and IP networks under the first three modes. A VoIP service provider that interconnects the PSTN and VoIP networks is needed for the first three modes when a call originates from a PSTN network and arrives at a VoIP network or vice versa. Voice travels exclusively across the IP network in the fourth mode.

1. VoIP Phone Overview

VoIP phones generally fall into three categories: PSTN phones, hardphones, and softphones. A PSTN phone is the type of phone almost every household has and is connected to a phone jack using a telephone cable. Technically, a PSTN phone in itself is not a VoIP device, but it can be used to make VoIP calls with the use of a phone adapter known as the Analog Telephone Adapter (ATA) that converts voice from analog to digital form.

A hardphone, also commonly known as an IP phone, can look identical to a PSTN phone. It is an independent device that understands VoIP protocols. Unlike a PSTN phone, a hardphone does not require an external device such as an ATA to make VoIP calls. All it needs is an Internet connection. Table 1 lists various types of hardphones and their corresponding descriptions from [3].

¹ Phone refers to a traditional phone and PC refers to a personal computer.

Description/Characteristics
Has an Ethernet port
Connects directly to the IP network
Has IP interface on base stations
Has built-in WiFi transceivers
Connects to a WiFi base station
Same as WLAN/WiFi phones but can
also transfer calls to GSM network
Supports for both voice and video

Table 1. Hardphones

A softphone is a VoIP phone in the form of software. A softphone runs on a computing device such as a desktop, laptop, or PDA, and is typically Operating System dependent. This type of phone needs audio support such as speakers and microphones for communication purposes. Appendix A has a survey of hard and softphones.

C. VOIP SERVICES

The VoIP technology is made up of four distinct services: signaling, encoding, transport, and gateway control [4]. A signaling VoIP protocol establishes and manages a connection between the endpoints when a call is made. Signaling protocols are discussed in Section D. When the conversation takes place, voice has to be encoded before it is transmitted over the IP network. The encoded voice packets will then be transported via the IP network to the destination. A gateway may be needed to convert voice into another format suitable for the receiving network. For example, a gateway will convert voice from digital PSTN to digital IP form when voice packets come into an IP network form a PSTN network.

1. Encoding

Voice, in its native form, cannot be transmitted over an IP network. A voice codec is used to convert voice from analog to digital data or digital to analog data, compress voice to optimize bandwidth usage, and packetize the voice data in preparation for transmission. A codec determines bandwidth usage and quality of voice. Higher quality voice transmission usually requires more bandwidth. The tradeoff between the two factors is critical when deciding what codec to use in VoIP applications. Various codecs exist to support VoIP. However, the three most commonly used codecs are G.711, G.723.1, and G.729A. More information on the above codec specifications can be found on the ITU-T website.

2. Transport

Media transport protocols such as Real Time Protocol (RTP) deliver the encoded voice packets over an IP network. RTP is a standard developed by Internet Engineering Task Force (IETF) to transport real-time audio and video data. RTP does not guarantee reliable transmission of packets. It usually runs on top of UDP due to the delay-intolerance of voice conversation and uses a dynamically assigned UDP port in the range 1024 – 65535.

The RTP Control Protocol (RTCP) is the control counterpart of RTP. RTCP, also developed by IETF, is not required to be used with RTP. However, RTCP can be used to monitor transmission performance. End users in a VoIP session can send transmission statistics in RTCP packets upon receiving packets. This information is useful to determine network and delivery performances and keep track of retransmission needs. Similar to RTP, RTCP uses a dynamically assigned UDP port.

3. Gateway Control

A gateway connects the PSTN and VoIP networks. Voice packets arriving at its IP interface will be converted by the gateway from a format understandable by IP to one that is understandable by PSTN and vice versa. A gateway is necessary for communications between Phone-to-Phone, Phone-to-PC and PC-to-Phone.

D. VOIP PROTOCOLS

Table 2 lists some well-known VoIP signaling protocols. A VoIP signaling protocol defines the formats of VoIP messages and rules for message exchange necessary

to establish a VoIP call. The signaling protocol is responsible for setting up a VoIP call, which includes tasks like locating users and negotiating session parameters between the two end devices. A media gateway control protocol control communication amongst the gateways in an IP networks.

Protocol	Organization	Туре
Н.323	ITU-T	Signaling
Session Initiation Protocol (SIP)	IETF	Signaling
MGCP	ITU-T	Signaling
Megaco/H.248	ITU-T/IETF	Signaling

Table 2.VoIP Protocols

1. H.323

H.323 is an open standard developed by ITU-T in 1996. H.323 was originally designed for multimedia conferencing and was later extended to support VoIP. H.323 is a suite of protocols that provide services such as end-to-end multipoint conferencing, audio and video codecs, management and accounting, and security. Since 1996, the protocol has undergone a series of changes, with the latest version (H.323v4) providing many enhanced feature and services. Refer to Chapter III for more details.

2. Session Initiation Protocol

The Session Initiation Protocol is developed by IETF. It is an application protocol designed to establish a two-way communication session. SIP is gaining popularity in the VoIP market despite the fact that it is a fairly young protocol developed in 1998. SIP is generally more scalable, simple, and extensible than H.323. Some believe that SIP will eventually become the official VoIP signaling protocol standard. Refer to Chapter III for more details.

3. MGCP

Media Gateway Control Protocol (MGCP), developed by IETF, controls communication among VoIP gateways in an IP network. Two components exist in the MGCP architecture: call agents, also known as media gateway controller, and gateways.

MGCP is a master-slave protocol in which the master call agent sends signaling, control, and processing commands to the gateway. The gateway acts as a slave and executes the commands sent by the call agent. MGCP does not replace SIP or H.323. Rather, the protocol is used to manage signaling and control activities for VoIP network gateways such as H.323, SIP, and SS7 signaling.

4. Megaco/H.248

Megaco/H.248, developed jointly by ITU-T and IETF, has the same architecture as MGCP. However, Megaco/H.248 offers several advantages over MGCP such as the support of multimedia and multipoint conferencing enhanced services, improved syntax for more efficient semantic message processing, TCP and UDP transport options, support for both text and binary encoding, and formalized extension process for enhanced functionality [5].

E. VOIP CHALLENGES

1. Quality of Service

Quality of Service (QoS) is not a major concern in PSTN systems because a fixed amount of bandwidth is dedicated to a call and transmission of voice follows the same circuit for the duration of the call. On the other hand, when a VoIP call is made, digitized voice will be transmitted using an IP network that has no fixed-bandwidth allocation mechanism. Thus, it is subject to jitter, latency, and packet loss problems, of which VoIP is intolerant.

There are many good reasons to deploy VoIP, however, it makes no sense to use VoIP if the quality of a VoIP call is lower than a traditional PSTN phone call. QoS must be addressed to an acceptable level such that end users can carry on a smooth conversation with minimal interruptions

2. Security

Security is another important aspect of VoIP. Convergence of voice and data networks means that both voice and data have to be protected. Eavesdropping a pure PSTN phone conversation is more difficult than a VoIP conversation, because interception of a regular PSTN call requires physical access to the phone lines or compromise of the corporate PBX. On the other hand, a VoIP conversation can be intercepted by an adversary anywhere along the path where the digitized voice packets travel. The security problem is intensified when sensitive personal information such as social security and credit card numbers are given out over a VoIP call.

The transmission of voice over an IP network is subject to security risks. It is important to ensure the confidentiality, integrity, and authenticity of a VoIP conversation and availability of resources when a VoIP call needs to be placed. In summary, the conversation and the VoIP network resources are the two main assets that require protection. Security mechanisms must be used to prevent both internal and external eavesdropping, spoofing, replay, and denial of service attacks. Many security mechanisms such as encryption, firewalls, and Network Address Translation (NAT) exist to address these threats. However, almost every one of them raises problems or affects the overall performance of a VoIP in some ways.

Encryption effectively protects the confidentiality and possibly authenticity of VoIP packets by making it impossible for people other than the intended recipient to read the packets. However, encrypting every packet, at the sending end and decrypting it at intermediate nodes and at the receiving end could cause an immense amount of delay, thus lowering the QoS. The size of an encrypted packet is often bigger than the plaintext packet, thus requiring more bandwidth and leading to a possibility of packet drop. This is a typical tradeoff between security and performance.

A firewall is often the first layer of defense in securing a network. It sits between the internal and external network, inspects every incoming and outgoing packet, and blocks those packets that it thinks is malicious. Firewalls usually inspect packets by examining certain fields, such as IP addresses, ports, and protocol type, in the packet headers. However, some VoIP protocols such as H.323 use dynamic ports to send or receive messages. A stateless firewall that only looks at header information to determine packet admissibility might drop some of the messages. To ensure the admission of those messages, the stateless firewall would have to open many ports and leave itself in a vulnerable statue. A stateful firewall, one that stores information about a session along with previous packet transactions, can inspect a packet's application layer data and can manage the dynamic port problem. However, a stateful firewall introduces latency due to the extensive packet inspection. As a result, network performance may not be optimal. Network Address Translation (NAT) is a method of mapping a group of private IP addresses to a group of public network IP addresses. NAT conserves IP addresses by sharing a limited number of public IP addresses among many internal hosts. A public IP address can be mapped to multiple internal hosts. Furthermore, NAT hides internal IP addresses from the outside world so that adversaries outside the network cannot directly attack internal hosts. VoIP signaling and media transport protocols often use different ports. Furthermore, RTP and RTCP use random ports to exchange data, thus complicating the NAT process. When NAT receives the actual digitized voice packets, it has no knowledge of where to send it. As a result, the packets may get dropped.

Similar to the use of encryption, the use of firewalls and NAT will also affect QoS because every packet coming in will have to be processed to determine admission. The uses of encryption, firewall, and NAT are just three examples of defense mechanisms against possible VoIP threats. However, these defenses often cause problems in the operation of VoIP processing and performance.

F. NAT

Network Address Translation (NAT) is primarily used for two purposes: public IP address conservation and security. The advantage of using NAT is that any number of internal hosts using un-routable private IP addresses can be connected to another network, such as the Internet, using a small number of public IP addresses. When an internal host wants to communicate with an external host, NAT maps the private IP address of the internal host to one of its un-used public IP addresses. The process of NAT rewriting the private IP address with a public IP address in the source IP address field of all packets initiated from a local host is known as Source Network Address Translation (SNAT). Destination Network Address Translation (DNAT) refers to the process of NAT rewriting the public IP address with a private IP address in the destination IP address field of all packets received at its public interface. Note that a NAT device must have routing capabilities to route packets in and out of two different networks. SNAT and DNAT allow an internal host to communicate with an external host without ever exposing its internal IP address. This mechanism of hiding internal IP address provides another layer of protection for system security.

1. netfilter/iptables

Any Linux system can be turned into a NAT device using *netfilter* and *iptables*. These two open source kernel modules are included in most Linux distributions that provide networking functions including NAT, routing, and firewall. Furthermore, *iptables* has a powerful connection tracking mechanism that allows it to associate packets with their corresponding sessions. This mechanism is essential in stateful firewalls. More information about *netfilter* and *iptables* can be found at [6]. The next section describes a component in the MYSEA architecture that uses *netfilter* to do NAT.

netfilter/iptables consults the *nat* table to determine if the IP address and/or port of a packet needs to be rewritten and how those fields should be rewritten. The *nat* table contains three chains of rules. Two of them are PREROUTING and POSTROUTING. The PREROUTING chain is referenced when a DNAT decision has to be made while the POSTROUTING chain is used to make SNAT decisions. The following are two sample NAT rules:

iptables -t nat -A POSTROUTING -o eth0 -j SNAT --to 192.168.0.1 iptables -t nat -A PREROUTING -ieth0 -j DNAT --to 192.168.1.10

The first rule instructs the NAT device to modify the source IP address of all outgoing packets to 192.168.0.1 after the packet is processed by the routing logic. The second rule tells the NAT device to rewrite the destination IP address of all incoming packets to 192.168.1.10 before routing logic takes place.

2. SIP with NAT

SIP-based VoIP calls rely on two protocols: SDP for negotiating of session parameters and RTP for transporting of voice data. Two endpoints setup a VoIP connection with exchange of the INVITE and 200 OK messages. Each message has SDP information embedded in the payload specifying the IP address the endpoint expects to receive RTP voice packets. Before sending out either the INVITE or 200 OK packet during the call setup, an endpoint located behind a NAT device writes its private IP address as part of the SDP data. The NAT device, a layer three device, performs SNAT to the message it receives from the endpoint and then sends the packet to the destination address. Since SDP is a layer five protocol, the NAT device is unable to examine and rewrite the private IP address embedded in the SDP section of the message. When the other endpoint wants to send RTP packets, it will send it to the private IP address indicated in the SDP portion of the received message and hence the RTP packets will get dropped.

G. MYSEA OVERVIEW

The Monterey Security Architecture (MYSEA) is a multi-level distributed operating environment designed to allow secure access to information at different classifications. MYSEA consists of a combination of commercial-off-the-shelf (COTS) and high assurance components. The COTS components are used to perform common user tasks whereas the high assurance applications are used to enforce security policies. Such a design is especially advantageous to organizations such as the DoD that invest heavily on COTS products but has a need to manage information with different sensitivities [7].

Figure 1 is an illustration of the MYSEA network architecture. Communication between an untrusted client on the MLS LAN and another client is mediated by a MLS server running XTS-400. The MLS server enforces security policies and provides a number of security-related services. Each MLS LAN client communicates with the MYSEA server via an inline Trusted Path Extension (TPE). The TPE establishes an encrypted trusted path and negotiates session level information with the MLS server on behalf of the client. Each TPE is also a NAT device that hides the internal IP address of the clients. Currently every TPE on the MYSEA testbed has a unique private IP address whereas every client uses the same private IP addresses. Refer to [8] for more detail discussion of MYSEA.



Figure 1. MYSEA Network Architecture [From Ref. 8]

H. SUMMARY

This chapter presents background information that is relevant to this project. To prepare for testing, a VoIP protocol must be selected as the test protocol. The next chapter compares two popular VoIP protocols, namely H.323 and SIP, and ends with a protocol selection for testing.
III. TECHNICAL COMPARISON BETWEEN H.323 AND SIP

The purpose of this chapter is to compare two dominant VoIP signaling protocols: H.323 and Session Initiation Protocol (SIP). At the end of the study, one of the two protocols will be selected for testing. Selection is based on the protocols' simplicity and flexibility, extensibility, scalability, and security. This chapter consists of two sections. The first section describes the protocols whereas the second section is a summary of two SIP and H.323 comparisons presented in [9] and [10].

A. H.323 AND SIP OVERVIEW

H.323 and SIP are the front-runners in the VoIP industry. H.323 came about in 1996, two years before the birth of SIP in July 1998. H.323 is still widely used in enterprises and continues to be improved, while SIP is gaining popularity and undergoes more development. The following subsections present a high level overview of the two protocols.

1. Background

H.323v1 was developed by ITU-U as a "standard for real-time videoconferencing over non-guaranteed quality of service LANs" [9]. The standard has undergone several revisions. The latest version, H.323v4, defines basic call control and signaling for multimedia applications. The protocol is specifically designed to support multimedia and voice applications. It was extended to support VoIP. The ITU-U initially concentrated on developing multimedia functionalities, supplementary services, and internetworking capabilities into H.323. As those capabilities become standardized, ITU-U works to address the protocol's security, QoS, and mobility issues.

SIP, IETF's standard for establishing VoIP connections, was standardized in 1999 and revised in 2002. SIP is an application layer protocol designed to setup, modify, and tear down generic sessions. Other fundamental services it provides include user location, session invitation and session negotiation. As with all IEFT protocols, SIP was not developed to support a particular type of application. Rather, SIP is designed to work with any application that may need its services. The IEFT initial focus was on standardizing the protocol to support session initiation. Currently, a large amount of effort is placed on defining specific applications, such as internetworking with legacy networks and providing supplementary services [9].

2. Architecture

Both H.323 and SIP have both peer-to-peer and client-server architectures. H.323 specifies a complete framework that defines the protocols and the message flows for multimedia communications. The standard covers all phases of a VoIP call including set-up, call control, and media transport. Other issues critical to the quality of a VoIP call such as QoS, security, and mobility are also addressed in the standard.

H.323 is actually a suite of protocols that can be broken down into six classes: call control and signaling, audio processing, video processing, data conferencing, media transportation, security, and supplementary services. Information regarding the different protocols used in H.323 can be found in [11].

Figure 2 depicts the H.323 protocol stack. The lighter colored blocks represent optional components whereas the darker colored blocks represent mandatory components necessary to complete a VoIP call. It is important to note that both H.323 and SIP rely on the support of several common protocols such as TCP/UDP, IP, RTP and RTCP and audio processing services. In summary, only H.245, H.225.0/Q.931, and H.225.0/RAS are essential to achieve the signaling part H.323 VoIP call.



Figure 2. H.323 Protocol Stack [From Ref. 9]

SIP by itself only defines setup and teardown of sessions. Advance signaling features are specified as SIP extensions. Furthermore, QoS and mobility are not addressed by SIP but can be supported by other protocols. SIP depends on the Session Description Protocol (SDP) to describe parameters for multimedia session between two endpoints. SDP is a text-based media-description format that is carried in SIP messages. Figure 3 depicts the SIP protocol stack. Again, the darker component is essential to the signaling part a SIP VoIP call.



Figure 3. SIP Protocol Stack [From Ref. 9]

3. Components

H.323 and SIP divide functions to components in a similar fashion. Basic call function controls are assigned to the terminals whereas services requiring network support are assigned to network servers. Table 3 lists SIP and H.323 network components by types.

	Client	Servers	in the network	
SIP (IETF)	Terminal	Proxy server, registrar	Conference server ¹	Gateway ^{1,2}
H.323 (ITU-T)	Terminal	Gatekeeper	MCU	Gateway
		now. ² Addressed in se init. Gateway: maintains		

Table 3.SIP and H.323 components [From Ref. 9]

An H.323 network consists of terminals and a gateway. A gatekeeper, Multipoint Control Unit (MCU), and Back End Service (BES) may also be deployed as part of the network. A terminal is any VoIP-enabled device. The gateway provides translation services for terminals that use different communication protocols including non-VoIP protocols such as PSTN. A gatekeeper performs address translation, controls accesses of terminals, manages bandwidth and makes routing decisions. Although a gatekeeper is optional, it is often an important component in an H.323 network because of the services it provides. A H.323 network can have a MCU that facilitates communication among multiple endpoints. A Back End Service usually exists to support the gatekeeper by maintaining information about endpoints such as the endpoints' permissions, configurations, and services [5].

A SIP network has endpoints, a proxy server or redirect server, location server, and a registrar. The registrar authenticates users and stores location information from users. A proxy server, which can be integrated with the registrar, resolves addresses and forwards messages on behalf of the endpoint to another proxy server or the destination endpoint during call setup and teardown. The redirect server performs tasks similar to those of a proxy sever but instead of forwarding the message, the redirect server sends the resolved address back to the endpoint and lets the endpoint communicate directly with the other endpoint. The location server supports the registrar by maintaining location information of endpoints [5].

4. Call Setup

Call setup refers to the actions necessary to establish a connection between two endpoints. This process must be completed before the endpoints can exchange actual voice data. The following subsections describe simple H.323 and SIP call setups. The scenarios assume that Alice initiates a non-local call to Bob.

a. H.323

H.225.0/RAS, Q.931 in H.225.0, and H.245 are necessary to establish an H.323 VoIP connection. These protocols provide functions necessary for call registration, call setup, and capability exchange. Figure 4 illustrates a simple H.323 call setup.



Figure 4. Simple H.323 Call Setup

When Alice dials Bob's phone number, (Step 1) Alice's terminal sends a Registration Admission Request to the gatekeeper using H.225.0/RAS. The gatekeeper registers Alice into the system, admits and grants resources to Alice and finds Bob's IP address. Next, (Step 2) the gatekeeper sends the IP address to Alice. Alice then establishes a TCP connection with Bob at the IP address she received (Step 3). Alice sends a SETUP message to Bob using Q.931/H.255.0, an ISDN-connection control protocol (Step 4). Bob sends Alice back a CONNECT (Step 5) message to Alice using the same protocol indicating acceptance to the connection. Finally, Alice and Bob negotiate terminal capabilities using H.245 (Step 6). Then H.245 will open logical channels for both endpoints to start the conversation.

b. SIP

Figure 5 illustrates a simple SIP call setup. In this example, an integration of the registrar into the proxy server is assumed. Before Alice calls Bob, Alice's terminal must register itself with the registrar (Step 1). This step is similar to the first step in the

H.323 simple call setup. After the registration is completed, Alice may call Bob by sending the proxy server an INVITE Bob message (Step 2). The proxy server looks up Bob's IP address and forwards the invitation to Bob (Step 3). An OK response will be received by the proxy server from Bob indicating acceptance to the call (Step 4) and the response will in turn be forwarded to Alice (Step 5). Throughout this process, session parameters and terminal capabilities are transparently exchanged inside the INVITE and OK messages from both parties using SDP or some other methods. From now on, the two parties may communicate in a peer-to-peer fashion.



Figure 5. Simple SIP Call Setup

5. Services

H.323 and SIP both provide basic call controls as well as advanced features. Table 4 lists the features common to both protocols.

Feature	H.323	SIP
Call Setup	Yes	Yes
Call Teardown	Yes	Yes
Call Waiting	Yes	Yes
Call Hold	Yes	Yes
Call Transfer	Yes	Yes
Call Forwarding	Yes	Yes
Call Return	Yes	Yes
Call Identification	Yes	Yes
Call Park	Yes	Yes
Capabilities Exchange	Yes	Yes

Table 4.Basic Call Control Features

B. H.323 AND SIP COMPARISON

H.323 and SIP are different in many ways despite the fact that they provide similar call control services and are widely used in VoIP applications. One of their fundamental differences lies in their original intents and designs. H.323 was designed with a focus on multimedia and voice communications whereas the SIP design focused on providing only session initiation services. H.323 uses a top-down approach to specify a complete framework for providing multimedia and voice services. It is telecommunication-oriented as it uses existing multimedia protocols in the ITU H-series to support provide various services. SIP, on the other hand, uses a bottom-up approach. Its modular design allows it to work with a wide range of applications. SIP takes on an Internet-oriented design by adopting a number of features from HTTP and SMTP, two of the most successful Internet protocols [9, 10].

Their implementation approaches lead to differences in the simplicity and flexibility, extensibility, scalability, and security of the protocols. The following subsections examine these differences.

1. Simplicity and Flexibility

Simplicity and flexibility are two important measurements to determine the quality of the protocols' design. This subsection compares H.323 and SIP based on these two aspects. Protocol specification, message encoding, and protocol interactions will be closely examined.

a. Protocol Specification

SIP is simpler in nature than H.323. According to [9], a SIP-based VoIP implementation can be done with four headers (To, From, Call-ID, and Cseq) and three types of requests (INVITE, ACK, and BYE).

H.323, on the other hand, consists of numerous protocols such as H.225.0 for call signaling, H.245 for call control, H.332 for conferences, H.450.1 to H.450.9 for supplementary services, H.235 for security and encryption, etc. Many services require a number of H.323 protocols to interact with each other. This further intensifies H.323's complexity problem [10].

b. Message Encoding

H.323 messages are encoded by the ASN.1, an international standard used to specify data used in communication protocols. Since ASN.1 messages exist in binary form, a special tool is needed to parse the messages. SIP adopts the HTTP tradition by using text-based messages. Hence, SIP messages are generally easy to parse, generate, and debug [10].

c. Protocol Interactions

H.323 is complicated because of the many of protocols it encompasses. A number of protocols are often required for a single service in H.323. For example, connection establishment, as illustrated in Figure 3, requires Q.931/H.255.0, H.225.0/RAS, and H.245. On the other hand, SIP uses a single INVITE request to establish the connection even though it depends on SDP to negotiate session parameters. H.323 also allows those three protocols to be used in different orders to establish a

connection. Thus, network devices such as firewalls, endpoints, gatekeepers, and gateways must support and understand all three connection establishment methods [12].

d. Applications

SIP is designed to create, manage, and tear down generic sessions. As a result, SIP has the flexibility to work with a wide range of applications. Voice and multimedia are just two applications of SIP. Others include voice-enriched e-commerce, web page click-to-dial, Instant Message, and IP Centrex services. H.323 was designed to focus on a specific type of communication, namely voice and multimedia conferencing. Thus, its applications are not as wide as SIP's. ITU-U is currently working toward providing non-VoIP services in H.323 [9].

2. Extensibility

Extensibility defines how easy it is to add new features to the existing protocols. This aspect of the protocols will be evaluated based on extensible mechanisms, backward-compatibility, and interoperability.

a. Extensible Mechanisms

Both H.323 and SIP have certain extensible mechanisms. H.323 has nonstandardParm fields in its ASN.1 messages. Each nonstandardParm field is identified by a unique vendor code and the information contained in this field is only meaningful to the specific vendor. These fields allow vendors to add extensions [10].

SIP adopts the HTTP's use of hierarchical numeric warning codes. Its warning codes are represented by three digit numbers where the first digits identify which of the six categories the codes belong to.² The list of warning codes can be easily extended under this hierarchical structure system. SIP features are also extensible. New SIP features can be officially added by registering the names of the features with the Internet Assigned Numbers Authority (IANA). New features will not cause confusion on the server side because SIP specifies that a server shall ignore the request of a feature in a SIP header if the server does not understand or support the feature.

² SIP warning codes are divided into six categories: provisional, redirection, request and server failure, busy everywhere responses, successful and bad requests.

b. Backward-Compatibility

H.323 supports full backward compatibility among different implementation versions. In other words, obsolete features have to be carried over from Hence, the code can become complicated. one version to the next. However, compatibility between two different versions of H.323 implementations is guaranteed. On the other hand, a new version of the SIP implementation does not need to support obsolete features from past versions. When an obsolete feature is requested from a server, the server, by default, ignores the request, informs the requestor of the unsupported feature and lets the requestor decide what to do. This way, a SIP implementation is typically cleaner while still maintaining some compatibility. Unlike H.323, different versions of SIP implementation may suffer from compatibility problems [10].

c. Interoperability

H.323 has higher interoperability than SIP. H.323 has well-defined implementation guidelines available to help improve interoperability among different H.323 vendors. Also, the H.32x family specifies standards to guarantee interoperability among circuit-switched networks such as ISDN, B-ISDN and GSTN. SIP is also highly interoperable with other protocols due to its flexibility and modular design. For example, SIP can be used in conjunction with H.323 where SIP provides the location service and H.323 performs the rest of the communication services. However, SIP is loosely defined and open to various interpretations. This may lead to potential interoperability issues. There is a growing effort focused on addressing interoperability issues in SIP [9].

3. Scalability

The scalability of the two protocols, or the ability to support small or large volume of data or users, is compared in below. The design, server components, and conference mechanisms of the protocols will be evaluated for scalability.

a. Protocol Design

H.323 was originally designed for local area networks. Addressing in a wide area network (WAN) and user location were not initial concerns for H.323. As networks employing H.323 have grown in size, H.323 has been augmented to address these issues. However, H.323 still has a scalability problem because its loop detection

algorithm using path values does not work well. SIP, on the other hand, was designed to support WAN addressing and user location. It uses a loop detection mechanism that is similar to the one employed by Border Gateway Protocol (BGP). Thus unlike H.323, the SIP loop detection algorithm scales well [10].

b. Servers

Scalability generally decreases if servers have to maintain state for all calls. Servers used in both protocols can be stateful or stateless. Endpoints in both protocols need to keep states in stateless call implementations. Endpoints as well as servers need to maintain states in stateful call implementation. The drawback of maintaining states is the large amount of memory and processing that is required. Most current H.323 gatekeeper implementations are designed to be call stateful whereas most SIP proxy implementations are designed to be call-stateless [12]. Therefore, SIP scales better in large networks.

c. Conferencing

H.323 relies on the Multipoint Control Unit (MCU) to manage signaling in multiparty conferences regardless of the number of participants. However, MCU can be a bottleneck in large conferences. SIP is more scalable with regard to conferencing because it employs a distributed control scheme [12].

4. Security

This section compares the security provided by H.323 and SIP based on [5]. More specifically, it examines the protection of authenticity, confidentiality, and integrity for both signaling and media data provided by H.323 and SIP.

a. H.323 Security - H.235

H.323's relies on H.235 to specify security standards. However, H.235 "does not mandate particular [security] features" [13]. To address interoperability among different H.235 vendors, H.235 defines security profiles corresponding different security levels. Table 5 summaries the different H.235 security profiles or annexes described in [5].³

³ H.235 Annex A (H.235 ASN.1), Annex B (H.323 Specific Topics), and Annex C (H.334 Specific Topics) are not listed in Table 4.

b. SIP Security

The SIP standard specifies several security features including HTTP Digest Authentication and S/MIME. The protocol does recommend other best security practices to address authentication, confidentiality, and integrity for both signaling and media data. Table 6 lists the existing SIP security features presented in [5].

c. Security Comparison

H.235, the security protocol for H.323, and SIP both have recommendations to protect the authenticity, confidentiality, and integrity for both signaling and media data. At the same time, ITU-T and IETF are making serious efforts to address security problems by continuously devising new security recommendations. Even though H.235 has effective security measures, H.323 does not mandate vendors to implement any of the H.235 security measures. According to an online website, not many H.323 products have support for H.235 and those that have "only use H.235 (baseline security) for the communication between gatekeeper and gateway and not for communication with the endpoint" [13]. SIP, on the contrary, has security mechanisms specified in the protocol implementation and is inherently more secure than H.323.

1 mmo	Nomo
Annex	Name Basolina Sagurity
D	Baseline Security Profile
E	Signatures Securit Profile
	Voice Encryption Option
F	Hybrid Security Profile
G (draft)	SRTP & MIKEY Usage
H (draft)	RAS Key Management
I	H.235 Annex D fo Direct Routed Scenarios
J	N/A

Table 5. H.235 Security Profiles

Name			
HTTP Digest	Chall) signai serv		
	passv		
S/MIME	Use		
RTP and SRTP	Encry u		
SDP	Uses		
	SIP re		
TLS	registra		
IPsec	Use IF		
AIB	Usea		
(draft)	fra		
Authentic ated Identity Management (draft)	Recom		
S/M IME AES	Use		
Requirement	mir		
(draft)	im		
Security Mechanism Agreement (draft)	Pro secu:		
End-to-Middle, Middle-to- Middle, Middle- to-End Security (draft)	Desc comm		

Table 6.SIP Security Features

5. Conclusion

Both protocols have strengths as well as weaknesses. SIP is more flexible and light-weight but less well-defined compared to H.323. H.323 has a detailed specification and offers higher interoperability but supports fewer applications. Nevertheless, H.323 and SIP are widely used in VoIP applications and both are undergoing more development to address their weaknesses. Neither of the two will become obsolete. Thus, interoperability between them will become necessary.

Nevertheless, SIP is simpler, more flexible, extensible, scalable, and can be more secure than H.323 based on the above comparison. SIP, the younger protocol of the two, is showing the potential to become a highly successful Internet protocol. Products based on SIP are becoming increasingly available for these reasons. For example, Microsoft has shifted H.323-based NetMeeting implementation to a SIP-based implementation in Windows XP. Furthermore, Microsoft also incorporates a SIP-like protocol stack in its .Net framework that can be used on desktops and mobile devices such as PDAs and smart phones [14].⁴ Further research on this young protocol is highly valuable to the community, as the number of applications supported by SIP is expected to grow. For this work, SIP has been selected for use in the experiments described in Chapter IV.

C. SUMMARY

H.323 and SIP provide similar VoIP services using different approaches. Thus they differ in simplicity and flexibility, extensibility, scalability, and security. Both protocols have advantages as well as disadvantages and they continue to be improved. For this project, SIP is chosen as the test protocol for research purposes.

⁴ NetMeeting is standard video-conferencing program included in Windows 2000 and XP.

IV. TESTING

This chapter describes the test methodology and test plan to verify the feasibility of SIP-based VoIP communications in different network architectures that included Network Address Translation (NAT) devices. An overview of the five tests and a brief summary of the findings are also presented. The testing described in this chapter is a preliminary step in integrating VoIP capabilities into the existing MYSEA architecture.

A. TEST METHODOLOGY

Testing is conducted on a dedicated testbed using an incremental approach. After each test, the result is thoroughly analyzed before proceeding to a more complicated test. The incremental testing approach is preferred in this study because it allows easy identification and debugging of problems that emerged during the tests.

A number of free tools are deployed in the testbed. In particular, SJPhone, a softphone developed by SJ Labs [15], is used to make and receive SIP-based VoIP calls. Ethereal [16], an open source packet capture tool, is used to capture packet exchanges during each VoIP session for post-testing analysis. *netfilter* and *iptables* [6], modules in Linux Operating System kernel, provide Network Address Translation and routing functions in the testbed. Finally, ZoneAlarm [17], a free software-based firewall, is used to block certain traffic during the tests.

A number of systems are used to model the different components that make up the MYSEA environment. For example, Windows laptops with SJPhone installed are in the testbed to represent the untrusted clients that sit behind the TPEs. Linux systems are used to perform NAT and/or routing functionalities. They simulate the TPEs in MYSEA.

This project focuses on testing the feasibility of making VoIP calls from the MLS LAN. Therefore, VoIP calls are always initiated from the clients located behind TPEs on the MLS LAN to the clients located on simulated single level networks. In terms of MYSEA, this is equivalent to allowing calls to be initiated from clients on the MLS LAN to clients on external networks.

B. TEST DESCRIPTION

The main objective of the tests described in the following subsections is to verify that VoIP conversations can be carried out in each network configuration. Procedures and results pertaining to each test can be found in Appendices B, C, D, E, F, and G. Note that private IP addresses assigned to network devices were used for demonstration purposes only. However, public devices such as public NATs and routers should use public IP addresses in practical scenarios.

1. Test 1: No NAT VoIP Configuration

The objective of this experiment is to observe the behavior of SJPhone in the simplest possible setup. The testbed consists of two directly connected VoIP-enabled clients as shown in Figure 6. In this scenario, Client B initiates a VoIP call to Client A. Test procedures and results are included in Appendix B.



Figure 6. Test 1: Physical and Logical Network Topology

2. Test 2: Single NAT VoIP Configuration

The goal of this experiment is to confirm the feasibility of SIP-based VoIP calls when a NAT system is present. The testbed for this experiment consists of two VoIPenabled clients and one NAT device as illustrated in Figure 7. The combination of the NAT device and Client B simulates the TPE-client pair in the MYSEA architecture. Client A is aware of Client B in this setup. Client B, on the other hand, is hidden behind a NAT device and is not visible to Client A. All packets exchanged between the two clients must traverse the NAT device that is configured with Source NAT and Destination NAT.

Two similar tests are conducted with this NAT configuration. The first test has a physical and logical network topology depicted in Figure 7. Even though the second test uses the same physical network topology as the first test, it has a logical topology

depicted in Figure 8. Since the NAT device is not configured to drop packets destined for private IP addresses, Client A can send RTP packets directly to the private IP address of Client B. This is exactly what Client A does based on the packet captures provided in Appendix C. In non-experimental scenarios, a firewall at the client is not necessary because packets destined for a private IP address will eventually be dropped as they traverse the networks. For demonstration purposes, a firewall is introduced at Client A to block packets initiated by Client A and destined for Client B. More information including the test procedures and results for both tests can be found in Appendix C.



Figure 7. Test 2: Physical Network Topology (with and without firewall)



Figure 8. Test 2: Logical Network Topology (with firewall)

3. Test 3: Double NAT VoIP Configuration

The goal of this experiment is to confirm the feasibility of a SIP-based VoIP call using SJPhone when two NAT systems are present. In this test, a VoIP session between two clients have to traverse two different NAT devices as depicted in Figure 9 and Figure 10. Similar to the previous test, Client B and NAT 2 represent the client-TPE pair in the MYSEA architecture. NAT 1 simulates the NAT device located between the MYSEA network and the Internet whereas Client A acts as a VoIP-enabled client in the Internet. Both NAT devices are configured to perform Source NAT and Destination NAT. Test procedures and results are included in Appendix D.



Figure 9. Test 3: Physical Network Topology



Figure 10. Test 3: Logical Network Topology

4. Test 4: Extended Double NAT VoIP Configuration

The purpose of this experiment is to confirm that two different VoIP sessions can take place at different times when the sessions have to traverse a common public NAT device. This and the next setup only work when the public NAT device implements a connection tracking mechanism that is similar to what *iptables* provides. The test is setup so that the public NAT device is not explicitly instructed to forward packets to any specific network. In other words, the public NAT only performs Source NAT but not Destination NAT. A firewall is installed on Client A to prevent Client A from sending RTP packets directly to the private address of Client B. The firewall is necessary in this demonstration because NAT 1 and NAT 2 are not configured to drop packets destined for private IP addresses.

This test consists of three VoIP-enabled clients and three NAT devices as depicted in Figures 11 and 12. Two client-TPE pairs are simulated in this setup, Client B and NAT 2 being one pair and Client A and NAT 3 being the second pair. NAT 1 resembles the public NAT that is located between the MLS LAN and the Internet. NAT 1 is only configured with a SNAT rule whereas NAT 2 and NAT 3 are configured with both SNAT and DNAT rules. The test proceeds as follows: Client B initiates a call to Client A, terminates the call, and then Client C initiates a call to Client A. Procedures and results can be found in Appendix D.



Figure 11. Test 4: Physical Network Topology



Figure 12. Test 4: Logical Network Topology

5. Test 5: Extended Double NAT VoIP Configuration with Simultaneous VoIP Sessions

The purpose of this test is to confirm the feasibility of two simultaneous VoIP sessions between two pairs of clients. The setup of this test, shown in Figures 13 and 14, closely resembles a simplified version of the MYSEA architecture. The IP addresses used for different components in this demonstration are the same as the ones used in the MYSEA testbed. This test consists of four VoIP-enabled clients, three NAT devices, and a router. The router is introduced here as a preparation for the next test. Refer to the next section for a description of the router. Similar to the previous test, two pairs of client-TPEs are simulated using Client C, NAT 2, Client D, and NAT 3. Furthermore, NAT 1 is not configured with a DNAT rule and two firewalls are installed on Client A and Client B

to block RTP packets destined to Client C and Client, respectively. In this scenario, Client C calls Client A and Client D calls Client B at the same time.



Figure 14. Test 5: Logical Network Topology

6. Test 6: MYSEA Configuration

The setup of this test, illustrated in figures 15 and 16, is an extension to the last one with the addition of a MLS server. The objective of this test is to verify that the MLS Server could support two simultaneous VoIP sessions between two pairs of clients. Since the MLS server does not perform routing in the testbed, a router is introduced to perform that function. The MLS server simply forwards the received packets to the correct network interfaces according to the network configurations. In this test, unexpected routing problems were encountered on the MLS server. Refer to the next section for a discussion of this test.



Figure 15. Test 6: Physical Network Topology



Figure 16. Test 6: Logical Network Topology

C. PROBLEMS ENCOUNTERED

Setting up and running the tests was fairly straightforward with the exception of the MYSEA Configuration. The major problem encountered that ultimately led to the failure of the MYSEA test was configuring the MLS server to perform proper routing. The MLS server, currently running XTS-400, has routing limitation such that only one static route can be configured for each network interface. An attempt to add a second route to the network interface X resulted in the following error message: "Route /dev/etherX already exists". Since every packet has to traverse the server, this limitation prevents an incoming or outgoing packet arriving at the MLS server from routing to the other side of the network. According to the customer service response to our inquiry,, "there is a known restriction on [the XTS-400] configuration tool tcpip_edit (not the network stack) that there can only be one route per interface device..." [18]. Four test scenarios were conducted to ensure that the MLS server, in fact, has routing limitation. Refer to Appendix G for details. In conclusion, the MYSEA Configuration test was not conducted successfully.

D. TEST RESULT

All the tests described in the previous section generate positive results, i.e. the results indicate that VoIP communications are possible in five of the six scenarios. However, it is important to recognize that the last test was unsuccessful not because of VoIP limitation or the network topology. Instead, the last test failed was due to configuration difficulties in the MLS server.

Several interesting findings are discovered from analyzing the packet captures. First, SJPhone will attempt to send RTP packets to the IP address indicated in the SDP data. If that fails, then SJPhone will resort to send subsequent RTP packets to the IP address it received RTP packets from. Second, the client that initiates the VoIP call is always the first to send out a RTP packet to the other party. Third, *iptables* has a connection tracking mechanism that allows it to associate incoming packets with previous outgoing packets and determine which VoIP session the incoming packets belong to. Since *iptables* creates an entry in its connection tracking table for the first RTP packet sent, subsequent incoming packets can be correctly forwarded to the correct next hop based on the information stored in the table. This mechanism plays a significant role in the success of tests 4 and 5 where the public NAT was not configured with a DNAT rule to forward incoming packets to any particular IP addresses. Refer to Appendices B through G for more details on the findings.

E. SUMMARY

The purposes and configurations of the experiments designed for this feasibility study are described in this Chapter. The results of the experiments are also briefly discussed. The results are optimistic and they indicate that the integration of VoIP into MYSEA is possible. THIS PAGE INTENTIONALLY LEFT BLANK

V. FUTURE WORK AND CONCLUSIONS

A. FUTURE WORK

The test results described in Chapter IV and various appendices suggest that VoIP capabilities can be potentially integrated into the existing MYSEA architecture with little effort. However, further research in the following areas is required.

1. Routing in MLS Server

Every MLS client communication is mediated by the MLS server that runs on XTS-400, a high-assurance Unix-like system. Unfortunately, the MLS server has routing limitation such that only one static route can be configured for each network interface. The ability to configure more than one route for each interface in the MYSEA server is necessary for VoIP packets to route between clients on the MLS network and on external networks. Therefore, further study of the routing configurations or capabilities is required to allow proper routing of VoIP packets.

2. VoIP Conversations Initiated from the Internet

This research study is primarily concerned with testing the scenarios in which VoIP conversations are initiated from the MLS LAN. The ability for externally initiated VoIP conversation is also desirable. Currently, a client on an external network only knows the IP address of the public NAT device and there exists no way of distinguishing calls intended for different clients on the MLS LAN. In order for an internal client to receive an external call, three features may have to be implemented. First, each internal client must own a unique SIP address that is publicly known. This allows an external client to direct call to a specific internal client. Second, a server must exist to translate a SIP address to the corresponding internal client IP address. Third, softphones with reconfigurable RTP port, such as the SipXphone, are needed for each internal client. Each client needs to use a different RTP port for sending and receiving RTP packets and the public NAT must be configured to perform port forwarding. This allows NAT to forward RTP packets to the correct client according to the destination port. Research on how to implement this scheme is highly recommended.

B. CONCLUSIONS

The tests conducted in this research study were generally successful. Furthermore, the test results indicate that VoIP conversations, at least in the scenario we studied, between internal and external clients are possible even when various NAT devices are present. It is important to recognize that the success of Test 4 and Test 5 was dependent on the connection tracking mechanism in *iptables*. NAT devices without connection tracking mechanisms were not tested in this project. Thus, it is unknown whether the tests will work if those devices are used instead. In conclusion, VoIP capabilities may be integrated into the existing MYSEA architecture.

APPENDIX A. A SURVEY OF VOIP HARDPHONES AND SOFTPHONES

A. HARDPHONES

The following table is a survey of some VoIP hardphones. Each hardphone is listed with information including its manufacture (Brand/Company), phone type (category and Sub-Category), the VoIP protocol (VoIP Protocol), and Wi-Fi protocol (Wi-Fi Protocol) it supports.

Name	Brand/Company	Category	Sub-Category	VoIP Protocol	Wi-Fi Proto col
	Advantage				
ACT P202	Century	WLANWIFI	Mobile IP	SIP	802.11b
000 T - 202	Telecomm Phones	Phone	Phone	¢	002.118
	Conso	WLANWIFI	Mobile IP	0	000 116
	oenau	Phone	Phone	엄	802.110
E4000		WLANWIFI	Mobile IP	00	000 446
r 1000		Phone	Phone	ę	8U2.110
		WLANWIFI	Cordless	0	000 116
0000142140		Phone	Handset	ġ	002.110
Cisco 7920	Cisco	WLANWiFi Phone	Cordless	Skinny	802.11b
		11010	10001		
WirelessIP5000	Hitachi Cable	WLANWiFi Phone	Cordless Handset	SIP	802.11b
ZyXEL P2000W	ZyXEL	WLANW/iFi Phone	Cordless Handset	SIP	802.11b
Vecta 100	Arkon Networke	WLANWIFI	Cordless	NIA	800 11 M/m
1 000 1 00		Phone	Handset		001.1 mg
Motorola CN620	Motorola	GSM/WiFi Phone	Handset	SIP	802.11a/b/g
Nostrand 200	Arkon Networks	WLANWiFi Phone	Handset	SIP	802.11b/g
Stonehenge WP150	Moimstone	WLANWiFi Phone	Wireless Phone	SIP	802.11b/g

Table 7.Summary of Hardphones

B. SOFTPHONES

The following table is a survey of some VoIP softphones. Each softphone is listed with information including what Operating System(s) and VoIP protocol(s) (VoIP Protocol) it supports and whether it is a commercial or an open source product.

		SIP NA	~	~	~	~ ~	-	Phone Skype
	;	1,010				:	;	Emnower Pro Internet
Y		SIP and			Υ			Asterisk
Y		dIS	Y	Y		Y		SF Lphone
Y		dIS			Y			Cornfed SIP-UA
¥		SР	Y	Y		Y		Shtoom
Y		dIS	Y	Y	Y			sipXphone
Y		SIP			Υ			Siphon
Y		ЯР			Y			Vovida
Y		NA			Y			Kphone
×		SIP			Y			Linphone
	Y	SIP and H. 323	Y	Ч	Υ	Y	γ	SJPhone
	Y	SIP	Y	Y				MySIP
	Ϋ́	SIP	¥	۲				EZ-Phone
Υ		ЫS	۲	Y				Ubiquity User Agent
	Y	SIP						SddIS
×		SIP	×	Y				eyeP Phone Lite
	×	SIP	×	×		Y	Y	X-Pro
	۲	SIP	×	Y		Y	Υ	X-Lite/eyeBeam
Open Source	Commercial	VolP Protocol	WinXP	Win 2K	Linux	MAC OS X	Pocket PC 2003	Name

Table 8.Summary of Softphones

APPENDIX B. TEST 1: NO NAT VOIP DEMONSTRATION USING SJPHONE

The instructions in this appendix describe how to setup and demonstrate a SIPbased VoIP communication between two directly connected SIP-enabled clients using SJPhone. Figure 6 illustrates the physical network as well as the logical topology for this demonstration. A VoIP session is initiated from Client B to Client A. Packet captures from both clients are included at the end of this appendix along with an analysis.

A. Network Topology

Refer to Figure 6 for the physical and logical network topology.

- B. Equipment Requirements
 - B.1. Clients A and B
 - B.1.1. Windows XP Operating System
 - B.1.2. Sound card
 - B.1.3. SJPhone v.1.60
 - B.1.4. Ethereal
 - B.2. Additional Equipment
 - B.2.1. Cross-over cable to implement the network architecture Figure 6
 - B.2.2. Microphones as audio input devices for clients A and B

C. Installation and Configuration

- C.1. Client A
 - IP Address: 192.168.0.10
 - Subnet Mask: 255.255.255.0
 - Default Gateway: 192.168.0.20
- C.2. Client B
 - IP Address: 192.168.0.20

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.0.10

C.3. SJPhone Installation and Configuration

C.3.1. Client A and Client B

- C.3.1.1. Download the Windows version of SJPhone v.1.60 from SJ Labs
- C.3.1.2. Install SJPhone v.1.60
- C.3.1.3. Launch SJPhone
- C.3.1.4. Right-click on SJPhone
- C.3.1.5. Go to Services
- C.3.1.6. Select PC-to-PC (SIP)
- C.4. Ethereal Installation and Configuration
 - C.4.1. Clients A and B
 - C.4.1.1. Download the latest Windows version of Ethereal
 - C.4.1.2. Install Ethereal
- D. Preparation and Testing
 - D.1. Adjust volume on both clients accordingly
 - D.2. Plug microphones into both clients
 - D.3. On Client A,
 - D.3.1. Launch Ethereal
 - D.3.2. Go to the Capture menu
 - D.3.3. Go to Interfaces
 - D.3.4. Click on Capture 192.168.0.10
 - D.4. On Client B,
 - D.4.1. Launch Ethereal
 - D.4.2. Go to the Capture menu
 - D.4.3. Go to Interfaces
 - D.4.4. Click on Capture 192.168.0.20
 - D.4.5. Call Client A by dialing 192.168.0.10 in SJPhone
 - D.5. On Client A,
 - D.5.1. Select Accept in the pop-up dialog box when SJPhone rings
 - D.5.2. Clients A and B may engage in a VoIP conversation at this point
 - D.5.3. Click on the Hang-Up bottom on either SJPhone to terminate the call when finished
 - D.6. On Clients A and B,
 - D.6.1. Stop packet captures by selecting Stop on Ethereal

E. Packet Captures

E.1. Client A

Figure 17 is a snapshot of the packets captured on Client A.

		× 🕲 🖥 🕅 🤇	 ♥ ♥ 주 ½ 			g	
er:			Expression Glear Appl	Y			
. Time		Destination	Protocol Info			1	
	100000 192.168.0.10	192.168.0.255		:: 5003 Destination port: 5003		1	
	103621 192.168.0.20	192.168.0.10	SIP/SDP Request: IN	WITE sip:192.168.0.10, with ses			rec
	121646 192.168.0.10	192.168.0.20	SIP Status: 100			J	
	268388 192.168.0.10	192.168.0.20	SIP Status: 180	Renaing			
	520406 192.168.0.10	192.168.0.255		NB WWW.SJLABS.COM<00>			
	908247 192.168.0.10	192.168.0.255	NBNS Name query	NB WWW.SJLABS.COM<00>			
	719904 192.168.0.10	192.168.0.20		e=GSM 06.10, SSRC=1755075, Seq=	19548, Time=O, Mark		
	725126 192.168.0.10 728938 192.168.0.20	192.168.0.20 192.168.0.10		0K, with session description K sip:192.168.0.10:5060		-	
	13002 132-100-0-10	132-100-0-20	KIT Fayload cyp	C-034 00.10, 334C-1/030/3, 350-	199497 1100-200	1	
	730829 192.168.0.20	192.168.0.10		e=GSM 06.10, SSRC=14249088, Seq	=18412, Time=O, Mark		
	732509 192.168.0.10	192.168.0.255		NB WWW.SJLABS.COM<00>			
	739945 192.168.0.10 741185 192.168.0.20	192.168.0.20 192.168.0.10		e=GSM 06.10, SSRC=1755075, Seq=: e=GSM 06.10, SSRC=14249088, Seq			
17 8.7		192.168.0.10		e=GSM 06.10, SSRC=14249088, Seq	In the second second second second	1	bl
	750433 192.168.0.10	192.168.0.20		e=GSM 06.10, SSRC=1755075, Seq=			
19 8.7		192.168.0.10	RTP Payload typ	e=GSM 06.10, SSRC=14249088, Seq	=18415, Time=480		
20 8.7	760818 192.168.0.10	192.168.0.20	RTP Payload typ	e=GSM 06.10, SSRC=1755075, Seq=:	19552, 11me=640		
7.000	t-Line: INVITE sip:192.1 e Header	98.0.10 SIF/2.0					
Hessagi Sess Se Co Se Se Se Se Se Se Se Se Se Se Se Se Se	e body ion Description Protocol ssion Description Protoco ner/Creator, Session Id ssion Name (s): SJphone nnection Information (c) me Description, active t ssion Attribute (a): dir dia Description, name an dia Attribute (a): rtpma	(c): - 3334021007 333402 : IN IP 192.168.0.20 ime (t) 0 0 ection:active d address (m): aud <mark>o</mark> 491	_				gre
Hessage Sess Se Co E Co E Ti E Se Me Me Me	ion Description Protocol ssion Description Protoco mer/Creator, Session Id ssion Name (s): SJphone nnection Information (c) me Description, active t ssion Attribute (a): dir dia Description, name an dia Attribute (a): rtpma	(c): - 3334021007 333402 : IN IP 192.168.0.20 ime (t) 0 0 ection:active d address (m): aud 0 491 p:3 65M/8000	RTP/AV 3 97 98 8 0				gre
Hessage Hessage How Se How Se How E Co H Me How Se S	ion Description Protocol ssion Description Protoco ner/Creator, Session Id ssion Name (s): SJphone nnection Information (c) me Description, active t ssion Attribute (a): dir dia Description, name an dia Attribute (a): rtpma 	(c): - 3334021007 333402 : IN IP 192.168.0.20 ime (t) 0 0 ection:active d address (m): aud 0 491 p:3 GSM/8000 d 20 33 33 33 34 30 d 30 32 35 35 d 30 30 30 37 d 30 30 30 d 30	RTP/AV 3 97 98 8 0 				gre
Hessage How Sess How Se Co How Fin E Co HTin E Se Me Me Me Me Me Me 0 04 0a 0 32 31 0 04 0a 0 30 24 0 20 40 0 30 24 0 30 30 0 30	ion Description Protocol ssion Description Protoco ner/Creator, Session Id ssion Name (s): SJphone nnection Information (c) me Description, active t ssion Attribute (a): dir dia Description, name an dia Attribute (a): rtpma dia Attribute (a): rtpma dia 0 00 07 20 38 38 38 38	(c): - 3334021007 333402 : IN IP 192.168.0.20 ime (t) 0 0 ection:active d address (m): aud 0 491 p:3 GSM/8000 d 20 33 33 33 34 30 4 30 32 31 30 30 37 9 32 22 91 36 38 22 1 3 70 68 67 66 65 00 0 31 39 32 22 81 36 a.c.	RTP/AV 3 97 98 8 0 o =- 33340 o =- 33340 o				gre

Figure 17. Test 1: Packet Capture on Client A

E.2. Client B

Figure 18 is a snapshot of the packets captured on Client B.

	B Call A) - Ethereal Gapture Analyze Statist	öcs Help		
			• • • • • • ± 🗏 🖳 • • • • • • • • • • • • • • • • • •	0
jiter:			▼ Expression Glear Apply	
Vo Time	Source	Destination	Protocol Info	~
3 7.367234	192.168.0.20	192.168.0.10	SIP/SDP Request: INVITE sip:192.168.0.10, with session description	
4 7.390962 5 7.412628	192.168.0.10	192.168.0.20	SIP Status: 100 Trying NBNS Name query NB WWW.SJLABS.COM.00>	
6 7.672186	192.168.0.10 192.168.0.10	192.168.0.255 192.168.0.20	SIP Status: 180 Ringing	
7 8.112268	192.168.0.10	192.168.0.255	NBNS Name query NB WWW.SJLABS.COM <do></do>	
8 8.503570	192.168.0.10	192.168.0.255	NBNS Name query NB WWW.SJLABS.COM <dd></dd>	
	192.105.0.10	192.100.0.20	KIP Payload type=634 06.10, 35KC=1/550/5, Seq=19546, IIme=0, Mark	
10 9.330833 11 9.334465	192.168.0.10 192.168.0.20	192.168.0.20 192.168.0.10	SIP/SDP Status: 200 0K, with session description SIP Reguest: ACK sip:192.168.0.10:5060	≻ orang
12 9.555518		192.105.0.20	KIP Payload type=55M U6.10, 55KL=1/55U/5, 5eg=19549, 11ME=160	
13 9.336387	192.168.0.20	192.168.0.10	RTP Payload type=GSM 06.10, SSRC=14249088, Seq=18412, Time=O, Mark	
14 9.338157	192.168.0.10	192.168.0.255	NBNS Name query NB WWW.SJLABS.COM.coo>	
15 9.345580 16 9.346743	192.168.0.10 192.168.0.20	192.168.0.20 192.168.0.10	RTP Payload type=GSM 06.10, SSRC=1755075, Seq=19550, Time=320 RTP Payload type=GSM 06.10, SSRC=14249088, Seq=18413, Time=160	
17 9.351943	192.168.0.20	192.168.0.10	RTP Payload type=GSM 06.10, SSRC=14249088, Seq=18414, Time=320	
18 9.356063	192.168.0.10	192.168.0.20	RTP Payload type=GSM 06.10, SSRC=1755075, Seq=19551, Time=480	
19 9.362359	192.168.0.20	192.168.0.10	RTP Payload type=GSM 06.10, SSRC=14249088, Seq=18415, Time=480	
20 9.366449	192.168.0.10	192.168.0.20	RTP Payload type=65M 06.10, SSRC=1755075, Seq=19552, Time=640	
21 9.372781	192.168.0.20	192.168.0.10	RTP Payload type=GSM 06.10, SSRC=14249088, Seq=18416, Time=640 PTP Payload type=GSM 06.10, SSRC=1755075, Sen=19553, Time=800	v
Session Initiat Status-Line: Message Heade Message Leade	SIP/2.0 200 OK er scription Protocol Description Protocol 1		2121 TM TD4 192 168 N 1N	
 ● Owner/Cre Session N ● Connectio ● Time Desc ● Session A ● Media Desc 	Name (s): SJphone on Information (c): D cription, active tim. Attribute (a): direct scription, name and a	ion:active ddress (m <mark>)</mark> : audio 491		> purpl
Gumer/Cre Session N Connectio Time Desc Session A Media Des Media Att 100 76 3d 30 0d 110 31 37 31 20 200 4e 20 49 50 31 30 0d 0a 200 34 94 e 20	Name (s): SJphone on Information (c): 1 cription, active tim- Attribute (a): direct scription, name and a tribute (a): rtoman:3 0a (57 30 20 20 33 33 33 33 34 30 34 3; 33 33 34 30 34 3; 34 20 31 39 32 2e 3; 73 30 53 4a 70 68 61 49 50 34 20 31 39 3;	N IP4 192.168.0.1 ion:active ddress (m): audio 491 SSM/SCCC 1 36 38 24 30 24 32 v= 1 36 38 24 30 24 1 66 85 04 08 63 107 7 66 85 04 08 63 107 2 28 31 36 18 20 = 1	70 RTP/. <mark>V</mark> P 3 101 2.g=- 3334042 13334 042171 I IP4 19 2.168.0. .s=50 phone.c V IP4 192.168.	purple
Gomer/Cre Session M Gonnectio Time Desc Session A Media Des Media Att 160 76 3d 30 0d 17 31 20 200 4e 20 49 50 210 31 30 0d 0a 220 30 2e 31 30	Name (s): SJphone on Information (c): D cription, active tim. Attribute (a): direct scription, name and a tribute (a): rtoman:3 0a (57 do 2d 00 33 3) 33 33 34 30 01 39 32 24 33 34 20 31 39 32 24 33 73 3d 53 4a 70 68 61 49 50 34 20 31 39 33 0d 0a 74 3d 30 20 30	N IP4 192.168.0.1 ion:active ddress (m): audio 491 (SW/8000 2 31 37 31 20 44 32 v= 2 31 37 31 20 44 32 v= 1 36 38 28 30 24 N 1 66 85 0d 0a 63 10 2 26 31 36 38 2e = II 0 0d 0a 61 36 64 0.1	70 RTP/(VP 3 101 	> purple
Gomer/Cre Session M Gonnectio Time Desc Session A Media Des Media Att 160 76 3d 30 0d 17 31 20 200 4e 20 49 50 210 31 30 0d 0a 220 30 2e 31 30	Name (s): SJphone on Information (c): 1 cription, active tim- Attribute (a): direct scription, name and a tribute (a): rtoman:3 0a (57 30 20 20 33 33 33 33 34 30 34 3; 33 33 34 30 34 3; 34 20 31 39 32 2e 3; 73 30 53 4a 70 68 61 49 50 34 20 31 39 3;	N IP4 192.168.0.1 ion:active ddress (m): audio 491 (SW/8000 2 31 37 31 20 44 32 v= 2 31 37 31 20 44 32 v= 1 36 38 28 30 24 N 1 66 85 0d 0a 63 10 2 26 31 36 38 2e = II 0 0d 0a 61 36 64 0.1	70 RTP/. <mark>V</mark> P 3 101 2.g=- 3334042 13334 042171 I IP4 19 2.168.0. .s=50 phone.c V IP4 192.168.	> purpl

Figure 18. Test 1: Packet Capture on Client B

E.3. Analysis

The packet captures indicate that as soon as Client B initiated a call to Client A, Client B sent out an "INVITE" message from 192.168.0.20:5060 to Client A at 192.168.0.10:5060 (red outline in Figure 17). The "INVITE" message had embedded SDP information to inform Client A that Client B will send and receive RTP voice packets at 192.168.0.20 on port 49192 (green outline in Figure 17). Client A acknowledged the invitation by sending Client B a "200 OK" message (orange outline in Figure 18) with embedded SDP information indicating that it will send and receive RTP voice packets at 192.168.0.10 on port 49170 (purple outline in Figure 18). Subsequent voice exchanges between the two clients were achieved via 192.168.0.20: 49192 on Client B and 192.16.0.10: 49170 on Client A (blue outline in Figure 17).

THIS PAGE INTENTIONALLY LEFT BLANK
APPENDIX C. TEST 2: SINGLE NAT VOIP DEMONSTRATION USING SJPHONE

The instructions contained in this appendix describe how to setup and demonstrate a SIP-based VoIP communication between two SIP-enabled clients via a Network Address Translation (NAT) device. In this setup, Clients A and B belong to different networks and Client B is located behind a NAT device. The NAT device is configured to act as a router and modify the destination or source IP address of all packets that traverse it. In this scenario, Client B initiates a VoIP call to Client A.

The demonstration consists of two parts. They are very similar in nature except that a firewall is introduced in the second part. Packet captures and an analysis are included for each part.

A. Without Firewall

A.1. Network Topology

Refer to Figure 7 for the physical and logical network topology.

A.2. Equipment Requirements

A.2.1. Client A and Client B

- A.2.1.1. Windows XP Operating System
- A.2.1.2. Sound Card
- A.2.1.3. SJPhone v.1.60
- A.2.1.4. Ethereal
- A.2.1.5. ZoneAlarm (Client A only)

A.2.2. NAT

- A.2.2.1. Linux Operating System (Fedora Core 4)
- A.2.2.2. netfilter and iptables
- A.2.2.3. Ethereal

A.2.2.4. Two network cards

A.2.3. Additional Equipment

- A.2.3.1. Cross-over cables to implement the network architecture illustrated in Figure 7
- A.2.3.2. Microphones as audio input devices for Client A and Client B

A.2.4. Installation and Configuration

A.2.4.1. Client A

IP Address: 192.168.0.10 Subnet Mask: 255.255.255.0 Default Gateway: 192.168.0.1

A.2.4.2. Client B

IP Address: 192.168.0.20 Subnet Mask: 255.255.255.0 Default Gateway: 192.168.1.1

A.2.4.3. NAT

- A.2.4.3.1. Configure eth0 by editing /etc/sysconfig/networkscripts/ifcfg-eth0: DEVICE=eth0 BOOTPROTO=NONE IPADDR=192.168.0.1 NETMASK=255.255.255.0
- A.2.4.3.2. Activate eth0 by running: ifup eth0
- A.2.4.3.3. Configure eth1 by editing /etc/sysconfig/networkscripts/ifcfg-eth1:

DEVICE=eth1

BOOTPROTO=NONE

IPADDR=192.168.1.1

NETMASK=255.255.255.0

A.2.4.3.4. Activate eth1 by running:

ifup eth1

A.2.4.3.5. Enable IP Forwarding by running:

echo 1 > /proc/sys/net/ipv4/ip_forward

A.2.4.3.6. Flush any existing firewall and NAT rules by running:

iptables -F

iptables -t nat -F

A.2.4.3.7. Configure NAT rules by running:

iptables -t nat -A POSTROUTING -o eth0 -j SNAT --to 192.168.0.1 iptables -t nat -A PREROUTING -i eth0 -j DNAT --to 192.168.1.10

- A.2.4.4. SJPhone Installation and Configuration
 - A.2.4.4.1. Client A and Client B

A.2.4.4.1.1.	Download the Windows version of SJPhone v.160
from S	SJLabs

A.2.4.4.1.2.	Install SJPhone v.160
A.2.4.4.1.3.	Launch SJPhone
A.2.4.4.1.4.	Right-click on SJPhone
A.2.4.4.1.5.	Go to Services
A.2.4.4.1.6.	Select PC-to-PC (SIP)

A.2.4.5. Ethereal Installation and Configuration

A.2.4.5.1. Client A and Client B

A.2.4.5.1.1.	Download the latest Windows version of Ethereal
A.2.4.5.1.2.	Install Ethereal

A.2.4.5.2. NAT

- A.2.4.5.2.1. Install Ethereal if it is not already installed:
 - A.2.4.5.2.1.1. Go to the Desktop menu
 - A.2.4.5.2.1.2. Go to System Settings
 - A.2.4.5.2.1.3. Go to Add/Remove Applications
 - A.2.4.5.2.1.4. Click on Details under System Tools

- A.2.4.5.2.1.5. Find and then check ethereal-gnome
- A.2.4.5.2.1.6. Click on Close
- A.2.4.5.2.1.7. Click on Update
- A.2.4.5.2.1.8. Put in the correct Fedora Core 4 CDs when

prompted

A.3. Preparation and Testing

- A.3.1. Adjust volume on both clients accordingly
- A.3.2. Plug microphones into both clients
- A.3.3. On client A,
 - A.3.3.1. Launch Ethereal
 - A.3.3.2. Go to the Capture menu
 - A.3.3.3. Go to Interfaces
 - A.3.3.4. Click on Capture 192.168.0.10

A.3.4. On client B,

- A.3.4.1. Launch Ethereal
- A.3.4.2. Go to the Capture menu
- A.3.4.3. Go to Interfaces
- A.3.4.4. Click on Capture 192.168.1.10

A.3.5. On NAT,

- A.3.5.1. Launch one instance of Ethereal
- A.3.5.2. Go to the Capture menu
- A.3.5.3. Go to Interfaces
- A.3.5.4. Click on Capture Eth0
- A.3.5.5. Launch another instance of Ethereal
- A.3.5.6. Go to the Capture menu
- A.3.5.7. Go to Interfaces
- A.3.5.8. Click on Capture Eth1
- A.3.6. On Client B,
 - A.3.6.1. Call A by dialing 192.168.0.10 in SJPhone
- A.3.7. On Client A,
 - A.3.7.1. Select Accept in the pop-up dialog box when SJPhone rings

- A.3.8. Clients A and B may engage in a VoIP conversation at this point
- A.3.9. Click on the Hang-Up bottom on either SJPhone to terminate the call when finished
- A.3.10.On Client A, Client B, and NAT,
 - A.3.10.1. Stop packet captures by selecting Stop on Ethereal

A.4. Packet Captures

A.4.1. Client A

Figure 19 is a snapshot of the packets captured on Client A.



Figure 19. Test 2: Packet Capture on Client A (without firewall)

A.4.2. Client B

Figure 20 is a snapshot of the packets captured on Client B.

B (No firewall B Call A) - Ethereal	io u onup		
Elle Edit Yew Go Capture Analyze Stat	istics Help		
왕왕왕왕왕 그 신	x 40 🗒 🕅 4	• ● ● 予 ⊻ 🗏 🗟 @ Q Q Q 🖸 🖉 🕅 🔛 🛠 🔞	
Eiter:		 Epression Qear Apply 	
No Time Source	Destination	Protocol lafo	Ā
1 0.000000 192.168.1.1	Broadcast	ARP who has 192.168.1.10? Tell 192.168.1.1	
2 0.000009 192.168.1.10	192.168.1.1	ARP 192.168.1.10 is at 00:0f:1f:18:d7:c5	
3 0.000053 192.168.0.10 4 0.000070 192.168.1.10	192.168.1.10 192.168.0.10	ICMP Echo (pîng) request ICMP Echo (pîng) reply	
5 23.452688 192.168.1.10 6 58.163531 192.168.1.10	192.168.1.255 192.168.1.255	UDP Source port: 5003 Destination port: 5003	
7 58.632910 192.168.1.10	192.168.0.10	BROWSE Domain/Workgroup Announcement WORKGROUP, NT Workstation, Domain Enum SIP/SD Request: INVITE sip:192.168.0.10, with session description	
8 58.770357 192.168.0.10 9 58.980857 192.168.0.10	192.168.1.10 192.168.1.10	SIP Status: 100 Trying SIP Status: 180 Rinning	
10 60.479220 192.168.0.10	192.168.1.10	SIP/SD Status: 200 OK, with session description) orange
11 60.483516 192.168.1.10 12 60.486993 192.168.1.10	192.168.0.10 192.168.0.10	SIP Request: ACK \$19:192.168.0.10:5060 RTP Payload type=GSM 06.10, SSRC=969333836, Seq=15618, Time=0, Mark	J
13 60.488752 192.168.0.10	192.168.1.10	RTP Payload type=GSM 06.10, SSRC=209846736, Seg=23035, Time=0, Mark	
14 60.489050 192.168.0.10 15 60.497380 192.168.1.10	192.168.1.10 192.168.0.10	RTP Payload type=GSM 06.10, SSRC=209846736, Seq=23036, Time=160 RTP Payload type=GSM 06.10, SSRC=969333836, Seq=15619, Time=160	
16 60.498366 192.168.0.10	192.168.1.10	RTP Payload type=GSM 06.10, SSRC=209846736, Seq=23037, Time=320	
17 60.507716 192.168.1.10 18 60.508798 192.168.0.10	192,168.0,10 192,168.1,10	RTP Payload type=GSM 06.10, SSRC=969333836, Seq=15620, Time=320 RTP Payload type=GSM 06.10, SSRC=209846736, Seq=23038, Time=480	
19 60.518293 192.168.1.10	192.168.0.10	RTP Payload type=GSM 06.10, SSRC=969333836, Seq=15621, Time=480	
20 60.519071 192.168.0.10 21 60.528587 192.168.1.10	192.168.1.10 192.168.0.10	RTP Payload type=GSM 06.10, SSRC=209846736, Seq=23039, Time=640 RTP Payload type=GSM 06.10, SSRC=969333836, Seq=15622, Time=640	
22 60.529552 192.168.0.10	192.168.1.10	RTP Payload type=G5M 06.10, SSRC=209846736, Seq=23040, Time=800	
23 60.539033 192.168.1.10 24 60.539951 192.168.0.10	192.168.0.10 192.168.1.10	RTP Payload type=GSM 06.10, SSRC=969333836, Seq=15623, Time=800 RTP Payload type=GSM 06.10, SSRC=209846736, Seq=23041, Time=960	
25 60.549443 192.168.1.10	192.168.0.10	RTP Payload type=GSM 06.10, SSRC=969333836, Seg=15624, Time=960	
26 60.550361 192.168.0.10 27 60.559892 192.168.1.10	192.168.1.10 192.168.0.10	RTP Payload type=GSM 06.10, SSRC=209846736, Seq=23042, Time=1120 RTP Payload type=GSM 06.10, SSRC=969333836, Seq=15625, Time=1120	
Internet Protocol, Src: 192.16 User Datagram Protocol, Src PG Session Initiation Protocol Session Initiation Protocol Message Header Message Header Bescape hndv Session Description Protoc Session Description Protoc	8.0.10 (192.168.0.10 rt: 5060 (5060), Dst 00 00 Version (v): 0 d (0): - 3334907423 e): N IP4 192.168.0 tim. (t): 0 0 tim. (t): 0 0 ti	3334907423 IN IP4 192.168.0.10 10 10 49152 RTP/A > 3 101	} purple
0010 02 a9 00 5d 00 00 7f 11 b 0020 01 0a 13 c4 13 c4 02 95 5 0030 30 20 32 30 30 20 4f 4b 0 0040 49 50 2f 32 2e 30 2f 55 4 0050 36 38 2e 31 2e 31 30 3b 7	0 7d 53 49 50 2f 32 d 0a 56 69 61 3a 20 4 50 20 31 39 32 2e 2 70 6f 72 74 3d 35 6 65 64 3d 31 39 32 2 72 61 6e 63 68 3d 1 38 30 31 30 61 30	88]	

Figure 20. Test 2: Packet Capture on Client B (without firewall)

A.4.3. NAT eth0

Figure 21 is a snapshot of the packets captured on the first interface (eth0) of the NAT device.

	1 21 01					E)	4.5	5 0	TI DE QQQE MMBX D
-			-	1 ^	48	2	-		
		_					_		Que Bah
B.+.	Tee 144,74058	5000		_	Detrution 192.1.68	4.144		Hotaci IENS	
42	144, 92214	142.1	144.0.1		192.168			ERS .	Nune query NB Wex.SSL485.COM/OD- Status: 180 Afriqing
- 63	143.48928	12.1	148.0.5		192.1,68	4.255		dest.	Name query ME WAX STLARS, COM (00)
54 41	145.23907	192.1	168.0.1	_	192.168			end in	Nume query NE WAX.12LABS.COM-02D Status: 200 GW, with session description
- 66	147, 50775	192.1	168.0.1		292.1.68	0.20		922	Request: ACK 456:192.1.68.0.10:5060
- 67	147.11436	192.1	168.0.1		192.1.68	4.10		179-	Payload type=GSM 06.10, SSHC+96833380, Sep-15618, Time=O, Mark Payload type=GSM 06.10, SSHC+208040736, Sep-23035, Time+O, Mark
	147.51760				1第.1册 192.1册			8	Mayload type-dam of.10, 196-4109946/16, 34041925), Fime+060 Payload type-dam of.10, 596-209946736, Sep-23036, Time+060
70	147.53430	192.1	168.1.1		152.1.68	0.10		172	Fayload time-G98 06.10, 19AC-966913896, Sep-11629, Time-D60
	147.5356				192.1.68			ext.	Name query NE WAK.SILABS.COM.OD
	147.59609 147.55467				182.148 182.148			472 172	Auylaud type-GDM 06.10, 55K-200646736, Sep-23037, Time-320 Paylaud type-GDM 06.10, 55K-946933866, Sep-25620, Time-320
74	147,55603	252.5	48.0.5		292.1.68	2.20		112	Payload type+GSM 06.10, SSRC-209846736, Sep-23058, Time+480
75	147.57438	192.1	168.1.1		192.1.68	0.10		17P	Paylisad type=G9K 06.10, 559C+96933836, Sep-15621, Time=480
10	147, 57570 147, 59467		168.0.1		192.168			17	Rejised Type+GSM 06.10, SSE-200046736, Sep-13036, Time+640 Rejised Type+GSM 06.10, SSR-960033836, Sep-13622, Time+640
18	147.59580	197.	168.0.1		152.168			17	Payload tjpe-GSM 06.10, SSRC-201896734, Sep-23040, Time-800
	147.6469				1號.1胡			12	Payload type=634 06.50, 554C=969333836, Sep-35623, Time=800
	147.61514				192.1.68 192.1.68			172 173	Payload type=CDM 06.10, SSRC=209646736, Sep=23041, Time=960 Payload type=CDM 06.10, SSRC=969833866, Sep=25624, Time=960
	147.63567				192.168				Payload type-GPM 06.10, 1992-200946736, Sep-23042, Time-1120
83	147,45407	192.1	168.1.1		192.1/6	0.10		CP	Payload type=GDM 06.10, SDR-209846736, Sep-13043, Time=1120 Payload type=GDM 06.10, SDR-980933886, Sep-13625, Time=1120
	10.67月 147.64月		64.0.5	2	192.1億			179- 179-	Rey10ad type=dax 06.10, SSRC+209846736, Sep+13043, Time+1280 Rey10ad type=dax 06.10, SSRC+968333636, Sep+13626, Time+1280
- 82	241,51425		100.0.0	_	182.168				Payroad Cyperson Study, Solutional Sectors, Sectors, Contractor
86	147, 67548			2	192.148	2.29		5P	Paylinad type=058 06.10. 558C-206646736. Sec-23044. Time=0440
Bő ST Frank E Cther	147.67548 147.69406 1 (60 by net 11, 5	tes or rc: 19	168.1.1 1 wire, 12.268.0	60 byc	icitat:	(8.10 red) 19:27:3	6), p	64	Payload tjpe-634 04.10, 559C-200946736, 5ep-20044, Ther-6440 Payload tjpe-634 04.10, 559C-4943535856, 5ep-21627, Ther-6440 Sudcast (Hith shidth shift)
Bő ST Frank Ether	147.67548 147.69406 1 (60 by	tes or rc: 19	168.1.1 1 wire, 12.268.0	60 byc	197.148 es captu lobfafra	(8.10 red) 19:27:3	6), p	64	Ayload type-09(0.10, 192-9603389, Sep-1927, Mer-144)
86 87 1 Frane 1 Cther 1 Addre 1 Addre 000 fr 000 fr 000 0	147.67548 147.69406 1 (60 by net 11, 5	195.1 tes or rc: 19 tion #	F 00 C	60 Dyr. 110 (0 (requ	257.165 toff.15f.t est/gr.t 27.16 27.16 27.00 00.00	4.50 red) 19:27:3 rt tous s 54 0 0 0 48 0	6), D 489) 0 (1	tt: Bro	Ayload type-09(0.10, 192-9603389, Sep-1927, Mer-144)

Figure 21. Test 2: Packet Capture on eth0 of NAT (without firewall)

A.4.4. NAT eth1

Figure 22 is a snapshot of the packets captured on the second interface (eth1) of the NAT device.

te bit lieu de Cat	diBcall A) - Ethenal		
· · · · · ·	tun Bulan Salata	26	
	i BEX	83 84	*****
ber:			Consin Der Bah
in The St	Wit	Detrain	httal 3fs
2 0.000104 15	0.166.1.1	Broadcast 192.168.1.1	APP 192.168.1.10 fs at 00:0f:10/10:05
3 0.000116 19		192.168.1.10	APP ancientary o el weintartanonco 109 Eche (ping) repert
4 0.000218 19 5 45.591883 19		192.168.0.10 192.168.1.255	100 Echo (ping) reply up Source port: 5001 cestimation port: 5001
6 115. 24522 19	2.168.1.10	192.168.1.255	UDP Source port: 5000 Destination port: 5000 SROWSE Convin/Apriatoup Announcement WCRKGROUP, wit workstation, Comain Enum
7 116.19816 19		192.168.0.10	SIP/SD Request: Journe stp:100.168.0.10, with sension description
8 116. 32072 19 9 116. 53122 19	2.168.0.10	192.168.1.10 192.168.1.10	SIP Status: 100 Trying SIP Status: 180 Alreing
10 119.10790 19	2.168.0.10	192.168.1.50 103.168.4.16	SIP Status: 180 Finging SIP/D Status: 200 or, with sestion description The Description of the Status of the Status
12 119, 12296 19	2.168.1.10	192.168.0.10 192.168.0.10	51# Repuest: ACK s1p:132.168.0.10:5000 #T# Fayload type-63M 04.10, 55RC-049333836, Sep-13418, Time-0, Mark
13 119.12674 19	2.168.0.10	197.168.1.10	HF Payload type-GM 04.10, SDRC-208846776, Sep-2005, The-4, Kark KF Payload type-GM 06.10, SDRC-208845776, Sep-2006, The-160
14 119, 12682 19 15 119, 1428E 19	2.168.1.10	192.168.1.10 192.168.0.10	KTP Payload type-coll 06.10, SSRC-066933836, Sep-1503, T18e-L60 KTP Payload type-coll 06.10, SSRC-066933836, Sep-15639, T18e-L60
16 119.14467 19	2.268.0.20	192.168.1.10	HTP Phyloid type-GP 06.10, SSRC-06033406, Sep-15036, Time-160 HTP Phyloid type-GP 06.10, SSRC-06846716, Sep-2007, Time-300
17 119, 16367 19 18 119, 16467, 19	12.168.0.10	192.168.0.10 192.168.1.10	RTP Payload type-cox 06.10, 55RC-80833886, 5ep-15620, T/me-320 RTP Payload type-cox 06.10, 55RC-30886736, 5ep-20038, T/me-480
19 119, 18299 19	2.168.1.10	192.168.0.10	RTP Payload type=GDM 06.10, SDRC=969333816, Sec=15621, T18E=480
20 119, 18434 19 21 119, 20267 19	2.168.1.10	192.168.1.10 192.168.0.19	RTP Payload type-com 06.10, 55RC-009646736, Seb-20039, Time-640 RTP Payload type-com 06.10, 55RC-069533836, Sep-15622, Time-640
22 119, 20444 19	2.168.0.10	192.168.1.10	RTF FRUISAG TVD8+G5K 06.10, 55RC+209846736, 560+23040, T188+800
23 119.22169 19 14 119.22437 19	2.168.1.10	192.168.0.10	RTP Payload type-cox 06.10, 55RC-168333836, 580-15633, t1ma-800 RTP Payload type-cox 06.10, 55RC-30866736, 580-2041, t1ma-860
25 119. 24265 19	2.168.1.10	192.168.0.10	RTF Payload type-GM 06.10, SSRC-969133816, Sec-15624, Time-960
26 119, 2430 19		192.168.1.10	877 Payload type-639 06.10, 55RC-209846736, Sep-23042, Time+1120
Frame 1 (42 bytes Ethernet 11, Src:	on vire, 42 byt 192.168.11.1 (00	:温:说:新:第:%), 0	<pre>xTP Payload type=CSP 06.10, SSRC=968338366, Seq=15635, Time=1120 st: aroudcust (ff:ff:ff:ff:ff:ff:ff)</pre>
Frame I (42 bytes	on vire, 42 byt 192.168.11.1 (00	es captured) :01:02:89:97:56), 0	FTP Fayload type=GPE 06.10, SIRC-96833836, Sep-1903, Time-1120
Frane I (42 bytes Ethernet II, src: Address Resolutio	f ff 60 01 02 42	es captured) 	#FP Fayloud type-cor 06.10, SSRC-96833836, Sep-15025, The-1120 st: aroudcast (ff:ff:ff:ff:ff:ff:ff)

Figure 22. Test 2: Packet Capture on eth1 of NAT (without firewall)

A.4.5. Analysis

Since all packets exchanged between Clients A and B are processed by the NAT rules, understanding those rules is essential when analyzing the traffic flow captured by Ethereal. The SNAT rule "iptables -t nat -A POSTROUTING -o eth0 -j SNAT --to 192.168.0.1" instructed the NAT device to modify the source IP address of all outgoing packets to 192.168.0.1 before routing them. Thus, all the packets received by Client A appeared to come from the NAT device (see packet capture for Client A). The DNAT rule "iptables -t nat -A PREROUTING -i eth0 -j DNAT --to 192.168.1.10" instructed the NAT device to change the destination IP address of all incoming packets to 192.168.1.10 before routing those packets. This operation allowed packets sent to the NAT to be routed to Client B.

The process of establishing a connection between Clients A and B in this test was very similar to the one described in Appendix B. First, Client B sent out an "INVITE" message from 192.168.1.10:5060 to 192.168.0.10:5060 on Client A (red outline in Figure 19). The "INVITE" message had embedded SDP information to inform Client A that Client B will send and receive RTP voice packets at 192.168.1.10 on port 49154 (green outline in Figure 19). Client A acknowledged the invitation by sending Client A an "200 OK" message with embedded SDP information indicating that it will send and receive RTP packets at 192.168.0.10 on port 49152 (orange outline in Figure 20).

Subsequent voice communication between the two clients was sent to the IP addresses and ports specified in SDP. In other words, Client B sent RTP packets directly to Client A at 192.168.0.10 and Client A sent RTP packets directly to Client B at 192.168.1.10 (blue outline in Figure 19). The former was legitimate because Client A was publicly reachable. But the latter was only possible in our setup since neither Client A nor the NAT device was configured to drop packets destined for private IP addresses. In this case, the NAT device simply forwarded the RTP packets to client B (see Figures 21 and 22). To simulate a more realistic network configuration, a firewall was needed to drop packets sent by Client A and destined for Client B.

- B. With Firewall
 - B.1. Network Topology

Refer to Figure 7 and Figure 8 for the physical and logical network topology.

B.2. Preparation and Testing (in addition to all steps described in Section A)

B.2.1. On Client A,

- B.2.1.1. Download the ZoneAlarm from Zone Labs
- B.2.1.2. Install ZoneAlarm
- B.2.1.3. When ZoneAlarm is being run for the first time, it will ask the user to choose between Basic ZoneAlarm or the trial version of ZoneAlarm Pro, select the trial version of ZoneAlarm
- B.2.1.4. When asked to select a security level for the detected network, select Allow into Trusted Zone
- B.2.1.5. Configure firewall rule in ZoneAlarm:
 - B.2.1.5.1. Go to Firewall menu on the left panel
 - B.2.1.5.2. Click on the Expert tab
 - B.2.1.5.3. Click on Add
 - B.2.1.5.4. Type in a name for the firewall rule in the Name textbox
 - B.2.1.5.5. Under Action, select Block
 - B.2.1.5.6. Under Destination,
 - B.2.1.5.6.1. Select Modify
 - B.2.1.5.6.2. Select Add Location
 - B.2.1.5.6.3. Select IP Address
 - B.2.1.5.6.4. Type in a description in the **Description** textbox
 - B.2.1.5.6.5. Type 192.168.1.10 in the IP Address textbox
 - B.2.1.5.6.6. Click OK
 - B.2.1.5.6.7. Click OK
 - B.2.1.5.6.8. Click Apply
- B.2.2. Run test as described in Section A

B.3. Packet Captures

B.3.1. Client A

Figure 23 is a snapshot of the packets captured on Client A.



Figure 23. Test 2: Packet Capture on Client A (with firewall)

B.3.2. Client B

Figure 24 is a snapshot of the packets captured on Client B.

@ B (1	NATO	tewal)	- Ether	ul.																										
(h (i	8 yr	. 9	Çaphure	finalize	Şahite	90	1																			30723				
	10	1 8	-	BE	X	1	8	9	4	44	4	ł	1		3	0	Q	91	1	1	1	1	X	0						
(Rer)										(orma		8	ety.																	
No.	Time	Turan	Source	Stussus		Desta	Nation	1.02		Protocol	245		111		12/5					vite	100	11/13/	s7/65	h:	 	 	- 6			
	0.0	00000	192.1	68.1.10		192	158,0	2,10		SIP/SI	Reque	it:	IN	TTE	stort	.92.1	68.0	10, 1	with	585	ston	descr	1pt1	00				1		
				68.0.10			10.1			11#	statu																	5	oron	~
				0110110						119/51	ALC: N				with With				al to al	(IN									oran	ge
				68.1.10 68.1.10			168.0			RTP	Pay10	ld 1	type	6-69	06.1	0, 1	SRC+	37954										1		
	1,9	99278	192.1	66.0.10		192	.140.1	.10		ATP	Fky10	1d 1	type	6-69	00.1	0, 1	SRC+	11794	0735	11	0+261	199, 1	100-	120						
				68.1.10 68.0.10			168.0			ATP ATP	Paylo		t ype t yne	1-69 1-69	00.1	0, 1		17954	025.	580	- 1921 C- 276	00. T	8×32 188×	480						
1	11.9	16590	192.1	68.1.10		192	.168.0	9,10		RTP.	Phylo	101	type	e-69	06.1	0, 1	SRC+.	37954	025.	Seq	+ 5921	• T -	6=43	2				1		
1	$\frac{1.9}{1.0}$	60106	192.1	68.0.10		192	168.1	1.10		RTP	Paylo	10 1	type	1+69	06.1	0, 1	SRC.	1794	0735	58	0-20 301/	191. T	188-	640					15 18	
-		NOTO D				- 677	ecine		-	11	1 Will	н	and.	DW.			100		0 ISA	-1	Ð		1110	100				ſ.	dark	re
				68.0.10			168.1			ATP					06.1									960			Π.)	quint	
- 1	71.9	87892	192,1	68.1.10		192	148.0	2,10		ATP	Pay10	10.1	týpi	e-69	05.1	0, 1	\$86.	37954	025.	Sec	• 193	11	8+96							
				68.0.10			168.1			ATP ATP					06.1															
2	0 2.0	01837.	192.1	68.0.10		192	168.1	1.10		ATP	Faylo	14 3	type	1-69	00,1	0, 1	\$80+	11794	0735.	. 54	q+26	191, T	10.8+	1280						
				68.1.10 68.0.10			168.1			RTP RTP	Paylo	101	type	1-09	06.1	0, 1	SIC .	17954	025,	Seq	+103	, Tis	8+12 1-4-	90 1440						
- 2	2.0	19207	192.1	68.1.10		192	148.0	0.10		RTP .	Paylo Paylo	id i	type	-69	06.1	0, 1	sk.	17954	025.	Seq	- 593	, Th	6+14	40						
				68.0.10 68.1.10			168.1			ATP ATP	Paylo	10	type	1-69	06.1	0, 1	SRC+	11794	0735,	- 54	Q+26	197 , T	164-	1600						
2	6 2.0	13192	192.1	68.0,10		192	168.1	.10		ATP	Paylo	Id.	type	e=69	06.1	0, 1	SRC+	11794	0735.	. 50	Q+26	198. T	ine-	1760						
				68.1.10 68.0.10			168.0			RTP RTP	Paylo	1	type	1-69	06.1	0, 1	SIC+	7954	025.	Seq	+591	. Th	4-17	60						
# Inte User So De Le Sess # St B Me H Me	innet bata iurce istina ingth: iatus- issage sessi Ses	Proto agram I port: ation p : 064 Enitia: Headd Hody Son Des Sion Des Sion Des Sion A Ha Des Sion A Ha Des Sia Att Sia Att	col, 5 Protoc Soco Soco Soco Soco Soco Soco Soco	2.168.1. rc: 192 0), Src (5060) 5060 (5060) 5060 (5060) ratocol 100 Prat protocol 100 Prat protocol 101 Prat protocol 102 Prat proto	,168.(Port: 000) (tocol nor nor tocol nor tocol nor tocol nor tocol nor tocol nor tocol nor tocol nor tocol nor tocol	1 ver 1 ver	(192,3 0 (500 0 (500 150 150 150 150 150 150 150 150 150	(v): 2.16 ve n) 0 hore	.10). Dot P 4 33 .0.1	osti 1 orti 50 14392277 0	92.168 60 (10 4 1N 1	40) 44 1	10 ((192.	.168.1							-							purț	ole
0010 0020 0030 0040	02 AC 01 08 30 20 49 50	07 20 13 64 32 30 27 32	00 0 13 0 10 2 2e 3	5 00 01 0 77 11 4 02 98 0 47 45 1 1A 94 1 1A 94 1 1A 94	4 14 0 00 0 44 5	e c0 2 53 4 56 0 20 A 4#	移 00 移 50 約 10 約	04 0 24 1 34 2	10 a8 12 2e 10 53	0 20	2 0 000 - 0/U D	SIR	2																	

Figure 24. Test 2: Packet Capture on Client B (with firewall)

B.3.3. NAT eth0

Figure 25 is a snapshot of the packets captured on the first interface (eth0) of the NAT device.

1-29 (Eth0	1 NATI	B Call /	firesi	di) - Ethe	real																							1
Edt Ver	9	Qeture	Boalyce	2alisti	a Anb																							
		鸙	6	X	¢	8	9	4	4 2	4	2			9	Q (5	KE								
e								•	Expression	n Ø	ar 8	ply																
. Tre		Source				nation			Protocol																			
2 0.03			168.0.			.168. .168.			SIP/SI SIP			100 Try		92.1	08.0.1	0, witi	n se	55101.0	esors.	001100	-	-	-	-	_	_	_	
3 0.05	1218	192.	168.0.	10		.168.			NENS	Name	que	ry NB W	W. SJL	ABS.	COM+00	Σ												
			168.0.			.168.			SIP			180 Rin																
			168.0. 168.0.				0.255		NENS NENS						COM<00													
7 3.67	73828	192.	168.0.	10	192	.168.	0.1		SIP/SD	Stat	US: 1	200 OK.	with :	sess	ston de	script	on											
			168.0.			168.	0.10		SIP						0.10:5 COMK00													
10 3.68						.168.			RTP								Se	q=5926,	Time	-0, Mar	sk.							
11 3.70						.168.			RTP									Q=5927,										
12 3.71						168.			RTP									eq=2688 q=5928,										
14 3.73	6228	192.	168.0.	10	192	.168.	0.1		RTP	Payl	pad	type=GS	M 06.1	0, 5	SSRC+11	794073	5, 5	eq=2689	0, Tİ	18=480								
15 3.74						.168.			RTP	Payl	oad 1	type=GS	4 06.1	0, 5	ssac+37	954025,	Se	q=5929,	Time	480								
16 3.79						.168.			RTP									eq=2689 q=5930,										
18 3.77	6368	192.	168.0.	10	192	168.	0.1		RTP	Payl	Old 1	type=GS	# 05.1	D, 5	SSRC+11	794073	5, 5	eq=2689	2, Th	18-800								
19 3.78						168.			RTP									q=5931,										
20 3.79 21 3.80						.168.			RTP									eq=2689 q=5932,										
22 3.81	6274	192.	168.0.	10	192	168.	0.1		RTP	Payl	Ded !	type=GS	M 06.1	0, 5	SSAC+11	794073	5, 5	eq=2689	, Ti	e=112								
23 3.82						.168.			RTP.									q=5933,										
24 3.83						.168.			RTP	Pavl	nad 1	урениз	H 06.1		SSRC=11 SSRC=37	954075	(a)	eq=2689 q=5934,	Tima	1280	-							
26 3.85	6209	192.	168.0.	10		168.			RTP	Payl	oad 1	type=GS	N 06.1	0, 5	SSAC+11	794073	5, 5	eq=2689	6, Th	18×144								
27 3.86						.168.			RTP									q=5935, en=7689										
E Own Ses Con Tim Ses Med Med Med Med Med	Proto agram port: tion ; 771 m: 0x initia : Headd : body on Des sion 0 er/Cra sion 1 ia Des ia Att ia Att ia Att ia Att	<pre>col, :: Proto 5060 port: 398a tion : : INV er script eator, Name (on Inf cripti tribut tribut tribut tribut tribut</pre>	Src: 11 (5060) 5060 (5060 (5060) (correce Protocol (correce (correce) (92.168. rc Port (5060) ct] ol protocol protocol protocol rtive t): dir ctive t): dir rtpma rtpma fmtp:	0.1 () : 506 68.0.1 01 Ver (o): - : IN I ime (t ection d addr p:3 GS p:97 1 p:98 1 96 mod	192.1 0 (50 10 51 10 br>10 51 10 10 51 10 10 10 10 10 10 10 10 10 10 10 10 10	68.0.1 60), (9/2.0 (v): 137161 82.168 0 (v): 137161 90 9000 8000	0 0 333 .1.10	st: 192 ort: 50 437161	.168. 60 (5	0.10 060)	(192.1 192.168	.1.10	0)	20)													
0 00 0f 0 03 17				rtpma 0 29 1 75				-						_			_									_		_

Figure 25. Test 2: Packet Capture on eth0 of NAT (with firewall)

B.3.4. NAT eth1

Figure 26 is a snapshot of the packets captured on the second interface (eth1) of the NAT device.

88	29 (E	th1 1 1	WITE	Call	A firewall)	Ether	al																8	6
<u>F</u> le	肤	Yen .	50 (Çapture	Brahran S	(alistics	Help																	
5		9	<u>e</u> i	1	6	x	69 🗄		4 1	¢ 🕫	4	2		0	G	29	*		X	0				
Elter:	C								•	Expression.	Ģer	Booly												
No. •		ine		Source			Destination			Protocol														
					168.1.10		192.16					100 1			100	SVILVI I	1110	session d	BCT IPC IC	/1				
					168.0.10		192.16					: 180 F			eete	a darad	lan ta							
					168.1.10		192.16									n descri 10:5060	ipt it	an .						
	63	. 6896	909 N40	192.	168.1.10		192.16			RTP I	ayloa	d type-	691 0	6.10,	558	C+379540	25,	Seq=5926,	Time=0,	Mark				
					168.0.10		192.16											Seq-5927, Seq-2688						
					168.1.10		192.16			RTP 3	ayloa	d type-	691 0	6.10,	SSR	C+379540	25.	Seq=5928,	Time=320					
					168.0.10		192.16											Seq=2689 Seq=5929,						
	12 3	.7563	84	192.	168.0.10		192.16			RTP I	ayloa	d type-	694 0	6.10,	\$58	C+117940	3735,	Seq=2689.	, Tine-6	40				
					168.1.10		192.16											Seq=5930, Seq=2689.						
	153	,7897	20	192,	168.1.10		192.16	8.0.10		RTP	ayloa	d type-	GSM (6.10,	558	C+37954(25,	Seq=5931,	Time=800					
					168.0.10 168.1.10		192.16											Seq=2689 Seq=5932,						
	18 3	. 8164	18	192.	168.0.10		192.16	8.1.10		RTP I	ayloa	d type-	G9N (6.10,	558	C-11794(0735,	Seq+2689	, Time-1	120				
					168.1.10		192.16			RTP I	ayloa	d type=	694 0 694 0	6.10,	SSR	C=379540	125.	Seq=5933, Seq=2689	Time-112	280				
					168.1.10		192.16			RTP I	ayloa	d type-	691 0	6.10,	558	c+379540	125,	Seq=5934,	Time-128	0				
					168.0.10		192.16											Sep=2689						
					168.1.10		192.16			RTP I	ayloa	d type= d type=	G91 0	6.10.	55R	C-117940	165, 1735.	Seq=5935, Seq=2689	. Tine-1	600				
	25.3	, 8897	20	192.	168.1.10		192.16	8.0.10		RTP I	ayloa	d type-	691 (6.10,	558	C+379540	25,	Seq=5936,	Time=160	0				
-					168.0.10		192.16			RTP I	ay loa ay loa	d type= d type=	G91 0 G91 0	6.10,	558	C=117940 C=379540	1755.	Seq=2689 Seq=5937,	Time+176	.760 0				
					168.0.10		192.16											540+2689						
E In E US E E	Hern Dest Sour Dest Leng Chec essio Requ Mess B Se E E E E E E E E E E E E E E E E E E E	et Pr atagr ce po inati th: 7 ksum: n Ini rest-L age H age b ssion Sessi Owner Sessi Owner Sessi Media Media Media Media	otoc am F rt: on p 71 0x3 tiat ine: eade ody Desc on D besc on A tt Att Att	col, Proto 5060 port: 3881 tion : INV er script escri ator, ame : INV er stript ttrii coript ribu ribu ribu ribu	92.168.1. Src: 192. col, src (5060) 5060 (50 [correct] Protocol ITE sip:1 tion Prot iption Prot ipti	168.1. Port: 60) 92.160 otocol Id (c one (c): tpmap: tpmap: tpmap: 92.160 stocol	10 (190 5060 () 8.0.10 9 versio)): - 33 IN IP4 we (t): tionac address 3 GSM/8 90 fLBC I mode-2	2.168.1 5060), 1 51P/2.0 n (v): 3437161 192.168 0 0 tive (m): a 000 (%000 0 0	10), st Po 0 3334 .1.10	Dst: 19 Pt: 506 4371610	.168.) (506	0.10 (1 0) 4 192.1	68.1.	10		0								
0000 0010 0020 0030 0040	03 00 20 30	17 4 0a 1 73 6 20 5 40 5	2 50 3 64 9 70 3 49 0 74	00 13 3a 50	56 00 0f 00 80 11 c4 03 03 31 39 32 2f 32 2e 0a 20 3f Cal A free P	73 21 38 81 2e 31 30 00	0a 56 50 30	01 0a 0 56 49 5 2e 30 2	0 a8 4 45 e 31	BP sipti 0 SIP/ ctn/0	s!. 8.1	INVITE 58.0.1												-

Figure 26. Test 2: Packet Capture on eth1 of NAT (with firewall)

B.3.5. Analysis

The signaling part of the call was processed as usual with the exchanges of "INVITE" (red outline in Figure 23) and "200 OK" (orange outline in Figure 24) messages between the two clients. Client B still told Client A to send RTP media packets to its private IP address or 192.168.1.10 (green outline in Figure 23). However, Client A can no longer send RTP packets directly to Client B at its private address because ZoneAlarm was configured to block those packets. The ZoneAlarm log files were examined to confirm that packets destined for 192.168.1.10 were, in fact, dropped. The packet captures on Client A indicate that when Client A failed to send RTP packets to the IP address of Client B, it tried to send subsequent RTP packets to the IP address from which it received RTP packets (due to the SNAT rule). In this case, Client A sent the RTP packets to the public IP address NAT or 192.168.0.1 (blue outline in Figure 23). When NAT received the packets, it modified the destination address in the packet header according to the configured DNAT rule. In other words, NAT changed the destination address from its own public IP address (192.168.0.1) to the private IP address of Client B (192.168.1.10) before forwarding the packets (dark red outline in Figure 24). Figures 25 and 26 confirm that DNAT and SNAT were done correctly.

APPENDIX D. TEST 3: DOUBLE NAT VOIP DEMONSTRATION USING SJPHONE

The instructions contained in this appendix describe how to setup and demonstrate a SIP-based VoIP communication between two SIP-enabled clients via two Network Address Translation (NAT) devices. In this setup, Client B is located behind two NATs. Each NAT is configured to act as a router and modifies the destination or source IP address of all packets that traverses it. Packet captures from both clients are included at the end of this appendix along with an analysis.

A. Network Topology

Refer to Figures 9 and Figure 10 for the physical and logical network topology.

- B. Equipment Requirements
 - B.1. Clients A and B
 - B.1.1. Windows XP Operating System
 - B.1.2. Sound card
 - B.1.3. SJPhone v.1.60
 - B.1.4. Ethereal
 - B.1.5. ZoneAlarm (Client A only)
 - B.2. NAT 1 and NAT 2
 - B.2.1. Linux Operating System (Fedora Core 4)
 - B.2.2. netfilter and iptables
 - B.2.3. Ethereal
 - B.2.4. Two network cards
 - B.3. Additional equipment
 - B.3.1. Cross-over cables to implement the network architecture illustrated in Figure 9
 - B.3.2. Microphones as audio input devices for clients A and B
- C. Installation and Configuration
 - C.1. Client A
 - IP Address: 192.168.0.10

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.0.1

C.2. Client B

IP Address: 192.168.2.10

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.2.1

C.3. NAT 1

C.3.1. Configure eth0 by editing /etc/sysconfig/network-scripts/ifcfg-eth0:

DEVICE=eth0 BOOTPROTO=NONE IPADDR=192.168.0.1 NETMASK=255.255.255.0

- C.3.2. Activate eth0 by running: ifup eth0
- C.3.3. Configure eth1 by editing /etc/sysconfig/network-scripts/ifcfg-eth1: DEVICE=eth1 BOOTPROTO=NONE

IPADDR=192.168.1.1

NETMASK=255.255.255.0

C.3.4. Activate eth1 by running:

ifup eth1

- C.3.5. Enable IP Forwarding by running: echo 1 > /proc/sys/net/ipv4/ip_forward
- C.3.6. Flush any existing firewall and NAT rules by running: iptables -F

iptables -t nat -F

- C.3.7. Configure NAT rules by running: iptables -t nat -A POSTROUTING -o eth0 -j SNAT --to 192.168.0.1 iptables -t nat -A PREROUTING -i eth0 -j DNAT --to 192.168.1.2
- C.4. NAT 2
 - C.4.1. Configure eth0 by editing /etc/sysconfig/network-scripts/ifcfg-eth0:

DEVICE=eth0 BOOTPROTO=NONE IPADDR=192.168.1.2 NETMASK=255.255.255.0 GATEWAY=192.168.1.1

- C.4.2. Activate eth0 by running: ifup eth0
- C.4.3. Configure eth1 by editing /etc/sysconfig/network-scripts/ifcfg-eth1: DEVICE=eth1

BOOTPROTO=NONE IPADDR=192.168.2.1 NETMASK=255.255.255.0

- C.4.4. Activate eth1 by running: ifup eth1
- C.4.5. Enable IP Forwarding by running: echo 1 > /proc/sys/net/ipv4/ip_forward
- C.4.6. Flush any existing firewall and NAT rules by running: iptables -F iptables -t nat -F
- C.4.7. Configure NAT rules by running: iptables -t nat -A POSTROUTING -o eth0 -j SNAT --to 192.168.1.2 iptables -t nat -A PREROUTING -i eth0 -j DNAT --to 192.168.2.10
- C.5. SJPhone Installation and Configuration
 - C.5.1. Clients A and B
 - C.5.1.1. Download the Windows version of SJPhone v.1.60 from SJ Labs
 - C.5.1.2. Install SJPhone v.1.60
 - C.5.1.3. Launch SJPhone
 - C.5.1.4. Right-click on SJPhone
 - C.5.1.5. Right-click
 - C.5.1.6. Go to Services
 - C.5.1.7. Select PC-to-PC (SIP)

- C.6. Ethereal Installation and Configuration
 - C.6.1. Clients A and B
 - C.6.1.1. Download the Windows version of Ethereal v.0.10.12
 - C.6.1.2. Install Ethereal v.0.10.12 by following on-screen instructions

C.6.2. NAT 1 and NAT 2

C.6.2.1.1. Install Ethereal if it is not already installed

C.6.2.1.1.1.	Go to the Desktop menu
C.6.2.1.1.2.	Go to System Settings
C.6.2.1.1.3.	Go to Add/Remove Applications
C.6.2.1.1.4.	Click on Details under System Tools
C.6.2.1.1.5.	Find and then check ethereal-gnome
C.6.2.1.1.6.	Click on Close
C.6.2.1.1.7.	Click on Update
C.6.2.1.1.8.	Put in the correct Fedora Core 4 CDs when
	. 1

prompted

- C.7. ZoneAlarm Installation and Configuration
 - C.7.1. On client A,
 - C.7.1.1. Download the free ZoneAlarm from Zone Labs
 - C.7.1.2. Install ZoneAlarm by following on-screen instructions
 - C.7.1.3. When ZoneAlarm is being run for the first time, it will ask the user to choose between Basic ZoneAlarm or trial version of ZoneAlarm Pro, select the trial version of ZoneAlarm
 - C.7.1.4. Answer on-screen questions
 - C.7.1.5. When asked to select a security level for the detected network, select Allow into Trusted Zone
 - C.7.1.6. Configure firewall rule in ZoneAlarm:
 - C.7.1.6.1. Go to Firewall menu on the left panel
 - C.7.1.6.2. Click on the Expert tab
 - C.7.1.6.3. Click on Add
 - C.7.1.6.4. Type in a name for the firewall rule in the Name textbox
 - C.7.1.6.5. Under Action, select Block

C.7.1.6.6. Under Destination,

C.7.1.6.6.1.	Select Modify
C.7.1.6.6.2.	Select Add Location
C.7.1.6.6.3.	Select IP Address
C.7.1.6.6.4.	Type in a description in the Description textbox
C.7.1.6.6.5.	Type 192.168.2.10 in the IP Address textbox
C.7.1.6.6.6.	Click OK
C.7.1.6.6.7.	Click OK
C.7.1.6.6.8.	Click Apply

D. Preparation and Testing

- D.1. Adjust volume on both clients accordingly
- D.2. Plug microphones into both clients
- D.3. On Client A,
 - D.3.1. Launch Ethereal
 - D.3.2. Go to the Capture menu
 - D.3.3. Go to Interfaces
 - D.3.4. Click on Capture 192.168.0.10

D.4. On Client B,

- D.4.1. Launch Ethereal
- D.4.2. Go to the Capture menu
- D.4.3. Go to Interfaces
- D.4.4. Click on Capture 192.168.2.10
- D.5.On NAT 1 (Ethereal not installed),
 - D.5.1. Launch one terminal and run: tcpdump -n -i eth0
 - D.5.2. Launch another terminal and run:

tcpdump -n -i eth1

D.6.On NAT 2,

- D.6.1. Launch one instance of Ethereal
 - D.6.1.1. Go to the Capture menu
 - D.6.1.2. Go to Interfaces

D.6.1.3. Click on Capture Eth0

D.6.2. Launch another instance of Ethereal

- D.6.2.1. Go to the Capture menu
- D.6.2.2. Go to Interfaces
- D.6.2.3. Click on Capture Eth1

D.7. On Client B,

D.7.1. Call A by dialing 192.168.0.10 in SJPhone

D.8. On Client A,

- D.8.1. Select Accept in the pop-up dialog box when SJPhone rings
- D.8.2. Clients A and B may engage in a VoIP conversation at this point.
- D.8.3. Click on the Hang-Up bottom on either SJPhone to terminate call when finished

D.8.4. On NAT 1,

- D.8.4.1. Stop tcpdump packet captures by pressing Control-C on the terminals
- D.8.5. On Client A, Client B and NAT 2,
 - D.8.5.1. Stop packet captures by selecting **Stop** on Ethereal

E. Packet Captures

E.1. Client A

The following is a snapshot of the packets captured on Client A.

24 24	The Party Party Party	itos Help		
005 665		x 🕲 📇 🕅 🔅	• • • • • • • • • • • • • • • • • • •	
			• Epreson Over Stally	
10.000		192,168.0.10	SIP/50 Request: Invite stp:192.168.0.10, with session description	} red
3 0.018	474 00:4c:69:6e:75:		ARP 192.168.0.1 is at 00:4c:69:6e:75:79	
4 0.018		192.168.0.1 192.168.0.255	STP Status: 100 Trying NBHS Name query NB WWW.53LABS.COM <dd></dd>	
6 0.162	533 192.168.0.10	192.168.0.1	SIP Status: 180 Ringing	
7 0.414	665 192.168.0.10 920 192.168.0.10	192.168.0.255 192.168.0.255	NENS Name query NB WWW.SJLABS.COM-00> NENS Name query NB WWW.SJLABS.COM-00>	
9.1.028	055 192.168.0.10	192.168.0.1	SIP/SD Status: 200 OK, with session description	
11 1.035	593 192.168.0.1	192.168.0.10	RTP Payload type=65M 06.10, 55RC-516040833, Seq=12039, Time=0, Mark	} blue
13 1.046	260 192.168.0.1	192.168.0.10	RTP Payload type=GSM 06.10, SSRC=\$16040833, Seq=12040, Time=160	
14 1.052		192.168.0.1 192.168.0.10	RTP Payload type=GSM 06.10, SSRC=264990281, Seq=1035, Time=320	
15 1.056	580 192.168.0.10	192.168.0.1	RTP Payload type=GSM 06.10, SSRC=516040833, Seq=12041, Time=320 RTP Payload type=GSM 06.10, SSRC=264990281, Seq=1036, Time=480	
17 1.066	777 192.168.0.1	192.168.0.10	RTP Payload type=GSM 06.10, SSRC=516040833, Seq=12042, Time=480	
18 1.073	014 192.168.0.10 520 192.168.0.1	192.168.0.1 192.168.0.10	RTP Payload type=GSM 06.10, SSRC=264990281, Seq=1037, Time=640 RTP Payload type=GSM 06.10, SSRC=S16040833, Seq=12043, Time=640	
20 1.0834	418 192.168.0.10	192.168.0.1	RTP Payload type=GSM 06.10, SSRC=264990281, Seq=1038, Time=800	
21 1.087		192.168.0.10	RTP Payload type=GSM 06.10, SSRC=516040833, Seq=12044, Time=800 RTP Payload type=GSM 06.10, SSRC=264990281, Sep=1039, Time=960	
23 1.098	916 192.168.0.10 078 192.168.0.1	192.168.0.1 192.168.0.10	RTP Payload type=GSM 06.10, SSRC=264990281, Seq=1039, Time=960 RTP Payload type=GSM 06.10, SSRC=S16040833, Seq=12045, Time=960	
24 1.104	547 192.168.0.10	192.168.0.1	<pre>RTP Payload type=GSM 06.10, SSRC=264990281, Seq=1040, Time=1120</pre>	
25 1.108	509 192.168.0.1 772 192.168.0.10	192.168.0.10 192.168.0.1	RTP Payload type=GSM 06.10, SSRC=S16040833, Seq=12046, Time=1120 RTP Payload type=GSM 06.10, SSRC=264990281, Seq=1041, Time=1280	
27 1.119	013 192.168.0.1	192.168.0.10	RTP Rayload type=CSM 06.10, SSRC=516040833, Seq=12047, Time=1280 RTP payload type=CSM 06.10, SSRC=516040833, Seq=1047, Time=1280	
nternet Pr		rt: 5060 (5060), Ost	Port: 5060 (5060)	
ser batag Source po Destinati Checksum: ession ini Request -L Message b Message b Session Sessi @ Owner Sessi @ Owner Sessi @ Conne @ Time @ Sessi @ Sessi @ Sessi @ Sessi @ Sessi @ Media	ort: 5060 (5060) ion port: 5060 (5060) i ux8aaf [correct] itiation Protocol ine: INXITE sip:192. Header body n Description Protoco fon Mame (s): Siphone sction Information (c Description, active on Attribute (a): di a Description, mame a	168.0.10 SIP/2.0 ol (o): - 3334024859 3 (o): - 3334024859 3 (o): - 1 4 192.168.2. time (t) - 0.0 interction:active ind address (m): audi	1334024859 IN IP4 192.168.2.10 10 49204 RTP/Ayp 3 97 96 8 0 101	} gree
ser Datag Source po Destinati Checksum: ession Ini Request-L Message M Bession Sessi © Conne Bitme Sessi © Sessi © Conne Bitme Sessi © Sessi © Media Bitmedia Bitmedia Bitmedia	ort: 5060 (5060) ion port: 5060 (5060) io voltation port: 5060 (5060) io voltation protocol titiztion protocol Line: INVITE sip:192. Header body n Description Protoco ion Description Protoco ion Description Protoco ion Session Id ion Name (s): Siphone ection Information (c Description, active ion Attribute (a): di	168.0.10 SIP/2.0 col Version (v): 0 f (0): - 3334024859 3 .): IN I 4 192.168.2. time (t : 0.0 rection:active nd address (m): audi ap:3 GSV(8000	10	} gree
ser Datag Source pp Destinati Checksum ession ini Request Message b Message b B Session B Session B Owner Session B Owner B Session B Conne B Time B Session B Media B Media B Media B Media	ort: 5060 (5060) ion port: 5060 (5060) i: 0x8aaf [correct] itiation Protocol Line: IwXTE sip:192. Header body 0 Description Protoco on Description Protoco on Description Protoco (on Mame (s): Siphone ection Information (c Description, artive ion Attribute (a): di a Attribute (a): rtpm Attribute (a): rtpm	168.0.10 SIP/2.0 col version (v): 0 t (o): - 3334024859 3 c): IN 1 4 192.168.2, time (t : 0.0, rection:active ap:36 36V/8000 ap:98 1.0C/8000 tap:88 1.0C/8000 tap:88 PDM/8000	10 49204 xTP/AyP 3 97 96 \$ 0 101	} gree

Figure 27. Test 3: Packet Capture on Client A

E.2. Client B

The following is a snapshot of the packets captured on Client B.



Figure 28. Test 3: Packet Capture on Client B

E.3. NAT 1 Eth0

The following is a snapshot of the packets captured on the first interface (eth0) of NAT 1.

+25_NAT1_2UAT_ETH0_B_CALL_A - WordPad	2 Microphone 👰 Tools 🔏 Handwriting	HDrawing Pad [] 📜
Edit View Insert Format Help	10 10 10 10	9 . I 9 13
6:49:34.013075 IP 192.168.0.10.5003 > 192.168.0.255.5003: UDP, length 125		
6:50:10.246156 IP 192.168.0.1.5060 > 192.168.0.10.5060: UDP, length 763		
6:50:10.281597 arp who-has 192.168.0.1 tell 192.168.0.10		
6:50:10.281648 arp reply 192.168.0.1 is-at 00:4c:69:6e:75:79		
6:50:10.281797 IP 192.168.0.10.5060 > 192.168.0.1.5060: UDP, length 377		
6:50:10.297025 IP 192.168.0.10.netbios-ns > 192.168.0.255.netbios-ns: NBT UDP PACKET(137):	QUERY; REQUEST; BROADCAST	
6:50:10.557888 IP 192.168.0.10.5060 > 192.168.0.1.5060: UDP, length 412		
6:50:11.041095 IP 192.168.0.10.netbios-ns > 192.168.0.255.netbios-ns: NBT UDP PACKET(137):		
6:50:11.790633 IP 192.168.0.10.netbios-ns > 192.168.0.255.netbios-ns: NBT UDP PACKET(137):	QUERY; REQUEST; BROADCAST	
5:50:12.261940 IP 192.168.0.10.5060 > 192.168.0.1.5060: UDP, length 658		
6:50:12.271112 IP 192.168.0.1.5060 > 192.168.0.10.5060: UDP, length 376		
6:50:12.276174 IP 192.168.0.1.49204 > 192.168.0.10.49182: UDP, length 45		
5:50:12.289297 IP 192.168.0.10.49182 > 192.168.0.1.49204: UDP, length 45		
5:50:12.296086 IP 192.168.0.1.49204 > 192.168.0.10.49182: UDP, length 45		
5:50:12.308339 IP 192.168.0.10.49182 > 192.168.0.1.49204: UDP, length 45		
6:50:12.316182 IP 192.168.0.1.49204 > 192.168.0.10.49182: UDP, length 45		
5:50:12.328013 IP 192.168.0.10.49182 > 192.168.0.1.49204: UDP, length 45		
5:50:12.335969 IP 192.168.0.1.49204 > 192.168.0.10.49182: UDP, length 45		
6:50:12.348013 IP 192.168.0.10.49182 > 192.168.0.1.49204: UDP, length 45		
6:50:12.356561 IP 192.168.0.1.49204 > 192.168.0.10.49182: UDP, length 45		
6:50:12.367951 IP 192.168.0.10.49182 > 192.168.0.1.49204: UDP, length 45		
6:50:12.376034 IP 192.168.0.1.49204 > 192.168.0.10.49182: UDP, length 45		
5:50:12.388070 IP 192.168.0.10.49182 > 192.168.0.1.49204: UDP, length 45		
6:50:12.395956 IP 192.168.0.1.49204 > 192.168.0.10.49182: UDP, length 45		
6:50:12.408445 IP 192.168.0.10.49182 > 192.168.0.1.49204: UDP, length 45		
6:50:12.415943 IP 192.168.0.1.49204 > 192.168.0.10.49182: UDP, length 45		
6:50:12.428041 IP 192.168.0.10.49182 > 192.168.0.1.49204: UDP, length 45		
6:50:12.436064 IP 192.168.0.1.49204 > 192.168.0.10.49182: UDP, length 45		
6:50:12.448135 IP 192.168.0.10.49182 > 192.168.0.1.49204: UDP, length 45		
6:50:12.455952 IP 192.168.0.1.49204 > 192.168.0.10.49182: UDP, length 45		
6:50:12.467980 IP 192.168.0.10.49182 > 192.168.0.1.49204: UDP, length 45		
6:50:12.475940 IP 192.168.0.1.49204 > 192.168.0.10.49182: UDP, length 45		
6:50:12.487996 IP 192.168.0.10.49182 > 192.168.0.1.49204: UDP, length 45		
6:50:12.495921 IP 192.168.0.1.49204 > 192.168.0.10.49182: UDP, length 45		
6:50:12.508149 IP 192.168.0.10.49182 > 192.168.0.1.49204: UDP, length 45		
6:50:12.516253 IP 192.168.0.1.49204 > 192.168.0.10.49182: UDP, length 45		
5:50:12.528281 IP 192.168.0.10.49182 > 192.168.0.1.49204: UDP, length 45		
5:50:12.535923 IP 192.168.0.1.49204 > 192.168.0.10.49182: UDP, length 45		
::50:12.543988 IP 192.168.0.10.netbios-ns > 192.168.0.255.netbios-ns: NBT UDP PACKET(137):	QUERY; REQUEST; BROADCAST	
5:50:12.548478 IP 192.168.0.10.49182 > 192.168.0.1.49204: UDP, length 45		
5:50:12.555954 IP 192.168.0.1.49204 > 192.168.0.10.49182: UDP, length 45		
6:50:12.567954 IP 192.168.0.10.49182 > 192.168.0.1.49204: UDP, length 45		
6:50:12.575939 IP 192.168.0.1.49204 > 192.168.0.10.49182: UDP, length 45		
5:50:12.588117 IP 192.168.0.10.49182 > 192.168.0.1.49204: UDP, length 45		
6:50:12.595921 IP 192.168.0.1.49204 > 192.168.0.10.49182: UDP, length 45		
5:50:12.607974 IP 192.168.0.10.49182 > 192.168.0.1.49204: UDP, length 45		
6:50:12.615900 IP 192.168.0.1.49204 > 192.168.0.10.49182: UDP, length 45		
6:50:12.627981 IP 192.168.0.10.49182 > 192.168.0.1.49204: UDP, length 45		
6:50:12.635963 IP 192.168.0.1.49204 > 192.168.0.10.49182: UDP, length 45		
6:50:12.645900 IP 192.168.0.1.49204 > 192.168.0.10.49182: UDP, length 45		
6:50:12.647982 IP 192.168.0.10.49182 > 192.168.0.1.49204: UDP, length 45		
6:50:12.665951 IP 192.168.0.1.49204 > 192.168.0.10.49182: UDP, length 45		
6:50:12.668234 IP 192.168.0.10.49182 > 192.168.0.1.49204: UDP, length 45		
lp, press F1		-

Figure 29. Test 3: Packet Capture on eth0 of NAT 1

E.4. NAT 1 Eth1

The following is a snapshot of the packets captured on the second interface (eth1) of NAT 1.

8-25_NAT1_2NAT_ETH1_B_CALL_A - WordPad	🧷 Microphone 😨 Tools 🔏 Handwriting 🕀 Drawing Pad 😨 🗧
Edit Vew Insert Format Help	
.6:50:10.246093 IP 192.168.1.2.5060 > 192.168.0.10.5060; UDP, length 763	
.6:50:10.281844 IP 192.168.0.10.5060 > 192.168.1.2.5060: UDP, length 377	
L6:50:10.557947 IP 192.168.0.10.5060 > 192.168.1.2.5060: UDP, length 412	
L6:50:12.262002 IP 192.168.0.10.5060 > 192.168.1.2.5060: UDP, length 658	
.6:50:12.271082 IP 192.168.1.2.5060 > 192.168.0.10.5060: UDP, length 376	
6:50:12.276141 IP 192.168.1.2.49204 > 192.168.0.10.49182: UDP, length 45	
6:50:12.289314 IP 192.168.0.10.49182 > 192.168.1.2.49204: UDP, length 45	
6:50:12.296071 IF 192.168.1.2.49204 > 192.168.0.10.49182: UDP, length 45	
6:50:12.308405 IP 192.168.0.10.49182 > 192.168.1.2.49204: UDP, length 45	
6:50:12.316163 IP 192.168.1.2.49204 > 192.168.0.10.49182: UDP, length 45	
6:50:12.328032 IP 192.168.0.10.49182 > 192.168.1.2.49204: UDP, length 45	
5:50:12.335953 IP 192.168.1.2.49204 > 192.168.0.10.49182: UDP, length 45	
6:50:12.348068 IP 192.168.0.10.49182 > 192.168.1.2.49204: UDP, length 45	
6:50:12.356540 IP 192.168.1.2.49204 > 192.168.0.10.49182: UDP, length 45	
6:50:12.367969 IP 192.168.0.10.49182 > 192.168.1.2.49204: UDP, length 45	
6:50:12.376018 IP 192.168.1.2.49204 > 192.168.0.10.49182: UDP, length 45	
5:50:12.388086 IP 192.168.0.10.49182 > 192.168.1.2.49204: UDP, length 45	
5:50:12.395905 IP 192.168.1.2.49204 > 192.168.0.10.49182: UDP, length 45	
5:50:12.408465 IP 192.168.0.10.49182 > 192.168.1.2.49204: UDP, length 45	
5:50:12.415925 IP 192.168.1.2.49204 > 192.168.0.10.49182: UDP, length 45	
6:50:12.428058 IP 192.168.0.10.49182 > 192.168.1.2.49204: UDP, length 45	
5:50:12.436012 IP 192.168.1.2.49204 > 192.168.0.10.49182: UDP, length 45	
5:50:12.448155 IP 192.168.0.10.49182 > 192.168.1.2.49204: UDP, length 45	
6:50:12.455931 IP 192.168.1.2.49204 > 192.168.0.10.49182: UDP, length 45	
6:50:12.468032 IP 192.168.0.10.49182 > 192.168.1.2.49204: UDP, length 45	
.6:50:12.475922 IP 192.168.1.2.49204 > 192.168.0.10.49182: UDP, length 45	
.6:50:12.488052 IP 192.168.0.10.49182 > 192.168.1.2.49204: UDP, length 45	
6:50:12.495901 IP 192.168.1.2.49204 > 192.168.0.10.49182: UDP, length 45	
.6:50:12.508168 IP 192.168.0.10.49182 > 192.168.1.2.49204: UDP, length 45	
6:50:12.516237 IP 192.168.1.2.49204 > 192.168.0.10.49182: UDP, length 45	
6:50:12.528349 IP 192.168.0.10.49182 > 192.168.1.2.49204: UDP, length 45	
6:50:12.535904 IP 192.168.1.2.49204 > 192.168.0.10.49182: UDP, length 45	
6:50:12.548496 IP 192.168.0.10.49182 > 192.168.1.2.49204: UDP, length 45	
6:50:12.555936 IP 192.168.1.2.49204 > 192.168.0.10.49182: UDP, length 45	
6:50:12.567970 IP 192.168.0.10.49182 > 192.168.1.2.49204: UDP, length 45	
6:50:12.575889 IP 192.168.1.2.49204 > 192.168.0.10.49182: UDP, length 45	
6:50:12.588138 IP 192.168.0.10.49182 > 192.168.1.2.49204: UDP, length 45	
6:50:12.595904 IP 192.168.1.2.49204 > 192.168.0.10.49182: UDP, length 45	
6:50:12.607989 IP 192.168.0.10.49182 > 192.168.1.2.49204: UDP, length 45	
6:50:12.615885 IP 192.168.1.2.49204 > 192.168.0.10.49182: UDP, length 45	
6:50:12.628035 IP 192.168.0.10.49182 > 192.168.1.2.49204: UDP, length 45	
6:50:12.635943 IP 192.168.1.2.49204 > 192.168.0.10.49182: UDP, length 45	
6:50:12.645882 IP 192.168.1.2.49204 > 192.168.0.10.49182: UDP, length 45	
6:50:12.647998 IP 192.168.0.10.49182 > 192.168.1.2.49204: UDP, length 45	
6:50:12.665900 IP 192.168.1.2.49204 > 192.168.0.10.49182: UDP, length 45	
6:50:12.668255 IP 192.168.0.10.49182 > 192.168.1.2.49204: UDP, length 45	
6:50:12.685878 IP 192.168.1.2.49204 > 192.168.0.10.49182: UDP, length 45	
6:50:12.688041 IP 192.168.0.10.49182 > 192.168.1.2.49204: UDP, length 45	
6:50:12.705932 IP 192.168.1.2.49204 > 192.168.0.10.49182: UDP, length 45	
6:50:12.707958 IP 192.168.0.10.49182 > 192.168.1.2.49204: UDP, length 45	
6:50:12.725904 IP 192.168.1.2.49204 > 192.168.0.10.49182: UDP, length 45	
6:50:12.728001 IP 192.168.0.10.49182 > 192.168.1.2.49204: UDP, length 45	
6:50:12.745909 IP 192.168.1.2.49204 > 192.168.0.10.49182: UDP, length 45	

Figure 30. Test 3: Packet Capture on eth1 of NAT 1

E.5. NAT 2 Eth0

The following is a snapshot of the packets captured on the first interface (eth0) of NAT 2.

By De your and/or 20000 Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Desc	🔇 8-25 NAT 2(EthO 2 NAT B Call A) - Etherea		
Image: Source	Elle Edit View Go Capture Analyze Statistic	s <u>H</u> elp	
Image: Source			
Image: The same Petrod Mo 1 0.00000000000000000000000000000000000			
1 0.00001 0.0100001 0.010001 0.	Elter:	▼ Expression.	Gear Apply
2 0.08865 19.186.00 92.08.12 919 Status: 100 Trying 3.02294 19.186.00 92.08.12 919 Status: 100 Trying 3.02294 19.186.00 92.08.12 919 Status: 100 Trying 3.02394 19.186.01 92.08.12 919 Status: 100 Trying 3.02395 19.186.01 92.08.01 919 Status: 100 Trying 3.02395 19.186.01 92.08.01 919 Status: 100 Trying 3.02395 19.186.01 92.08.12 917 Payload TypeGM (ALL), SSC-4404035, Sep120, The-U, Mark 5.00005 19.186.01 92.08.12 917 Payload TypeGM (ALL), SSC-4404035, Sep120, The-U, Mark 5.00005 19.186.01 92.08.12 917 Payload TypeGM (ALL), SSC-4404035, Sep120, The-U 12.02373 19.186.01 92.01.08.12 917 Payload TypeGM (ALL), SSC-4404035, Sep120, The-30 12.02373 19.186.01 92.01.08.12 917 Payload TypeGM (ALL), SSC-4404035, Sep120, The-30 12.02373 19.186.01 92.01.08.12 917 Payload TypeGM (ALL), SSC-4404035, Sep120, The-30 13.02378 19.186.01 92.01.08.12 917 Payload TypeGM (AL), SSC-4404035, Sep120, The-30 13.02378 19.186.01 92.01.08.12 917 Payload TypeGM (AL), SSC-4404035, Sep120, The-30 13.02378 19.186.01 92.01.08.12 917 Payload TypeGM (AL), SSC-4404035, Sep120, The-30 13.12478 19.186.01 92.01.08.12 917 Payload TypeGM (AL), SSC-4404035, Sep120, The-30 13.12478 19.186.01 92.01.08.12 917 Payload TypeGM (AL), SSC-4404035, Sep120, The-30 13.12478 19.186.01 92.01.08.12 917 Payload TypeGM (AL), SSC-4404035, Sep120, The-30 13.12478 19.186.01 92.01.08.12 917 Payload TypeGM (AL), SSC-4404035, Sep120, The-30 13.12478 19.186.01 92.01.08.12 917 Payload TypeGM (AL), SSC-4404035, Sep120, The-30 13.12485 19.186.01 92.01.08.12 917 Payload TypeGM (AL), SSC-4404035, Sep120, The-40 13.12478 19.186.01 92.01.08.12 917 Payload TypeGM (AL), SSC-4404035, Sep120, The-40 13.12478 19.186.01 92.01.08.12 917 Payload TypeGM (AL), SSC-4404035, Sep120, The-40 13.12478 19.186.01 92.01.00 917 Payload TypeGM (AL), SSC-4404035, Sep120, The-40 13.12478 19.186.01 92.01.00 917 Payload TypeGM (AL), SSC-4404035, Sep120, The-40 13.12478 19.186.01 92.01.00 917 Payload TypeGM (AL), SSC-4404035, Sep120, The-40 13.12478 19.186.01 92.01.00 917 Payload Type	a second a second a second		
 4. 20229 19.1.58.0.10 19.1.58.0.10 STP/05 TRADE 200 06, with session description 5. 20159 19.1.58.0.10 19.1.58.0.10 STP Payload type-GM 06.0.10 SSC-1004033, sept.0.35, The-0, Mark 7. 204636 19.1.58.0.12 19.1.58.0.10 STP Payload type-GM 06.0.10 SSC-1004033, sept.0.35, The-30 9. 2. 66136 19.1.58.0.12 19.1.58.0.10 STP Payload type-GM 06.0.10 SSC-1004033, sept.0.35, The-30 9. 2. 66136 19.1.58.0.12 19.1.58.0.10 STP Payload type-GM 06.0.10 SSC-1004033, sept.0.35, The-30 10.2.0755 19.1.68.0.10 19.1.68.1.2 STP Payload type-GM 06.0.10 SSC-1004033, sept.0.35, The-30 12.2.0755 19.1.68.0.10 STP Payload type-GM 06.0.10 SSC-1004033, sept.0.11, The-40 12.2.0075 19.1.68.0.10 STP Payload type-GM 06.0.10 SSC-1004033, sept.0.11, The-40 12.2.0075 19.1.68.0.10 STP Payload type-GM 06.0.10 SSC-1004033, sept.0.14, The-40 12.2.0075 19.1.68.0.10 STP Payload type-GM 06.0.10, SSC-1004033, sept.0.14, The-40 12.2.0075 19.1.68.0.10 STP Payload type-GM 06.0.10, SSC-1004033, Sept.0.14, The-40 12.2.0075 19.1.68.0.10 STP Payload type-GM 06.0.10, SSC-1004033, Sept.0.14, The-40 12.2.0075 19.1.68.0.10 STP Payload type-GM 06.0.10, SSC-1004033, Sept.0.14, The-40 12.2.0075 19.1.68.0.10 STP Payload type-GM 06.0.10, SSC-1004033, Sept.0.14, The-40 12.2.0075 19.1.68.0.10 STP Payload type-GM 06.0.10, SSC-1004033, Sept.0.14, The-40 12.2.0075 19.2.08.0.10 STP Payload type-GM 06.0.10, SSC-1004033, Sept.0.14, The-40 12.2.0075 19.2.08.0.10 STP Payload type-GM 06.0.10, SSC-1004033, Sept.0.14, The-40 12.2.0075 19.2.08.0.10 STP Payload type-GM 06.0.10 SSC-1004033, Sept.0.14, The-40 12.2.0075 19.2.08.0.10 STP Payload type-GM 06.0.10 SSC-1004033, Sept.0.14, The-100 12.2.0075 19.2.08.0.10 STP Payload type-GM 06.0.10 SSC-1004033, Sept.0.14, The-100 12.2.0075 19.2.08.0.10 STP Payload type-GM 06.0.10 S	2 0.036816 192.168.0.10	192.168.1.2 SIP	Status: 100 Trying
6 2.00056 132.188.1.2 102.188.1.2 102.188.1.2 107.188.	4 2.017209 192.168.0.10		
7 2.04405 102.168.1.2 NTP Paylod type-GM 06.10, SSC-04400028, Seq-0104, Thm=100 9 2.05516 102.168.1.2 NTP Paylod type-GM 06.10, SSC-0440028, Seq-0104, Thm=20 12 2.04715 102.168.1.2 NTP Paylod type-GM 06.10, SSC-0440028, Seq-0104, Thm=20 12 2.04871 102.168.1.2 NTP Paylod type-GM 06.10, SSC-0440028, Seq-0104, Thm=20 12 2.04944 102.168.1.2 NTP Paylod type-GM 06.10, SSC-0440028, Seq-0104, Thm=20 12 2.04944 102.168.1.2 NTP Paylod type-GM 06.10, SSC-0440028, Seq-0104, Thm=40 12 2.04944 102.168.1.2 NTP Paylod type-GM 06.10, SSC-0440028, Seq-0104, Thm=40 12 2.04164 102.168.1.2 NTP Paylod type-GM 06.10, SSC-0440028, Seq-0104, Thm=40 12 2.11052 11.68.1.0 102.168.1.2 NTP Paylod type-GM 06.10, SSC-0440028, Seq-0104, Thm=40 12 2.11052 11.68.1.0 102.168.1.2 NTP Paylod type-GM 06.10, SSC-0440028, Seq-0104, Thm=40 12 2.11052 11.68.1.0 102.168.1.2 NTP Paylod type-GM 06.10, SSC-0440028, Seq-0104, Thm=410 12 12.168.1.0			
9 2.062108 192.186.101 392.186.12 mTP Psylad type=30 60.10 Stort-2649008, tea-106.1 The=20 12.02776 192.08.12 392.186.10 392.186.12 mTP Psylad type=30 60.10 Stort-2649008, tea-106.1 Stort-2649008 12.00047 192.08.12 392.186.12 mTP Psylad type=30 60.10 Stort-2649008, tea-106.1 Stort-2649008 12.00047 192.186.12 302.186.10 392.186.12 mTP Psylad type=30 60.10 Stort-2649008, tea-106.1 Stort-2649008 12.12077 192.186.10 392.186.12 mTP Psylad type=30 60.10 Stort-2649008, tea-106.1 Stort-2649008 12.12077 192.186.10 392.186.12 mTP Psylad type=30 60.10 Stort-2649008, tea-106.1 Stort-2649008 12.12077 192.186.10 192.186.12 mTP Psylad type=30 60.10 Stort-2649008, tea-106.1 Stort-2649008 12.12078 192.186.10 192.186.12 mTP Psylad type=30 60.10 Stort-2649008, tea-106.1 Stort-2649008 12.12078 192.186.10 192.186.12 mTP Psylad type=30 60.10 Stort-2649008, tea-106.1 Stort-2649008 12.12078 192.186.10 192.186.12 mTP Psylad type=30 60.10 Stort-2649008, tea-106.1 Stort-2649008 12.12080 192.186.12 mTP Psylad type=30 60.10 Stort-2649008, tea-106.1 Stort-2649008 12.12080 192.186.12 mTP Psylad type=30 60.10 Stort-2649008, tea-100.1 The=100 12.12081 192.186.10 192.186.12 mTP Psylad type=30 60.10 Stort-2649008, tea-100.1 The=100 12.12081 192.186.10 192.186.12 mTP Psylad type=30 60.10 Stort-2649008, tea-100.1 The=100 12.12081 192.186.10 192.186.12 mTP Psylad type=30 60.10 Stort-264908, tea-100.1 The=100 12.22000 192.186.12 MTP Psylad type=30 60.10 Stort-264908, tea-100.1 The=100 12.22000 192.186.12 MTP Psylad type=30 60.10 Stort-264908, tea-100.1 The=100 12.22000 192.186.12 MTP Psylad type=30 60.10 Stort-264908, tea-100.1 The=100 12.22000 192.186.12 MTP Psylad type=30 60.10 Stort-264908, tea-100.1 The=100 12.22000 192.186.12 MTP Psylad type=30 60.10 Stort-264908, tea-100.1 The=100 12.22000 192.186.12 MTP Psylad type=30 60.10 Stort-264908, tea-100.1 The=100 12.22000 192.186.12 MTP Psylad type=30 60.10 Stort-264908, tea-100.1 The=100 12.22000 192.186.12 MTP Psylad type=30 60.10 Stort-264908, tea-100.1 The=100 12.22000 192.186.12 MTP Psylad type=	7 2.044036 192.168.0.10	192.168.1.2 RTP	Payload type=GSM 06.10, SSRC=264990281, Seq=1034, Time=160
11 2.02739 192.186.10 192.186.12 NTP PyNat type-GM 6.0. SSC-02469031, seq.020, The-400 12 2.02073 192.186.10 192.186.12 NTP PyNat type-GM 6.0. SSC-02469031, seq.020, The-400 13 2.02073 192.186.10 192.186.12 NTP PyNat type-GM 6.0. SSC-02469031, seq.020, The-400 14 2.1102 192.186.10 192.186.12 NTP PyNat type-GM 6.0. SSC-02469031, seq.020, The-400 15 2.12073 192.186.10 192.186.12 NTP PyNat type-GM 6.0. SSC-02469031, seq.020, The-400 15 2.12073 192.186.10 192.186.12 NTP PyNat type-GM 6.0. SSC-02469031, seq.020, The-400 15 2.12073 192.186.10 192.186.12 NTP PyNat type-GM 6.0. SSC-02469031, seq.020, The-400 15 2.12073 192.186.10 192.186.12 NTP PyNat type-GM 6.0. SSC-02469031, seq.020, The-400 12 2.12073 192.186.10 192.186.12 NTP PyNat type-GM 6.0. SSC-02469031, seq.020, The-400 12 2.12073 192.186.10 192.186.12 NTP PyNat type-GM 6.0. SSC-02469031, seq.020, The-400 12 2.12073 192.186.10 192.186.12 NTP PyNat type-GM 6.0. SSC-02469031, seq.020, The-400 12 2.12073 192.186.10 192.186.12 NTP PyNat type-GM 6.0. SSC-02469031, seq.020, The-410 12 2.12074 192.186.10 192.186.12 NTP PyNat type-GM 6.0. SSC-02469031, seq.020, The-410 12 2.12074 192.186.10 192.186.12 NTP PyNat type-GM 6.0. SSC-02469031, seq.020, The-410 12 2.12074 192.186.10 192.186.12 NTP PyNat type-GM 6.0. SSC-02469031, seq.020, The-410 12 2.12075 192.186.10 192.186.12 NTP PyNat type-GM 6.0. SSC-02469031, seq.020, The-410 12 2.12075 192.186.10 192.186.12 NTP PyNat type-GM 6.0. SSC-02469031, seq.020, The-410 12 2.12075 192.186.10 192.186.12 NTP PyNat type-GM 6.0. SSC-02469031, seq.020, The-410 12 2.12075 192.186.10 192.186.12 NTP PyNat type-GM 6.0. SSC-02469031, seq.020, The-410 12 3.12074 192.186.10 192.186.12 NTP PyNat type-GM 6.0. SSC-02469031, seq.020, The-410 12 3.12074 192.186.10 192.186.12 NTP PyNat type-GM 6.0. SSC-02469031, seq.020, The-410 12 3.12074 192.186.10 192.186.12 NTP PyNat type-GM 6.0. SSC-02469031, seq.020, The-410 12 3.12074 192.186.10 192.186.12 NTP PyNat type-GM 6.0. SSC-02469031, seq.020, The-410 12 Status Antinter (S) Type-SSC (SSG) 12 Statu	9 2.063108 192.168.0.10	192.168.1.2 RTP	Payload type=GSM 06.10, SSRC=264990281, Seq=1035, Time=320
12 2.00447 92.153.1.2 192.158.0.0 PT Provided Type-SM 60.0 SSC-1540483, Sep-1242, Thre-40 13 2.1073 52.0158.1.0 192.158.1.2 PT Provided Type-SM 60.0 SSC-1540483, Sep-1243, Thre-40 15 2.1027 32.0158.1.0 192.158.1.2 PT Provided Type-SM 60.0 SSC-1540483, Sep-1243, Thre-40 15 2.1027 32.0158.1.0 192.158.1.2 PT Provided Type-SM 60.0 SSC-1540483, Sep-1244, Thre-40 15 2.1027 32.0158.1.0 192.158.1.2 PT Provided Type-SM 60.0 SSC-1540483, Sep-1244, Thre-40 15 2.1027 32.0158.1.0 192.158.1.2 PT Provided Type-SM 60.0 SSC-1540483, Sep-1244, Thre-40 15 2.1037 152.158.1.0 192.158.1.2 PT Provided Type-SM 60.0 SSC-1540483, Sep-1244, Thre-40 15 2.1037 152.158.1.0 192.158.1.2 PT Provided Type-SM 60.0 SSC-1540483, Sep-1244, Thre-40 15 2.1037 152.158.1.0 192.158.1.2 PT Provided Type-SM 60.0 SSC-1540483, Sep-1244, Thre-40 15 2.1037 152.158.1.0 192.158.1.2 PT Provided Type-SM 60.0 SSC-1540483, Sep-1244, Thre-410 12 2.1027 152.158.1.0 192.158.1.2 PT Provided Type-SM 60.0 SSC-1540483, Sep-1244, Thre-410 12 2.1027 152.158.1.0 192.158.1.2 PT Provided Type-SM 60.0 SSC-1540483, Sep-1244, Thre-410 12 2.1027 152.158.1.0 192.158.1.2 PT Provided Type-SM 60.0 SSC-1540483, Sep-1244, Thre-1240 12 2.1027 152.158.1.0 192.158.1.2 PT Provided Type-SM 60.0 SSC-1540483, Sep-1244, Thre-1240 12 2.1027 152.158.1.0 192.158.1.2 PT Provided Type-SM 60.0 SSC-1540483, Sep-1244, Thre-1240 12 2.1027 152.158.1.0 192.158.1.2 PT Provided Type-SM 60.0 SSC-1540483, Sep-1244, Thre-1240 12 2.1027 152.158.1.0 192.158.1.2 PT Provided Type-SM 60.0 SSC-1540483, Sep-1244, Thre-1240 12 2.1027 122.158.1.0 192.158.1.2 PT Provided Type-SM 60.0 SSC-1540483, Sep-1244, Thre-140 12 2.1027 122.158.1.0 PT Provided Type-SM 60.0 SSC-1540483, Sep-1244, Thre-140 12 2.1027 122.158.1.0 PT Provided Type-SM 60.0 SSC-1540483, Sep-1244, Thre-140 12 2.1027 122.158.1.0 PT Provided Type-SM 60.0 SSC-1540483, Sep-1244, Thre-140 12 2.1027 122.158.1.0 PT Provided Type-SM 60.0 SSC-1540483, Sep-1244, Thre-140 12 2.1027 122.158.1.0 PT Provided Type-SM 60.0 SSC-1540483, Sep-1244, Thre-140 12 2.1028 122.158		192.168.0.10 RTP 192.168.1.2 RTP	Payload type=GSM 06.10, SSRC=516040833, Seq=12041, Time=320 Payload type=GSM 06.10, SSRC=264990281, Seq=1036, Time=480
14 2.111022 92.163.1.2 92.163.1.2 92.168.1.2 97 FP Pyload Type-SM 06.10, SSRC-11640833, Sep-1204, Three-60 15.12627 92.168.1.0 92.168.1.2 92.168.1.2 97 FP Pyload Type-SM 06.10, SSRC-11640833, Sep-1204, Three-60 17.14727 92.168.1.0 92.168.1.2 92.168.0.0 FT FP Pyload Type-SM 06.10, SSRC-11640833, Sep-1204, Three-60 18.215396 92.168.1.1 92.168.1.2 92.168.0.0 FT FP Pyload Type-SM 06.10, SSRC-11640833, Sep-1204, Three-60 18.215396 92.168.1.1 92.168.1.2 92.168.0.0 FT FP Pyload Type-SM 06.10, SSRC-11640833, Sep-1204, Three-120 27.14727 92.168.1.1 92.168.0.0 FT FP Pyload Type-SM 06.10, SSRC-11640833, Sep-1204, Three-120 27.15727 92.168.1.2 92.168.1.2 92.168.0.1 FT FP Pyload Type-SM 06.10, SSRC-11640833, Sep-1204, Three-120 27.15727 92.168.1.2 92.168.1.1 92.168.0.1 FT FPyload Type-SM 06.10, SSRC-11640833, Sep-1204, Three-120 27.212727 92.168.1.2 92.168.0.1 97 FPyload Type-SM 06.10, SSRC-11640833, Sep-1204, Three-120 27.22274 92.168.1.1 92.168.0.1 97 FPyload Type-SM 06.10, SSRC-11640833, Sep-1204, Three-140 27.24276 92.168.1.1 92.168.1.2 FT FPyload Type-SM 06.10, SSRC-11640833, Sep-1204, Three-140 27.24276 92.168.1.0 192.168.1.2 FT FPyload Type-SM 06.10, SSRC-11640833, Sep-1204, Three-140 27.24276 92.168.1.0 192.168.1.2 FT FPyload Type-SM 06.10, SSRC-11640833, Sep-1204, Three-140 27.24276 92.168.1.0 192.168.1.2 FT FPyload Type-SM 06.10, SSRC-11640833, Sep-1204, Three-140 27.24276 92.168.1.1 192.168.1.1 FT FPyload Type-SM 06.10, SSRC-11640833, Sep-1204, Three-140 27.24276 92.168.1.2 92.168.1.1 192.168.1.2 FT FPyload Type-SM 06.10, SSRC-11640833, Sep-1204, Three-140 27.24475 92.168.1.1 192.168.1.2 FT FPYload Type-SM 06.10, SSRC-11640833, Sep-1204, Three-140 27.24475 92.168.1.1 192.168.1.2 FT FPYload Type-SM 16.10, SSRC-11640833, Sep-1204, Three-140 27.24476 92.168.1.2 91.168.1.2 91.168.1.2 FT FPYload Type-SM 16.10, SSRC-11640833, Sep-1204, Three-140 28.2501 A171507 (SRC 1007 1900) 29.25007 1900 1900 1900 1900 1900 1900 1900 1	12 2.090447 192.168.1.2	192.168.0.10 RTP	Payload type=GSM 06.10, SSRC=516040833, Seq=12042, Time=480
18 2.13051 192.168.1.2 192.168.1.2 192.168.1.2 8TP Payload type=00 (6.10, SSR.25404083, Seq-130, Time=00 18 2.151096 192.168.1.2 192.168.1.2 8TP Payload type=00 (6.10, SSR.25404083, Seq-130, Time=00 18 2.151096 192.168.1.2 192.168.1.2 8TP Payload type=00 (6.10, SSR.25404083, Seq-130, Time=100 20 2.12010 192.168.1.2 192.168.1.2 8TP Payload type=00 (6.10, SSR.25404083, Seq-130, Time=100 21 2.18276 192.168.0.10 192.168.1.2 8TP Payload type=00 (6.10, SSR.25404083, Seq-1304, Time=120 22 2.19501 192.168.0.10 192.168.1.2 8TP Payload type=00 (6.10, SSR.25404083, Seq-1304, Time=120 22 2.19501 192.168.0.10 192.168.1.2 8TP Payload type=00 (6.10, SSR.25404028, Seq-1304, Time=120 22 2.19501 192.168.0.10 192.168.1.2 8TP Payload type=00 (6.10, SSR.25404028, Seq-1304, Time=120 22 2.20216 192.168.0.10 192.168.1.2 8TP Payload type=00 (6.10, SSR.25404028, Seq-1304, Time=120 22 2.20216 192.168.0.10 192.168.1.2 8TP Payload type=00 (6.10, SSR.25404028, Seq-1304, Time=140 22 2.20216 192.168.0.10 192.168.1.2 8TP Payload type=00 (6.10, SSR.25404028, Seq-1304, Time=140 22 2.20216 192.168.0.10 192.168.1.2 8TP Payload type=00 (6.10, SSR.25404028, Seq-1304, Time=140 22 2.20216 192.168.0.10 192.168.1.2 8TP Payload type=00 (6.10, SSR.25404028, Seq-1304, Time=140 23 2.0020 Type.168.1.2 192.168.0.10 192.168.1.2 8TP Payload type=00 (6.10, SSR.25404028, Seq-1304, Time=140 24 2.01426 192.168.0.10 192.168.1.2 8TP Payload type=00 (6.10, SSR.25404028, Seq-1304, Time=140 25 2.20217 192.168.0.10 192.168.1.2 8TP Fayload type=00 (6.10, SSR.25404028, Seq-1304, Time=140 25 2.20217 192.168.0.10 192.168.0.10 STP.2.0 8TP eayload type=00 (6.10, SSR.25404028, Seq-1304, Time=140 35 SSR.01 SSR.01 (500 (5160) 25 SSR.01 SSR.01 (500 (5160) .5 PT : 506 (5160) 55 SSR.01 SSR.01 (500 (5160) .5 PT : 506 (5160) 55 SSR.01 SSR.01 (500 (5160) .5 PT : 506 (5160) 55 SSR.01 SSR.01 (500 (5160) .5 PT : 500 (5060) 55 SSR.01 SSR.01 (500 (5160) .5 PT : 500 (5160) .5 PT : 500 (5160) 55 SSR.01 SSR.01 (500 (5160) .5 PT : 500 (5160) .4 PT : 500 (5160) .5 PT : 500	14 2.111032 192.168.1.2	192.168.0.10 RTP	Payload type=GSM 06.10, SSRC=516040833, Seq=12043, Time=640
17 2.142767 192.186.1.0 192.168.1.2 RTP Payload type=00 (6.10, SSR.24900281, Seq.2409, Time=00 18 2.15096 192.186.0.10 192.168.1.2 192.168.0.10 RTP Payload type=00 (6.10, SSR.24900281, Seq.2404, Time=120 20 2.110/20 192.168.1.2 192.168.0.10 RTP Payload type=00 (6.10, SSR.24900281, Seq.2404, Time=120 21 2.11678 192.186.0.10 192.168.1.2 RTP Payload type=00 (6.10, SSR.249400281, Seq.2404, Time=120 22 2.10002 192.168.1.2 192.168.0.10 RTP Payload type=00 (6.10, SSR.249400281, Seq.1244, Time=120 23 2.02085 192.168.0.10 192.168.1.2 RTP Payload type=00 (6.10, SSR.249400281, Seq.1244, Time=120 23 2.02085 192.168.0.10 Str.250.00 RTP Payload type=00 (6.10, SSR.249400281, Seq.1244, Time=120 23 2.02085 192.168.0.10 RTP Payload type=00 (6.10, SSR.249400281, Seq.1248, Time=120 24 2.02085 192.168.1.2 192.168.1.2 RTP Payload type=00 (6.10, SSR.249400281, Seq.1248, Time=120 25 2.02047 192.168.1.1 192.168.1.2 RTP Payload type=00 (6.10, SSR.249400281, Seq.1248, Time=120 27 2.0276 192.168.1.1 192.168.1.2 RTP Payload type=00 (6.10, SSR.249400281, Seq.1248, Time=120 27 2.0276 192.168.1.1 192.168.1.2 RTP Payload type=00 (6.10, SSR.249400281, Seq.1248, Time=120 28 2.02085 192.168.1.2 192.168.1.2 (192.168.1.2) RTP Payload type=00 (6.10, SSR.249400281, Seq.1248, Time=120 28 2.02085 192.168.1.2 (192.168.1.2) RTP Payload type=00 (6.10, SSR.249400281, Seq.1248, Time=120 28 2.02085 192.168.1.2 (192.168.1.2) RTP Payload type=00 (6.10, SSR.249400281, Seq.1248, Time=120 29 2.02767 80 (0.00) 20 Sever ontext, 192.168.1.2 (192.168.0.10 STP.2.168.0.10) 20 Sever part: 500 (500) 20 Sever payload rype=00 (0.00) 20 Sever payload rype=00 (0.00) 20 Sever payload rype=00 (0.00) 20 Sever payload rype=00 (0.00) 20 Sever rotator, sever tyme (7): 0 30 Sever tyme (3): Tympayload 20 Sever (3) 20 Sever	15 2.122672 192.168.0.10 16 2.130511 192.168.1.2		
19 2.133166 192.166.0.10 192.168.1.2 RTP Payload type=CM 06.10 spc:22490028. seq-12046, Time-120 20.171420 192.168.1.2 192.168.0.10 RTP Payload type=CM 06.10 spc.35404038. seq-12046, Time-120 22.10052 192.168.1.2 192.168.0.10 RTP Payload type=CM 06.10 spc.35404038. seq-12047, Time-1280 22.2.10456 192.168.1.2 192.168.0.10 RTP Payload type=CM 06.10 spc.35404038. seq-12047, Time-1280 22.2.10456 192.168.1.2 192.168.0.10 RTP Payload type=CM 06.10 spc.35404038. seq-12047, Time-1280 22.2.10456 192.168.0.10 92.168.1.2 RTP Payload type=CM 06.10 spc.35404038. seq-12047, Time-1260 23.2.10476 192.168.0.10 92.168.1.2 RTP Payload type=CM 06.10, Spc.35404038. seq-12047, Time-1260 23.2.22340, T192.168.0.10 92.168.1.2 RTP Payload type=CM 06.10, Spc.35404038. seq-12047, Time-1260 24.2.2235 192.168.0.10 92.168.1.2 RTP Payload type=CM 06.10, Spc.35404038. seq-1204, Time-1260 24.2.22376 192.168.0.10 92.168.1.2 RTP Payload type=CM 06.10, Spc.35404038. seq-1204, Time-1260 24.2.2236 192.168.0.10 92.168.1.2 RTP Payload type=CM 06.10, Spc.35404038. seq-1204, Time-1260 24.2.22376 192.168.0.10 92.168.1.2 RTP Payload type=CM 06.10, Spc.35404038. seq-1204, Time-1260 24.2.22376 192.168.0.10 92.168.1.2 NPP Payload type=CM 06.10, Spc.35404038. seq-1204, Time-1260 25.2.23417 192.168.0.10 92.168.1.2 NPP Payload type=CM 06.10, Spc.35404038. seq-1204, Time-1260 25.2.23417 192.168.0.10 Stp.454 NPP 192.168.0.10 Stp.254 NPP 192.168.0.10 (192.168.0.10) 24.2.2476 Stp.254 NPP 192.168.0.10 Stp.27 25.2.510 NB34 [Correct] 25.5510 NB34 [Correct]	17 2.142787 192.168.0.10	192.168.1.2 RTP	Payload type=GSM 06.10, SSRC=264990281, Seq=1039, Time=960
21 2.12763 192.168.0.10 192.168.1.2 RTP Payload type=GM 06.10, SSRC-264090281, Seq-1047, Time-1280 22 2.10905 192.168.0.10 192.168.1.2 RTP Payload type=GM 06.10, SSRC-264090281, Seq-1042, Time-1280 23 2.20285 192.168.0.10 192.168.1.2 RTP Payload type=GM 06.10, SSRC-264090281, Seq-1042, Time-1280 24 2.20285 192.168.0.10 192.168.1.2 RTP Payload type=GM 06.10, SSRC-264090281, Seq-1042, Time-1280 25 2.22740 192.168.1.2 192.168.0.10 RTP Payload type=GM 06.10, SSRC-264090281, Seq-1049, Time-1600 27 2.24276 192.168.0.10 192.168.1.2 RTP Payload type=GM 06.10, SSRC-264090281, Seq-1044, Time-1760 28 7.240307 192.168.1.2 192.168.0.10 RTP Payload type=GM 06.10, SSRC-264090281, Seq-1044, Time-1760 28 7.240307 192.168.1.2 192.168.0.10 RTP Payload type=GM 06.10, SSRC-264090281, Seq-1044, Time-1760 28 restore three, 050 bytes on wire, 050 bytes captured) Bitternett 1, Scription 197.166.0.10 Stription 197.166.0.10 29 targan Protocol, Src: 192.168.0.10 Str/2.0 Bitternett 1, Scription 197.10 Stription 197.10 Checksum: 0x83ae [correct] Session bescription Protocol Session 197.10 Session 197.10 20 Session bescription Protocol Session 197.10 Session	19 2.163166 192.168.0.10	192.168.1.2 RTP	Payload type=GSM 06.10, SSRC=264990281, Seq=1040, Time=1120
22 2.109002 192,168.1.2 192,168.0.10 RT Paylad type=CM 06.10, SSR=3604033, Sep-1047, Time-1240 23 .20236 192,168.0.10 192,168.0.2 RT Paylad type=CM 06.10, SSR=3604038, Sep-1047, Time-1440 24 .201426 192,168.0.10 192,168.0.2 RT Paylad type=CM 06.10, SSR=36040938, Sep-1047, Time-1440 25 .202740 192,168.1.2 192,168.0.10 RT Paylad type=CM 06.10, SSR=36040938, Sep-1044, Time-1460 26 .202417 192,168.1.2 192,168.0.10 RT Paylad type=CM 06.10, SSR=36040938, Sep-1044, Time-1460 27 .20275 192,168.0.10 192,168.1.2 RT Paylad type=CM 06.10, SSR=36409028, Sep-1044, Time-1600 27 .20277 192,168.1.2 192,168.0.10 RT Paylad type=CM 06.10, SSR=36409028, Sep-1044, Time-1600 27 .20277 192,168.1.2 192,168.0.10 RT Paylad type=CM 06.10, SSR=36409028, Sep-1044, Time-1600 28 .20207 192,168.1.2 192,168.0.10 RT Paylad type=CM 06.10, SSR=36409028, Sep-1049, Time-1600 28 .20207 192,168.1.2 192,168.0.10 RT Paylad type=CM 06.10, SSR=36409028, Sep-1049, Time-1600 28 .20207 192,168.1.2 192,168.0.10 RT Paylad type=CM 06.10, SSR=36409028, Sep-1049, Time-1600 29 .20207 192,168.1.2 192,168.0.10 RT Paylad type=CM 06.10, SSR=36409028, Sep-1049, Time-1600 20 Sep 104, SSR=36409 20 Sesion Initiation Protocol 20 Sesion Initiation Protocol 20 Sesion Intervention 20	20 2.1/0420 192.168.1.2 21 2.182763 192.168.0.10		
24 2.10026 192.188.1.2 192.168.0.10 RTP Paylad type=300 66.10, SSR-51640033, Seq=12048, Time=1400 25 2.223047 192.168.1.2 192.168.0.10 192.168.1.2 RTP Paylad type=300 66.10, SSR-51640833, Seq=12049, Time=1600 27 2.42735 192.168.0.10 192.168.1.2 RTP Paylad type=30 66.10, SSR-51640833, Seq=12049, Time=1600 27 2.42735 192.168.0.1 (00:e012967)set3() hort star Paylad type=30 66.10, SSR-51640833, Seq=12049, Time=1760 8 Prame 1 (805 bytes on wire, 805 bytes captured) # Themer TI, Src: 192.168.0.1 (00:e012967)set3() hort star bayland type=30 66.10, SSR-51640833, Seq=12049, Time=1760 # User Datagram Protocol, Src: 192.168.0.1 (00:e012967)set3() hort star star star star star star star st	22 2.190502 192.168.1.2 23 2 202856 192 168 0 10	192.168.0.10 RTP	Payload type=GSM 06.10, SSRC=516040833, Seq=12047, Time=1280
26 2.33417 192.168.1.2 192.168.0.10 RTP Payload type=300 65.10. SSC=51604033, Seq=12049, Time=1600 27 2.42475 192.168.1.1 192.168.0.1 RTP Payload type=300 65.10, SSC=546902031, Seq=12049, Time=1760 28 2.50397 192.168.1.2 192.168.0.1 0 RTP Payload type=300 65.10, SSC=516040033, Seq=12050, Time=1760 28 Tchernet II, Src: 192.168.0.1 (00:e0:29:67:9e:9c), Dst: Linksy56_ef:af:ab (00:0c:41:ef:af:eb) 20 tchernet II, Src: 192.168.1.2 (192.168.1.2), Dst: Payload type=300 30 user parts: 5060 (5060) 30 user partagram Protocol, Src Part: 5060 (5060) 50 user part: 5060 (5060) Length: 771 40 session Infinition protocol 40 session Infinition Protocol 41 session Description Protocol 42 session Infinition Protocol 43 session Description Protocol 44 session Description Protocol 45 session Description Protocol 45 session Information (c): 10 HT 4192.168.2.10 45 session Information (c): 11 HT 4192.168.2.10 45 session Information (c): 11 HT 4192.168.2.10 45 session Information (c): 11 HT 4192.168.2.10 45 session Attribute (a): direction:attive 45 media Attribute (a): direction:attive 45 media Attribute (a): trimp:97 iLEC/8000 46 media Attribute (a): trimp:97 iLEC/8000 45 media Attribute (a): trimp:98 000 45 media Attribute (a)	24 2.210426 192.168.1.2	192.168.0.10 RTP	Payload type=GSM 06.10, SSRC=516040833, Seq=12048, Time=1440
27 2.242756 192.168.0.10 192.168.0.10 TP Payload type=GSM 06.10, SSG=26490281, Seq=2144, Time=1760 9 7.20037 192.168.0.1 100:e0/29:67:98:90, Dst: Linksyst_fraf:eb (00:0c:41:ef:af:eb) ************************************	26 2.222/40 192.168.0.10 26 2.230417 192.168.1.2	192.168.1.2 RTP 192.168.0.10 RTP	Payload type=GSM U6.10, SSRC=264990281, Seq=1043, Time=1600 Payload type=GSM 06.10, SSRC=516040833, Seq=12049, Time=1600
<pre># thernet II, Src: 192.168.0.1 (00:e0:29:67:92:9C), Dst: LinksysG_ef:af:eb (00:0C:41:ef:af:eb) # Intermet Protocol, Src: 192.168.1.2 (192.168.1.2), Dst: 192.168.0.10 (192.168.0.10) Source port: 5060 (5060) Destination port: 5060 (5060) Length: 771 Checksum: 0x89ae [correct] # Request-Line: INVITE sip:192.168.0.10 SIP/2.0 # Message body # Request-Line: INVITE sip:192.168.0.10 SIP/2.0 # Message body # Session Description Protocol Session Description Protocol Session Description Protocol Session Name (5): Siphone # Connection Information (c): IN IP4 192.168.2.10 # Session Attribute (a): crimpa:93 A024859 3334024859 IN IP4 192.168.2.10 # Session Attribute (a): direction:active # Media Attribute (a): rtpmap:93 (lbC/8000 # Media Attribute (a): rtpmap:93 flbC/8000 # Media Attribute (a): flmp:98 mode=20 # Media Attri</pre>			
<pre># Internet Protocol, src: 192.468.1.2 (192.168.1.2), ost: 192.168.0.10 (192.168.0.10) # User batagram Protocol, src Port: 5060 (5060) Destination port: 5060 (5060) Length: 771 Checksu: Cv89ae [correct] # Session Initiation Protocol # Message Header # Ressage body # Session Description Protocol # Message body # Session Description Protocol # Session Name (5): Siphone # Connection Information (c): IN IP4 192.168.2.10 # The Description, name and address (m): audio 49204 RTP/AVP 3 97 98 8 0 101 # Media Attribute (a): rtpmap:9 fLbC/8000 # Media Attribute (a): rtpmap:9 f</pre>			
□ User Datagram Protocol, Src Port: 5060 (5060), Dit Port: 5060 (5060) Source port: 5060 (5060) Length: 771 Checksum: 0x89ae [correct] ■ Session Initiation Protocol ■ Request-the: INVTE sip:192.168.0.10 SIP/2.0 ■ Message Header ■ Message body ■ Session Description Protocol Session Description Protocol Version (V): 0 ■ Owner/Creator, Session 1d (0): - 3334024859 3334024859 IN IP4 192.168.2.10 ■ Session Name (s): Siphone ■ Connection Information (C): IN IP4 192.168.2.10 ■ Time Description, active time (t): 0 0 ■ Session Attribute (a): rtpmap:97 HEC/8000 ■ Media Attribute (a): rtpmap:97 HEC/8000 ■ Media Attribute (a): rtpmap:98 HEC/8000 ■ Media Attribute (a): rtpmap:98 HEC/8000 ■ Media Attribute (a): rtpmap:98 HEC/8000 ■ Media Attribute (a): rtpmap:88 HEC/8000 ■ Media Attribute (a): rtpmap:97 HEC/8000 ■ Media Attribute (a): rtpmap:98 HEC/8000 ■ Media Attribute (a): rtpmap:88 HEC/8000 ■ Media Attribute (a): rtpmap:98 HEC/8000 ■ Media Attribute (a): rtpmap:98 HEC/8000 ■ Media Attribute (a): rtpma			
Destination port: 5060 (5060) Length: 771 Checksum: 0x89ae [correct] = Session Intitation Protocol # Request-Line: INVITE sip:192.168.0.10 SIP/2.0 # Message Header = Message body = Session Description Protocol Version (V): 0 # owner/Creator, Session Id (0): - 3334024859 334024859 IN IP4 192.168.2.10 Session name (s): Sophone # Connection Information (c): IN IP4 192.168.2.10 # Time Description, active time (t): 0 0 # Session Attribute (a): connective # Media Attribute (a): rtpmap:3 GSM/8000 # Media Attribute (a): rtpmap:97 LES/8000 # Media Attribute (a): rtpmap:98 L		: 5060 (5060), Dst Port: 506	iū (5060)
Checksum: 0x89ae [correct] B Session Initiation Protocol M Resguest-Line: INVITE sip:192.168.0.10 SIP/2.0 M Ressage Meader Message Meader Message body B Session Description Protocol Session Description Protocol Version (V): 0 B Owner/Creator, Session Id (0): - 3334024859 3334024859 IN IP4 192.168.2.10 Session Name (s): Sightone B Connection Information (c): IN IP4 192.168.2.10 B Time Description, active time (t): 0 0 B Session Attribute (a): direction:active B Media Attribute (a): rtpmap:3 SigN8000 B Media Attribute (a): rtpmap:9 iLEC/8000 B Media Attribute (a): rtpmap:9 iLEC/8000 B Media Attribute (a): rtpmap:8 IEC/8000 B Media Attribute (a): rtpmap:8 POMA/8000 0000 00 00 cf 1f eff eb 00 e0 29 67 9e 9c 08 00 45 00 3.7 2b 5b 00 00 7f 11 8b 1c 0 a8 01 02 co a8 .+[]WITE 0000 00 317 2b 5b 00 00 7f 11 8b 1c 0 a8 01 02 co a8 .+[]WITE 0000 02 07 36 97 03 a1 39 32 2e 31 36 38 2e 30 2e 31 .sip:192.168.0.1 0040 30 20 73 49 70 27 32 22 30 00 da 56 66 16 3a 20 0 SIP(2) 0.Via: 0 SIP 22 3b 20 72 22 32 00 da 56 66 66 15 32 0 SIP(2) 0.Via: 0 SIP(2) SIP 22 3b 00 27 20 27 20 27 20 30 0 SIP(2) 0.Via: 0 SIP(2) SIP 22 2b 20 20 Ca 20 SIP(2) 0.Via: 0 SIP 22 3b 20 72 22 30 00 da 56 66 66 15 32 0 SIP(2) 0.Via: 0 SIP(2) SIP 22 3b 00 27 30 SIP 22 2b 20 2b 30 SIP(2) 0.Via: 0 SIP(2) SIP 22 2b 20 2b 30 SIP 22 2b 20 2b 30 SIP(2) 0.Via: 0 SIP 22 3b 20 SIP 22 2b 20 2b 30 SIP(2) 2b 20 SIP(2) 0.Via: 0 SIP 22 3b 20 SIP 22 3b 20 SIP 22 3b 20 SIP 22 3b 20 SIP(2) 0.Via: 0 SIP 22 3b 20 SIP 22 3b 20 SIP 22 3b 20 SIP 22 3b 20 SIP(2) 0.Via: SIP 20 SIP 22 3b 20 SIP(2) 0.Via: SIP 20 SIP 22 3b 20 SIP 22 3b 20 SIP 22 3b 20 SIP(2) 0.Via: SIP 20 SIP 22 3b 20 SIP 22 3b 20 SIP 22 3b 20 SIP 22 3b 20 SIP(2) 0.Via: SIP 20 SIP 22 3b 20 SIP 22			
<pre> Session Initiation Protocol # Request-Line: INVITE sip:192.168.0.10 SIP/2.0 # Message Header B Message body Session Description Protocol Session Description Protocol C owner/Creator, Session Id (0): - 3334024859 IN IP4 192.168.2.10 Session Name (s): Siphone C onnection Information (c): IN IP4 192.168.2.10 Time Description, active time (t): 0 0 Session Attribute (a): offection:active Media Description, name and address (m): audio 49204 RTP/AVP 3 97 98 8 0 101 Media Attribute (a): rtpmap:3 GSM/8000 Media Attribute (a): rtpmap:97 LEC/8000 Media Attribute</pre>			
Hessage Header Message Header Message body Session Description Protocol Session Description Protocol Session Description Protocol Session Name (s): Saphone Connection Information (c): IN IP4 192.168.2.10 Session Attribute (s): Saphone Media Attribute (a): rtpmap:3 GN/8000 Media Attribute (a): rtpmap:97 /LEC/8000 Media Attribute (a): rtpmap:98 /LEC/8000 Media Attribute (a): rtpmap:8 LEC/8000 Media Attribute (a): rtpmap:9 LEC/8000 Media Attribute (a): rtpmap:8 LEC/8000	Session Initiation Protocol		
Hessage body Bescription Protocol Session Description Protocol Session Description Protocol Version (V): 0 Bowner/Creator, Session Id (o): - 3334024859 3334024859 IN IP4 192.168.2.10 Session Name (s): Sighone Connection Information (c): IN P4 192.168.2.10 B time Description, active time (t): 0 0 Session Attribute (a): direction:active Media Attribute (a): direction:active Media Attribute (a): rtpmap:36 SW/8000 Media Attribute (a): rtpmap:86 ILEC/8000 Med		38.0.10 SIP/2.0	
Session Description Protocol Version (V): 0 @ Owner/Creator, Session 1d (0): - 3334024839 334024839 IN IP4 192.168.2.10 Session Name (s): Slybone @ Connection Information (c): IN IP4 192.168.2.10 @ Time Description, active time (t): 0 0 @ Session Attribute (a): direction:active M Media Description, mame and address (m): audio 49204 RTP/AVP 3 97 98 8 0 101 @ Media Attribute (a): rtpmap:3 GSM/8000 @ Media Attribute (a): rtpmap:97 ILEC/8000 @ Media Attribute (a): rtpmap:98 ILEC/8000 @ Media Attribute (a): rtpmap:98 ILEC/8000 @ Media Attribute (a): rtpmap:88 PCMA/8000 0000 00 00 C 41 ef af eb 00 e0 29 67 9e 9c 08 00 45 00A)gE. 0000 00 17 Zb 56 00 00 77 11 86 1e c0 a8 01 02 c0 a8+(INVTE 0000 00 17 2b 56 00 00 77 11 86 1e c0 a8 01 02 c0 a8+(
Session Name (s): SJphone @ Connection Information (c): IN IP4 192.168.2.10 @ Time Description, active time (t): 0 @ Session Attribute (i): direction:active @ Media Attribute (a): rtpmap:3 GSW/8000 @ Media Attribute (a): rtpmap:3 GSW/8000 @ Media Attribute (a): rtpmap:97 iLEC/8000 @ Media Attribute (a): rtpmap:98 POMA/8000 @ Media Attribute (a): rtpmap:8 POMA/8000 @ Media Attribute (a): rtpmap:		ol version (v): O	
B connection Information (c): IN IP4 192.168.2.10 B Time Description, active time (t): 0 0 B Session Attribute (a): direction:active Media Description, name and address (m): audio 49204 RTP/AVP 3 97 98 8 0 101 B Media Attribute (a): rtpmap:3 GSM/8000 Media Attribute (a): rtpmap:97 LEE/8000 Media Attribute (a): rtpmap:98 LEE/8000 Media Attribute (a): rtpmap:98 LEE/8000 Media Attribute (a): rtpmap:97 LEE/8000 Media Attribute (a): rtpmap:98 LEE/8000 Media Attribute (a): rtpmap:98 LEE/8000 Media Attribute (a): rtpmap:98 PCMA/8000 Media Attribute ((o): - 3334024859 3334024859	IN IP4 192.168.2.10
B session Attribute (a): direction:active Media Description, name and address (m): audio 49204 RTP/AVP 3 97 98 8 0 101 Media Attribute (a): rtpmap:3 GSM/8000 Media Attribute (a): rtpmap:98 iLBC/8000 Media Attribute (a): rtpmap:98 iLBC/8000 Media Attribute (a): rtpmap:89 Node=20 Media Attribute (a): rtpmap:8 POM/8000 Media Attribute (a): rtpmap:8 POM/8000 Media Attribute (a): rtpmap:98 ILBC/8000 Media Attribute (a): rtpmap:98 Node=20 Media Attribute (a): rtpmap:98 POM/8000 Media Attribute (a): rtpmap:8 POM/8000 Media Attribut	■ Connection Information (c):		
Hedia Description, name and address (m): audio 49204 RTP/AVP 3 97 98 8 0 101 Media Attribute (a): rtpmap;3 GSW/8000 Media Attribute (a): rtpmap;97 1LBC/8000 Media Attribute (a): rtpmap;98 1LBC/8000 Media Attribute (a): rtpmap;98 1LBC/8000 Media Attribute (a): rtpmap;98 PCMA/8000 Media Attribute (a): rtpmap;98 1LBC/8000 Media Attribute (a): rtpmap;98 PCMA/8000 Media Attribute (a): rtpmap;99 PCMA/8000 Media Attribute (a): rtpma			
■ Media Attribute (a): rtpmap:97 iLBC/8000 ■ Media Attribute (a): rtpmap:97 iLBC/8000 ■ Media Attribute (a): rtpmap:86 iLBC/8000 ■ Media Attribute (a): rtpmap:8 PCMA/8000 0000 00 0c 41 ef af eb 00 e0 29 67 9e 9c 08 00 45 004	🗄 Media Description, name and	d address (m): audio 49204 R	TP/AVP 3 97 98 8 0 101
# Media Attribute (a): fmtp:98 mode=20 # Media Attribute (a): rtpmap:8 POMA/8000 0000 00 0c 41 ef af eb 00 e0 29 67 9e 9c 08 00 45 00			
■ Media Attribute (a): rtpmap:8 PCMA/8000 00000 00 0c 41 ef af eb 00 e0 29 67 9e 9c 08 00 45 00			
0010 03 17 2b 5b 00 00 7f 11 8b 1e c0 a8 01 02 c0 a8+[8
0020 00 0a 13 c4 13 c4 03 03 89 ae 49 4e 56 49 54 45)gE.
0040 30 20 53 49 50 2F 32 2e 30 0d 0a 56 69 61 3a 20 0 51P/2. 0. Via:	0020 00 0a 13 c4 13 c4 03 03 89 a	ae 49 4e 56 49 54 45	INVITE
	0030 20 73 69 70 3a 31 39 32 2e 3 0040 30 20 53 49 50 2f 32 2e 30 0	.1 36 38 2e 30 2e 31 sip:)d 0a 56 69 61 3a 20 0 SIP	192 .168.0.1 /2. 0via:
			0/ IIIn 103

Figure 31. Test 3: Packet Capture on eth0 of NAT 2

E.6. NAT 2 Eth1

The following is a snapshot of the packets captured on the first interface (eth0) of NAT 2.

	🗑 🖻 🖁 🗙		🔿 🔁 🛨 📃 🗟 I Q, Q, Q, 🖭 I 🎬 🕅 🎛 🔆 🔯
er:		•	· Expression Jear Apply
. Time	Source	Destination	Protocol Info
	192.168.2.10 192.168.1.10	192.168.2.255 Broadcast	BROWSE Local Master Announcement DHQ4L351, Workstation, Server, NT Workstation, Potential Browser, M ARP Who has 192,168.2.1? Tell 192.168.2.10
	192.168.1.1	192.168.1.10	ARP 192.168.2.1 is at 00:01:02:89:97:5b
	192.168.2.10 192.168.0.10	192.168.0.10 192.168.2.10	SIP/SD Request: INVITE sip:192.168.0.10, with session description SIP Status: 100 Trying
6 7.886863	192.168.0.10	192.168.2.10	SIP Status: 180 Ringing
	192.168.0.10	192.168.2.10	SIP/SD Status: 200 OK, with session description
	192.168.2.10 192.168.2.10	192.168.0.10 192.168.0.10	SIP Request: ACK sip:192.168.0.10:5060 RTP Payload type=GSM 06.10, SSRC=516040833, Seg=12039, Time=0, Mark
10 9.617927	192.168.0.10	192.168.2.10	RTP Payload type=GSM 06.10, SSRC=264990281, Seq=1034, Time=160
	192.168.2.10	192.168.0.10	RTP Payload type=GSM 06.10, SSRC=516040833, Seq=12040, Time=160
	192.168.0.10 192.168.2.10	192.168.2.10 192.168.0.10	RTP Payload type=GSM 06.10, SSRC=264990281, Seq=1035, Time=320 RTP Payload type=GSM 06.10, SSRC=516040833, Seq=12041, Time=320
14 9.656631	192.168.0.10	192.168.2.10	RTP Payload type=GSM 06.10, SSRC=264990281, Seq=1036, Time=480
	192.168.2.10	192.168.0.10	RTP Payload type=GSM 06.10, SSRC=516040833, Seq=12042, Time=480
	192.168.0.10 192.168.2.10	192.168.2.10 192.168.0.10	RTP Payload type=GSM 06.10, SSRC=264990281, Seq=1037, Time=640 RTP Payload type=GSM 06.10, SSRC=516040833, Seq=12043, Time=640
	192.168.0.10	192.168.2.10	RTP Payload type=GSM 06.10, SSRC=264990281, Seq=1038, Time=800
19 9.704303	192.168.2.10	192.168.0.10	RTP Payload type=GSM 06.10, SSRC=516040833, Seq=12044, Time=800
	192.168.0.10 192.168.2.10	192.168.2.10 192.168.0.10	RTP Payload type=GSM 06.10, SSRC=264990281, Seq=1039, Time=960 RTP Payload type=GSM 06.10, SSRC=516040833, Seq=12045, Time=960
	192.168.0.10	192.168.2.10	RTP Payload type=GSM 06.10, SSRC=264990281, Seq=1040, Time=1120
23 9.744245	192.168.2.10	192.168.0.10	RTP Payload type=GSM 06.10, SSRC=516040833, Seq=12046, Time=1120
	192.168.0.10 192.168.2.10	192.168.2.10 192.168.0.10	RTP Payload type=GSM 06.10, SSRC=264990281, Seq=1041, Time=1280 RTP Payload type=GSM 06.10, SSRC=516040833, Seq=12047, Time=1280
	192.168.0.10	192.168.2.10	RTP Payload type=GSM 06.10, SSRC=264990281, Seq=1042, Time=1440
27 9.784253	192.168.2.10 192.168.0.10	192.168.0.10 192.168.2.10	RTP Payload type=GSM 06.10, SSRC=516040833, Seq=12048, Time=1440 RTP Payload type=GSM 06.10, SSRC=264090281, Seq=1043, Time=1600
Internet Proto User Datagram Source port: Destination Length: 209 Checksum: Ox NetBIOS Datagr SMB (Server Me SMB MailSlot P	ocol, Src: 192.168.2 Protocol, Src Port: netbios-dgm (138) port: netbios-dgm (f05c [correct] am Service essage Block Protoco	2.10 (192.168.2.10), : netbios-dgm (138), (138) 51)	Dst: Broadcast (ff:ff:ff:ff:ff) , 0st: 192.168.2.255 (192.168.2.255) , Dst Port: netbios-dgm (138)

Figure 32. Test 3: Packet Capture on eth1 of NAT 2

E.7. Analysis

This demonstration was very similar to the one described in Appendix C. It differed in that now Client B is located behind two NAT devices instead of one. In other words, two layers of network address translation occurred before any packet can be moved between Client A and Client B.

The "INVITE" message (red outline in Figure 27) indicated that Client B will be sending and receiving RTP packets at 192.168.2.10 on port 49204 (purple outline in Figure 28). Client A acknowledged the invitation by sending a "200 OK" message to Client B with embedded SDP information indicating that it would send and receive RTP packets at 192.168.2.10 on port 49182 (green outline in Figure 27). Figures 27 and 29 show that Client A sends and receives RTP packet directly to/from the public IP address of NAT 1. As explained in Appendix C, SJPhone will first attempt to send RTP media packets to the IP address indicated in the SDP message (or the private IP address of Client B). Since the firewall installed on Client A was configured to drop packets destined to for Client B, none of the packets sent out by Client A ever reached Client B. Therefore, Client A resorted to sending subsequent RTP packets to the IP address from which it received Client B's RTP media packets (blue outline in Figure 27). In this case, the packets were sent to the public IP address of the NAT 1 device (192.168.0.1). Figures 29 and 30 confirmed that the configured NAT operated correctly.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX E. TEST 4: EXTENDED DOUBLE NAT VOIP DEMONSTRATION USING SJPHONE

The instructions contained in this appendix describe how to setup and demonstrate a SIP-based VoIP communication between two SIP-enabled clients via Network Address Translation (NAT) devices. In this setup, NAT 1 is no longer configured with a DNAT rule to rewrite the destination IP address of the packets that traverse it. Therefore, NAT 1 only performs SNAT. NAT 2 and NAT 3 are each configured with both SNAT and DNAT rules. The demonstration is conducted as follows: Client B initiates a call to Client A. Then Client C initiates a call to Client A after the VoIP session between Client B and A is terminated. Packet captures from all three clients and the NATs are included at the end of this appendix along with an analysis.

A. Network Topology

Refer to Figure 13 and Figure 14 for the physical and logical network topology.

- B. Equipment Requirements
 - B.1. Clients A, B and C
 - B.1.1. Windows XP Operating System
 - B.1.2. Sound card
 - B.1.3. SJPhone v.1.60
 - B.1.4. Ethereal
 - B.1.5. ZoneAlarm (Client A only)
 - B.2. NAT 1, NAT 2 and NAT 3
 - B.2.1. Linux Operating System (Fedora Core 4)
 - B.2.2. netfilter and iptables
 - B.2.3. Ethereal
 - B.2.4. Two network cards
 - B.3. Additional Equipment
 - B.3.1. Cross-over cables and a switch or hub to implement the network architecture illustrated in Figure 13

B.3.2. Microphones as audio input devices for clients A, B, and C

C. Installation and Configuration

- C.1. Client A
 - IP Address: 192.168.0.10

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.0.1

C.2. Client B

IP Address: 192.168.2.10

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.2.1

C.3. Client C

IP Address: 192.168.3.10

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.3.1

C.4. NAT 1

C.4.1. Configure eth0 by editing /etc/sysconfig/network-scripts/ifcfg-eth0:

DEVICE=eth0 BOOTPROTO=NONE IPADDR=192.168.0.1 NETMASK=255.255.255.0

C.4.2. Activate eth0 by running:

ifup eth0

C.4.3. Configure eth1 by editing /etc/sysconfig/network-scripts/ifcfg-eth1:

DEVICE=eth1

BOOTPROTO=NONE

IPADDR=192.168.1.1

NETMASK=255.255.255.0

C.4.4. Activate eth1 by running: ifup eth1

C.4.5. Enable IP Forwarding by running: echo 1 > /proc/sys/net/ipv4/ip_forward C.4.6. Flush any existing firewall and NAT rules by running:

iptables -F

iptables -t nat -F

C.4.7. Configure NAT rule by running: iptables -t nat -A POSTROUTING -o eth0 -j SNAT --to 192.168.0.1

C.5. NAT 2

- C.5.1. Configure eth0 by editing /etc/sysconfig/network-scripts/ifcfg-eth0: DEVICE=eth0 BOOTPROTO=NONE IPADDR=192.168.1.2 NETMASK=255.255.255.0 GATEWAY=192.168.1.1
- C.5.2. Activate eth0 by running: ifup eth0
- C.5.3. Configure eth1 by editing /etc/sysconfig/network-scripts/ifcfg-eth1: DEVICE=eth1 BOOTPROTO=NONE

IPADDR=192.168.2.1

NETMASK=255.255.255.0

C.5.4. Activate eth1 by running:

ifup eth1

- C.5.5. Enable IP forwarding by running:
 - echo 1 > /proc/sys/net/ipv4/ip_forward
- C.5.6. Flush any existing firewall and NAT rules by running: iptables -F

iptables -t nat -F

C.5.7. Configure NAT rules by running: iptables -t nat -A POSTROUTING -o eth0 -j SNAT --to 192.168.1.2 iptables -t nat -A PREROUTING -i eth0 -j DNAT --to 192.168.2.10

C.6. NAT 3

C.6.1. Configure eth0 by editing /etc/sysconfig/network-scripts/ifcfg-eth0: DEVICE=eth0 BOOTPROTO=NONE IPADDR=192.168.1.3 NETMASK=255.255.255.0 GATEWAY=192.168.1.1

- C.6.2. Activate eth0 by running: ifup eth0
- C.6.3. Configure eth1 by editing and saving /etc/sysconfig/network-scripts/ifcfg-eth1:

DEVICE=eth1 BOOTPROTO=NONE IPADDR=192.168.3.1 NETMASK=255.255.255.0

- C.6.4. Activate eth1 by running: ifup eth1
- C.6.5. Enable IP forwarding by running: echo 1 > /proc/sys/net/ipv4/ip_forward
- C.6.6. Flush any existing firewall and NAT rules by running: iptables –F iptables -t nat -F
- C.6.7. Configure NAT rules by running: iptables -t nat -A POSTROUTING -o eth0 -j SNAT --to 192.168.1.3

iptables -t nat -A PREROUTING -ieth0 -j DNAT --to 192.168.3.10

- C.7. SJPhone Installation and Configuration
 - C.7.1. Clients A, B, and C
 - C.7.1.1. Download the Windows version of SJPhone v.1.60 from SJ Labs
 - C.7.1.2. Install SJPhone v.1.60
 - C.7.1.3. Launch SJPhone

C.7.1.3.1. On SJPhone,

C.7.1.3.1.1.	Right-click
C.7.1.3.1.2.	Go to Services
C.7.1.3.1.3.	Select PC-to-PC (SIP)

- C.8. Ethereal Installation and Configuration
 - C.8.1. Clients A, B, and C
 - C.8.1.1. Download the Windows version of Ethereal v.0.10.12
 - C.8.1.2. Install Ethereal v.0.10.12
 - C.8.2. NAT 2 and 3
 - C.8.2.1. Install Ethereal if it is not already installed
 - C.8.2.1.1. Go to the Desktop menu
 - C.8.2.1.2. Go to System Settings
 - C.8.2.1.3. Go to Add/Remove Applications
 - C.8.2.1.4. Click on Details under System Tools
 - C.8.2.1.5. Find and then check ethereal-gnome
 - C.8.2.1.6. Click on Close
 - C.8.2.1.7. Click on Update
 - C.8.2.1.8. Put in the correct Fedora Core 4 CDs when prompted
 - C.8.2.1.9.
- C.9. ZoneAlarm Installation and Configuration
 - C.9.1. On client A,
 - C.9.1.1. Download the free ZoneAlarm from Zone Labs
 - C.9.1.2. Install ZoneAlarm by following on-screen instructions
 - C.9.1.3. When ZoneAlarm is being run for the first time, it will ask the user to choose between Basic ZoneAlarm or trial version of ZoneAlarm Pro, select the trial version of ZoneAlarm
 - C.9.1.4. Answer on-screen questions
 - C.9.1.5. When asked to select a security level for the detected network, select Allow into Trusted Zone
 - C.9.1.6. Configure firewall rule in ZoneAlarm:
 - C.9.1.6.1. Go to Firewall menu on the left panel
 - C.9.1.6.2. Click on the Expert tab
 - C.9.1.6.3. Click on Add
 - C.9.1.6.4. Type in a name for the firewall rule in the Name textbox
 - C.9.1.6.5. Under Action, select Block

C.9.1.6.6. Under Destination,

C.9.1.6.6.2. Select Add Location

C.9.1.6.6.3. Select IP Address

C.9.1.6.6.4. Type in a description in the **Description** textbox

C.9.1.6.6.5. Type 192.168.2.10 in the IP Address textbox

C.9.1.6.6.6. Click OK

C.9.1.6.7. Repeat steps C.9.1.6.1 to C.9.1.6.6.6 to create a rule to block

192.168.3.10

C.9.1.6.8. Click OK

C.9.1.6.9. Click Apply

D. Preparation and Testing

- D.1. Adjust volume on both clients accordingly
- D.2. Plug microphones into both clients
- D.3. On Client A,
 - D.3.1. Launch Ethereal
 - D.3.2. Go to the Capture menu
 - D.3.3. Go to Interfaces
 - D.3.4. Click on Capture 192.168.0.10

D.4. On Client B,

- D.4.1. Launch Ethereal
- D.4.2. Go to the Capture menu
- D.4.3. Go to Interfaces
- D.4.4. Click on Capture 192.168.2.10

D.5.On NAT 1,

D.5.1. Launch one terminal and run:

tcpdump -n -i eth0

D.5.2. Launch another terminal and run:

tcpdump -n -i eth1

D.6. On NAT 2 and NAT 3,

D.6.1. Launch one instance of Ethereal
- D.6.1.1. Go to the Capture menu
- D.6.1.2. Go to Interfaces
- D.6.1.3. Click on Capture Eth0
- D.6.2. Launch another instance of Ethereal
 - D.6.2.1. Go to the Capture menu
 - D.6.2.2. Go to Interfaces
 - D.6.2.3. Click on Capture Eth1

D.7. On Client B,

- D.7.1. Call A by dialing 192.168.0.10 in SJPhone
- D.8. On Client A,
 - D.8.1. Select Accept in the pop-up dialog box when SJPhone rings
 - D.8.2. Clients A and B may engage in a VoIP conversation at this point.
 - D.8.3. Click on the Hang-Up bottom on either SJPhone to terminate call when finished

D.9. On Client A,

Stop tcpdump packet captures by pressing Control-C

- D.10. On Client A, Client B, NAT 1, NAT 2 and NAT 3,
 - D.10.1. Stop packet captures by selecting Stop on Ethereal
 - D.10.2. Stop packet captures on NAT Box 1 by pressing Control-C
 - D.10.3. Repeat steps D.3 to D.8 for Clients A, Client C, NATs 1 and NAT 3

E. Packet Captures

- E.1. Client B Calls A
 - E.1.1. Client A

The following is a snapshot of the packets captured on Client A when Client B calls Client A.

He bit jew is Capture Analyze 5	atatica tato		Houtes (Tak () :	x laix
Conference of the second second			10×10	
her		Domain. Der Boly		
n The Source	Destrution	Protocol (2H)		1
1 0.000000 192.168.0.10 2 60.363499 192.168.0.10	192,168,0,255 192,168,0,255	UDP Source port: 5003 Destination port: 5003 UDP Source port: 5003 Destination port: 5003		
4.01.631007.107.168.0.1	197.168.0.10 Broadcast	519750 ACOURTE 150714 5107102-165.0.10, with session ARP who has 102.165.0.17 Tell 102.165.0.10	desc/10/100	red بر red
C ANOTHER AND WALL	192.100.0.10	AND AND AND AND AN		
7 91,653551 192,168,0,10 8 91,660928 192,168,0,10	192.168.0.1 192.168.0.255	SIP Status: 100 Trying NBNS Name query NB WWW.SJLABS.COM<00>		
9 91,783735 192,168,0.10 10 92,031929 192,168,0.10	192,168,0,1 192,168,0,255	SIP Status: 180 kinging NBNS Name query NB WWN.53LABS.CON<00>		
11 92.436193 192.168.0.10	192.168.0,255	NBNS Name query NE WW. S3LABS. COM+00>		
12 94.996537 192.168.0.10 13 95.000549 192.168.0.1	192.168.0.1 192.168.0.10	SIP/SD Status: 200 GK, with session description SIP Request: ACK sip:192,168.0,10:5060		
14 95.002974 192.168.0.1	192.168.0.10	RTP Payload type=GSM 08.10, SSRC=112995514, Seq=187	703, Time-O, Hark	
15 95,008629 192,168.0.10 16 95,013767 192,168.0.1	192.168.0.255 192.168.0.10	NBNS Name query NE WWW.53(A85.CON+00> RTF Payload type=GSM 06.10, SIRC=112995534, Seq=187		
18 95.033895 192.188.0.1 19 95.038163 192.168.0.10	192.168.0.10 192.168.0.1	RTP Payload type=GSR 06.10, SSRC=112995534, Seq=183 RTP Rayload type=GSR 06.10, SSRC=112818322, Sen=100	012. Tite=640	}-blac
20 95.053742 192.168.0.1 21 95.058391 192.168.0.10	192,168.0,10	RTP Payload type=GM 06.10, SSRC=112895394, Seq=120 RTP Payload type=GM 06.10, SSRC=112818322, Seq=120		a blue
23 95.078199 192.168.0.10 24 95.093871 192.168.0.1	192.168.0.1	RTP Payload type=GSH 06.10, SSRC=112818122, Seq=110 RTP Payload type=GSH 06.10, SSRC=112995514, Seq=110	015, Tise-000 708, Tise-000	blue بر
26 95.113660 192.168.0.1	192,168,0,1	RTP Payload type=GSM 06.10, SSMC=112955514, Seq=187	NEW, TIMPALEY	1
<pre># Request-Line: INVITE sip:1) # Message meader # Message body</pre>	in high and the			
Session Description Pro	otocol version (v): 0 Id (o): + 3334103399 3 Sne	334103399 1% 194 192.168.3.10 10		
Jession Description Work Session Description Pro Domer/Creator, Session Session Name (s): Sybe Disconnection Information Diffice Description, acti Session Attribute (a):	tocol version (V): 0 1d (0): - 3334103393 3 90 (c): 1% 1P4 192,164.2, ve time (t): 0 direction:active and addres: (s): audi pmap:3 GM/8000 pmap:97 fuE/8000 tp:08 node-20 tp:08 node-20 smap:8 PCH4/8000]} gre

Figure 33. Test 4: Packet Capture on Client A (Client B Calls Client A)

E.1.2. Client B

The following is a snapshot of the packets captured on Client B when Client B calls Client A.



Figure 34. Test 4: Packet Capture on Client B (Client B Calls Client A)

E.1.3. NAT 1 Eth0

The following is a snapshot of the packets captured on the first interface

3_IAT_NAT1_eth0_B_CALL_A - WordPad	🗾 🦉 Microphone 🖓 Tools 🔏 Handwriting 🎲 Drawing Pad [🕽 🕻
Edt Vew Inset Format Help	
cpdump: verbose output suppressed, use -v or -vv for full protocol decode	
istening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes	
4:36:05.451001 IP 192.168.0.10.5003 > 192.168.0.255.5003: UDP, length 125	
4:38:05.445026 IP 192.168.0.10.5003 > 192.168.0.255.5003: UDP, length 125	
4:38:16.380332 IP 192.168.0.10.netbios-dgm > 192.168.0.255.netbios-dgm: NBT UDP PACKET(138)
4:39:07.582019 IP 192.168.0.1.5060 > 192.168.0.10.5060: UDP, length 762	
4:39:07.644250 arp who-has 192.168.0.1 tell 192.168.0.10	
4:39:07.644286 arp reply 192.168.0.1 is-at 00:4c:69:6e:75:79	
4:39:07.644435 IP 192.168.0.10.5060 > 192.168.0.1.5060: UDP, length 376	
4:39:07.658561 IP 192.168.0.10.netbios-ns > 192.168.0.255.netbios-ns: NBT UDP PACKET(137):	QUERY; REQUEST; BROADCAST
4:39:07.893957 IF 192.168.0.10.5060 > 192.168.0.1.5060: UDP, length 411	
4:39:08.407937 IP 192.168.0.10.netbios-ns > 192.168.0.255.netbios-ns: NBT UDP PACKET(137):	QUERY; REQUEST; BROADCAST
4:39:09.157907 IP 192.168.0.10.netbios-ns > 192.168.0.255.netbios-ns: NBT UDP PACKET(137):	QUERY; REQUEST; BROADCAST
4:39:14.159658 IP 192.168.0.10.5060 > 192.168.0.1.5060: UDP, length 657	
4:39:14.167109 IP 192.168.0.1.5060 > 192.168.0.10.5060: UDP, length 375	
4:39:14.171761 IP 192.168.0.1.49232 > 192.168.0.10.49204: UDP, length 45	
4:39:14.182768 IP 192.168.0.10.netbios-ns > 192.168.0.255.netbios-ns: NBT UDP PACKET(137):	OUERY; REQUEST; BROADCAST
4:39:14.191603 IP 192.168.0.1.49232 > 192.168.0.10.49204: UDP, length 45	
4:39:14.196213 IP 192.168.0.10.49204 > 192.168.0.1.49232: UDP, length 45	
4:39:14.211730 IP 192.168.0.1.49232 > 192.168.0.10.49204: UDP, length 45	
4:39:14.216115 IP 192.168.0.10.49204 > 192.168.0.1.49232: UDP, length 45	
4:39:14.231583 IP 192.168.0.1.49232 > 192.168.0.10.49204: UDP, length 45	
4:39:14.236346 IP 192.168.0.10.49204 > 192.168.0.1.49232: UDP, length 45	
4:39:14.252295 IP 192.168.0.1.49232 > 192.168.0.10.49204: UDP, length 45	
.4:39:14.256147 IP 192.168.0.10.49204 > 192.168.0.1.49202: UDP, length 45	
4:39:14.271708 IP 192.168.0.1.49232 > 192.168.0.10.49204: UDP, length 45	
4:39:14.276156 IP 192.168.0.10.49204 > 192.168.0.1.49232: UDP, length 45	
4:39:14.291510 IP 192.168.0.1.49232 > 192.168.0.10.49204: UDP, length 45	
4:39:14.295868 IP 192.168.0.10.49204 > 192.168.0.1.49232: UDP, length 45 4:39:14.311544 IP 192.168.0.1.49232 > 192.168.0.10.49204: UDP, length 45	
4:39:14.316005 IP 192.168.0.10.49204 > 192.168.0.1.49232: UDP, length 45	
4:39:14.331617 IP 192.168.0.1.49232 > 192.168.0.10.49204: UDP, length 45	
4:39:14.335856 IP 192.168.0.10.49204 > 192.168.0.1.49232: UDP, length 45	
4:39:14.351605 IP 192.168.0.1.49232 > 192.168.0.10.49204: UDP, length 45	
4:39:14.355846 IP 192.168.0.10.49204 > 192.168.0.1.49232: UDP, length 45	
4:39:14.371573 IP 192.168.0.1.49232 > 192.168.0.10.49204: UDP, length 45	
4:39:14.375879 IP 192.168.0.10.49204 > 192.168.0.1.49232: UDP, length 45	
4:39:14.391506 IP 192.168.0.1.49232 > 192.168.0.10.49204: UDP, length 45	
4:39:14.395869 IP 192.168.0.10.49204 > 192.168.0.1.49232: UDP, length 45	
4:39:14.411628 IP 192.168.0.1.49232 > 192.168.0.10.49204: UDP, length 45	
4:39:14.415894 IP 192.168.0.10.49204 > 192.168.0.1.49232: UDP, length 45	
4:39:14.431491 IP 192.168.0.1.49232 > 192.168.0.10.49204: UDP, length 45	
4:39:14.435840 IP 192.168.0.10.49204 > 192.168.0.1.49232: UDP, length 45	
4:39:14.451515 IP 192.168.0.1.49232 > 192.168.0.10.49204: UDP, length 45	
4:39:14.455848 IP 192.168.0.10.49204 > 192.168.0.1.49232: UDP, length 45	
4:39:14.471501 IP 192.168.0.1.49232 > 192.168.0.10.49204: UDP, length 45	
4:39:14.475850 IP 192.168.0.10.49204 > 192.168.0.1.49232: UDP, length 45	
4:39:14.491524 IP 192.168.0.1.49232 > 192.168.0.10.49204: UDP, length 45	
4:39:14.495894 IP 192.168.0.10.49204 > 192.168.0.1.49232: UDP, length 45	
4:39:14.511575 IP 192.168.0.1.49232 > 192.168.0.10.49204: UDP, length 45	
4:39:14.515835 IP 192.168.0.10.49204 > 192.168.0.1.49232: UDP, length 45	
4:39:14.531597 IP 192.168.0.1.49232 > 192.168.0.10.49204: UDP, length 45	
4:39:14.535888 IP 192.168.0.10.49204 > 192.168.0.1.49232: UDP, length 45	

(eth0) of NAT 1 when Client B calls Client A.

Test 4: Packet Capture on eth0 of NAT 1 (Client B Calls Client A)

E.1.4. NAT 1 Eth1

The following is a snapshot of the packets captured on the second interface (eth1) of NAT 1 when Client B calls Client A.

3_NAT_NATL_eth1_B_CALL_A-WordPad	2 Microphone 😨 Tools 🔥 Handwiting 3 Drawing Pad 🕄 💷
Edit Vew Inset Format Help)⊯III ⊕ Cal HI K 1921 Con Raj	
codump: verbose output suppressed, use -v or -vv for full protocol decode	
listening on eth1, link-type EN10MB (Ethernet), capture size 96 bytes	
14:39:07.581937 IP 192.168.1.2.5060 > 192.168.0.10.5060: UDP, length 762	
14:39:07.644480 IP 192.168.0.10.5060 > 192.168.1.2.5060: UDP, length 376	
14:39:07.894018 IP 192:168.0.10.5060 > 192:168.1.2.5060: UDP, length 411	
14:39:12.579842 arp who-has 192.168.1.1 tell 192.168.1.2	
14:39:12.579877 arp reply 192.168.1.1 is-at 00:0c:41:ef:af:eb	
14:39:14.159724 IP 192.168.0.10.5060 > 192.168.1.2.5060: UDP, length 657	
14:39:14.167083 IP 192.168.1.2.5060 > 192.168.0.10.5060; UDP, length 375	
14:39:14.171723 IP 192.168.1.2.49232 > 192.168.0.10.49204: UDP, length 45	
14:39:14.191569 IP 192.168.1.2.49232 > 192.168.0.10.49204: UDP, length 45	
14:39:14.196233 IP 192.168.0.10.49204 > 192.168.1.2.49232: UDP, length 45	
14:39:14.211710 IP 192.168.1.2.49232 > 192.168.0.10.49204: UDP, length 45	
14:39:14.216131 IP 192.168.0.10.49204 > 192.168.1.2.49232: UDP, length 45	
14:39:14.231528 IP 192.168.1.2.49232 > 192.168.0.10.49204: UDP, length 45	
14:39:14.236366 IP 192.168.0.10.49204 > 192.168.1.2.49232: UDP, length 45	
14:39:14.252276 IP 192.168.1.2.49232 > 192.168.0.10.49204: UDP, length 45	
14:39:14.256164 IP 192.168.0.10.49204 > 192.168.1.2.49232: UDP, length 45	
14:39:14.271650 IP 192.168.1.2.49232 > 192.168.0.10.49204: UDP, length 45	
14:39:14.276177 IP 192.168.0.10.49204 > 192.168.1.2.49232: UDP, length 45	
14:39:14.291489 IP 192.168.1.2.49232 > 192.168.0.10.49204: UDP, length 45	
14:39:14.295885 IP 192.168.0.10.49204 > 192.168.1.2.49232: UDP, length 45	
14:39:14.311529 IP 192.168.1.2.49232 > 192.168.0.10.49204: UDP, length 45	
14:39:14.316027 IP 192.168.0.10.49204 > 192.168.1.2.49232: UDP, length 45	
14:39:14.331563 IP 192.168.1.2.49232 > 192.168.0.10.49204: UDP, length 45	
14:39:14.335880 IP 192.168.0.10.49204 > 192.168.1.2.49232: UDP, length 45	
14:39:14.351586 IP 192.168.1.2.49232 > 192.168.0.10.49204: UDP, length 45	
14:39:14.355863 IP 192.168.0.10.49204 > 192.168.1.2.49232: UDP, length 45	
14:39:14.371517 IP 192.168.1.2.49232 > 192.168.0.10.49204: UDP, length 45	
14:39:14.375912 IP 192.168.0.10.49204 > 192.168.1.2.49232: UDP, length 45	
14:39:14.391486 IP 192.168.1.2.49232 > 192.168.0.10.49204: UDP, length 45	
14:39:14.395885 IP 192.168.0.10.49204 > 192.168.1.2.49232: UDP, length 45	
14:39:14.411574 IP 192.168.1.2.49232 > 192.168.0.10.49204: UDP, length 45	
14:39:14.415914 IP 192.168.0.10.49204 > 192.168.1.2.49232: UDP, length 45	
14:39:14.431472 IP 192.168.1.2.49232 > 192.168.0.10.49204: UDP, length 45	
14:39:14.435861 IP 192.168.0.10.49204 > 192.168.1.2.49232: UDP, length 45	
14:39:14.451501 IP 192.168.1.2.49232 > 192.168.0.10.49204: UDP, length 45	
14:39:14.455904 IP 192.168.0.10.49204 > 192.168.1.2.49232: UDP, length 45	
14:39:14.471479 IP 192.168.1.2.49232 > 192.168.0.10.49204: UDP, length 45	
14:39:14.475870 IP 192.168.0.10.49204 > 192.168.1.2.49232: UDP, length 45	
14:39:14.491508 IP 192.168.1.2.49232 > 192.168.0.10.49204: UDP, length 45	
14:39:14.495910 IP 192.168.0.10.49204 > 192.168.1.2.49232: UDP, length 45	
14:39:14.511521 IP 192.168.1.2.49232 > 192.168.0.10.49204: UDP, length 45	
14:39:14.515854 IP 192.168.0.10.49204 > 192.168.1.2.49232: UDP, length 45	
14:39:14.531579 IP 192.168.1.2.49232 > 192.168.0.10.49204: UDP, length 45	
14:39:14.535904 IP 192.168.0.10.49204 > 192.168.1.2.49232: UDP, length 45	
14:39:14.551554 IP 192.168.1.2.49232 > 192.168.0.10.49204: UDP, length 45	
14:39:14.555902 IP 192.168.0.10.49204 > 192.168.1.2.49232: UDP, length 45	
14:39:14.333902 IP 192:100.0.10.49204 / 192:100.12.49232. 0DP, length 43 14:39:14.571458 IP 192.168.1.2.49232 > 192.168.0.10.49204: UDP, length 45	
14:39:14.3/1436 1P 192:166.1.2.49232 / 192:166.0.10.49204; ODP, length 43 14:39:14.575898 IP 192:168.0.10.49204 > 192:168.1.2.49232; UDP, length 45	
14:39:14.593636 1F 192.100.0.10.49204 / 192.100.12.49232. ODF, length 45 14:39:14.591522 IP 192.168.1.2.49232 > 192.168.0.10.49204: UDF, length 45	
14:39:14.391322 IP 192.100.1.2.49232 > 192.100.0.10.49204: ODP, length 43 14:39:14.596229 IP 192.168.0.10.49204 > 192.168.1.2.49232: UDP, length 45	
14:39:14.611520 IP 192.168.1.2.49232 > 192.168.0.10.49204: UDP, length 45	



E.1.5. NAT 2 Eth0

The following is a snapshot of the packets captured on the first interface (eth0) of NAT 2 when Client B calls Client A.

E-24 15 C	Call A) - Ethereal	in Uile									Microphone PTools [•	_
Edit View Go	Capture Analyze Statist										~		
	() 🕒 🚺)	: 🖗 🕹 🖻 🌾	i 📫 🖏	₹⊻		¥ 0,	Θ, Θ, [M M E	× 1			
:			 Expression 	Clear Ap	yv.								
<u> </u>					~/								
Time	Source 192.168.1.2	Destination 192.168.0.10	Protocol I		TNVTTE S	in•107	168.0.10,	wîth s	ession des	crintion			
2 0.063612	192.168.0.10	192.168.1.2	SIP :	tatus: 1	.00 Tryin	ig	100.0.10,	arten o	ession des	er iperon			
	192.168.0.10 192.168.1.2	192.168.1.2 LinksysG_ef:af:el			.80 Ringi 92 168 1		ell 192.168	12					
5 4.998727	192.168.1.1	192.168.1.2	ARP 1	92.168.1	.1 is at	00:0c	:41:ef:af:e	b					
	192.168.0.10 192.168.1.2	192.168.1.2 192.168.0.10					ssion descr 3.0.10:5060						
8 6.590388	192.168.1.2	192.168.0.10					SSRC=11299		Seq=18703,	Time=0,	Mark		
	192.168.1.2	192.168.0.10					SSRC=11299 SSRC=13281						
	192.168.0.10 192.168.1.2	192.168.1.2 192.168.0.10					SSRC=15281 SSRC=11299						
	192.168.0.10	192.168.1.2	RTP I	ayload t	ype=GSM	06.10,	SSRC=13281	8322, :	Seq=32013,	Time=640			
	192.168.1.2 192.168.0.10	192.168.0.10 192.168.1.2					SSRC=11299 SSRC=13281						
	192.168.1.2	192.168.0.10	RTP I	ayload t	ype=GSM	06.10,	SSRC=11299	5534, 1	Seq=18707,	Time=640			
	192.168.0.10 192.168.1.2	192.168.1.2 192.168.0.10					SSRC=13281 SSRC=11299						
18 6.695052	192.168.0.10	192.168.1.2	RTP I	ayload t	ype=GSM	06.10,	SSRC=13281	8322, 1	Seq=32016,	Time=112	0		
	192.168.1.2 192.168.0.10	192.168.0.10 192.168.1.2					SSRC=11299 SSRC=13281						
21 6.730192	192.168.1.2	192.168.0.10	RTP I	ayload t	ype=GSM	06.10,	SSRC=11299	5534, 1	Seq=18710,	Time=112	0		
	192.168.0.10	192.168.1.2					SSRC=13281						
	192.168.1.2 192.168.0.10	192.168.0.10 192.168.1.2		ay i uau i		00.10,	SSRC=11299	5554, 1					
25 6 770251			NIC I	ayload t	ype=GSM	06.10,	SSRC=13281	8322, :	5eq=32019,	1106=100	0		
26 6.774743 came 1 (804 k chernet II, s nternet Proto ser Datagram ession Initia Request-Line	ocol, Src: 192.168 Protocol, Src Por ation Protocol e: INVITE sip:192.	00:e0:29:67:9e:9c), .1.2 (192.168.1.2), t: 5060 (5060), Dst	RTP RTP Dst: 192.7	ayload t ayload t 68.1.1 68.0.10	ype=GSM ype=GSM (00:0c:41	06.10, 06.10, .:ef:af	SSRC=13281 SSRC=11299 SSRC=13281 :eb)	5534, 1	Seq=18712,	Time=144	0		
26 6.774743 rame 1 (804 k thernet II, S iternet Proto ser Datagram assion Initia Request-Line Message Head Message body ⊕ Session De Session ⊞ Owner/Cr Session	192.168.0.10 bytes on wire, 804 Src: 192.168.1.2 (ocol, Src: 192.168 Protocol, Src Por ation Protocol e: INVITE sip:192 der yescription Protoco Description Protoco Description Protoco Mame (s): Siphone	192.168.1.2 bytes captured) 00:e0:29:67:9e:9c), .1.2 (192.168.1.2), t: 5060 (5060), Dst 168.0.10 SIP/2.0 1 col version (v): 0 (o): - 3334103399 3	RTP 1 RTP 1 Dst: 192. Dst: 192. Port: 506	ayload t ayload t 68.1.1 68.0.10 (5060)	ype=GSM ype=GSM (00:0c:41 (192.168	06.10, 06.10, .:ef:af 3.0.10)	SSRC=11299 SSRC=13281	5534, 1	Seq=18712,	Time=144	0		
26 6.774743 Tame 1 (804 k thernet II, s iternet Protoser ere Datagram ession Initia Request-Line Message body Bession De Session De Session De Session B Onner(Ti B Time Des B Session B Session B Media At B Media At B Media At B Media At	192.168.0.10 bytes on wire, 804 Src: 192.168.1.2 (ocol, src: 192.168 Protocol, Src Por ation Protocol e: INVITE sip:192 der yescription Protoco Description Protoco Description Protoco cription, active Attribute (a): siphone isscription, active thribute (a): rtpm.	192.168.1.2 bytes captured) 00:e0:29:67:9e:9C), .1.2 (192.168.1.2), t: 5060 (5060), bst 168.0.10 SIP/2.0 1 10 Version (v): 0 (o): - 3334103399 3): IN IP4 192.168.2. time (t): 0 0 rection:active nd address (m): audi ap:3 GSV(8000 ap:98 iLBC/8000	RTP 1 RTP 1 Dst: 192.: Dst: 192.: Port: 5060 1334103399 10	ayload t ayload t 68.1.1 (68.0.10 (5060)	ype=GSM ype=GSM (00:0c:41 (192.168 92.168.2	06.10, 06.10, .:ef:af 8.0.10)	SSRC=11299 SSRC=13281	5534, 1	Seq=18712,	Time=144	0		
26 6.774743 Tame 1 (804 H thernet Protoson ternet Protoson rer Datagram assion Initi Request-Line Message Head Message Head Message Head Session B Connecti B Time Des Session B Media At B Media At	192.168.0.10 bytes on wire, 804 Src: 192.168.1.2 (occl, src: 192.168 Protocol, Src Por ation Protocol e: INVITE sip:192. der y scription Protoco Description Protoco Description Protoco con Information (c) scription, active t Attribute (a): Siphone ion Information (c) cription, active t Attribute (a): di scription, active t Attribute (a): rtpm trribute (a): rtpm trribute (a): rtpm trribute (a): rtpm trribute (a): rtpm trribute (a): rtpm	192.168.1.2 bytes captured) 00:e0:29:67:9e:9C), .1.2 (192.168.1.2), t: 5060 (5060), Dst 168.0.10 SIP/2.0 10 10 (0: - 3334103399 3 1: IN IP4 192.168.2. time (t): 0 0 rection:active nd address (m): audi mp:35 SCH/A000 98 mode=20 98 mode=20 98: Deck/A000 90: 0 - 2000	RTP I RTP I Dst: 192.: Dst: 192.: Dst: 192.: Port: 506 I334103399 I0 0 49232 R1 I	ayload t 68.1.1 68.0.10 (5060)	ype=GSM ype=GSM (00:0c:41 (192.168.2) 92.168.2) 97 98 8 (06.10, 06.10, .:ef:af 8.0.10)	SSRC=11299 SSRC=13281	5534, 1	Seq=18712,	Time=144	0		
26 6.774743 ame 1 (804 k thermet 11, 5 tternet Protoconsection assion Initia Request-Line Message Heady ■ Session De Session De Session De Session De Session De © Onnection ■ Connection ■ Connection ■ Session ■ Media At ■ Media A	192.168.0.10 bytes on wire, 804 Src: 192.168.1.2 (ocol, src: 192.168 Protocol, Src Por ation Protocol Src Por ation Protocol e: INVITE sip:192 der scription Protoco Description Protoco Description Protoco Description Protoco Information (C, scription, active 1 Attribute (a): siphone of Information (C, scription, active 1 Attribute (a): rtpm tribute (192.168.1.2 bytes captured) 00:e0:29:67:9e:9C), 1.2 (192.168.1.2), t: 5060 (3060), Dst 168.0.10 SIP/2.0 1 101 Version (v): 0 (o): - 3334103399 3 1: IN IP4 192.168.2. time (t): 0 0 rection:active nd address (m): audi p:3 Six/8000 ap:97 iLBC/8000 ap:97 iLBC/8000 ap:98 mode-20 ap:8 PCMA/8000	RTP I RTP I RTP I DSt: 192.: I DSt: 192.: I PORT: 506 I I0 I0 I0 I0 I0 I0 I0 0 I0 I0 0 I0 I0 0 I0 I0	ayload t ayload t 68.1.1 (68.0.10 (5060)	ype=GSM 00:0c:41 (192.168 92.168.2 97 98 8 (06.10, 06.10, .:ef:af 8.0.10)	SSRC=11299 SSRC=13281	5534, 1	Seq=18712,	Time=144	0		

Figure 36.

Test 4: Packet Capture on eth0 of NAT 2 (Client B Calls Client A)

E.1.6. NAT 2 Eth1

The following is a snapshot of the packets captured on the second interface (eth1) of NAT 2 when Client B calls Client A.

		2 Microphone 🖉 Tools 🔃 🗧	_ 6
jle Edit <u>Vi</u> ew <u>G</u> o <u>C</u> apture <u>A</u> nalyze	e <u>S</u> tatistics <u>H</u> elp	• 30 - 80 - 80 - 80 - 80 - 80 - 80 - 80 -	
	🛊 🔊 占 🕲 🗴 🖹	🔿 🖓 🌆 🖳 🗐 🕄 O, Q, Q, 🔟 🖼 🖾 🖽 🛠 🗑	
iter:		Epression [dear goly	
b Time Source 1 0.000000 192.168.2.	Destination 10 192.168.2.255	Protocol Info BROWSE Domain/Workgroup Announcement WORKGROUP, NT Workstation, Domain Enum	
2 49.310980 192.168.2.	10 Broadcast	ARP who has 192.168.2.1? Tell 192.168.2.10	
3 49.311019 192.168.2. 4 49.311212 192.168.2.	1 192.168.2.10 10 192.168.0.10	ARP 192.168.2.1 is at 00:01:02:89:97:5b	
5 49.374948 192.168.0.		SIP/SD Request: INVITE sip:192.168.0.10, with session description SIP Status: 100 Trying	
6 49.624525 192.168.0.	10 192.168.2.10	SIP Status: 180 Ringing	
7 54.373778 192.168.2. 8 54.373890 192.168.2.		ARP who has 192.168.2.10? Tell 192.168.2.1 ARP 192.168.2.10 is at 00:0f:1f:18:d7:c5	
9 55.890437 192.168.0.	10 192.168.2.10	SIP/SD Status: 200 OK, with session description	
10 55.896727 192.168.2. 11 55.901637 192.168.2.		SIP Request: ACK sip:192.168.0.10:5060 RTP Payload type=GSM 06.10, SSRC=112995534, Seq=18703, Time=0, Mark	
12 55.921455 192.168.2.	10 192.168.0.10	RTP Payload type=G5M 06.10, SSRC=112995534, Seq=18704, Time=160	
13 55.926444 192.168.0.	10 192.168.2.10	RTP Payload type=G5M 06.10, S5RC=132818322, Seq=32012, Time=480	
14 55.941584 192.168.2. 15 55.946368 192.168.0.		RTP Payload type=65W 06.10, S5RC=112995534, seq=18705, Time=320 RTP Payload type=65W 06.10, S5RC=132818322, seq=32013, Time=640	
16 55.961408 192.168.2.	10 192.168.0.10	RTP Payload type=G5M 06.10, SSRC=112995534, Seq=18706, Time=480	
17 55.966551 192.168.0. 18 55.982195 192.168.2.		RTP Payload type=65W 06.10, S5RC=132818322, Seq=32014, Time=800 RTP Payload type=65W 06.10, S5RC=112995534, Seq=18707, Time=640	
19 55.986343 192.168.0.		RTP Payload type=GSM 06.10, SSRC=11299553, Seq=10.01, Time=040	
20 56.001529 192.168.2.	10 192.168.0.10	RTP Payload type=GSM 06.10, SSRC=112995534, Seq=18708, Time=800	
21 56.006352 192.168.0. 22 56.021413 192.168.2.	10 192.168.2.10 10 192.168.0.10	RTP Payload type=65W 06.10, S5RC=132818322, Seq=32016, Time=1120 RTP Payload type=65W 06.10, S5RC=112995534, Seq=18709, Time=960	
23 56.026054 192.168.0.		RTP Payload type=GSM 06.10, SSRC=132818322, Seq=32017, Time=1280	
24 56.041416 192.168.2.	10 192.168.0.10	RTP Payload type=GSM 06.10, SSRC=112995534, Seq=18710, Time=1120	
Ethernet II, Src: 192.168 Internet Protocol, Src: 1 User Datagram Protocol, S NetBIOS Datagram Service	10 192.168.0.10 e, 251 bytes captured) .2.10 (00:0f:1f:18:d7:c5), .2168.2.10 (192.168.2.10) rc Port: netbios-dgm (138)	RTP Payload type=GSM 06.10, SSRC=132818322, Seq=32018, Time=1440 RTP Payload type=GSM 06.10, SSRC=112995534, Seq=18711, Time=1280 Dst: Broadcast (ff:ff:ff:ff:ff:ff:ff) Dst: 192,168.2.255 (192,168.2.255) Dst Port: netbios-dgm (138)	
26 56.061471 192.168.2. Frame 1 (251 bytes on wir Ethernet II, Src: 192.168 Internet Protocol, Src: 1	10 192.168.0.10 a, 251 bytes captured) .2.10 (00:0f:1f:18:d7:c5), .2.168.2.10 (192.168.2.10)	RTP Payload type=GSM 06.10, SSRC=112995534, Seq=18711, Time=1280 Dst: Broadcast (ff:ff:ff:ff:ff:ff) Dst: 192.168.2.255 (192.168.2.255)	



E.1.7. Analysis

As soon as Client B dialed the IP address of Client A, Client B sent out an "INVITE" message to Client A (red outline in Figure 33). The message had embedded SDP information to inform Client A that Client B would be sending and receiving RTP packets at 192.168.2.10 on port 49232 (purple outline in Figure 34). To acknowledge the invitation, Client A sent a "200 OK" packet to Client B with embedded SDP information indicating that it would send and receive RTP packets at 192.168.2.10 on port 49204 (green outline in Figure 33). The packets captured on Client A indicate that Client A sent and received RTP packet directly to/from the public IP address of NAT 1. As explained in Appendix C, SJPhone will first attempt to send RTP media packets to the IP address indicated in the SDP message (or the private IP address of Client B). Since the firewall installed on Client A was configured to drop packets destined to the private IP address of Client B, none of the packets sent out by Client A could reach Client B. Therefore, Client A then sent subsequent RTP packets to the IP address in which received the RTP media packets (blue outline in Figure 34)

The packet captures indicate that the first RTP packet is sent by Client B (black outline in Figure 33). Even though NAT 1 was not explicitly configured to rewrite the destination IP address of incoming packets to 192.168.1.2 (public IP address of NAT 2), NAT 1 intelligently does this on its own. A reasonable explanation for this behavior is that *iptables* in NAT 1 maintained information for packets that are initiated from the local network [19]. In our scenario, the first RTP packet is processed according to the SNAT rule when it arrives at NAT 1. At the same time, NAT 1 created an entry in its connection tracking table to store essential information (such as source and destination IP addresses and ports) that would allow it to associate incoming packets with the session between Client A and Client B. Packets determined to belong to a certain packet previously received from NAT 2 (refer to Figures 35 through 38). This is evident from observing the packet captures on eth1 of NAT 2.

E.2. Client C Calls Client A

E.2.1. Client A

The following is a snapshot of the packets captured on Client A when Client C calls Client A.

		e Manaphane (@Tools [?] ;
<u>File Edit View Go Capture Analyze Sta</u>		
	x 🕲 📇 💽 💠 🐳 🖓 🟠	2 0 0 0 0 0 0 0 0 0 0
Elter:	▼ <u>Expression</u> <u>Q</u> le	r aon
No Time Source	Destination Protocol Info	2
1 0.000000 192.168.0.10		e port: 5003 Destination port: 5003
2 60.176582 192.168.0.10 3 62.423265 192.168.0.1	Broadcast ARP Who I	e port: 5003 Destination port: 5003 nas 192.168.0.107 Tell 192.168.0.1
4 62.423278 192.168.0.10 5 62.423351 192.168.0.1		68.0.10 is at 00:0f:1f:19:27:36 st: INVITE sip:192.168.0.10, with session description
6 62.457945 192.168.0.10	192.168.0.1 SIP State	is: 100 Trying
7 62.469516 192.168.0.10 8 62.590691 192.168.0.10		query NB WWw.SJLABS.COM <oo> is: 180 Ringing</oo>
9 62.858943 192.168.0.10	192.168.0.255 NBNS Name	query NB WWW.SJLABS.COM<00>
10 63.245316 192.168.0.10 11 65.081662 192.168.0.10	192.168.0.255 NBNS Name 192.168.0.1 SIP/SD State	query NB WWW.SJLABS.COM<00> us: 200 OK, with session description
12 65.084592 192.168.0.1	192.168.0.10 SIP Requ	est: ACK sip:192.168.0.10:5060
13 65.089033 192.168.0.10 14 65.093222 192.168.0.1		query NB wWw.SJLABS.COM<00> pad type=GSM 06.10, SSRC=7619304, Seq=18868, Time=O, Mark
15 65.095716 192.168.0.10	192.168.0.1 RTP Payle	oad type=GSM 06.10, SSRC=354435158, Seq=10101, Time=160
16 65.103673 192.168.0.1 17 65.105557 192.168.0.10		ad type=GSM 06.10, SSRC=7619304, Seq=18869, Time=160 ad type=GSM 06.10, SSRC=354435158, Seq=10102, Time=320
18 65.114026 192.168.0.1	192.168.0.10 RTP Payle	oad type=GSM 06.10, SSRC=7619304, Seq=18870, Time=320
19 65.115980 192.168.0.10 20 65.124500 192.168.0.1		ad type=GSM 06.10, SSRC=354435158, Seq=10103, Time=480 ad type=GSM 06.10, SSRC=7619304, Seq=18871, Time=480
21 65.126414 192.168.0.10	192.168.0.1 RTP Payle	oad type=GSM 06.10, SSRC=354435158, seq=10104, Time=640
22 65.134890 192.168.0.1 23 65.137048 192.168.0.10		ad type=GSM 06.10, SSRC=7619304, Seq=18872, Time=640 ad type=GSM 06.10, SSRC=354435158, Seq=10105, Time=800
24 65.145403 192.168.0.1	192.168.0.10 RTP Payle	oad type=GSM 06.10, SSRC=7619304, Seq=18873, Time=800
25 65.147296 192.168.0.10 26 65.155763 192.168.0.1	192.168.0.1 RTP Paylo 192.168.0.10 RTP Paylo	ad type=GSM 06.10, SSRC=354435158, Seq=10106, Time=960 ad type=GSM 06.10, SSRC=7619304, Seq=18874, Time=960
□ User Datagram Protocol, Src P. Session Initiation Protocol Request-time: INVITE siplig: Message Header Message beader Session Description Protocol Session Description Protocol Ommer/Creator, Session J Session Name (s): Siphor ⊕ Connection Information (⊕ Time Description, active ⊞ Session Attribute (a): c	tol tocol Version (v): 0 td (o): - 3334083070 3334083070 IN J me (c): IN IP4 192.168.3.10 time(t): 0 0 time(t): 0 0 timection:active and address (m): audio 49156 RTP/AV omap: 97 iLBC/8000 map:98 iLBC/8000	P4 192.168.3.10
⊞ Media Attribute (a): rtp ⊞ Media Attribute (a): rtp	map:8 PCMA/8000 map:0 PCMU/8000	
0000 00 0f 1f 19 27 36 00 4c 6 0010 03 15 06 22 00 00 7e 11 b 0020 00 0a 13 c4 13 c4 03 01 6	02 5a cO a8 00 01 cO a8"~ 53 1e 49 4e 56 49 54 45 c 2e 31 36 38 2e 30 2e 31 sip:192 .	Z .INVITE

Figure 38. Test 4: Packet Capture on Client A (Client C Calls Client A)

E.2.2. Client C

The following is a snapshot of the packets captured on Client C when Client C calls Client A.

-26 (C 3 NAT C CA	LL A) - Ethereal			Z Microphone 🖉 Tools 👔 🕽	_ 8
<u>E</u> dit <u>Vi</u> ew <u>G</u> o	<u>Capture Analyze Statis</u>	tics <u>H</u> elp			
		(@ ₽ @ 4	🔹 🕸 🛧 🖞 🗐 📑 🔍 Q 🍳 🖭 📓 🛛	B 💥 🔯	
n			<u> Expression Qear Apply</u>		
 Tme 1.0.000000 	Source 192.168.3.10	Destination Broadcast	Protocol Info ARP who has 192.168.3.1? Tell 192.168.3.10		
2 0.000173	192.168.3.1	192.168.3.10	ARP 192.168.3.1 is at 00:0c:41:ef:af:be	1	
3 0.000182 4 0.070941		192.168.0.10 192.168.3.10	SIP/SD Request: INVITE sip:192.168.0.10, with session SIP Status: 100 Trying	description	
5 0.325338 6 5.070669	192.168.0.10 192.168.3.1	192.168.3.10 192.168.3.10	SIP Status: 180 Ringing ARP Who has 192.168.3.10? Tell 192.168.3.1		
7 5.070688	192.168.3.10	192.168.3.1	ARP 192.168.3.10 is at 00:0d:56:38:24:0d		
9 5.177237		192.168.3.10 192.168.0.10	SIP Request: ACK sip:192.168.0.10:5060		
10 5.194096 11 5.199484		192.168.0.10 192.168.3.10	RTP Payload type=GSM 06.10, SSRC=7619304, Seq=18866 RTP Payload type=GSM 06.10, SSRC=354435158, Seq=103		
12 5.214111	192.168.3.10	192.168.0.10	RTP Payload type=GSM 06.10, SSRC=7619304, Seq=18869	9, Time=160	
13 5.218309 14 5.234050		192.168.3.10 192.168.0.10	RTP Payload type=GSM 06.10, SSRC=354435158, Seq=101 RTP Payload type=GSM 06.10, SSRC=7619304, Seq=1887(
15 5.238272	192.168.0.10	192.168.3.10	RTP Payload type=GSM 06.10, SSRC=354435158, Seq=101	103, Time=480	
10 5.254041	192.168.3.10 192.168.0.10	192.168.0.10 192.168.3.10	RTP Payload type=GSM 06.10, SSRC=7619304, Seq=18871 RTP Payload type=GSM 06.10, SSRC=354435158, Seq=103	1, 11me=480 L04, Time=640	
18 5.274048	192.168.3.10	192.168.0.10	RTP Payload type=GSM 06.10, SSRC=7619304, Seq=1887.	2, Time=640	
	192.168.0.10 192.168.3.10	192.168.3.10 192.168.0.10	RTP Payload type=GSM 06.10, SSRC=354435158, Seq=101 RTP Payload type=GSM 06.10, SSRC=7619304, Seq=1887	3, Time=800	
	192.168.0.10 192.168.3.10	192.168.3.10 192.168.0.10	RTP Payload type=GSM 06.10, SSRC=354435158, Seq=101 RTP Payload type=GSM 06.10, SSRC=7619304, Seq=18874		
	192.108.3.10	192.168.3.10	RTP Payload type=GSM 06.10, SSRC=/019304, Seq=103/4 RTP Payload type=GSM 06.10, SSRC=354435158, Seq=101		
24 5.334090 25 5.338311	192.168.3.10 192.168.0.10	192.168.0.10 192.168.3.10	RTP Payload type=GSM 06.10, SSRC=7619304, Seq=1887 RTP Payload type=GSM 06.10, SSRC=354435158, Seq=101	5, Time=1120	
26 5.354058		192.168.0.10	RTP Payload type=65M 06.10, 55RC=7519304, 5eq=16876		
Session Initi Status-Line IMESSAGE Heal Message bod Session D Session Owner/CI Session Connect: Time De: Session Media Ai Media Ai Media Ai Media Ai	ation Protocol : SIP/2.0 200 ok der y escription Protoco Description Protor reator, Session Id Name (s): SJphone ion Information (c scription, active Attribute (a): di escription, name a ttribute (a): rtpm	col version (v): 0 (o): - 3334126547): IN IP4 192.168.0 time (t): 0 0 rection:active nd address (m): aud ap:3 GSM/8000 ap:101 telephone-ev	334126547 IN IP4 192.168.0.10 10 0 49212 RTP/AVP 3 101		
0 49 50 27 0 36 38 2e 0 36 30 3b 0 31 36 38 0 39 68 47 0 30 30 30 0 30 30 30 0 30 30 34 0 43 6f 6e 0 32 31 38 0 69 70 3a	22 2e 30 2f 55 44 33 2e 31 30 3b 72 72 65 63 65 69 72 72 62 92 2e 31 3b 62 34 62 4b 63 30 61 30 31 64 34 33 30 37 66 65 30 30 30 74 65 6e 74 2d 4c 0d 0a 43 6f 6e 74 31 39 32 2e 31 36	Da 56 69 61 3a 20 50 20 31 39 32 2e 70 61 72 74 30 32 2e 56 64 3d 31 39 32 2e 56 64 3d 31 39 32 2e 56 64 3d 31 39 32 72 61 66 68 3d 33 33 30 33 30 33 30<	Content-Length: 218.Contact: <s a ip:192.1 68.0.10:</s 		

Figure 39. Test 4: Packet Capture on Client C (Client C Calls Client A)

E.2.3. NAT 1 Eth0

The following is a snapshot of the packets captured on the first interface (eth0) of NAT 1 when Client C calls Client A.

3_NAT_NATL_eth0_C_CALL_A-WordPad = Edit View Inset Format Heb	🧷 🖉 Mcrophone 🖉 Tools 🛛 🔏 Handwriting 🖓 Drawing Pad [🤉 💷
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode	
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes	
15:12:05.343305 IP 192.168.0.10.5003 > 192.168.0.255.5003: UDP, length 125	
15:12:09.848537 arp who-has 192.168.0.10 tell 192.168.0.1	
15:12:09.848653 arp reply 192.168.0.10 is-at 00:0f:1f:19:27:36	
15:12:09.848666 IP 192.168.0.1.5060 > 192.168.0.10.5060; UDP, length 761	
15:12:09.915163 IP 192.168.0.10.5060 > 192.168.0.1.5060: UDP, length 375	
15:12:09.937317 IP 192.168.0.10.netbios-ns > 192.168.0.255.netbios-ns: NBT UDP PACKET(137) · OUFRY · REOUFST · BROADCAST
15:12:10.169579 IP 192.168.0.10.5060 > 192.168.0.1.5060: UDP, length 410	, welki, hegelei, skonsensi
15:12:10.683671 IP 192.168.0.10.netbios-ns > 192.168.0.255.netbios-ns: NBT UDP PACKET(137	· OUFRY. REOURST. BROADCAST
15:12:11.433633 IP 192.168.0.10.netbios-ns > 192.168.0.255.netbios-ns: NBT UDP PACKET(137	
15:12:15.017096 IP 192.168.0.10.5060 > 192.168.0.1.5060: UDP, length 656	/. WOENI, NEWOLDI, DRONDCADI
15:12:15.022473 IP 192.168.0.1.5060 > 192.168.0.10.5060: UDP, length 374	
15:12:15.031145 IP 192.168.0.10.netbios-ns > 192.168.0.255.netbios-ns: NBT UDP PACKET(137	· OHERV. REOHERT. REOLOGICT
15:12:15.039016 IP 192.168.0.1.49156 > 192.168.0.10.49212: UDP, length 45	/. WOEKI, KEWOESI, BROADCASI
15:12:15.059010 1P 192.100.0.1.49130 > 192.100.0.10.49212. ODP, length 45 15:12:15.043942 IP 192.168.0.10.49212 > 192.168.0.1.49156: UDP, length 45	
15:12:15.059094 IP 192.168.0.1.49156 > 192.168.0.10.49212: UDP, length 45	
15:12:15.062793 IP 192.168.0.10.49212 > 192.168.0.1.49156: UDP, length 45	
15:12:15.02/95 IP 122:100.0.10.42212 / 122:100.0.1.49150. 0DF, length 45 15:12:15.078938 IP 192.168.0.1.49156 > 192.168.0.10.49212: UDP, length 45	
15:12:15.078938 IP 192.168.0.10.49218 > 192.168.0.1.49156: UDP, length 45	
15:12:15.099013 IP 192.168.0.1.49156 > 192.168.0.10.49212: UDP, length 45	
15:12:15.102766 IP 192.168.0.10.49212 > 192.168.0.1.49156: UDP, length 45	
15:12:15.118927 IP 192.168.0.1.49156 > 192.168.0.10.49212: UDP, length 45	
15:12:15.123153 IP 192.168.0.10.49212 > 192.168.0.1.49156: UDP, length 45	
15:12:15.139059 IP 192.168.0.1.49156 > 192.168.0.10.49212: UDP, length 45	
15:12:15.142788 IP 192.168.0.10.49212 > 192.168.0.1.49156: UDP, length 45	
15:12:15.158931 IP 192.168.0.1.49156 > 192.168.0.10.49212: UDP, length 45 15:12:15.162873 IP 192.168.0.10.49212 > 192.168.0.1.49156: UDP, length 45	
15:12:15.178973 IP 192.168.0.1.49156 > 192.168.0.10.49212: UDP, length 45	
15:12:15.182766 IP 192.168.0.10.49212 > 192.168.0.1.49156: UDP, length 45	
15:12:15.198986 IP 192.168.0.1.49156 > 192.168.0.10.49212: UDP, length 45	
15:12:15.202767 IP 192.168.0.10.49212 > 192.168.0.1.49156: UDP, length 45	
15:12:15.218950 IP 192.168.0.1.49156 > 192.168.0.10.49212: UDP, length 45	
15:12:15.222769 IP 192.168.0.10.49212 > 192.168.0.1.49156: UDP, length 45	
15:12:15.239103 IP 192.168.0.1.49156 > 192.168.0.10.49212: UDP, length 45	
15:12:15.242836 IP 192.168.0.10.49212 > 192.168.0.1.49156: UDP, length 45	
15:12:15.258924 IP 192.168.0.1.49156 > 192.168.0.10.49212: UDP, length 45	
15:12:15.262800 IP 192.168.0.10.49212 > 192.168.0.1.49156: UDP, length 45	
15:12:15.278968 IP 192.168.0.1.49156 > 192.168.0.10.49212: UDP, length 45	
15:12:15.282766 IP 192.168.0.10.49212 > 192.168.0.1.49156: UDP, length 45	
15:12:15.298936 IP 192.168.0.1.49156 > 192.168.0.10.49212: UDP, length 45	
15:12:15.302774 IP 192.168.0.10.49212 > 192.168.0.1.49156: UDP, length 45	
15:12:15.318972 IP 192.168.0.1.49156 > 192.168.0.10.49212: UDP, length 45	
15:12:15.322765 IP 192.168.0.10.49212 > 192.168.0.1.49156: UDP, length 45	
l5:12:15.338997 IP 192.168.0.1.49156 > 192.168.0.10.49212: UDP, length 45	
15:12:15.343141 IP 192.168.0.10.49212 > 192.168.0.1.49156: UDP, length 45	
15:12:15.358925 IP 192.168.0.1.49156 > 192.168.0.10.49212: UDP, length 45	
15:12:15.363191 IP 192.168.0.10.49212 > 192.168.0.1.49156: UDP, length 45	
15:12:15.379073 IP 192.168.0.1.49156 > 192.168.0.10.49212: UDP, length 45	
15:12:15.383038 IP 192.168.0.10.49212 > 192.168.0.1.49156: UDP, length 45	
15:12:15.398964 IP 192.168.0.1.49156 > 192.168.0.10.49212: UDP, length 45	
15:12:15.402797 IP 192.168.0.10.49212 > 192.168.0.1.49156: UDP, length 45	
15:12:15.418980 IP 192.168.0.1.49156 > 192.168.0.10.49212: UDP, length 45	



Test 4: Packet Capture on eth0 of NAT 1 (Client C Calls Client A)

E.2.4. NAT 1 Eth1

The following is a snapshot of the packets captured on the second interface (eth1) of NAT 1 when Client C calls Client A.

3_IAT_NATL_thLC_CALL A - WordPad	🤌 Microphone 😨 Tools 🔏 Handwriting 🖓 Drawing Pad [🕽 🗧
Edit Vew Inset Format Help Inset I State Control Con	
cpdump: verbose output suppressed, use -v or -vv for full protocol decode	
istening on eth1, link-type EN10MB (Ethernet), capture size 96 bytes	
5:12:09.847034 arp who-has 192.168.1.1 tell 192.168.1.3	
5:12:09.847093 arp reply 192.168.1.1 is-at 00:0c:41:ef:af:eb	
5:12:09.847882 IP 192.168.1.3.5060 > 192.168.0.10.5060: UDP, length 761	
5:12:09.915243 IP 192.168.0.10.5060 > 192.168.1.3.5060: UDP, length 375	
5:12:10.169641 IP 192.168.0.10.5060 > 192.168.1.3.5060: UDP, length 410	
5:12:14.913769 arp who-has 192.168.1.3 tell 192.168.1.1	
5:12:14.914013 arp reply 192.168.1.3 is-at 00:50:da:c0:50:ff	
5:12:15.017160 IP 192.168.0.10.5060 > 192.168.1.3.5060: UDP, length 656	
5:12:15.022452 IP 192.168.1.3.5060 > 192.168.0.10.5060: UDP, length 374	
5:12:15.038985 IP 192.168.1.3.49156 > 192.168.0.10.49212: UDP, length 45	
5:12:15.043996 IP 192.168.0.10.49212 > 192.168.1.3.49156: UDP, length 45	
5:12:15.059032 IP 192.168.1.3.49156 > 192.168.0.10.49212: UDP, length 45	
5:12:15.062816 IP 192.168.0.10.49212 > 192.168.1.3.49156: UDP, length 45	
5:12:15.078915 IP 192.168.1.3.49156 > 192.168.0.10.49212: UDP, length 45	
5:12:15.082786 IP 192.168.0.10.49212 > 192.168.1.3.49156: UDP, length 45	
5:12:15.098961 IP 192.168.1.3.49156 > 192.168.0.10.49212: UDP, length 45	
5:12:15.102787 IP 192.168.0.10.49212 > 192.168.1.3.49156: UDP, length 45	
5:12:15.118909 IP 192.168.1.3.49156 > 192.168.0.10.49212: UDP, length 45	
5:12:15.123168 IP 192.168.0.10.49212 > 192.168.1.3.49156: UDP, length 45	
5:12:15.139008 IP 192.168.1.3.49156 > 192.168.0.10.49212: UDP, length 45	
5:12:15.142808 IP 192.168.0.10.49212 > 192.168.1.3.49156: UDP, length 45	
5:12:15.158910 IP 192.168.1.3.49156 > 192.168.0.10.49212: UDP, length 45	
5:12:15.162889 IP 192.168.0.10.49212 > 192.168.1.3.49156: UDP, length 45	
5:12:15.178958 IP 192.168.1.3.49156 > 192.168.0.10.49212: UDP, length 45	
5:12:15.182817 IP 192.168.0.10.49212 > 192.168.1.3.49156: UDP, length 45	
15:12:15.198967 IP 192.168.1.3.49156 > 192.168.0.10.49212: UDP, length 45	
5:12:15.202787 IP 192.168.0.10.49212 > 192.168.1.3.49156: UDP, length 45	
5:12:15.218935 IP 192.168.1.3.49156 > 192.168.0.10.49212: UDP, length 45	
5:12:15.222784 IP 192.168.0.10.49212 > 192.168.1.3.49156; UDP, length 45	
5:12:15.239052 IP 192.168.1.3.49156 > 192.168.0.10.49212: UDP, length 45 5:12:15.242855 IP 192.168.0.10.49212 > 192.168.1.3.49156: UDP, length 45	
5:12:15.258902 IP 192.168.1.3.49156 > 192.168.0.10.49212; UDP, length 45	
5:12:15.262816 IP 192.168.0.10.49212 > 192.168.1.3.49156: UDP, length 45	
5:12:15.278917 IP 192.168.1.3.49156 > 192.168.0.10.49212: UDP, length 45	
5:12:15.282786 IP 192.168.0.10.49212 > 192.168.1.3.49156: UDP, length 45	
5:12:15.298918 IP 192.168.1.3.49156 > 192.168.0.10.49212: UDP, length 45	
5:12:15.302790 IP 192.168.0.10.49212 > 192.168.1.3.49156: UDP, length 45	
5:12:15.318921 IP 192.168.1.3.49156 > 192.168.0.10.49212: UDP, length 45	
5:12:15.322785 IP 192.168.0.10.49212 > 192.168.1.3.49156: UDP, length 45	
5:12:15.338978 IP 192.168.1.3.49156 > 192.168.0.10.49212: UDP, length 45	
5:12:15.343157 IP 192.168.0.10.49212 > 192.168.1.3.49156: UDP, length 45	
5:12:15.358897 IP 192.168.1.3.49156 > 192.168.0.10.49212: UDP, length 45	
5:12:15.363210 IP 192.168.0.10.49212 > 192.168.1.3.49156: UDP, length 45	
5:12:15.379022 IP 192.168.1.3.49156 > 192.168.0.10.49212: UDP, length 45	
5:12:15.383058 IP 192.168.0.10.49212 > 192.168.1.3.49156: UDP, length 45	
5:12:15.398946 IP 192.168.1.3.49156 > 192.168.0.10.49212: UDP, length 45	
5:12:15.402813 IP 192.168.0.10.49212 > 192.168.1.3.49156: UDP, length 45	
5:12:15.418930 IP 192.168.1.3.49156 > 192.168.0.10.49212: UDP, length 45	
5:12:15.422787 IP 192.168.0.10.49212 > 192.168.1.3.49156: UDP, length 45	
5:12:15.438931 IP 192.168.1.3.49156 > 192.168.0.10.49212: UDP, length 45	
5:12:15.442838 IP 192.168.0.10.49212 > 192.168.1.3.49156: UDP, length 45	

Figure 41. Test 4: Packet Capture on eth1 of NAT 1 (Client C Calls Client A)

E.2.5. NAT 3 Eth0

The following is a snapshot of the packets captured on the first interface (eth0) of NAT 3 when Client C calls Client A.

8-26 (3 NATS	5 NAT 3 e	th0 C Call A) - Ethereal		2 ⁹ Microphone @Tools (2) :	
e <u>E</u> dit <u>Vi</u> er	w <u>G</u> o (<u>C</u> apture <u>A</u> nalyze <u>S</u> tatis	tics <u>H</u> elp		
		🕍 🕒 🖪 🕽	(@ B Q () 🔿 🕫 🛧 📳 🗐 🕃 (Q, Q, Q, 19) 👪 🖾 🎛 🔆 (🞯	
in:				Epression [Dear Apply]	
- Time		Source	Destination	Protocol Info	
		192.168.1.3 192.168.1.1	Broadcast 192.168.1.3	ARP who has 192.168.1.1? TE() 192.168.1.3 ARP 192.168.1.1 is at 00:0c:41:ef:af:eb	
3 0.0	00256	192.168.1.3	192.168.0.10	SIP/SD Request: INVITE sip:192.168.0.10, with session description	
		192.168.0.10 192.168.0.10	192.168.1.3 192.168.1.3	SIP Status: 100 Trying SIP Status: 180 Ringing	
6 5.0	66542	192.168.1.1	192.168.1.3	ARP Who has 192.168.1.3? Tell 192.168.1.1	
		192.168.1.3 192.168.0.10	192.168.1.1 192.168.1.3	ARP 192.168.1.3 is at 00:50:da:c0:50:ff SIP/SD Status: 200 OK, with session description	
9 5.1	74745	192.168.1.3	192.168.0.10	SIP Request: ACK sip:192.168.0.10:5060	
		192.168.1.3	192.168.0.10	RTP Payload type=G5M 06.10, S5RC=7619304, Seq=18868, Time=O, Mark	
		192.168.0.10 192.168.1.3	192.168.1.3 192.168.0.10	RTP Payload type=GSM 06.10, SSRC=354435158, Seq=10101, Time=160 RTP Payload type=GSM 06.10, SSRC=7619304, Seq=18869, Time=160	
13 5.2	15588	192.168.0.10	192.168.1.3	RTP Payload type=GSM 06.10, SSRC=354435158, Seq=10102, Time=320	
		192.168.1.3 192.168.0.10	192.168.0.10 192.168.1.3	RTP Payload type=GSM 06.10, SSRC=7619304, Seq=18870, Time=320 RTP Payload type=GSM 06.10, SSRC=354435158, Seq=10103, Time=480	
16 5.2	51507	192.168.1.3	192.168.0.10	RTP Payload type=GSM 06.10, SSRC=7619304, Seq=18871, Time=480	
		192.168.0.10 192.168.1.3	192.168.1.3 192.168.0.10	RTP Payload type=65M 06.10, SSRC=354435158, Seq=10104, Time=640 RTP Payload type=65M 06.10, SSRC=7619304, Seq=18872, Time=640	
19 5.2	75934	192.168.0.10	192.168.1.3	RTP Payload type=GSM 06.10, SSRC=354435158, Seq=10105, Time=800	
		192.168.1.3 192.168.0.10	192.168.0.10	RTP Payload type=GSM 06.10, SSRC=7619304, Seq=18873, Time=800 RTP Payload type=GSM 06.10, SSRC=354435158, Seq=10106, Time=960	
		192.168.0.10	192.168.1.3 192.168.0.10	RTP Payload type=GSM 06.10, SSRC=354435158, Seq=10106, Time=960 RTP Payload type=GSM 06.10, SSRC=7619304, Seq=18874, Time=960	
		192.168.0.10	192.168.1.3	RTP Payload type=GSM 06.10, SSRC=354435158, Seq=10107, Time=1120	
		192.168.1.3 192.168.0.10	192.168.0.10 192.168.1.3	RTP Payload type=GSM 06.10, SSRC=7619304, Seq=18875, Time=1120 RTP Payload type=GSM 06.10, SSRC=354435158, Seq=10108, Time=1280	
		192.168.1.3	192.168.0.10	RTP Payload type=GSM 06.10, SSRC=7619304, Seq=18876, Time=1280	
0 80 0	06 04		c0 50 ff 08 06 00 c0 50 ff c0 a8 01 01		

Figure 42. Test 4: Packet Capture on eth0 of NAT 3 (Client C Calls Client A)

E.2.6. NAT 3 Eth1

The following is a snapshot of the packets captured on the second interface (eth1) of NAT 3 when Client C calls Client A.

-	h1 C Call A) - Ethereal		Amorphone 🖓 Tools 😰 🗧	
	apture <u>A</u> nalyze <u>S</u> tatistics			
	🏽 🗁 🖁 🗙	1 d 4	♦ ♥ 주 ½ = 3 Q, Q, Q, III # 10 X Ø	
er:		•	Expression glear Apply	
- Time	Source	Destination	Protocol Info	
	192.168.3.10	Broadcast	ARP Who has 192.168.3.1? Tell 192.168.3.10	
2 0.000202 3 0.000103		192.168.3.10 192.168.0.10	ARP 192.168.3.1 is at 00:0c:41:ef:af:be SIP/SD Request: INVITE sip:192.168.0.10, with session description	
4 0.070499	192.168.0.10	192.168.3.10	SIP Status: 100 Trying	
5 0.324894 6 5.069694		192.168.3.10 192.168.3.10	SIP Status: 180 Ringing ARP Who has 192.168.3.107 Tell 192.168.3.1	
7 5.069825 8 5.172230		192.168.3.1 192.168.3.10	ARP 192.168.3.10 is at 00:0d:56:38:24:0d SIP/SD Status: 200 0K, with session description	
9 5.176440		192.168.0.10	SIP Request: ACK sip:192.168.0.10:5060	
10 5.193226 11 5.198511		192.168.0.10 192.168.3.10	RTP Payload type=GSM 06.10, SSRC=7619304, Seq=18868, Time=0, Mark RTP Payload type=GSM 06.10, SSRC=354435158, Seq=10101, Time=160	
12 5.213241	192.168.3.10	192.168.0.10	RTP Payload type=GSM 06.10, SSRC=7619304, Seq=18869, Time=160	
13 5.217334 14 5.233169		192.168.3.10 192.168.0.10	RTP Payload type=GSM 06.10, SSRC=354435158, Seq=10102, Time=320 RTP Payload type=GSM 06.10, SSRC=7619304, Seq=18870, Time=320	
15 5.237296	192.168.0.10	192.168.3.10	RTP Payload type=GSM 06.10, SSRC=354435158, Seq=10103, Time=480	
16 5.253164 17 5.257302		192.168.0.10 192.168.3.10	RTP Payload type=GSM 06.10, SSRC=7619304, Seq=18871, Time=480 RTP Payload type=GSM 06.10, SSRC=351435158, Seq=10104, Time=640	
18 5.273161	192.168.3.10	192.168.0.10	RTP Payload type=G5M 06.10, S5RC=7619304, Seq=18872, Time=640	
19 5.277676 20 5.293260		192.168.3.10 192.168.0.10	RTP Payload type=GSM 06.10, SSRC=354435158, Seq=10105, Time=800 RTP Payload type=GSM 06.10, SSRC=7619304, Seq=18873, Time=800	
21 5.297364	192.168.0.10	192.168.3.10	RTP Payload type=GSM 06.10, SSRC=354435158, Seq=10106, Time=960	
22 5.313156 23 5.317392		192.168.0.10 192.168.3.10	RTP Payload type=GSM 06.10, SSRC=7619304, Seq=18874, Time=960 RTP Payload type=GSM 06.10, SSRC=354435158, Seq=10107, Time=1120	
24 5.333204	192.168.3.10	192.168.0.10	RTP Payload type=GSM 06.10, SSRC=7619304, Seq=18875, Time=1120	
25 5.337323 26 5.353169		192.168.3.10 192.168.0.10	RTP Payload type=GSM 06.10, SSRC=354435158, Seq=10108, Time=1280 RTP Payload type=GSM 06.10, SSRC=7619304, Seq=18876, Time=1280	



E.2.7. Analysis

The sequences of packet exchanges between Clients A and C are similar to that of Clients A and B described in the previous subsection. See Section E.1.7 for explanation.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX F. TEST 5: EXTENDED DOUBLE NAT VOIP WITH SIMULTANEOUS VOIP SESSIONS DEMONSTRATION USING SJPHONE

The instructions contained in this appendix describe how to setup and demonstrate a SIP-based VoIP communication using the network topology illustrated in the Figure 13. In this test scenario, two VoIP communication sessions will take place simultaneously, i.e. one between Clients A and C and the other between Clients B and D. Similar to the previous test, the DNAT rule is purposely taken out from NAT 1. Packet captures from all four clients are included at the end of this appendix along with their corresponding analysis.

A. Network Topology

Refer to Figure 13 and Figure 14 for the physical and logical network topology.

- B. Equipment Requirements
 - B.1. Clients A, B, C, and D
 - B.1.1. Windows XP Operating System
 - B.1.2. Sound card
 - B.1.3. SJPhone v.1.60
 - B.1.4. Ethereal
 - B.1.5. ZoneAlarm (for Clients A and B only)
 - B.2. NAT 1, NAT 2, NAT 3 and Router
 - B.2.1. Linux Operating System (Fedora Core 4)
 - B.2.2. netfilter and iptables
 - B.2.3. Ethereal
 - B.2.4. Two network cards (for NAT 1, NAT 2, and NAT 3)
 - B.2.5. Three network cards (for Router only)
 - B.3. Additional Equipment
 - B.3.1. Cross-over cables and a switch or hub to implement the network architecture illustrated in Figure 13.
 - B.3.2. Microphones as audio input devices for clients A, B, C and D

- C. Installation and Configuration
 - C.1. Client A

IP Address: 131.120.9.16

Subnet Mask: 255.255.255.0

Default Gateway: 131.120.9.15

C.2. Client B

IP Address: 131.120.9.17

Subnet Mask: 255.255.255.0

Default Gateway: 131.120.9.15

C.3. Clients C and D

IP Address: 192.168.3.11

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.3.1

- C.4. Router
 - C.4.1. Configure eth0 by editing /etc/sysconfig/network-scripts/ifcfg-eth0 to

include the following:

DEVICE=eth0

BOOTPROTO=NONE

IPADDR=192.168.100.27

NETMASK=255.255.255.0

GATEWAY=192.168.100.88

- C.4.2. Activate eth0 by running: ifup eth0
- C.4.3. Configure eth1 by editing /etc/sysconfig/network-scripts/ifcfg-eth1 to include the following:

DEVICE=eth1 BOOTPROTO=NONE IPADDR=192.168.202.1

NETMASK=255.255.255.0

C.4.4. Activate eth1 by running: ifup eth1 C.4.5. Configure eth2 by editing and saving /etc/sysconfig/networkscripts/ifcfg-eth2 to include the following:

> DEVICE=eth2 BOOTPROTO=NONE IPADDR=192.168.2.1 NETMASK=255.255.255.0

- C.4.6. Activate eth2 by running: ifup eth2
- C.4.7. Enable IP Forwarding by running:
 - echo 1 > /proc/sys/net/ipv4/ip_forward
- C.4.8. Flush any existing firewall and NAT rules by running: iptables -F iptables -t nat -F
- C.5. NAT 1
 - C.5.1. Configure eth0 by editing /etc/sysconfig/network-scripts/ifcfg-eth0 to include the following:

DEVICE=eth0 BOOTPROTO=NONE IPADDR=131.120.9.15 NETMASK=255.255.255.0

C.5.2. Activate eth0 by running:

ifup eth0

C.5.3. Configure eth1 by editing and saving /etc/sysconfig/network-

scripts/ifcfg-eth1 to include the following:

DEVICE=eth1

BOOTPROTO=NONE

IPADDR=192.168.100.88

NETMASK=255.255.255.0

- C.5.4. Activate eth1 by running: ifup eth1
- C.5.5. Configure static routes by running:

route add -net 192.168.202.0 netmask 255.255.255.0 gw 192.168.100.27 eth1 route add -net 192.168.2.0 netmask 255.255.255.0 gw 192.168.100.27 eth1

C.5.6. Enable IP Forwarding by running:

echo 1 > /proc/sys/net/ipv4/ip_forward

- C.5.7. Flush any existing firewall and NAT rules by running: iptables -F iptables -t nat -F
- C.5.8. Configure NAT rule by running:

iptables -t nat -A POSTROUTING -o eth0 -j SNAT --to 131.120.9.15

- C.6. NAT 2
 - C.6.1. Configure eth0 by editing and saving /etc/sysconfig/network-

scripts/ifcfg-eth0 to include the following:

DEVICE=eth0

BOOTPROTO=NONE

IPADDR=196.168.202.11

NETMASK=255.255.255.0

GATEWAY=198.168.202.1

- C.6.2. Activate eth0 by running: ifup eth0
- C.6.3. Configure eth1 by editing and saving /etc/sysconfig/network-

scripts/ifcfg-eth1 to include the following:

DEVICE=eth1

BOOTPROTO=NONE

IPADDR=192.168.3.1

NETMASK=255.255.255.0

- C.6.4. Activate eth1 by running: ifup eth1
- C.6.5. Enable IP Forwarding by running: echo 1 > /proc/sys/net/ipv4/ip_forward
- C.6.6. Flush any existing firewall and NAT rules by running: iptables -F iptables -t nat -F

C.6.7. Configure NAT rules by running:

iptables -t nat -A POSTROUTING -o eth0 -j SNAT --to 192.168.202.11 iptables -t nat -A PREROUTING -i eth0 -j DNAT --to 192.168.3.11

C.7. NAT 3

C.7.1. Configure eth0 by editing /etc/sysconfig/network-scripts/ifcfg-eth0 to include the following:

DEVICE=eth0 BOOTPROTO=NONE IPADDR=192.168.2.11 NETMASK=255.255.255.0 GATEWAY=192.168.2.1

- C.7.2. Activate eth0 by running: ifup eth0
- C.7.3. Configure eth1 by editing /etc/sysconfig/network-scripts/ifcfg-eth1 to include the following:

DEVICE=eth1 BOOTPROTO=NONE IPADDR=192.168.3.1 NETMASK=255.255.255.0

C.7.4. Activate eth1 by running:

ifup eth1

C.7.5. Enable IP Forwarding by running:

echo 1 > /proc/sys/net/ipv4/ip_forward

- C.7.6. Flush any existing firewall and NAT rules by running: iptables -F iptables -t nat -F
- C.7.7. Configure NAT rules by running:

iptables -t nat -A POSTROUTING -o eth0 -j SNAT --to 192.168.2.11 iptables -t nat -A PREROUTING -i eth0 -j DNAT --to 192.168.3.11

- C.8. SJPhone Installation and Configuration
 - C.8.1. Clients A, B, C and D
 - C.8.1.1. Download the Windows version of SJPhone v.1.60 from SJ Labs

- C.8.1.2. Install SJPhone v.1.60
- C.8.1.3. Launch SJPhone
- C.8.1.4. Right-click on SJPhone
- C.8.1.5. Go to Services
- C.8.1.6. Select PC-to-PC (SIP)
- C.9. Ethereal Installation and Configuration
 - C.9.1. Clients A, B, C and D
 - C.9.1.1. Download the Windows version of Ethereal v.0.10.12
 - C.9.1.2. Install Ethereal v.0.10.12 by following on-screen instructions
 - C.9.2. Router, NAT 2 and NAT 3
 - C.9.2.1.1. Install Ethereal if it is not already installed

C.9.2.1.1.1.	Go to the Desktop menu
C.9.2.1.1.2.	Go to System Settings
C.9.2.1.1.3.	Go to Add/Remove Applications
C.9.2.1.1.4.	Click on Details under System Tools
C.9.2.1.1.5.	Find and then check ethereal-gnome
C.9.2.1.1.6.	Click on Close
C.9.2.1.1.7.	Click on Update
C.9.2.1.1.8.	Put in the correct Fedora Core 4 CDs when

prompted

- C.10. ZoneAlarm Installation and Configuration
 - C.10.1. On clients A and B,
 - C.10.1.1. Download the free ZoneAlarm from Zone Labs
 - C.10.1.2. Install ZoneAlarm by following on-screen instructions
 - C.10.1.3. When ZoneAlarm is being run for the first time, it will ask the user to choose between Basic ZoneAlarm or trial version of ZoneAlarm Pro, select the trial version of ZoneAlarm
 - C.10.1.4. Answer on-screen questions
 - C.10.1.5. Click to use Trial Version
 - C.10.1.6. When asked to select a security level for the detected network, select Allow into Trusted Zone

- C.10.1.7. Allow all pop-ups for testing
- C.10.1.8. Configure firewall rule in ZoneAlarm:
 - C.10.1.8.1. Go to Firewall menu on the left panel
 - C.10.1.8.2. Click on the Expert tab
 - C.10.1.8.3. Click on Add
 - C.10.1.8.4. Type in a name for the firewall rule in the Name textbox
 - C.10.1.8.5. Under Action, select Block
 - C.10.1.8.6. Under Destination,

Select Modify
Select Add Location
Select IP Address
Type in a description in the Description textbox
Type 192.168.3.11 in the IP Address textbox
Click OK
Click OK
Click Apply

- D. Preparation and Testing
 - D.1. Adjust volume on both clients accordingly
 - D.2. Plug microphones into all clients
 - D.3. On Client A,
 - D.3.1. Launch Ethereal
 - D.3.2. Go to the Capture menu
 - D.3.3. Go to Interfaces
 - D.3.4. Click on Capture 131.120.9.16
 - D.4. On Client B,
 - D.4.1. Launch Ethereal
 - D.4.2. Go to the Capture menu
 - D.4.3. Go to Interfaces
 - D.4.4. Click on Capture 131.120.9.17
 - D.5. On Client C and Client D,
 - D.5.1. Launch Ethereal

D.5.2. Go to the Capture menu

D.5.3. Go to Interfaces

D.5.4. Click on Capture 192.168.3.11

D.6. On Router,

- D.6.1. Launch one instance of Ethereal
 - D.6.1.1. Go to the Capture menu
 - D.6.1.2. Go to Interfaces
 - D.6.1.3. Click on Capture Eth0
- D.6.2. Launch a second instance of Ethereal
 - D.6.2.1. Go to the Capture menu
 - D.6.2.2. Go to Interfaces
 - D.6.2.3. Click on Capture Eth1
- D.6.3. Launch a third instance of Ethereal
 - D.6.3.1. Go to the Capture menu
 - D.6.3.2. Go to Interfaces
 - D.6.3.3. Click on Capture Eth2
- D.7.On NAT 1, NAT 2 and NAT 3,
 - D.7.1. Launch one instance of Ethereal
 - D.7.1.1. Go to the Capture menu
 - D.7.1.2. Go to Interfaces
 - D.7.1.3. Click on Capture Eth0
 - D.7.2. Launch another instance of Ethereal
 - D.7.2.1. Go to the Capture menu
 - D.7.2.2. Go to Interfaces
 - D.7.2.3. Click on Capture Eth1
- D.8. On Client C,
 - D.8.1. Call A by dialing 131.120.9.16 in SJPhone

D.9. On Client A,

- D.9.1. Select Accept in the pop-up dialog box when SJPhone rings
- D.9.2. Clients A and C may engage in a VoIP conversation at this point.
- D.10. On Client D,

D.10.1.Call B by dialing 131.120.9.17 in SJPhone

D.11. On Client B,

D.11.1.Select Accept in the pop-up dialog box when SJPhone rings

- D.12. Clients B and D may engage in a VoIP conversation at this point.
- D.13. Click on the Hang-Up bottom on either SJPhone to terminate call when finished
- D.14. On all clients, NATs and Router,
 - D.14.1. Stop packet captures selecting Stop on Ethereal

E. Packet Captures

E.1. Client A

The following is a snapshot of the packets captured on Client A when it receives a call from Client C.

ier:		Connico One lipole	
. The Source	Destavation	Petrod Mr	6
35 261, 68864: 131, 120, 9, 17	131,120,9,255	Nana Inana yaki yi nu www.sochusicumoso Nana Nana quary NB WW.SJLABS.COM(00)	1 .
37 269,57021: 131, 120, 0,15	131,120,9,16	519/50 Requests 144/176 stp1131.120.9.16, with session description	<pre>} red</pre>
39 270.03361 131.120.9.16	131.120.9.255	ALEALE	
40 270.28189 131.120.9.16	131.120.9.15	SIP Status: 190 Ringing	
41 270,79623(131,120,9,16 42 271,54625(131,120,9,16	131.120.9.255 131.120.9.255	NENS Name guery HE MW, SILAES, COM(00) NENS Name guery HE MW, SILAES, COM(00)	
43 274,96868 131,120,9,15	131.120.9.16	ARP who has 131.120.9.167 Tell 131.120.9.15	
44 274,96870 131,120,9,16 45 277,50032(131,120,9,16	131.120.9.15	AMP 131.120.9.16 is at 00:0d:36:35:35:56 S1P/S0 Status: 200 0K, with session description	
46 277.10844 131.120.9.15	131.120.9.16	SIP Request: ACK sip:131.120.9.16:500	
48 277,55000 131,120,9,15	131.120.9.16	ATP Fayload type-GSM 06.10, 558C-83818212, Seg-29481, Time-320	black
	121 110 0 16	ave Authord Finances of the star-star aver a second at the star	- Viauk
50 277.57828.181.120.9.16 51 277.59010/131.120.9.15	131,120,9,18	RTF Payload type=SSM 06.10, ISRC=39818112, Sep=5688, Time=480 RTF Payload type=SSM 06.10, SSRC=83818212, Sep=29483, Time=640	,
52 277, 59309 131, 120, 9, 16	131,120,9,15	ATP Payload type+GSM 06.10, SSRC+39818112, Sec+3687, Time+640.	
53 277, 61007: 131, 120, 9, 15	131,120,9,16	RTP Payload type=594 06.10, 558C-81818212, Seg-29484, Time=800	1.19.27
35 277, 63019 131, 120, 9, 15	131,120,9,16	#TF Payload type-GSM 06.10, SSPC-83818212, Seq-29485, Time-990	l blue
56 277, 63308 131, 120, 0, 16	131.120.9.15	RTP Payload type=55H 06.10, 158C+39010112, Sep-5600, Time=960	
58 277.65312-131.120.9.16	131.120.9.15	RTP Payload type-GSM 06.10, SSRC-39818112, Seq-5690, Time-1120	
59 277,67001.131,120,9,15 60 277,67308,131,120,9,16	131.320.9.16 131.120.9.13	RTF Fuyload type=GSM 06.10, SSRC=83818212, Seg=29487, time=1280 RTF Fuyload type=GSM 06.10, SSRC=39818112, Seg=3691, Time=1280	
61 277, 69000 131, 120, 9, 15	131.120.9.16	RTP Payload type=GSM 06.10, SSRC-99818112, Seq=5691, Time=1200 RTP Payload type=GSM 06.10, SSRC-83818212, Seq=29488, Time=1440	
62 277.69307:131.120.9.16	131.120.9.15	RTP Payload type=20M 06.10, 35RC=39818112, Sep=5692, Time=1440	
63 277,70998 131,120,9,15 64 277,71309 131,120,9,16	131.120.9.16 131.120.9.15	RTP Payload type=SSM 00.10, SSRC=83818212, Seq=29489, Time=1600 RTP Payload type=SSM 06.10, SSRC=39818112, Seq=3693, Time=1600	
65 277,73001 131,120,9,15	131,120,9,16	RTP Payload type=SSM 06.10, 15RC+83818212, Sep=29490, Time=1760	- 91
Frame 37 (804 bytes on wire, 804	111 130 0.11	and and elements of the exercitalitation exercitation reaction	
User batagram Protocol, Src Port Session Intilation Protocol # Request-Line: Invite Sipila.3 # Hessame Neader = Hessame Neader = Bestion Description Protocol Session Description Protocol & Owner/Creator, Session Id Session Name (s): Siphone # Connection Information (c) # The Description, active t # Session Attribute (a): dir	<pre>ti 5000 (5080), Dst i20,9,16 SIP/2.0 o) version (v): 0 (o): - 3334628221 3) i: 1h [P4 192.168.3, ima 0): 0.0 ection:active id address (e): udit </pre>	4628121 IN 194 192.168.3.11	gree

Figure 44. Test 5: Packet Capture on Client A

E.2. Client C

The following is a snapshot of the packets captured on Client C when it calls



(m)			Epresson. Gee Boly	
	inarce	Destination	Potocil Me	
2 0.000079 1	wechate_181d71c5 icom_8919715b	WPcbaTe_18:d7:c5	AMP who has 192.168.3.17 Tell 192.168.3.11 AMP 192.168.3.1 is at 00:01:02:89:97:10	
	92.168.3.11 31.120.9.16	131,120.9.16 192,168,3.11	SIP/SD Request i InvITE afpil31,120.9.16, with session description SIP - Status: 100 Teylog	
	31.120.9.16	192.168.3.11 W#PcbaTe_18:d7:c5	SIP Status: 180 #inging	1
13 431114	Sectors Division	Loss Shidtalk	AND AND A REAL AND	orongo
1.020710 9 1.033348	0403161	107.168.3.11 131.170.9.16	SIF/10 Status: 200 km, with sesion description STP Represent ACK s10:131.120.9.16:5000	For a construction of a constructing a construction of a construction of a constr
AN ACCOUNTS A	911209.0144	414-440-9-10	ETF Fairbard Cyclescol Volton, Collectories, 2005; PEPP, 100490, No.3.	
11 3,944733 3 12 3,955154 3		131.120.9.16 131.120.9.16	RTF Payload type=GM 06.10, SSRC=B3818212, Seq=29480, Time=160 RTP Payload type=GM 06.10, SSRC=B3818212, Seq=29481, Time=320	
13 3.965615 3	92,165,1,11	131,120.9.10	ETP Favload type=G98 06.10, 1582=81818712, 5et=29482, 1fme=480	
14 3.967614 1 15 3.976093 1	92,168,1,11	192.168.3.11 131.120.9.16	RTP Payload type=GSM 06.10, ISBC=30818212, Seq=5606, Time=4800 RTP Payload type=GSM 06.10, SSMC=83818212, Seq=20483, Time=640	
16 3.977954 1	31,120,9,16	192.168.3.11	ATP Payload type=GSM 06.10, SSAC=30018112, Seq=3687, Time=640	
17 3,986472 1 18 3,988497 1	92,169,1,11	131.120.9.16 192.168.3.11	RTP Payload type=GSM 06.10, 558C=K3818212, 5eq=29484, Time=800 RTP Payload type=GSM 06.10, 558C=39818112, 5eq=5688, Time=800	
19 3,994925 1 20 3,998821 1	92.168.1.11	131.120.9.16	RTP Fayload type=GSM 06.10, SSRC=R3818212, Seg=29485, Time=960	
20 3.998821 1 21 4.007368 1	31.120.9.16	192.168.3.11 131.120.9.16	ATP Payload type=GSM 06.10, 15AC=19018112, 1eq=5689, Time=960 ATP Payload type=GSM 06.10, 15AC=83818212, 5eq=29486, Time=1120	
22 4.009257 1	31.120.9.16	197.168.3.11	RTP Payload type=GSM 06.10, SSRC=39818112, Sed=3690, Time=1120	
23 4,017760 3 24 4,019673 3		131.120.9.16 192.168.3.11	<pre>RTP Payload type=05M 06.10, 55RC=63818212, 5aq=29487, T1me=1280 RTP Payload type=05M 06.10, 55RC=39818112, 5aq=5681, T1me=1280</pre>	
25 4,028201 3	92.108.3.11	131,120,9,16	RTF Payload type-69M 06.10, 558C-83818212, 5eq-29488, Time-1440	
26 4.030113 1 27 4.038637 3		192.168.3.11 131.120.9.16	ATP Payload type-GSM 06.10, SSRC-99818122, Seq-5692, Time-1440 ATP Payload type-GSM 06.10, SSRC-93838212, Seq-29489, Time-1660	
28 4.040558 3	31,120.9,16	192.168.3.11	RTP Payload type+GM 06.10, SSRC+83818212, Seq=29489, Time+1600 RTP Payload type+GM 06.10, SSRC+39818112, Seq=5603, Time+1600	
29 4,049068 3 30 4,050935 3	92.165.1.11	131,120.9,16 192,168,3,11	<pre>KTP Payload type=094 06.10, SSAC=BJB18212, Seq=29490, Time=1760 KTP Payload type=094 06.10, SSAC=99818112, Seq=5664, Time=1760</pre>	
31 4.059500 3	92,168,3,11	131.120.9.16	ATP Payload type=GSM 06.10, SSRC=83818212, Seg=29491, Time=1920	
32 4.061388 1	31.120.9.16	192.168.3.11	ATP Payload type-GSM 06.10, SSAC-39818112, Seq-5695, Time-1920	
Internet Protoco User Datagram Pr Session Initiati a Status-Line: S Message Header Message Heade	 src: 131.120.9 otocol, src Port: on Protocol tP/2.0 200 0k ription Protocol sription Protocol tar, Session 10 (en (s): Sphone (s): Sphone (s): Sphone iption, active th 	16 (131.120.9.16), 1060 (1060), pst P 1 version (v): 0 c): - 3334607793 33	4603798 IN IP4 131.120.9.16	purple

Figure 45. Test 5: Packet Capture on Client C

E.3. NAT 2 Eth0

The following is a snapshot of the packets captured on the first interface (eth0) of NAT 2.

Edit	Yiew (<u>io</u> <u>c</u>	apture A	ynalyze	e Stati	istics	Help																				
2		01		Ъ	2	x	3	6	9	\$	¢ 🕅) 7	⊉			Ð	Θ	0	++		V	6	X	0			
		vade /	0007						_	1	Expressio								_								
	Time		Source		_	T	Destina	tion			Protocol	1													 	 	
1	0.0000	00	192.16				Broad	icast			ARP		has	192.1	i 8. 20	2.1?	Tell	192.	168.2	02.11							
	0.0001								02.11		ARP			202.1								Concession of					
4	0.0001	30 11	192.10	3.20 0.9.	2.11			L20.9 L68.2	.10 02.11		SIP/SU SIP			100 TI			.120.	9.10,	with	sess	TUN	lescr	perio				
5	0.3127	51	131.12	0.9.	16	1	192.1	168.2	02.11		SIP	Stat	us:	180 R	ingin	g		_									
	5.0342 5.0342								02.11		ARP			192.1													
	7.5308								02.1 02.11		ARP SIP/SE			202.11													
- 9	7.5382	01	192.16	8.20	2.11	1	131.1	L20.9	.16		SIP	Requ	est:	ACK :	ip:1	31.12	0.9.1	6:506	i0								
10	7.5401	85	192.16	8.20	2.11			L20.9			RTP			type=(
	7.5599							L20.9 L20.9			RTP	Payl	oad	type=(type=(SM U	6.10.	SSRC	=8381	8212.	Seq=	2948	, Tin	e=10 e=32	0			
13	7.5999	64	192.16	8.20	2.11	1	131.1	L20.9	.16		RTP	Payl	oad	type=(SSM 0	6.10,	SSRC	=8381	.8212,	Seq=	29482	, Tin	e=48	0			
	7.6035								02.11		RTP	Payl	oad	type=(SSM Ö	6.10,	SSRC	=3981	.8112,	Seq=	5686,	Time	=480				
	7.6200							L20.9	.16 02.11		RTP RTP			type=(type=(
17	7.6399	41	192.16	8.20	2.11			L20.9			RTP	Payl	oad	type=(SSM 0	6.10,	SSRC	=8381	8212,	Seq=	29484	, Tin	e=80	0			
18	7.6436	02	131.12	0.9.	16	1	192.1	168.2	02.11		RTP	Payl	oad	type=(ISM 0	6.10,	SSRC	=3981	.8112,	Seq=	5688,	Time	=800				
	7.6599							120.9			RTP	Payl	oad	type=(SM 0	6.10,	SSRC	=8381	8212,	Seq=	2948	, Tin	e=96	0			
	7.6634							L68.2 L20.9	02.11 .16		RTP	Pavl	Dau	type=(SSM ()	6.10,	SSRC	=5981 =8381	.8212	Seq=	29486	Tine.	=900 e=11	20			
22	7.6834	00	131.12	0.9.	16				02.11		RTP			type=(
23	7.6999	05	192.16	8.20	2.11	1	131.1	L20.9	.16		RTP	Payl	oad	type=(SSM 0	6.10,	SSRC	=8381	.8212,	Seq=	2948	, Tin	e=12	80			
	7.7033								02.11		RTP			type=(
	7.7233							L20.9	.16 02.11		RTP			type=(
27	7.7399	20	192.16	8.20	2.11	1	131.1	L20.9	.16		RTP	Payl	oad	type=(SSM 0	6.10,	SSRC	=8381	.8212,	Seq=	29489	, Tin	e=16	00			
	7.7433								02.11		RTP			type=(
	7.7599							L20.9 L68.2	.16 02.11		RTP RTP			type=(type=(
	7.7799							L20.9			RTP			type=(
32	7,7833	14	131.12	0.9.	16	1	192.1	.68.2	02.11		RTP			type=(
ddre Har Pro Har Opo Sen Sen Tar	net II Iss Resi dware 1 tocol 1 dware 5 tocol 5 tocol 5 tocol 7 get MAG get IP	olut type size size add add add	ion Pro : Ether : IP ((: 6 : 4 dress: 1 dress: 1 dress: 1	otoci net 0x080 0001] 192.1 00:0	ol (r (0x0) 00) .168.3 168.20 00:00	eques 001) 202.1 02.11 _00:0	st) L1 (C L (19 D0:00)0:e0)2.16)) (00	:29:6 3.202 :00:0	7:9e: .11)):00:	9c)						,										
0 f	f ff ff 8 00 00		00 01)g)g														
0 0	0 00 00	00 (00.00		18 C		9C 9		a0 Ca																		

Figure 46. Test 5: Packet Capture on eth0 of NAT 2

E.4. NAT 2 Eth1

The following is a snapshot of the packets captured on the second interface (eth1) of NAT 2.

	Capture Analyze Statistics		
	💓 🖻 🖁 🗙	@ 🗄 🖣 🖗	🔶 🏵 🛧 🛂 🗐 📴 I OL Q. Q. 🔍 📅 I 🎬 🕅 🎛 🔆 I 💆
r		•	Expression Clear Apply
. Time	Source	Destination	Protocol Info
	WwPcbaTe_18:d7:c5 3com_89:97:5b	Broadcast WwPcbaTe_18:d7:c5	ARP who has 192.168.3.1? Tell 192.168.3.11 ARP 192.168.3.1 is at 00:01:02:89:97:5b
	192.168.3.11	131.120.9.16	SIP/SD Request: INVITE sip:131.120.9.16, with session description
4 0.036591	131.120.9.16	192.168.3.11	SIP Status: 100 Trying
	131.120.9.16	192.168.3.11	SIP Status: 180 Ringing
	3com_89:97:5b WwPcbaTe_18:d7:c5	WWPcbaTe_18:d7:c5 3com 89:97:5b	ARP Who has 192.168.3.11? Tell 192.168.3.1 ARP 192.168.3.11 is at 00:0f:1f:18:d7:c5
	131.120.9.16	192.168.3.11	SIP/SD Status: 200 OK, with session description
9 7.538688	192.168.3.11	131.120.9.16	SIP Request: ACK sip:131.120.9.16:5060
10 7.540704		131.120.9.16	RTP Payload type=GSM 06.10, SSRC=83818212, Seq=29479, Time=0, Mark
11 7.560455 12 7.580429	192.168.3.11	131.120.9.16 131.120.9.16	RTP Payload type=GSM 06.10, SSRC=83818212, Seq=29480, Time=160 RTP Payload type=GSM 06.10, SSRC=83818212, Seq=29481, Time=320
13 7.600478	192.168.3.11	131.120.9.16	RTP Payload type=GSM 06.10, SSRC=03010212, Seq=29482, Time=480
14 7.604215	131.120.9.16	192.168.3.11	RTP Payload type=GSM 06.10, SSRC=39818112, Seq=5686, Time=480
15 7.620559	192.168.3.11	131.120.9.16	RTP Payload type=GSM 06.10, SSRC=83818212, Seq=29483, Time=640
16 7.624024 17 7.640452	131.120.9.16	192.168.3.11 131.120.9.16	RTP Payload type=GSM 06.10, SSRC=39818112, Seq=5687, Time=640 RTP Payload type=GSM 06.10, SSRC=83818212, Seq=29484, Time=800
	131.120.9.16	192.168.3.11	RTP Payload type=GSM 06.10, SSRC=65616212, Seq=29464, Time=600 RTP Payload type=GSM 06.10, SSRC=39818112, Seq=5688, Time=800
19 7.660483	192.168.3.11	131.120.9.16	RTP Payload type=GSM 06.10, SSRC=83818212, Seq=29485, Time=960
20 7.664027	131.120.9.16	192.168.3.11	RTP Payload type=GSM 06.10, SSRC=39818112, Seq=5689, Time=960
21 7.680503 22 7.684027	192.168.3.11 131.120.9.16	131.120.9.16	RTP Payload type=GSM 06.10, SSRC=83818212, Seq=29486, Time=1120 RTP Payload type=GSM 06.10, SSRC=39818112, Seq=5690, Time=1120
23 7.700416	192.168.3.11	192.168.3.11 131.120.9.16	RTP Payload type=usM 00.10, 55xC=39010112, 5eq=3090, Time=1120 RTP Payload type=GSM 06.10, SSRC=83818212, Seq=29487, Time=1280
24 7.703990	131.120.9.16	192.168.3.11	RTP Payload type=GSM 06.10, SSRC=39818112, Seq=5691, Time=1280
25 7.720429		131.120.9.16	RTP Payload type=GSM 06.10, SSRC=83818212, Seq=29488, Time=1440
26 7.724001 27 7.740431	131.120.9.16	192.168.3.11 131.120.9.16	RTP Payload type=GSM 06.10, SSRC=39818112, Seq=5692, Time=1440
28 7.740431		192.168.3.11	RTP Payload type=GSM 06.10, SSRC=83818212, Seq=29489, Time=1600 RTP Payload type=GSM 06.10, SSRC=39818112, Seq=5693, Time=1600
29 7.760421		131.120.9.16	RTP Payload type=GSM 06.10, SSRC=83818212, Seq=29490, Time=1760
30 7.763907		192.168.3.11	RTP Payload type=GSM 06.10, SSRC=39818112, Seq=5694, Time=1760
31 7.780415 32 7.783942		131.120.9.16	RTP Payload type=GSM 06.10, SSRC=83818212, Seq=29491, Time=1920
52 7.783942	131,120,9,10	192.168.3.11	RTP Payload type=GSM 06.10, SSRC=39818112, Seq=5695, Time=1920
Hardware type Protocol type Hardware size Protocol size Opcode: reque Sender MAC ad	2: 4 2st (0x0001) ddress: WwPcbaTe_18 dress: 192.168.3.11 ddress: 00:00:00_00) :d7:c5 (00:0f:1f:18 (192.168.3.11) :00:00 (00:00:00:00	
	mess: 192.108.3.1	(192.168.3.1)	

Figure 47. Test 5: Packet Capture on eth1 of NAT 2

E.5. Router Eth0

The following is a snapshot of the packets captured on the first interface (eth0) of Router.

Image: Bit Unit Source Control Image: Source Source Description Description 1 Source Description Description Description Description 2 Source Description Description Description Description Description 3 Source Description Description Description Description<	Router Et																										
Image: Source: Decknome Decknome Decknome Decknome 2 Source: Decknome Source: Decknome Source: Decknome Source: Decknome 2 Source: Decknome Source: Decknome Source: Decknome Source: Decknome 2 Source: Decknome Source: Decknome Source: Decknome Source: Decknome 3 Source: Decknome Source: Decknome Source: Decknome Source: Decknome 4 Source: Decknome Source: Decknome Source: Decknome Source: Decknome 5 Source: Decknome Source: Decknome Source: Decknome Source: Decknome 5 Source: Decknome Source: Decknome Source: Decknome Source: Decknome 5 Source: Decknome Source: Decknome Source: Decknome Source: Decknome 5 Source: Decknome Source: Decknome Source: Decknome Source: Decknome 5 Source: Decknome Source: Decknome Source: Decknome Source: Decknome 7 Source: Decknome Source: Decknome Sourcechone Source: Decknone <th>e <u>E</u>dit ⊻ Nresri</th> <th>jew <u>G</u>o Far Art</th> <th>Capture</th> <th></th> <th></th> <th></th> <th></th> <th></th> <th>4</th> <th></th> <th>_</th> <th></th> <th></th> <th></th> <th>0</th> <th>0</th> <th>0</th> <th></th> <th></th> <th></th> <th></th> <th>St 0</th> <th>879</th> <th></th> <th></th> <th></th> <th></th>	e <u>E</u> dit ⊻ Nresri	jew <u>G</u> o Far Art	Capture						4		_				0	0	0					St 0	879				
The Surv Destration Product 160 10 0000001 100.4569,00281 000041 100.4569,00281 000041 100.4569,00281 10 0000041 100.4569,00281 101.1569,0021 101.156		91 (N		6	X	Q		9	(Ŧ	1		¥	(÷)	Q		**	Ŭ.	Ě	Ð	X	Ø				
0.00000 42.8458/00.841 62.870 42.84 82.08.820 62.83<	er: 🗌								•	Expression	<u>C</u> le	ar App	oly														
2 0.0004 192.148.20.1 192.148.20.1 197.1 197.1 40 192.118.20.1 1 5 at 00.110.238.9746 4 0.05790 131.120.9.1 192.148.20.1 197.5 status: 100 Trying 5 0.0014 192.148.20.1 192.148.20.1 197.5 status: 100 Trying 7 0.0014 192.148.20.1 197.1 197.148.20.1 197.1 197.148.20.1 197.1197.147.1497.1497.1497.1497.1497.14																											
3 0.0004 192.165.02.11 33.120.9.5 STAUS: 10 Minging 4 0.03799 31.220.9.5 (9).8.302.11 SP STAUS: 10 Minging 5 0.31269 131.120.9.15 192.168.02.11 SP STAUS: 10 Minging 7 5.02481 02.156.02.11 192.168.02.11 SP STAUS: 10 Minging 7 5.02481 02.156.02.11 192.168.02.11 SP STAUS: 10 Minging 7 5.02481 02.150.9.12 192.169.02.11 SP STAUS: 10 Minging 7 5.02481 02.150.9.12 11 SP STAUS: 10 Minging 11 7.55994 192.156.02.11 SP STAUS: 10 Minging 12 7.55994 192.156.02.11 SP STAUS: 10 Minging 13 7.6000 192.156.02.11 SP STAUS: 10 Minging 14 7.6000 192.156.02.11 SP STAUS: 10 Minging 15 7.6000 192.156.02.11 SP STAUS: 10 Minging 15 7.7127 SP STAUS: 10 Minging 15 7.7127 SP STAUS: 10 Minging 15 7.7127 SP STAUS: 10 Minging											192.1	nas 1 168.2	92.16 02.1	8.202 is at	.12	Tell 1:02	192. :89:9	168.2 7:6f	02,1	1							
5 0.32629 131.120.9.16 192.136.2021 192.053.2021 1 54 P	3 0.	000194	192.1	.68.20	2.11	131	120.	9.16		SIP/SD	Requi	est:	INVIT	E sip	0:131.	120.	9.16,	with	ses	sion	desc	ripti	on				
6 5 04401 192.108.02.1 192.108.02.1 192.108.02.1 7 5 04402 192.108.02.1 192.108.02.11 192.108.02.11 7 5 05402 192.108.02.11 131.100.01.6 197.100.01 17 7 55402 192.108.02.11 131.100.01.6 197.100.01 17 7 55402 192.108.02.11 131.100.01.6 197.100.01 17 7 55402 192.108.02.11 131.100.01.6 197.100.01 17 7 55403 192.108.02.11 131.100.01.6 197.100.01 18 7 55004 192.108.02.11 131.100.01.6 197.100.01 18 7 55004 192.108.02.11 131.100.01.6 197.100.01 18 7 55004 192.108.02.11 131.100.01.6 197.100.01 19 7 55004 192.108.02.11 131.100.01.6 197.100.01 19 7 55004 192.108.02.11 131.100.01.6 197.100.01 19 7 55004 192.108.02.11 131.100.01.6 197.100.01 17 7 55094 192.108.02.11 131.100.01.6 197.100.01 17 7 55094 192.108.02.11 131.100.01.6 197.100.01 17 7 55094 192.108.02.11 131.100.01.6 197.100.01 17 7 55094 192.108.02.11 131.100.01.6 197.100.01 17 7 55094 192.108.02.11 131.100.01.6 197.100.01	4 U. 5 O.	312629	131.1	20.9.	10 16						Stat	us: 1 us: 1	.00 Ir .80 Ri	naina	1												
8 7.30799 13.120.9.16 192.468.20.11 331/20.9.16 ST P sequent: xx: split13.120.9.16.1000 10 7.50276 192.168.20.211 331.20.9.16 RTP seyload type=300.61.0, SSX=5381321, Seq-2449, Time=100 17.755984 192.168.20.211 331.20.9.16 RTP seyload type=300.61.0, SSX=5381321, Seq-2449, Time=100 17.755994 192.168.20.211 331.20.9.16 RTP seyload type=300.61.0, SSX=5381321, Seq-2449, Time=400 15.760003 192.168.20.11 131.20.9.16 RTP seyload type=300.61.0, SSX=5381321, Seq-2449, Time=400 15.760003 192.168.20.11 131.20.9.16 RTP seyload type=300.61.0, SSX=5381321, Seq-2448, Time=400 15.760003 192.168.20.11 131.20.9.16 RTP seyload type=300.61.0, SSX=5381321, Seq-2448, Time=400 15.760003 192.168.20.11 RTP seyload type=300.61.0, SSX=5381321, Seq-2448, Time=400 RT 15.760003 192.168.20.11 RTP seyload type=300.61.0, SSX=5381321, Seq-2448, Time=400 RT 15.760004 192.168.20.11 RTP seyload type=300.61.0, SSX=5381321, Seq-2448, Time=400 RT 15.760004 192.168.20.11 131.20.9.16 RTP seyload type=300.61.0, SSX=5381321, Seq-2448, Time=400 RT 15.760005 192.168.20.11 131.20.9.16 RTP seyload type=	65.	034161	192.1	.68,20	2.1	192	.168.3	202.11		ARP	who I	has 1	.92.16	8.202	2.11?					1							
9 7.58277 192.188.02.11 131.120.9.16 STP Regulat YAC signal 1.120.9.16:500 17.5926 192.188.02.11 131.120.9.16 RTP Reylad types30 6.10, 55X-63838121, sep-2449, The-40 17.59294 192.188.02.11 131.120.9.16 RTP Reylad types30 6.10, 55X-63838121, sep-2449, The-40 17.69394 192.188.02.11 131.120.9.16 RTP Reylad types30 6.10, 55X-63838121, sep-2449, The-40 17.63394 132.109.16 192.188.02.11 131.120.9.16 RTP Reylad types30 6.10, 55X-63838121, sep-2449, The-40 17.76394 132.109.16 192.188.02.11 131.120.9.16 RTP Reylad types30 6.10, 55X-63838121, sep-2449, The-40 17.76394 131.120.9.16 192.168.02.11 171 RTP Reylad types30 6.10, 55X-63838121, sep-2449, The-40 17.76394 131.120.9.16 192.168.02.11 RTP Reylad types30 6.10, 55X-63838121, sep-2449, The-40 17.76394 131.120.9.16 192.168.02.11 RTP Reylad types30 6.10, 55X-63838121, sep-2449, The-40 17.76394 131.120.9.16 192.168.02.11 RTP Reylad types30 6.10, 55X-63838121, sep-2449, The-40 17.76394 131.120.9.16 192.168.02.11 RTP Reylad types30 6.10, 55X-63838121, sep-2449, The-40 17.63041 192.168.02.11 131.120.9.16 192.168.02.11 RTP Reylad types30 6.10, 55X-63838121, sep-2449, The-10 17.76394 131.120.9.16 192.168.02.11 RTP Reylad types30 6.10, 55X-63838121, sep-2449, The-10 17.779907 192.168.02.11 131.120.9.16 192.168.02.11 RTP Reylad types30 6.10, 55X-63838121, sep-549, The-110 17.779917 192.168.02.11 131.120.9.16 192.168.02.11 RTP Reylad types30 6.10, 55X-63838121, sep-549, The-120 17.779917 192.168.02.11 131.120.9.16 192.168.02.11 RTP Reylad types30 6.10, 55X-63838121, sep-549, The-120 17.779917 192.168.02.11 131.120.9.16 RTP Reylad types30 6.10, 55X-63838121, sep-549, The-120 17.779917 192.168.02.11 131.120.9.16 RTP Reylad types30 6.10, 55X-63838121, sep-549, The-120 17.779917 192.168.02.11 131.120.9.16 RTP Reylad types30 6.10, 55X-63838121, sep-549, The-120 17.779917 192.168.02.11 131.120.9.16 RTP Reylad types30 6.10, 55X-63838121, sep-549, The-120 17.779971 192.168.02.11 131.120.9.16 RTP Reylad types30 6.10, 55X-63838121, sep-549, The-120 17.779971 192.168.02.																											
11 7.59994 192.188.02.11 31.120.9.16 NTP Psylad type=30 60.10, SSR=838121, Sep=2490, The=160 12 7.69021 92.188.02.11 31.120.9.16 NTP Psylad type=30 60.10, SSR=838121, Sep=2493, The=260 13 7.60021 92.188.02.11 31.120.9.16 NTP Psylad type=30 60.10, SSR=838121, Sep=2493, The=40 14 7.60350 31.120.9.16 120.9.16 NTP Psylad type=30 60.10, SSR=838121, Sep=2493, The=40 15 7.60021 92.188.02.11 31.120.9.16 NTP Psylad type=30 60.10, SSR=838121, Sep=2493, The=40 16 7.63344 31.120.9.16 120.9.16 NTP Psylad type=30 60.10, SSR=838121, Sep=2493, The=40 17 7.639995 192.188.02.11 31.120.9.16 NTP Psylad type=30 60.10, SSR=838121, Sep=2493, The=40 17 7.639995 192.188.02.11 31.120.9.16 NTP Psylad type=30 60.10, SSR=838121, Sep=2493, The=40 17 7.63997 192.188.02.11 31.120.9.16 NTP Psylad type=30 60.10, SSR=838121, Sep=2493, The=40 17 7.63997 192.188.02.11 31.120.9.16 NTP Psylad type=30 60.10, SSR=838121, Sep=5493, The=40 17 7.63997 192.188.02.11 31.120.9.16 NTP Psylad type=30 60.10, SSR=838121, Sep=5493, The=40 17 7.63907 192.188.02.11 31.120.9.16 NTP Psylad type=30 60.10, SSR=838121, Sep=5493, The=100 17 7.63907 192.188.02.11 31.120.9.16 NTP Psylad type=30 60.10, SSR=838121, Sep=5493, The=120 12 7.63834 13.120.9.16 132.120.9.16 NTP Psylad type=30 60.10, SSR=838121, Sep=5493, The=120 12 7.739957 192.188.02.11 31.120.9.16 NTP Psylad type=30 60.10, SSR=838121, Sep=5493, The=120 12 7.739957 192.188.02.11 31.120.9.16 NTP Psylad type=30 60.10, SSR=9381321, Sep=5493, The=120 12 7.739957 192.188.02.11 31.120.9.16 NTP Psylad type=30 60.10, SSR=9381321, Sep=5493, The=120 12 7.739957 192.188.02.11 31.120.9.16 NTP Psylad type=30 60.10, SSR=9381321, Sep=5493, The=120 12 7.739957 192.188.02.11 31.120.9.16 NTP Psylad type=30 60.10, SSR=9381321, Sep=5493, The=140 12 7.739957 192.188.02.11 31.120.9.16 NTP Psylad type=30 60.10, SSR=9381321, Sep=5493, The=140 12 7.73957 192.188.02.11 31.120.9.16 NTP Psylad type=30 60.10, SSR=9381321, Sep=5493, The=140 13 7.73957 192.188.02.11 31.120.9.16 NTP Psylad type=30 60.10, SSR=9381321, Sep=5493, The=150 13 7.739	97.	538277	192.1	68,20	2.11	131	.120.	9.16		SIP	Requi	est:	ACK S	ip:13	31.120	.9.1	6:506	0									
12 7.59972 192.168.202.11 131.102.9.16 PT Psylad type=S9 06.10, SSR-388.22, Seq-248.1, Thme=30 13 7.60031 92.168.202.11 131.102.9.16 PT Psylad type=S9 06.10, SSR-388.22, Seq-248.1, Thme=40 15 7.62032 192.168.202.11 131.102.9.16 PT Psylad type=S9 06.10, SSR-388.22, Seq-248.1, Thme=40 17 7.63995 192.168.202.11 131.102.9.16 PT Psylad type=S9 06.10, SSR-388.22, Seq-368.7, Thme=40 17 7.63995 192.168.202.11 131.102.9.16 PT Psylad type=S9 06.10, SSR-388.22, Seq-368.7, Thme=40 17 7.63995 192.168.202.11 131.102.9.16 PT Psylad type=S9 06.10, SSR-388.22, Seq-368.7, Thme=40 17 7.63995 192.168.202.11 131.102.9.16 PT Psylad type=S9 06.10, SSR-388.22, Seq-368.7, Thme=40 17 7.63995 192.168.202.11 131.102.9.16 PT Psylad type=S9 06.10, SSR-388.22, Seq-368.7, Thme=40 17 7.63995 192.168.202.11 131.102.9.16 PT Psylad type=S9 06.10, SSR-388.22, Seq-368.7, Thme=40 17 7.63997 192.168.202.11 131.102.9.16 PT Psylad type=S9 06.10, SSR-388.22, Seq-368.7, Thme=40 17 7.63997 192.168.202.11 131.102.9.16 PT Psylad type=S9 06.10, SSR-388.22, Seq-368.7, Thme=120 17 7.73997 192.168.202.11 131.102.9.16 PT Psylad type=S9 06.10, SSR-388.22, Seq-368.7, Thme=120 17 7.73997 192.168.202.11 131.102.9.16 PT Psylad type=S9 06.10, SSR-388.22, Seq-368.7, Thme=120 17 7.73977 131.102.9.16 192.168.202.11 131.102.9.16 PT Psylad type=S9 06.10, SSR-388.22, Seq-368.7, Thme=120 17 7.73977 132.120.9.16 192.168.202.11 131.102.9.16 PT Psylad type=S9 06.10, SSR-388.22, Seq-368.7, Thme=120 17 7.73977 132.120.9.16 192.168.202.11 PT Psylad type=S9 06.10, SSR-388.22, Seq-368.7, Thme=140 17 7.73977 132.120.9.16 192.168.202.11 PT Psylad type=S9 06.10, SSR-388.22, Seq-368.7, Thme=140 17 7.73977 132.120.9.16 P32.16 P32.01 PT Psylad type=S9 06.10, SSR-388.22, Seq-368.7, Thme=140 17 7.73977 132.120.9.16 P32.16 P32.01 P32.02	10 7.	540236	192.1	68.20	2.11																			k			
137.600018 192.168.202.11 31.120.9.16 PT Psylad type-S9 06.10, SSR-981812, Seq-9481, Time-400 147.60350 191.048.002.11 31.120.9.16 PT Psylad type-S9 06.10, SSR-981812, Seq-9481, Time-400 147.6334 131.120.9.16 192.168.002.11 PT Psylad type-S9 06.10, SSR-981812, Seq-9481, Time-400 147.63540 131.20.9.16 192.168.002.11 PT Psylad type-S9 06.10, SSR-981812, Seq-9481, Time-400 147.63540 131.20.9.16 192.168.002.11 PT Psylad type-S9 06.10, SSR-981812, Seq-9481, Time-400 147.63560 131.20.9.16 192.168.002.11 PT Psylad type-S9 06.10, SSR-981812, Seq-9481, Time-400 147.63560 131.20.9.16 192.168.002.11 PT Psylad type-S9 06.10, SSR-981812, Seq-9481, Time-400 147.63570 131.20.9.16 192.168.002.11 PT Psylad type-S9 06.10, SSR-981812, Seq-9481, Time-400 147.63570 131.120.9.16 192.168.002.11 PT Psylad type-S9 06.10, SSR-981812, Seq-9481, Time-400 147.63570 131.120.9.16 192.168.002.11 PT Psylad type-S9 06.10, SSR-981812, Seq-9481, Time-400 147.70320 131.120.9.16 192.168.001.11 PT Psylad type-S9 06.10, SSR-981812, Seq-9481, Time-400 147.70320 131.120.9.16 192.168.001.11 PT Psylad type-S9 06.10, SSR-981812, Seq-969, Time-120 147.70320 131.120.9.16 192.168.001.11 PT Psylad type-S9 06.10, SSR-981812, Seq-969, Time-120 147.70320 131.120.9.16 P30.11 PT Psylad type-S9 06.10, SSR-981812, Seq-969, Time-120 147.70397 192.168.001.11 31.100.9.16 PT Psylad type-S9 06.10, SSR-981812, Seq-969, Time-120 147.70397 192.168.001.11 31.100.9.16 PT Psylad type-S9 06.10, SSR-981812, Seq-969, Time-140 147.70397 192.168.001.11 31.100.9.16 PT Psylad type-S9 06.10, SSR-981812, Seq-969, Time-140 147.70397 192.168.001.11 31.100.9.16 PT Psylad type-S9 06.10, SSR-981812, Seq-969, Time-140 147.7397 192.168.001.11 31.100.9.16 PT Psylad type-S9 06.10, SSR-981812, Seq-969, Time-140 147.7397 192.168.001.11 (92.168.001.11 PT Psylad type-S9 06.10, SSR-981812, Seq-969, Time-140 147.7397 192.168.001.11 (92.168.001.11 PT Psylad type-S9 06.10, SSR-981812, Seq-969, Time-140 147.7397 192.168.001.11 (92.168.001.11 PT Psylad type-S9 06.10, SSR-981812, Seq-969, Time-140 153.7.7																											
137 F62002 192.168.202.11 131.120.9.16 PT Psylad type-S90 06.10, SSR-938182.2, Seq-9484, Thme-60 147 F63999 192.168.202.11 131.120.9.16 PT Psylad type-S90 06.10, SSR-938182.2, Seq-959, Thme-60 147 F63099 192.168.202.11 131.120.9.16 PT Psylad type-S90 06.10, SSR-938182.2, Seq-959, Thme-60 147 F6300 131.20.9.16 120.18.202.11 PT Psylad type-S90 06.10, SSR-938182.2, Seq-959, Thme-60 147 F6300 192.168.202.11 131.120.9.16 PT Psylad type-S90 06.10, SSR-938182.2, Seq-959, Thme-60 147 F6300 192.168.202.11 131.120.9.16 PT Psylad type-S90 06.10, SSR-938182.2, Seq-9498, Thme-10 147 F63004 192.168.202.11 131.120.9.16 PT Psylad type-S90 06.10, SSR-938182.2, Seq-9498, Thme-1120 147 F63004 192.168.202.11 131.120.9.16 PT Psylad type-S90 06.10, SSR-938182.2, Seq-9498, Thme-120 157 F63004 192.168.202.11 131.120.9.16 PT Psylad type-S90 06.10, SSR-938182.2, Seq-9498, Thme-120 157 F7397 192.168.202.11 131.120.9.16 PT Psylad type-S90 06.10, SSR-938182.2, Seq-9498, Thme-120 157 F7397 192.168.202.11 131.120.9.16 PT Psylad type-S90 06.10, SSR-938182.2, Seq-9498, Thme-140 157 F7397 192.168.202.11 131.120.9.16 PT Psylad type-S90 06.10, SSR-938182.2, Seq-9498, Thme-140 157 F7397 192.168.202.11 131.120.9.16 PT Psylad type-S90 06.10, SSR-938182.2, Seq-9498, Thme-140 157 F7397 192.168.202.11 131.120.9.16 PT Psylad type-S90 06.10, SSR-938182.2, Seq-9498, Thme-140 157 F7397 192.168.202.11 131.120.9.16 PT Psylad type-S90 06.10, SSR-938182.2, Seq-9498, Thme-140 157 F7397 192.168.202.11 131.120.9.16 PT Psylad type-S90 06.10, SSR-938182.2, Seq-959, Thme-140 157 F7397 192.168.202.11 131.100.9.16 PT Psylad type-S90 06.10, SSR-938182.2, Seq-959, Thme-140 157 F7397 192.168.202.11 (02.168.202.11 PT Psylad type-S90 06.10, SSR-938182.2, Seq-959, Thme-140 157 F7397 192.168.202.11 (02.168.202.11 PT Psylad type-S90 06.10, SSR-938182.2, Seq-959, Thme-140 157 F7397 192.168.202.11 (02.168.202.11 PT Psylad type-S90 06.10, SSR-938182.2, Seq-959, Thme-140 157 F7397 192.168.202.11 (02.168.202.11 PT Psylad type-S90 06.10, SSR-938182.2, Seq-959, T	13 7.	600018	192.1	68.20	2.11	131	.120.	9.16		RTP	Payli	oad t	ype=G	SM OF	i.10,	SSRC	=8381	8212,	Seq	=2948	2, Т	ime=4	80				
16 7.63344 131.120.9.16 192.168.202.11 RTP Payload type-GS 06.10, SRC-3981812, Sep-568, Time-400 18 7.643560 131.120.9.16 192.168.202.11 RTP Payload type-GS 06.10, SRC-3981812, Sep-368, Time-800 17 7.63007 131.120.9.16 192.168.202.11 RTP Payload type-GS 06.10, SRC-3981812, Sep-368, Time-800 17 7.63007 131.120.9.16 192.168.202.11 RTP Payload type-GS 06.10, SRC-3981812, Sep-568, Time-800 17 7.63007 131.120.9.16 192.168.202.11 RTP Payload type-GS 06.10, SRC-3981812, Sep-369, Time-400 17 7.63007 131.120.9.16 192.168.202.11 RTP Payload type-GS 06.10, SRC-38818212, Sep-369, Time-400 17 7.63007 131.120.9.16 192.168.202.11 RTP Payload type-GS 06.10, SRC-38818212, Sep-569, Time-400 17 7.73907 192.168.202.11 131.120.9.16 RTP Payload type-GS 06.10, SRC-38818212, Sep-569, Time-120 17 7.73907 192.168.202.11 131.120.9.16 RTP Payload type-GS 06.10, SRC-38818212, Sep-569, Time-120 17 7.73907 192.168.202.11 131.120.9.16 RTP Payload type-GS 06.10, SRC-38818212, Sep-2948, Time-140 17 7.73907 192.168.202.11 131.120.9.16 RTP Payload type-GS 06.10, SRC-38818212, Sep-2948, Time-140 17 7.73907 192.168.202.11 131.120.9.16 RTP Payload type-GS 06.10, SRC-38818212, Sep-2948, Time-140 17 7.73907 192.168.202.11 131.120.9.16 RTP Payload type-GS 06.10, SRC-38818212, Sep-2948, Time-140 17 7.73907 192.168.202.11 131.120.9.16 RTP Payload type-GS 06.10, SRC-38818212, Sep-2949, Time-160 17 7.73907 192.168.202.11 131.120.9.16 RTP Payload type-GS 06.10, SRC-38818212, Sep-2949, Time-160 17 7.73907 192.168.202.11 RTP Payload type-GS 06.10, SRC-38818212, Sep-2949, Time-160 17 7.73927 131.120.9.16 192.168.202.11 RTP Payload type-GS 06.10, SRC-3881812, Sep-5095, Time-160 17 7.73927 131.120.9.16 192.168.202.11 RTP Payload type-GS 06.10, SRC-3881812, Sep-5095, Time-160 17 7.73927 131.120.9.16 192.168.202.11 RTP Payload type-GS 06.10, SRC-3881812, Sep-5095, Time-160 17 7.73927 131.120.9.16 192.168.202.11 RTP Payload type-GS 06.10, SRC-3881812, Sep-5095, Time-170 18 7.0682.00 SA 05 0.00 0.00 0.00 0.00 0.00 0.00 0.00																											
17 7.63995 192.468.202.11 131.120.9.16 RTP Payload type-GS 06.10, SSRC-83818212, Sep-588, Time-900 19 7.660018 192.168.202.11 131.120.9.16 RTP Payload type-GS 06.10, SSRC-83818212, Sep-588, Time-900 17 7.66002 S102.068.202.11 131.120.9.16 RTP Payload type-GS 06.10, SSRC-83818212, Sep-2948, Time-900 17 7.66002 S104.82.02.11 131.120.9.16 RTP Payload type-GS 06.10, SSRC-83818212, Sep-2948, Time-900 17 7.66002 S104.82.02.11 131.120.9.16 RTP Payload type-GS 06.10, SSRC-83818212, Sep-2948, Time-120 17 7.07320 131.120.9.16 192.168.202.11 RTP Payload type-GS 06.10, SSRC-83818212, Sep-2948, Time-120 17 7.07320 131.120.9.16 192.168.202.11 RTP Payload type-GS 06.10, SSRC-83818212, Sep-2948, Time-120 17 7.07320 131.120.9.16 192.168.202.11 RTP Payload type-GS 06.10, SSRC-83818212, Sep-2948, Time-120 17 7.07320 131.120.9.16 192.168.202.11 RTP Payload type-GS 06.10, SSRC-83818212, Sep-5949, Time-120 17 7.7397 192.168.202.11 131.120.9.16 RTP Payload type-GS 06.10, SSRC-83818212, Sep-5949, Time-140 17 7.73967 192.168.202.11 131.120.9.16 RTP Payload type-GS 06.10, SSRC-83818212, Sep-5949, Time-1600 18 7.73327 131.120.9.16 192.168.202.11 RTP Payload type-GS 06.10, SSRC-83818212, Sep-5949, Time-1600 19 7.78324 131.120.9.16 RTP Payload type-GS 06.10, SSRC-83818212, Sep-5949, Time-1600 17 7.78327 132.168.202.11 131.120.9.16 RTP Payload type-GS 06.10, SSRC-83818212, Sep-5949, Time-1600 17 7.78327 132.168.202.11 131.120.9.16 RTP Payload type-GS 06.10, SSRC-83818212, Sep-5949, Time-1600 17 7.78327 132.109.16 192.168.202.11 RTP Payload type-GS 06.10, SSRC-83818212, Sep-5949, Time-1600 17 7.78327 132.120.9.16 192.168.202.11 RTP Payload type-GS 06.10, SSRC-83818212, Sep-5949, Time-1600 17 7.78327 132.120.9.16 192.168.202.11 RTP Payload type-GS 06.10, SSRC-83818212, Sep-5949, Time-1600 17 7.78277 132.108.202.11 (92.168.202.11 RTP Payload type-GS 06.10, SSRC-83818212, Sep-5949, Time-160 17 7.78277 192.168.202.11 (92.168.202.11 RTP Payload type-GS 06.10, SSRC-83818121, Sep-5963, Time-160 10 00 00 00 00 00 00 00 00 00 00 0	16 7.	623344	131.1	20.9.	16																						
197.660018 192.168.202.11 311.120.9.16 RTP Payload type-GSM 06.10, SSRC-9381.8121, Seq-5689, Time-960 207.663367 131.120.9.16 192.168.202.11 RTP Payload type-GSM 06.10, SSRC-9381.8121, Seq-5689, Time-100 277.630369 131.120.9.16 192.168.202.11 RTP Payload type-GSM 06.10, SSRC-9381.8122, Seq-59487, Time-120 277.0320 131.120.9.16 192.168.202.11 RTP Payload type-GSM 06.10, SSRC-9381.8122, Seq-5488, Time-120 277.73320 131.120.9.16 192.168.202.11 RTP Payload type-GSM 06.10, SSRC-9381.8112, Seq-5692, Time-120 277.73320 131.120.9.16 192.168.202.11 RTP Payload type-GSM 06.10, SSRC-9381.8112, Seq-5692, Time-140 277.73967 192.168.202.11 311.120.9.16 RTP Payload type-GSM 06.10, SSRC-9381.8112, Seq-5692, Time-140 277.73967 192.168.202.11 311.120.9.16 RTP Payload type-GSM 06.10, SSRC-9381.8121, Seq-5692, Time-140 277.73967 192.168.202.11 311.20.9.16 RTP Payload type-GSM 06.10, SSRC-9381.8121, Seq-5693, Time-140 277.73967 192.168.202.11 311.20.9.16 RTP Payload type-GSM 06.10, SSRC-9381.8121, Seq-5693, Time-140 277.7397 192.168.202.11 311.20.9.16 RTP Payload type-GSM 06.10, SSRC-9381.8121, Seq-5694, Time-140 277.7397 192.168.202.11 311.20.9.16 RTP Payload type-GSM 06.10, SSRC-9381.8121, Seq-5694, Time-140 277.7397 192.168.202.11 311.20.9.16 RTP Payload type-GSM 06.10, SSRC-9381.8121, Seq-5694, Time-140 277.7397 192.168.202.11 311.20.9.16 RTP Payload type-GSM 06.10, SSRC-9381.8121, Seq-5694, Time-140 277.7397 192.168.202.11 031.120.9.16 RTP Payload type-GSM 06.10, SSRC-9381.8121, Seq-5694, Time-120 277.8272 131.120.9.16 192.168.202.11 RTP Payload type-GSM 06.10, SSRC-9381.8121, Seq-5694, Time-120 277.8272 131.120.9.16 192.168.202.11 RTP Payload type-GSM 06.10, SSRC-9381.8121, Seq-5694, Time-120 278.74987, Time-120 (0000) 279.74987, Time-120.01 (000.00.00.000) 279.7597, Time-120.01 (000.00.000.000) 279.7597, Time-120.01 (000.000.0000) 279.7597, Time-120.01 (000.00000) 279.7597, Time-120, Tim	17 7.	639995	192.1	.68.20	2.11	131	120.	9.16		RTP	Payli	oad t	ype=G	SM Of	i.10,	SSRC	=8381	8212,	Seq	=2948	4, T	ime=8	300				
20 7.63367 131.120.9.16 192.168.00.11 RTP Payload type=GS9 06.10, SSGC-39381312, Seq-3660, Time=460 21 7.63004 192.168.00.11 131.120.9.16 RTP Payload type=GS9 06.10, SSRC-39381312, Seq-3660, Time=120 23 7.63993 131.20.9.16 192.168.00.11 RTP Payload type=GS9 06.10, SSRC-33813212, Seq-3660, Time=120 23 7.79967 192.168.00.11 131.120.9.16 RTP Payload type=GS9 06.10, SSRC-3381312, Seq-569, Time=120 23 7.79967 192.168.00.11 131.120.9.16 RTP Payload type=GS9 06.10, SSRC-3381312, Seq-569, Time=120 23 7.73967 192.168.00.11 131.120.9.16 RTP Payload type=GS9 06.10, SSRC-3381312, Seq-569, Time=120 23 7.73967 192.168.00.11 131.120.9.16 RTP Payload type=GS9 06.10, SSRC-3381312, Seq-569, Time=140 27 7.73967 192.168.00.11 131.120.9.16 RTP Payload type=GS9 06.10, SSRC-3381312, Seq-569, Time=140 28 7.73349 131.120.9.16 192.168.00.11 RTP Payload type=GS9 06.10, SSRC-3381312, Seq-569, Time=140 27 7.73967 192.168.00.11 131.120.9.16 RTP Payload type=GS9 06.10, SSRC-3381312, Seq-29490, Time=140 27 7.73977 192.168.00.11 131.120.9.16 RTP Payload type=GS9 06.10, SSRC-3381312, Seq-29490, Time=140 27 7.73977 192.168.00.11 RTP Payload type=GS9 06.10, SSRC-3381312, Seq-29490, Time=140 27 7.73977 192.168.00.211 131.120.9.16 RTP Payload type=GS9 06.10, SSRC-3381312, Seq-29490, Time=1400 27 7.73977 192.168.00.211 031.120.9.16 RTP Payload type=GS9 06.10, SSRC-3381312, Seq-29490, Time=1400 27 7.73977 192.168.00.211 (01:0:02):67:96:9c), bst: Broadcast (ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:	18 7.	643560	131.1	20.9.	16																						
21 7.60042 192.168.202.11 131.120.9.16 mTP Payload type-GSM 06.10, SSRC-89813212, Seq-2986, Time-1120 22 7.603956 131.120.9.16 192.168.202.11 mTP Payload type-GSM 06.10, SSRC-89813212, Seq-2986, Time-120 23 7.70397 131.120.9.16 192.168.202.11 mTP Payload type-GSM 06.10, SSRC-89813212, Seq-2986, Time-120 27 7.73967 120.168.202.11 131.120.9.16 mTP Payload type-GSM 06.10, SSRC-89813212, Seq-2986, Time-140 27 7.73967 120.198.202.11 131.120.9.16 mTP Payload type-GSM 06.10, SSRC-89813212, Seq-2986, Time-140 27 7.73967 120.198.202.11 131.120.9.16 mTP Payload type-GSM 06.10, SSRC-89813212, Seq-2986, Time-1600 28 7.74349 131.120.9.16 192.168.202.11 mTP Payload type-GSM 06.10, SSRC-89813212, Seq-2986, Time-1600 28 7.74349 131.120.9.16 192.168.202.11 mTP Payload type-GSM 06.10, SSRC-89813212, Seq-2989, Time-1700 20 7.79957 192.168.202.11 131.120.9.16 mTP Payload type-GSM 06.10, SSRC-89813212, Seq-2989, Time-1700 31 7.779957 192.168.202.11 131.120.9.16 mTP Payload type-GSM 06.10, SSRC-89813212, Seq-2989, Time-1700 32 7.78327 131.120.9.16 192.168.202.11 mTP Payload type-GSM 06.10, SSRC-89813212, Seq-2989, Time-1920 32 7.78327 131.120.9.16 192.168.202.11 mTP Payload type-GSM 06.10, SSRC-89813212, Seq-2989, Time-1920 32 7.78327 131.120.9.16 192.168.202.11 mTP Payload type-GSM 06.10, SSRC-89813212, Seq-2989, Time-1920 32 7.78327 131.120.9.16 192.168.202.11 mTP Payload type-GSM 06.10, SSRC-89813212, Seq-2989, Time-1920 32 7.78327 131.120.9.16 192.168.202.11 mTP Payload type-GSM 06.10, SSRC-89813212, Seq-2989, Time-1920 32 7.78327 131.120.9.16 192.168.202.11 mTP Payload type-GSM 06.10, SSRC-89813212, Seq-2989, Time-1920 32 7.78327 131.120.9.16 sol 0.000.000 sol 0.0000.0000 40 sol 0.00000 sol 0.00000000000000000000000000000000000	20 7.	663367	131.1	20.9.	16																						
237.09958 192.186.202.11 131.120.9.16 PT Payload type-GSM 06.10, SSRC-83813212, Seq-2687, fime-1280 247.70967 192.186.202.11 131.120.9.16 PT Payload type-GSM 06.10, SSRC-83813212, Seq-2687, fime-1280 277.73967 192.186.202.11 131.120.9.16 PT Payload type-GSM 06.10, SSRC-83813212, Seq-2688, fime-1440 277.73967 192.186.202.11 131.120.9.16 PT Payload type-GSM 06.10, SSRC-83813212, Seq-2688, fime-1600 287.74349 131.120.9.16 192.168.202.11 PT Payload type-GSM 06.10, SSRC-83813212, Seq-2689, fime-1600 287.74349 131.120.9.16 192.168.202.11 PT Payload type-GSM 06.10, SSRC-83813212, Seq-2689, fime-1600 287.74349 131.120.9.16 192.168.202.11 PT Payload type-GSM 06.10, SSRC-83813212, Seq-2689, fime-1700 297.759956 192.168.202.11 131.120.9.16 PT Payload type-GSM 06.10, SSRC-83813212, Seq-2689, fime-1700 277.75977 192.168.202.11 131.120.9.16 PT Payload type-GSM 06.10, SSRC-83813212, Seq-2689, fime-1900 277.87272 131.120.9.16 192.168.202.11 PT Payload type-GSM 06.10, SSRC-83813212, Seq-2689, fime-1900 27.763272 131.120.9.16 192.168.202.11 PT Payload type-GSM 06.10, SSRC-8381321, Seq-2689, fime-1900 27.763272 131.120.9.16 192.168.202.11 PT Payload type-GSM 06.10, SSRC-8381321, Seq-569, fime-1920 27.78377 131.100.9.16 192.168.202.11 PT Payload type-GSM 06.10, SSRC-8381321, Seq-569, fime-1920 27.78377 131.100.9.16 192.168.202.11 PT Payload type-GSM 06.10, SSRC-8381321, Seq-569, fime-1920 27.78377 131.100.9.16 192.168.202.11 (00:e0:29:67:9e:9C), Dst: Broadcast (ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:	21 7.	680042	192.1	68.20	2.11	131	.120.	9.16			Payli	oad t	ype=G	SM Of	i.10,	SSRC	=8381	8212,	Seq	=2948	6, T	ime=1	120				
24 7.73320 131.120.9.16 192.168.202.11 RTP Payload type=GSM 06.10, SSRC=3981312, Seq-5963, Time=1240 25 7.73327 192.168.202.11 131.120.9.16 RTP Payload type=GSM 06.10, SSRC=3981312, Seq-5493, Time=1440 27 7.733967 192.168.202.11 131.120.9.16 RTP Payload type=GSM 06.10, SSRC=3981312, Seq-5493, Time=1600 28 7.73349 131.120.9.16 192.168.202.11 RTP Payload type=GSM 06.10, SSRC=3981312, Seq-5493, Time=1600 28 7.73349 131.120.9.16 192.168.202.11 RTP Payload type=GSM 06.10, SSRC=3981312, Seq-5493, Time=1600 28 7.73352 192.168.202.11 131.120.9.16 RTP Payload type=GSM 06.10, SSRC=3981312, Seq-5493, Time=1600 27 7.739327 192.168.202.11 131.120.9.16 RTP Payload type=GSM 06.10, SSRC=3981322, Seq-24490, Time=1760 30 7.763249 131.120.9.16 192.168.202.11 RTP Payload type=GSM 06.10, SSRC=3981322, Seq-5494, Time=1760 32 7.783272 131.120.9.16 192.168.202.11 RTP Payload type=GSM 06.10, SSRC=3981312, Seq-5494, Time=1760 32 7.783272 131.120.9.16 192.168.202.11 RTP Payload type=GSM 06.10, SSRC=3981312, Seq-5494, Time=1200 32 7.783272 131.120.9.16 192.168.202.11 RTP Payload type=GSM 06.10, SSRC=3981312, Seq-5494, Time=1200 32 7.783272 131.120.9.16 192.168.202.11 RTP Payload type=GSM 06.10, SSRC=3981312, Seq-5494, Time=1200 32 7.783272 131.120.9.16 192.168.202.11 RTP Payload type=GSM 06.10, SSRC=3981312, Seq-5494, Time=1200 32 7.783272 131.120.9.16 192.168.202.11 (00:e0:29:67:9e:9C), Sstc = Broadcast (ff:ff:ff:ff:ff:ff:ff:ff:ff: ddress Resolution Protocol (request) Hardware type: IP (0x0000) Protocol type: IP (0x0001) Sender MAC address: 192.168.202.11 (00:e0:29:67:9e:9C) Sender FD address: 192.168.202.11 (192.168.202.1) Target MAC address: 192.168.202.1 (192.168.202.1) 0 ff 0 e0 29 67 9e 9c 08 06 00 01)g 0 d8 00 00 60 40 00 00 e0 23 67 9e 9c c0 8 6 00 001	22 7.	683369	131.1	20.9.	16																						
25 7.79967 192.168.202.11 31.120.9.16 RTP Payload type-GSM 06.10, SSRC-83818212, Sep-28488, Time-1440 26 7.733967 192.168.202.11 31.120.9.16 RTP Payload type-GSM 06.10, SSRC-83818212, Sep-28489, Time-1600 28 7.43349 131.120.9.16 192.168.202.11 RTP Payload type-GSM 06.10, SSRC-83818212, Sep-593, Time-1600 29 7.799567 192.168.202.11 131.120.9.16 RTP Payload type-GSM 06.10, SSRC-83818212, Sep-593, Time-1600 30 7.763249 131.120.9.16 192.168.202.11 RTP Payload type-GSM 06.10, SSRC-83818212, Sep-593, Time-1600 31 7.779357 192.168.202.11 131.120.9.16 RTP Payload type-GSM 06.10, SSRC-83818212, Sep-593, Time-1920 32 7.78927 131.120.9.16 192.168.202.11 RTP Payload type-GSM 06.10, SSRC-83818212, Sep-593, Time-1920 32 7.78927 131.120.9.16 192.168.202.11 RTP Payload type-GSM 06.10, SSRC-83818212, Sep-593, Time-1920 32 7.78927 131.120.9.16 192.168.202.11 RTP Payload type-GSM 06.10, SSRC-83818212, Sep-593, Time-1920 32 7.78927 131.120.9.16 192.168.202.11 RTP Payload type-GSM 06.10, SSRC-83818212, Sep-593, Time-1920 32 7.78927 131.120.9.16 192.168.202.11 RTP Payload type-GSM 06.10, SSRC-83818212, Sep-593, Time-1920 32 7.78927 131.120.9.16 192.168.202.11 RTP Payload type-GSM 06.10, SSRC-83818212, Sep-593, Time-1920 32 7.78927 131.120.9.16 192.168.202.11 RTP Payload type-GSM 06.10, SSRC-83818212, Sep-593, Time-1920 32 7.78927 131.120.9.16 192.168.202.11 RTP Payload type-GSM 06.10, SSRC-83818212, Sep-593, Time-1920 32 7.78927 131.120.9.16 192.168.202.11 RTP Payload type-GSM 06.10, SSRC-83818212, Sep-593, Time-1920 32 7.78927 131.120.9.16 192.168.202.11 RTP Payload type-GSM 06.10, SSRC-83818212, Sep-593, Time-1920 32 7.78927 131.120.9.16 192.168.202.11 RTP Payload type-GSM 06.10, SSRC-83818212, Sep-593, Time-1920 32 7.78927 192.168.202.11 (00:e0:29:67:9e:9c), Ost: Broadcast (ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:																											
27 7.739067 192.168.202.11 131.120.9.16 RFP Payload type-GSM 06.10, SSRC-35818212, Seq-5093, Time-1600 28 7.73956 192.168.202.11 131.120.9.16 HFP Payload type-GSM 06.10, SSRC-35818212, Seq-5093, Time-1700 30 7.763249 131.120.9.16 192.168.202.11 HFP Payload type-GSM 06.10, SSRC-35818212, Seq-5094, Time-1700 31 7.779957 192.168.202.11 131.20.9.16 HFP Payload type-GSM 06.10, SSRC-35818212, Seq-5695, Time-1700 32 7.783272 131.120.9.16 192.168.202.11 HFP Payload type-GSM 06.10, SSRC-35818212, Seq-5695, Time-1920 32 7.783272 131.120.9.16 192.168.202.11 RFP Payload type-GSM 06.10, SSRC-35818212, Seq-5695, Time-1920 32 7.783272 131.120.9.16 192.168.202.11 RFP Payload type-GSM 06.10, SSRC-35818212, Seq-5695, Time-1920 32 7.783272 131.120.9.16 192.168.202.11 RFP Payload type-GSM 06.10, SSRC-35818212, Seq-5695, Time-1920 32 7.783272 131.120.9.16 192.168.202.11 RFP Payload type-GSM 06.10, SSRC-35818212, Seq-5695, Time-1920 32 7.783272 131.120.9.16 192.168.202.11 RFP Payload type-GSM 06.10, SSRC-35818212, Seq-5695, Time-1920 32 7.783272 131.120.9.16 192.168.202.11 RFP Payload type-GSM 06.10, SSRC-35818212, Seq-5695, Time-1920 32 7.783272 131.120.9.16 192.168.202.11 RFP Payload type-GSM 06.10, SSRC-35818212, Seq-5695, Time-1920 32 7.783272 131.120.9.16 192.168.202.11 RFP Payload type-GSM 06.10, SSRC-35818212, Seq-5695, Time-1920 32 7.783272 131.120.9.16 192.168.202.11 SFC 39818112, Seq-5695, Time-1920 32 7.783272 131.120.9.16 192.168.202.11 SFC 3981812, Seq-5695, Time-1920 32 7.783272 131.120.9.16 192.168.202.11 SFC 3981812, Seq-5695, Time-1920 32 7.783274 State Sta	25 7.	719967	192.1	.68.20	2.11	131	.120.	9.16		RTP	Payl	oad t	ype=G	SM Of	i.10,	SSRC	=8381	8212,	Seq	=2948	8, T	ime=1	.440				
28 7.73349 131.120.9.16 192.168.202.11 RTP Payload type-GSM 06.10, SSRC-39818121, Seq-593, Time-1600 29 7.73956 192.168.202.11 131.120.9.16 RTP Payload type-GSM 06.10, SSRC-3981812, Seq-29490, Time-1760 31 7.77957 192.168.202.11 131.120.9.16 RTP Payload type-GSM 06.10, SSRC-3981812, Seq-264964, Time-1760 32 7.783272 131.120.9.16 192.168.202.11 RTP Payload type-GSM 06.10, SSRC-3981812, Seq-5695, Time-1920 Tame 1 (60 bytes on whre, 60 bytes captured) thermer II, Scri 192.168.202.11 (00:01.29:67:9e:9c), Dst: Broadcast (ff:ff:ff:ff:ff:ff) ddress Resolution Protocol (request) Hardware type: Ethernet (0x0001) Protocol type: IP (0x0800) Hardware type: ID (0x0800) Hardware type: 100:00:00:00:00:00:00:00:00:00 Sender MLC address: 192.168.202.11 (00:e0:29:67:9e:9c) Sender MLC address: 192.168.202.11 (192.168.202.11) Target IP address: 192.168.202.11 (192.168.202.1) Target IP address: 192.168.202.11 (192.168.202.1)	26 7.	723327	131.1	20.9.	16 2 11						Payli	oad t	ype=G	SM DE SM DE	5.10, 5.10	SSRC	=3981 -8381	8112, 8717	Seq	=5692 -2049	, Til 9 т	ne=14 im⊳_1	40				
29 7.759956 192.168.202.11 131.120.9.16 RTP Payload type-GSM 06.10, SSRC-39818212, Seq.2490, Time-1760 30 7.763249 131.120.9.16 192.168.202.11 131.120.9.16 RTP Payload type-GSM 06.10, SSRC-39818212, Seq.2490, Time-1760 31 7.779957 192.168.202.11 131.120.9.16 192.168.202.11 RTP Payload type-GSM 06.10, SSRC-39818212, Seq.2490, Time-1760 32 7.783272 131.120.9.16 192.168.202.11 RTP Payload type-GSM 06.10, SSRC-39818212, Seq.2490, Time-1760 start resolution Protocol (request) RTP Payload type-GSM 06.10, SSRC-39818112, Seq.2490, Time-1920 rame 1 (60 bytes on wire, 60 bytes captured) therwers thermet (twool) protocol type: Sthermet (twool) Protocol type: IP (0x0800) Hardware size: 6 Protocol size: 4 opcode: request (twool) Sender MAC address: 192.168.202.11 (00:e0:29:67:9e:9c) Sender MAC address: 192.168.202.11 (192.168.202.1) sender MAC address: 192.168.202.1 (192.168.202.1) arget IP address: 192.168.202.1 (192.168.202.1)	28 7.	743349	131.1	20.9.	16																						
31 7.779937 192.168.202.11 131.120.9.16 RTP Payload týpe=GSM 06.10, SSRC=33818212, Seq=29491, Time=1920 32 7.783272 151.120.9.16 192.168.202.11 RTP Payload týpe=GSM 06.10, SSRC=33818212, Seq=26953, Time=1920 rame 1 (60 bytes on wire, 60 bytes captured) tthernet II, Src: 192.168.202.11 (00:e0:29:67:9e:9c), Dst: Broadcast (ff:ff:ff:ff:ff:ff) ddress Resolution Protocol (request) Hardware type: Ethernet (0x0001) Protocol type: IP (0x0800) Hardware type: Stenes: 192.168.202.11 (00:e0:29:67:9e:9c) Sender Request (0x0001) Sender MAC address: 192.168.202.11 (00:e0:29:67:9e:9c) Sender Paddress: 192.168.202.11 (192.168.202.11) Target NAC address: 192.168.202.11 (192.168.202.1) Target IP address: 192.168.202.11 (192.168.202.1) Target IP address: 192.168.202.11 (192.168.202.1) 0 ff fff ff ff ff ff ff 00 e0 29 67 9e 9c 08 06 00 01	29 7.	759956	192.1	.68.20	2.11						Payli	oad t	:ype=G	SM 06	i.10,	SSRC	=8381	8212,	Seq	=2949	0, T	ime=1	.760				
32 7.783272 131.120.9.16 192.168.202.11 RTP Payload type=GSM 06.10, SSRC=39618112, Seq=5695, Time=1920 rrame 1 (60 bytes on wire, 60 bytes captured) thermet II, Src: 192.168.202.11 (00:e0:29:67:9e:9C), Dst: Broadcast (ff:ff:ff:ff:ff:ff) widness Resolution Protocol (request) Hardware Size: 6 Protocol type: IP (0x0800) Hardware size: 6 Protocol size: 4 Opcode: request (0x0001) Sender MAC address: 192.168.202.11 (00:e0:29:67:9e:9c) Sender MAC address: 192.168.202.11 (192.168.202.11) Target IP address: 192.168.202.11 (192.168.202.11) Target IP address: 192.168.202.1 (192.168.202.1) Target IP address: 192.168.202.1 (192.168.202.1)											Payl	oad t nad t	:ype=G :vne=G	SM DE	5.10, 5.10.	SSRC	=3981 =8381	8112, 8212.	Seq Seq	=3094 =7949	, I1 1. т	me=⊥≀ ime=1	920				
<pre>thernet II, Src: 192.168.202.11 (00:e0:29:67:9e:9c), Dst: Broadcast (ff:ff:ff:ff:ff:ff:ff) ddress Resolution Protocol (request) Hardware stype: IP (0x0800) Hardware size: 6 Protocol size: 4 Opcode: request (0x0001) Sender MAC address: 192.168.202.11 (00:e0:29:67:9e:9c) Sender IP address: 192.168.202.11 (192.168.202.11) Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00) Target IP address: 192.168.202.1 (192.168.202.1)</pre>	32.7.	783272	131.1	20.9.	16																						
.0 08 00 06 04 00 01 00 e0 29 67 9e 9c c0 a8 ca 0b	Address Hardw Proto Hardw Proto Opcod Sende Sende Targe	Resolu are typ col typ are siz col siz col siz e: requ r MAC a r IP ad t MAC a	tion P e: Eth e: IP e: 6 e: 4 est (0 ddress ddress: ddress:	rotoci ernet (0x08) x0001] : 192. 192. : 00:0	ol (rec (0x000 00) 168.20 168.202 00:00_0	uest) 1) 2.11 .11 (0:00:	(00:e(192.16 00 (00):29:6 58.202):00:0	7:9e: .11) 0:00:	9c)	Broad	cast	(ff:f	ť:ff	ff:fi	:ff)											
10 08 00 06 04 00 01 00 e0 29 67 9e 9c c0 a8 ca 0b	Sender Targe	r IP ad t MAC a	dress: ddress	192.1 : 00:0	L68.202 D0:00_0	.11 (0:00:	192.10 00 (00	58.202):00:0	.11) 0:00:																		
	LO 08 (20 00 (00 06 04 00 00 01	4 00 0: 0 00 0!	L 00 e D c0 a	20 29 18 ca	67 9e 01 00	90 00	a8 ca	a Ob))ğ													 	 	
: "K:/Router/Router Eth 1 (3 NAT)" 1058 KE P: 10507 D: 10507 M: 0					_	_			_			_		_	_	_	_			_		_			 		

Figure 48. Test 5: Packet Capture on eth0 of Router

E.6. Router Eth1

The following is a snapshot of the packets captured on the second interface (eth1) of Router.

Edit <u>V</u> iew	<u>G</u> o g										_	_											
			6	X	¢		9		0 7	1			•		. 🔍	**		¥		5			
								 Express 	ion ⊆	jear <u>A</u>	yply												
Time		Source			Destina	ation		Protoco	l Info														
1 0.00	0000	192.16	8.202.	11	Broa	dcast	07 11	ARP					02.1?				02.11						
2 0.00					192.	168.2 120.9	16	ARP					at 00:				cace	ion d	escrip	tion			
4 0.03	5790	131.12	0.9.16	5		168.2		SIP			100					wren	5055	inon a		c rom			
5 0.31	2629	131.12	0.9.16	j	192.3	168.2	02.11	SIP	Sta	tus:	180 1	Ringi	ng										
6 5.034	161	192.16	8.202.	1		168.2		ARP					02.11?										
7 5.034	1293	192.16	8.202.	11		168.2		ARP					at OC										
8 7.53 9 7.53	1799 2777	107 16	0.9.10) 11		168.2 120.9		SIP/S	SD Sta				10n se 131.12				on						
10 7.54	0236	192.16	8.202.	11		120.9		RTP	Pav	load	type:	GSM I	06.10.	SSRC	=8381	8212.	Seo-	29479	Time	=0, Mar	k		
11 7.55	9984	192.16	8.202.	11		120.9		RTP											Time				
12 7.57	9972	192.16	8.202.	11	131.1	120.9	.16	RTP	Pay	load	type:	GSM I	06.10,	SSRO	=8381	8212,	Seq=	29481	Time	=320			
13 7.60	0018	192.10	8.202.	11	131.	120.9	.16	RTP	Pay	load	type	=GSM	06.10,	SSRO	=8381	8212,	Seq=	29482	Time	=480			
14 7.60						168.2		RTP	Pay	load	type	GSM I	06.10,	SSRO	=3981	8112,	Seq=	5686,	Time=	480			
15 7.62						120.9		RTP	Pay	load	type:	GSM I	J6.10,	55K0	-2001	8212,	Seq=	29483	Time	=040			
16 7.62 17 7.63						168.2 120.9		RTP RTP	Pay	load	type	-GSM	16.10	SSPO	=8381	8212	Seq=	20484	Time= Time	=800			
18 7.64						168.2		RTP	Pay	load	type:	GSM I	06.10.	SSRO	=3981	8112.	Seg=	5688.	Time=	B00			
19 7.66						120.9		RTP	Pay	load	type	GSM I	06.10,	SSRO	=8381	8212,	Seq=	29485	Time	=960			
20 7.66	3367	131.12	0.9.16	i		168.2		RTP	Pay	load	type:	=GSM I	06.10,	SSRO	=3981	8112,	Seq=	5689,	Time=	960			
21 7.68						120.9		RTP											Time				
22 7.68						168.2		RTP											Time=				
23 7.69						120.9		RTP											Time				
24 7.70 25 7.71						168.2 120.9		RTP RTP											Time= Time				
						168.2		RTP											Time=				
26 7.72	9967	192.16	8.202.	11		120.9		RTP	Pay	load	type	GSM I	06.10,	SSRO	=8381	8212,	Seq=	29489	Time	=1600			
28 7.74	3349	131.12	0.9.16	i	192.1	168.2	02.11	RTP	Pay	load	type	GSM (06.10,	SSRO	=3981	8112,	Seq=	5693,	Time=	1600			
29 7.75	9956	192.16	8.202.	11		120.9		RTP											Time				
30 7.76	5249 2057	131.12	0.9.10	11		168.2		RTP RTP											Time=				
31 7.77						120.9 168.2		RTP											Time Time=				
33 7.79						120.9		RTP											, Time				
34 7.80						168.2		RTP											Time=				
35 7.81	9955	192.16	8.202.	11	131.3	120.9	.16	RTP	Pay	load	type	=GSM_I	06.10,	SSRO	=8381	8212,	Seq=	29493	Time	=2240			
36 7.82	3293	131.12	0.9.16	j		168.2		RTP	Pay	load	type:	-GSM	06.10,	SSRO	=3981	8112,	Seq=	5697,	Time=	2240			
37 7.84						120.9		RTP											Time				
38 7.84 39 7.85						168.2 120.9		RTP RTP											Time= Time				
40 7.86						168.2		RTP											Time=				
ame 1 (6 Hernet 1 Hdress Re	II, Sr	c: 192	.168.2	02.11	(00:e			c), Dst	: Broa	dcas	t (ff	:ff:f	f:ff:f	f:ff])								
08 00	06 04	00 01	00 e0	29.6	57 9e 9	9c c0	06 00 a8 ca 00 00	Ob)ğ												 	

Figure 49. Test 5: Packet Capture on eth1 of Router

E.7. Router Eth2

The following is a snapshot of the packets captured on the third interface (eth2) of Router.

വിപിപ്പ				
) 7 2 8 3 0 0 0 0 1 8 1 8 1 0
:			 Expression 	n Qear Apply
. Time	Source	Destination	Protocol	
1 0.000000		131.120.9.17 192.168.2.11	SIP/SD SIP	D Request: INVITE sip:131.120.9.17, with session description Status: 100 Trying
3 0.321477		192.168.2.11	SIP	Status: 180 Ringing
4 2.849151		192.168.2.11	SIP/SD	
5 2.855053 6 2.862468		131.120.9.17 131.120.9.17	SIP RTP	Request: ACK sip:131.120.9.17:5060 Payload type=GSM 06.10, SSRC=295543500, Seq=5423, Time=0, Mark
7 2.879196		192.168.2.11	RTP	Payload type=GSM 06.10, SSRC=26034300, SEq=3423, Time=160
8 2.882430) 192.168.2.11	131.120.9.17	RTP	Payload type=GSM 06.10, SSRC=295543500, Seq=5424, Time=160
9 2.898298		192.168.2.11	RTP	Payload type=G5M 06.10, SSRC=568970784, Seq=32284, Time=320
10 2.902353 11 2.918337		131.120.9.17 192.168.2.11	RTP RTP	Payload type=GSM 06.10, SSRC=295543500, Seq=5425, Time=320 Payload type=GSM 06.10, SSRC=568970784, Seq=32285, Time=480
12 2.922409		131.120.9.17	RTP	Payload type=GSM 06.10, SSRC=295543500, Seq=5426, Time=480
13 2.938419		192.168.2.11	RTP	Payload type=GSM 06.10, SSRC=568970784, Seq=32286, Time=640
14 2.942364		131.120.9.17	RTP	Payload type=GSM 06.10, SSRC=295543500, Seq=5427, Time=640
15 2.958279 16 2.962321		192.168.2.11 131.120.9.17	RTP RTP	Payload type=GSM 06.10, SSRC=568970784, Seq=32287, Time=800
17 2.978727		192.168.2.11	RTP	Payload type=GSM 06.10, SSRC=295543500, seq=5428, Time=800 Payload type=GSM 06.10, SSRC=568970784, seq=32288, Time=960
18 2.982400		131.120.9.17	RTP	Payload type=GSM 06.10, SSRC=295543500, Seq=5429, Time=960
19 2.998271		192.168.2.11	RTP	Payload type=GSM 06.10, SSRC=568970784, Seq=32289, Time=1120
20 3.002398		131.120.9.17	RTP	Payload type=GSM 06.10, SSRC=295543500, Seq=5430, Time=1120
21 3.018393 22 3.022341		192.168.2.11 131.120.9.17	RTP RTP	Payload type=GSM 06.10, SSRC=568970784, seq=32290, Time=1280 Payload type=GSM 06.10, SSRC=295543500, seq=5431, Time=1280
23 3.038271		192.168.2.11	RTP	Payload type=GSM 06.10, SSRC=568970784, Seq=32291, Time=1440
24 3.042314	192.168.2.11	131.120.9.17	RTP	Payload type=GSM 06.10, SSRC=295543500, Seq=5432, Time=1440
25 3.058285		192.168.2.11	RTP	Payload type=GSM 06.10, SSRC=568970784, Seq=32292, Time=1600
26 3.062400) 192.168.2.11 131.120.9.17	131.120.9.17 192.168.2.11	RTP RTP	Payload type=GSM 06.10, SSRC=295543500, Seq=5433, Time=1600 Payload type=GSM 06.10, SSRC=568970784, Seq=32293, Time=1760
	192.168.2.11	131.120.9.17	RTP	Payload type=65M 06.10, SSRC=295543500, Seq=3434, Time=1760
29 3.098271	. 131.120.9.17	192.168.2.11	RTP	Payload type=GSM 06.10, SSRC=568970784, Seq=32294, Time=1920
	192.168.2.11	131.120.9.17	RTP	Payload type=GSM 06.10, SSRC=295543500, Seq=5435, Time=1920
	131.120.9.17 192.168.2.11	192.168.2.11 131.120.9.17	RTP RTP	Payload type=GSM 06.10, SSRC=568970784, Seq=32295, Time=2080 Payload type=GSM 06.10, SSRC=295543500, Seq=5436, Time=2080
) 131.120.9.17	192.168.2.11	RTP	Payload type=65M 06.10, 55RC=250345060, 56q=54306, Time=2080 Payload type=65M 06.10, 55RC=568970784, Seq=32296, Time=2240
34 3.142340) 192.168.2.11	131.120.9.17	RTP	Payload type=GSM 06.10, SSRC=295543500, Seq=5437, Time=2240
		192.168.2.11	RTP	Payload type=GSM 06.10, SSRC=568970784, Seq=32297, Time=2400
39 3.192367	192.168.2.11	131.120.9.17	RTP	
40 3.198245	131.120.9.17	192.168.2.11	RTP	Pavlnad tvne=GSM 06.10. SSRC=568970784. Sed=32299. Time=2720
35 3.158299 36 3.162432 37 3.178213 38 3.182305 39 3.192367 40 3.198245 rame 1 (803 thernet II, nternet Prot	<pre>9 131.120.9.17 192.168.2.11 131.120.9.17 192.168.2.11 192.168.2.11 192.168.2.11 131.120.9.17 bytes on wire, 803 Src: 192.168.2.11 ()</pre>	192.168.2.11 131.120.9.17 192.168.2.11 131.120.9.17 131.120.9.17 192.168.2.11 bytes captured) 00:50:da:c0:50:ff] 2.11 (192.168.2.11	RTP RTP RTP RTP RTP RTP , Dst: 19), Dst: 1	Payload type=GSM 06.10, SSRC=568970784, Seq=32297, Time=2400 Payload type=GSM 06.10, SSRC=2959543500, Seq=3438, Time=2400 Payload type=GSM 06.10, SSRC=295543500, Seq=5439, Time=2560 Payload type=GSM 06.10, SSRC=295543500, Seq=5439, Time=2560 Payload type=GSM 06.10, SSRC=295543500, Seq=5440, Time=2720 Pavload type=GSM 06.10, SSRC=29554500, Seq=5440, Time=2720 Pavload type=GSM 06.10, SSRC=29554500, Seq=54209, Time=2720 Pavload type=GSM 06.10, SSRC=2955400, Seq=54200, Seq=54000, Seq=54000, Seq=54000, Seq=54000, Seq=54000, Seq=54000, Seq=54000, Seq=5400, Seq=54000, Seq=54000, Seq=54000, Seq=54000, Seq=54000, Seq=54000, Seq=54000, Seq=540

Figure 50. Test 5: Packet Capture on eth2 of Router

E.8. Client B

The following is a snapshot of the packets captured on Client B when it receives a call from Client D.

(3 NA	Ts D c	all B)	- Ethe	real																								Ľ
Edit	Yiew				alyze <u>S</u>									_														
				C) 🖁	X	¢		9	4	¢ 🗘	7	1			•		2, 00,	•••			ţ	X	Ø				
r:										•	Expression	<u>C</u> le	ar Ap	ply														
	lime		Source				Destir				Protocol																 000000000000000000000000000000000000000	
	145.4							120.9																				owser, Ma
15 1	153.6	0845:	131.	120.	9.15		Broa	idcast			ARP	who H	nas :	131.1	20.9.	.17?	Tel	131.	120.9.									
	153.6 153.6							120.9			ARP							:19:2			cion d	loc co	i et i e					
	153.6					_		120.9		_	SIP/SD SIP			100 T			• 121	1.9.17	, with	565	S TUTE U	ies cr	ipun	JEL		_	 	
191	153.6	7139;	131.	120.	9.17		131.	120.9	.255		NBNS	Name	que	ry NB	Welw.	SJLAE	S.CC	M<00>										
	153.8							120.9			SIP			180 R														
	L54.3 L54.6							120.9			NBNS NBNS							M<00> M<00>										
	155.3							120.9			SIP/SD								cripti	on								
	155.3							120.9			SIP							17:50	60									
	L55.3 L55.3							120.9			NBNS RTP							M<00>	543500	50	a-5423	Tá	ma_0	Marel	,			
	155.3							120.9			RTP								970784						· · · · ·			
28 1	155.3	3485:	131.	120.	9.15		131.	120.9	9.17		RTP	Paylo	bad '	type=	GSM (06.10,	SSF	C=295	543500	, Se	q=5424	, Ti	me=10	i0				
	155.3							120.9			RTP								970784									
	LSS.34 LSS.3							120.9			RTP								543500 970784									
	155.3							120.9			RTP								543500									
33 1	155.3	6386	131.	120.	9.17		131.	120.9	9.15		RTP	Paylo	bad :	type=	GSM (06.10,	SSF	C=568	970784	, Se	q=3228	16, T	ime=0	640				
	155.3							120.9			RTP								543500									
	L55.3 L55.3							120.9			RTP								970784 543500									
	155.3							120.9			RTP								970784									
38 1	155.3	8701	131.	120.	9.15		131.	120.9	9.17		RTP	Paylo	bad '	type=	GSM (06.10,	SSF	C=295	543500	, Se	q=5429), Ti	me=96	i0				
	155.3							120.9			RTP								970784									
	L55.3 L55.4							120.9			RTP								543500 970784									
	155.4							120.9			RTP								543500									
	155.4							120.9			RTP								970784									
	155.4: 155.4							120.9			RTP	Pay lo Davide	oad : ood :	type=	GSM (CSM ()6.10,)6.10	SSF	C=295	543500 070794	, Se	q=5432 q=2220	, Τί 22 Τ	me=14 imo_1	40				
ntern ser D Requ Mess Mess Se E Se E E E E E E E E E E E E E E E E	Net Pi Natagi N In Nest-L Sage H Sessi Owner Sessi Owner Sessi Media Media Media	rotoc ram F itiat ine: Heade oody 1 Des on D c/Cre on N cctio Desc on A cos con A cos cos con A cos cos con A cos cos cos cos cos cos cos cos cos cos	col, :: Proto- cript : INV: er cript escri ator, aame (n Inf ripti ttrik cript ribut ribut ribut	Src: col, Prot ITE tion ipti Se (s): form ion, cute con con ce (ce (ce (ce (ce (ce) con con con con con con con con con con	131.: Src ocol sip:1: Proto on Pro ssion SJpho activ (a):	120.9 Port: 31.12 stocol itocol itoco itoc	.15 (5060).9.1 Ver)): - IN I e (t :tion addr :3 GS :97 i :98 i	131.1 (506 7 SIF 3334 P4 19): 0 :acti ess (M/800 LBC/8	.20.9. (v): (v): (v): (v): 2.168 0 ve m): a: 0 0000	15), st P 0 4 333	Dst: 13: Dst: 1 ort: 50 34605784 L 49162 F	31.12 50 (5)	0.9. 060) :P4 :	17 (1	31.12	11		36)										
	0f 1 15 (11 1 73 (1 Att f 19 Ja CO .3 C4 j9 70	27 3 00 0 13 0 3a 3	:e (36 0 00 7 54 0 31 3	a): rt 0 4c d 11	pmap 69 60 17 00 60 do 2e 31	8 PC 75 83 49 32	MA/80 79 08 78 09 4e 56 30 2e	00 4 0f 8 49 5 39 2	3 78 4 45 e 31	 sip:	.}. ; 131 . /2. (X. .IN 120.	/ITE /9.1													 	

Figure 51. Test 5: Packet Capture on Client B

E.9. Client D

The following is a snapshot of the packets captured on Client D when it calls Client B.

Edit Vie	w <u>G</u> o y	Capture	Analyz	e <u>S</u> tati	stics	Help																			
			B	8	x (è [) 4	¢ 🕅	7	1		ş (Ð	Ð, 🖸			1		X	0				
:				38 96				•	Expressio	<u>C</u> lear	Apply														
Time		Source				Destinatio	1		Protocol	Info															
	00000					192.16												IT Wor	ksta	tion,	Doma	in Enu	m		
	740037					192.16 192.16			UDP UDP			t: 500 t: 500													
4 300	00140	192.1	168.3.	.11	8	192.16	3.3.2	55	BROWSE	Domain	n/wor	kgroup	Annou	uncer	ent WC	ORKGR	DUP, I	IT Wor	ksta	tion,	Doma	in Enu	m		
	. 74519 . 58122					192.16 Broadc		55	UDP ARP	Source	e por	t: 500	3 Des	tina	tion p	port:	5003								
	. 58139					Broauc 192.16		1	ARP			2.168. 1 is a					.11								
8 333	. 58141	192.1	168.3	.11		131.12	0.9.1	7	SIP/SD	Reques	st: I	NVITE	sip:13				th se	sion	desc	ripti	on				
	. 68377					192.16			SIP			0 Tryi													
	.90478					192.16 192.16			SIP SIP/SC			O Ring O OK,		iess	on des	crin	tion								
12 336	0.43279 0.43722	192.1	.68.3.	.11		131.12).9.1	7	SIP	Reques	st: A	CK sip	:131.1	20.9	.17:50	060									
13 336	.44499	192.1	168.3.	.11		131.12			RTP	Payloa	ad ty	pe=GSM	06.10), 55	RC=295	5435	00, SK	eq=542	3, T	ime=0	, Mar	k			
	.46223. .46497:					192.16 131.12			RTP			pe=GSM pe=GSM													
	.48125					192.16			RTP	Payloa	ad ty	pe=GSM	06.10), 59	RC=568	39707	34, SI	q=322	84,	Time=	320				
17 336	.48488	192.1	168.3	.11	3	131.12).9.1	7	RTP	Payloa	ad ty	pe=GSM	06.10), 59	RC=295	55435	00, SK	eq=542	5, T	ime=3	20				
	50128 5.50487					192.16 131.12			RTP			pe=GSM													
	52139					192.16			RTP			pe=GSM pe=GSM													
21 336	52489	192.1	68.3	.11		131.12	0.9.1	7	RTP	Payloa	ad ty	pe=GSM	06.10), 59	RC=295	5435	00, SK	eq=542	7, T	ime=6	40				
	54125					192.16			RTP	Payloa	ad ty	pe=GSM	06.10), 59	RC=568	39707	34, SI	eq=322	87,	Time=	800				
	5, 54487) 5, 561734					131.12 192.16			RTP			pe=GSM pe=GSM													
	5. 56492.					131.12			RTP	Payloa	ad ty	pe=GSM	06.10), 59	RC=295	55435	00, SK	eq=542	9, T	ime=9	60				
26 336	58125	131.1	20.9.	.17		192.16	8.3.1	1	RTP			pe=GSM pe=GSM													
	5.58495 5.60140					131.12 192.16			RTP RTP	Paylo	ad ty ad ty	pe=GSM	06.10), SS	RC=295 pc=569	36435	00, SK 84 e	2q=543	0, T 90	1me=1 ⊤i∞⊳-	120				
	60140 6.60488					131.12			RTP	Pavlo	ad ty	pe=GSM pe=GSM	06.10	7, 53), 59	RC=206	5435	эн, эн 20, 54	2q=543	эл, 1, т	ime=1	280				
30 336	62125	131.1	120.9	.17		192.16	3.3.1	1	RTP	Payloa	ad ty	pe=GSM	06.10), SS	RC=568	39707	34, SK	eq=322	91,	Time=	1440				
	64135					131.12			RTP			pe=GSM													
	64125 . (700 ł					192.16			RTP	Payloa	au ty	pe=GSM	00.10	<i>i</i> , SS	кC=300	59707	54, Si	:q=322	92,	1 11/18=	T000				
nternet ser Dat ession Status Messag Messag Bess Bess Bess Bess Bess Bess Bess Bes	Protoc agram F Initiat -Line: e Heada e body ion Des ssion D ner/Cre ssion N nnectio me Desc ssion A	col, s protoc ion P SIP/2 er cript ator, aame (: n Infu ripti ttribu cript ribut ribut	irc: 1 iol, s vrotoc .0 20 ion P ption Sess s): S s): S s): S cormat ute (ion, e (a) e (a)	31.12 irc Pol col 0 OK Protoco phone ion Ic Ctive a): di name a : rtpm : rtpm)] rt:)] (col ((o) ();] time rect (ap:3 (ap:3	Versic Versic : - 3 : (t): :ion:ac ddress : GSM/8 .01 te	n (v) 34649 131.1 0 0 tive (m) 000 ephor	.9.17) , Dst 1 273 33 20.9.1 audic	49218	92.168 60 (50)	.3.11 60) 94 13:	1.120.	168.3.		<i></i>										
02 a 03 0 30 2 49 5	d 56 38 e 9d 4e b 13 c4 0 32 30 0 2f 32	00 0 13 c 30 2 2e 3	0 7d 4 02 0 4f	11 40 9a c0 4b 00 55 44	64 16 0a 50	83 78 53 49 56 69 20 31	09 11 50 21 61 33 39 33	32 2e 20 53	N 0 20) OK 0/U DF	.x SIP/ Via:	2. 5												 	

Figure 52. Test 5: Packet Capture on Client D

E.10. NAT 3 Eth0

The following is a snapshot of the packets captured on the first interface (eth0) of NAT 3.

NAT 3 EthO (3	NAT)	- Ethere	al																				F
jle Edit View	<u>G</u> o <u>C</u> a	apture A	nalyze Sta	tistics	Help																		
			5 🖪	X	è) (8	a 4	🔹 🕸	4	₽					* *			X	0				
iter:	1000 / 1	560 /	4			_	_	 Expression 							_								
lo Time	9	Source			Destina	stion		Protocol	Info												 	 	
1 0.000						120.9							1.12	0.9.17,	with	sessio	n des	cript	on				
2 0.101						168.2. 168.2.		SIP			00 Tryi 80 Rino												
4 2.850	369 1	131.12	0.9.17		192.1	168.2.	.11		Statu	s: 21	00 OK,	with s		on desc		n							
5 2.855						120.9. 120.9.		SIP RTP						.17:506 RC=2955		Sea=54	23.	Time=(). Mar	k			
7 2.879	909 1	131.12	0.9.17		192.1	168.2.	.11	RTP	Paylo	ad t	ype=GSM	06.10	, SS	RC=5689	70784,	Seq=3	2283,	Time:	160				
8 2.882 9 2.899						120.9. 168.2.		RTP RTP	Paylo	ad ty	ype=GSM	06.10	, SS	RC=2955 RC=5689	43500,	Seq=54	24,	Time=1	.60				
10 2.902						120.9.		RTP						RC=2955									
11 2.919						168.2.		RTP						RC=5689									
12 2.922						120.9. 168.2.		RTP RTP						RC=2955 RC=5689									
14 2.942	834 1	192.16	8.2.11		131.1	120.9.	.17	RTP	Paylo	ad t	ype=GSM	06.10	, SS	RC=2955	43500,	Seq=54	27,	Time=0	640				
15 2.958	976 1	131,12	0.9.17		192.1	168.2.	.11	RTP	Paylo	ad t	ype=GSM	06.10	, SS	RC=5689	70784,	Seq=3	2287,	Time:	800				
16 2.962 17 2.979						120.9. 168.2.		RTP RTP						RC=2955 RC=5689									
18 2.982	859 1	192.16	8.2.11		131.1	120.9.	.17	RTP	Paylo	ad t	ype=GSM	06.10	, SS	RC=2955	43500,	Seq=5	129,	Time=9	960				
19 2.998						168.2.		RTP						RC=5689									
20 3.002						120.9. 168.2.		RTP RTP						RC=2955 RC=5689									
22 3.022	788 1	192.16	8.2.11		131.1	120.9.	.17	RTP	Paylo	ad t	ype=GSM	06.10	, SS	RC=2955	43500,	Seq=5	31,	Time=1	280				
23 3.038						168.2.		RTP						RC=5689									
24 3.042 25 3.058						120.9. 168.2.		RTP RTP						RC=2955 RC=5689									
26 3.062	849 1	192.16	8.2.11		131.1	120.9.	.17	RTP	Paylo	ad t	ype=GSM	06.10	, SS	RC=2955	43500,	Seq=5	33,	Time=1	.600				
27 3.078						168.2. 120.9.		RTP						RC=5689									
29 3.098						168.2.		RTP						RC=2955 RC=5689									
30 3.102						120.9.		RTP						RC=2955									
31 3.119 32 3.122						168.2. 120.9.		RTP RTP						RC=5689 RC=2955									
Frame 1 (80								NIF	rayio	au tj	урс-ази	1 00.10	,	NC-2999	+5500,	Seq-5	.50,	r niie-z	.000				
 Owner Sessi Conne Time Sessi Media Media Media Media Media Media Media 	rotocc ram Pr itiati ine: Header body Desc on De Crea on Na Desc On At Desc On At Desc On At Chea Chea Chea Chea Chea Chea Chea Chea	ol, Src rotocol ion Proc INVITE scriptio scription iption iption tribut riptio ibute ibute ibute	:: 192.1 , Src P ptocol : sip:13: n Protoc ion Prot ession I : SJphor mation (, active e (a): c	68.2. ort: 1.120 col cocol cd (o re (c): e tim direc and irec and irec and irec smap: cmap: p:98	11 (1 5060 1.9.17 Vers): - IN IP e (t) tion: addre 3 GSM 97 iL 98 iL mode	192.16 (5060 7 SIP/ 33346 4 192 1: 0 0 activ 2:ss (m 0.BC/80 BC/80 2:20	i8.2.11))), Dst /2.0 v): 0 05784 3 .168.3. e): audi 00 00), Dst: 1 Port: 50 334605784	31.120 60 (50	.9.1 60) P4 19	7 (131.	3.11		4)									
000 00 a0 d 010 03 15 0 020 09 11 1 030 20 73 6 040 37 20 5 050 52 40 5 le: "K:/Router/NAT	a c0 3 c4 : 9 70 3 49 0 75	00 00 13 c4 3a 31 50 2f 23 30	7f 11 0 03 01 2 33 31 2 32 2e 3 20 2f 9	de db 2a b0 2e 31 30 Od	CO a 49 4 32 3 0a 5 50 7	8 02 e 56 0 2e 6 69	Ob 83 7 49 54 4 39 2e 3	8 5 1 sip	131 .1 2/2. 0.	.INVI 120.9	X ITE 9.1 4:												

Figure 53. Test 5: Packet Capture on eth0 of NAT 3

E.11. NAT 3 Eth1

The following is a snapshot of the packets captured on the second interface (eth1) of NAT 3.

00000	Source	๗₿₫ ♦		0			
00068	Saura		🔿 🖗 🐐		ପ୍ ପ୍ ପ୍	M 🛛 🖪 💥 🔘	
00068	Cauro		Expression Clear	r <u>A</u> pply			
00068	Juarce	Destination	Protocol Info				
	192.168.3.11	Broadcast			Tell 192.168.3.1	1	
	localhost-2.local			68.3.1 is at 00:			
36591	192.168.3.11 131.120.9.16	131.120.9.16 192.168.3.11		is: 100 Trying	151.120.9.10, WIU	n session description	
13382	131.120.9.16	192.168.3.11		s: 180 Ringing			
35809	localhost-2.local				? Tell 192.168.3.	1	
						00	
						IUN	
	192.168.3.11	131.120.9.16	RTP Paylo	ad type=GSM 06.1	10, SSRC=83818212,	Seq=29479, Time=0, Mark	
			RTP Paylo	ad type=GSM 06.1	LO, SSRC=83818212,	Seq=29480, Time=160	
04215							
	192.168.3.11	131.120.9.16		ad type=GSM 06.1	10, SSRC=83818212,	Seq=29483, Time=640	
	131.120.9.16	192.168.3.11	RTP Paylo	ad type=GSM 06.1	10, SSRC=39818112,	Seq=5687, Time=640	
64027	131.120.9.16	192.168.3.11					
	192.168.3.11	131.120.9.16					
				ad type=GSM 06.1	10, SSRC=39818112.	Seq=29467, Time=1280	
	192.168.3.11	131.120.9.16	RTP Paylo	ad type=GSM 06.1	10, SSRC=83818212,	Seq=29488, Time=1440	
24001	131.120.9.16	192.168.3.11	RTP Paylo	ad type=GSM 06.1	LO, SSRC=39818112,	Seq=5692, Time=1440	
40431	192.168.3.11		RTP Paylo	ad type=GSM 06.1 ad type=GSM 06.1	10, SSRC=83818212, 10, SSRC=20818112	Seq=29489, Time=1600	
63907	131.120.9.16	192.168.3.11	RTP Paylo	ad type=GSM 06.1	10, SSRC=39818112,	Seq=5694, Time=1760	
80415	192.168.3.11						
20416	192.168.3.11	131.120.9.16	RTP Paylo	ad type=GSM 06.1	10, SSRC=83818212,	Seq=29493, Time=2240	
		192.168.3.11		ad type=GSM 06.1	10. SSRC=39818112.	Sen=5699. Time=2560	
	31550 38688 10704 30455 30429 304429 30425 20545 20424 341215 20424 30423 34027 30503 34027 304403 34027 30416 33900 04416 339422 30415 33942 33941 0581 313999 50400 33942 313993 50400 33907	38688 192.168.3.11 0704 192.168.3.11 0705 192.168.3.11 0475 192.168.3.11 04475 192.168.3.11 04479 192.168.3.11 04479 192.168.3.11 0475 192.168.3.11 0471 131.120.9.16 1055 192.168.3.11 0405 192.168.3.11 0405 192.168.3.11 0405 192.168.3.11 0407 131.120.9.16 04083 192.168.3.11 0407 131.120.9.16 0401 131.120.9.16 0402 192.168.3.11 0401 131.120.9.16 0402 192.168.3.11 0401 131.120.9.16 0402 192.168.3.11 192.168.3.11 192.168.3.11 19300 131.120.9.16 0401 192.168.3.11 19304 131.120.9.16 192.168.3.11 13942 192.168.3.11 13942 192.168.3.11	$\begin{array}{rrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrr$	11550 131.120.9.16 192.168.3.11 SIP/SD Statu 8688 192.168.3.11 131.120.9.16 SIP Reque 8688 192.168.3.11 131.120.9.16 RTP Paylo 8695 192.168.3.11 131.120.9.16 RTP Paylo 8695 192.168.3.11 131.120.9.16 RTP Paylo 8695 192.168.3.11 131.120.9.16 RTP Paylo 8697 83.11 131.120.9.16 RTP Paylo 8617 192.168.3.11 131.120.9.16 RTP Paylo 8617 192.168.3.11 131.120.9.16 RTP Paylo 8617 192.168.3.11 131.120.9.16 RTP Paylo 8618 192.168.3.11 131.120.9.16 RTP Paylo 8618 192.168.3.11 131.120.9.16 RTP Paylo 8619 192.168.3.11 131.120.9.16 RTP Paylo 86101 192.168.3.11 RTP Paylo 131.120.9.16 RTP Paylo 86102 192.168.3.11 131.120.9.16 RTP Paylo 131.120.9.16 RTP Paylo 8612 <t< td=""><td>11550 131.120.9.16 192.168.3.11 SIP/5D Status: 200 oK, with 18688 192.168.3.11 131.120.9.16 SIP Request: ACK stp131. 10704 192.168.3.11 131.120.9.16 RTP Payload type=GSM 06.1 10745 192.168.3.11 131.120.9.16 RTP Payload type=GSM 06.1 10747 192.168.3.11 131.120.9.16 RTP Payload type=GSM 06.1 10747 192.168.3.11 131.120.9.16 RTP Payload type=GSM 06.1 107519 192.168.3.11 131.120.9.16 RTP Payload type=GSM 06.1 10421 131.120.9.16 192.168.3.11 RTP Payload type=GSM 06.1 10421 192.168.3.11 131.120.9.16 RTP</td><td>11510 131.120.9.16 192.168.3.11 SIP/SD Status: 200 oK, with session descripti 18688 192.168.3.11 131.120.9.16 SIP Request: ACK sip:131.120.9.16:506 10704 192.168.3.11 131.120.9.16 RTP Payload type=GSM 06.10, SSR-83818212, 00419 1074 192.168.3.11 131.120.9.16 RTP Payload type=GSM 06.10, SSR-83818212, 00429 1074 192.168.3.11 131.120.9.16 RTP Payload type=GSM 06.10, SSR-83818212, 00429 1074 192.168.3.11 131.120.9.16 RTP Payload type=GSM 06.10, SSR-83818212, 4024 131.120.9.16 192.168.3.11 RTP Payload type=GSM 06.10, SSR-83818212, 4024 1451.120.9.16 192.168.3.11 RTP Payload type=GSM 06.10, SSR-83818212, 4024 1451.120.9.16 192.168.3.11 RTP Payload type=GSM 06.10, SSR-83818212, 4027 1472 131.120.9.16 RTP Payload type=GSM 06.10, SSR-83818212, 4027 131.120.9.16 192.168.3.11 RTP Payload type=GSM 06.10, SSR-83818212, 4027 131.120.9.16 192.168.3.11 RTP Payload type=GSM 06.10, SSR-83818212, 4027 <t< td=""><td>11510 131.120.9.16 192.168.3.11 SIP/SD Status: 200 OK, with session description 8688 192.168.3.11 131.120.9.16 SIP Request: ACK stp:131.120.9.16:5060 0704 192.168.3.11 131.120.9.16 RTP Payload type=GSM 06.10, SSRC=8318212, Seq=29480, Time=160 04129 192.168.3.11 131.120.9.16 RTP Payload type=GSM 06.10, SSRC=8318212, Seq=29480, Time=480 04129 192.168.3.11 131.120.9.16 RTP Payload type=GSM 06.10, SSRC=8318212, Seq=29483, Time=480 0415 192.168.3.11 131.120.9.16 RTP Payload type=GSM 06.10, SSRC=3818212, Seq=29483, Time=480 0415 192.168.3.11 131.120.9.16 RTP Payload type=GSM 06.10, SSRC=3818212, Seq=29483, Time=400 14024 131.120.9.16 192.168.3.11 RTP Payload type=GSM 06.10, SSRC=3818212, Seq=29483, Time=400 1431 131.120.9.16 RTP Payload type=GSM 06.10, SSRC=3818212, Seq=29483, Time=400 1431 131.120.9.16 RTP Payload type=GSM 06.10, SSRC=3818212, Seq=29483, Time=400 1431 131.120.9.16 RTP Payload type=GSM 06.10, SSRC=3818212, Seq=29483, Time=400 1431 131.120.9.16 RTP Payload type=GSM 06.10</td></t<></td></t<>	11550 131.120.9.16 192.168.3.11 SIP/5D Status: 200 oK, with 18688 192.168.3.11 131.120.9.16 SIP Request: ACK stp131. 10704 192.168.3.11 131.120.9.16 RTP Payload type=GSM 06.1 10745 192.168.3.11 131.120.9.16 RTP Payload type=GSM 06.1 10747 192.168.3.11 131.120.9.16 RTP Payload type=GSM 06.1 10747 192.168.3.11 131.120.9.16 RTP Payload type=GSM 06.1 107519 192.168.3.11 131.120.9.16 RTP Payload type=GSM 06.1 10421 131.120.9.16 192.168.3.11 RTP Payload type=GSM 06.1 10421 192.168.3.11 131.120.9.16 RTP	11510 131.120.9.16 192.168.3.11 SIP/SD Status: 200 oK, with session descripti 18688 192.168.3.11 131.120.9.16 SIP Request: ACK sip:131.120.9.16:506 10704 192.168.3.11 131.120.9.16 RTP Payload type=GSM 06.10, SSR-83818212, 00419 1074 192.168.3.11 131.120.9.16 RTP Payload type=GSM 06.10, SSR-83818212, 00429 1074 192.168.3.11 131.120.9.16 RTP Payload type=GSM 06.10, SSR-83818212, 00429 1074 192.168.3.11 131.120.9.16 RTP Payload type=GSM 06.10, SSR-83818212, 4024 131.120.9.16 192.168.3.11 RTP Payload type=GSM 06.10, SSR-83818212, 4024 1451.120.9.16 192.168.3.11 RTP Payload type=GSM 06.10, SSR-83818212, 4024 1451.120.9.16 192.168.3.11 RTP Payload type=GSM 06.10, SSR-83818212, 4027 1472 131.120.9.16 RTP Payload type=GSM 06.10, SSR-83818212, 4027 131.120.9.16 192.168.3.11 RTP Payload type=GSM 06.10, SSR-83818212, 4027 131.120.9.16 192.168.3.11 RTP Payload type=GSM 06.10, SSR-83818212, 4027 <t< td=""><td>11510 131.120.9.16 192.168.3.11 SIP/SD Status: 200 OK, with session description 8688 192.168.3.11 131.120.9.16 SIP Request: ACK stp:131.120.9.16:5060 0704 192.168.3.11 131.120.9.16 RTP Payload type=GSM 06.10, SSRC=8318212, Seq=29480, Time=160 04129 192.168.3.11 131.120.9.16 RTP Payload type=GSM 06.10, SSRC=8318212, Seq=29480, Time=480 04129 192.168.3.11 131.120.9.16 RTP Payload type=GSM 06.10, SSRC=8318212, Seq=29483, Time=480 0415 192.168.3.11 131.120.9.16 RTP Payload type=GSM 06.10, SSRC=3818212, Seq=29483, Time=480 0415 192.168.3.11 131.120.9.16 RTP Payload type=GSM 06.10, SSRC=3818212, Seq=29483, Time=400 14024 131.120.9.16 192.168.3.11 RTP Payload type=GSM 06.10, SSRC=3818212, Seq=29483, Time=400 1431 131.120.9.16 RTP Payload type=GSM 06.10, SSRC=3818212, Seq=29483, Time=400 1431 131.120.9.16 RTP Payload type=GSM 06.10, SSRC=3818212, Seq=29483, Time=400 1431 131.120.9.16 RTP Payload type=GSM 06.10, SSRC=3818212, Seq=29483, Time=400 1431 131.120.9.16 RTP Payload type=GSM 06.10</td></t<>	11510 131.120.9.16 192.168.3.11 SIP/SD Status: 200 OK, with session description 8688 192.168.3.11 131.120.9.16 SIP Request: ACK stp:131.120.9.16:5060 0704 192.168.3.11 131.120.9.16 RTP Payload type=GSM 06.10, SSRC=8318212, Seq=29480, Time=160 04129 192.168.3.11 131.120.9.16 RTP Payload type=GSM 06.10, SSRC=8318212, Seq=29480, Time=480 04129 192.168.3.11 131.120.9.16 RTP Payload type=GSM 06.10, SSRC=8318212, Seq=29483, Time=480 0415 192.168.3.11 131.120.9.16 RTP Payload type=GSM 06.10, SSRC=3818212, Seq=29483, Time=480 0415 192.168.3.11 131.120.9.16 RTP Payload type=GSM 06.10, SSRC=3818212, Seq=29483, Time=400 14024 131.120.9.16 192.168.3.11 RTP Payload type=GSM 06.10, SSRC=3818212, Seq=29483, Time=400 1431 131.120.9.16 RTP Payload type=GSM 06.10, SSRC=3818212, Seq=29483, Time=400 1431 131.120.9.16 RTP Payload type=GSM 06.10, SSRC=3818212, Seq=29483, Time=400 1431 131.120.9.16 RTP Payload type=GSM 06.10, SSRC=3818212, Seq=29483, Time=400 1431 131.120.9.16 RTP Payload type=GSM 06.10

Figure 54. Test 5: Packet Capture on eth1 of NAT 3
E.12. NAT 1 Eth0

The following is a snapshot of the packets captured on the first interface (eth0) of NAT 1.

NAT1_ETH0 - WordPad	
e Edit View Insert Format Help	
) 📽 🖬 🗧 💁 👗 階 🛍 🕫 💁	
16:25:49.519295 IP 131.120.9.15.49284 > 131.120.9.16.49162:	
16:25:49.532642 IP 131.120.9.16.49162 > 131.120.9.15.49284:	
16:25:49.539430 IP 131.120.9.15.49284 > 131.120.9.16.49162:	
16:25:49.552142 IP 131.120.9.16.49162 > 131.120.9.15.49284:	DP, length 45
16:25:49.559306 IP 131.120.9.15.49284 > 131.120.9.16.49162:	DP, length 45
16:25:49.572149 IP 131.120.9.16.49162 > 131.120.9.15.49284:	DP, length 45
16:25:49.579251 IP 131.120.9.15.49284 > 131.120.9.16.49162:	DP, length 45
16:25:49.582311 IP 131.120.9.16.49162 > 131.120.9.15.49284:	
16:25:49.599409 IP 131.120.9.15.49284 > 131.120.9.16.49162:	DP, length 45
16:25:49.602181 IP 131.120.9.16.49162 > 131.120.9.15.49284:	DP, length 45
16:25:49.619294 IP 131.120.9.15.49284 > 131.120.9.16.49162:	DP, length 45
16:25:49.622193 IP 131.120.9.16.49162 > 131.120.9.15.49284:	DP, length 45
16:25:49.639268 IP 131.120.9.15.49284 > 131.120.9.16.49162:	DP, length 45
16:25:49.642178 IP 131.120.9.16.49162 > 131.120.9.15.49284:	DP, length 45
16:25:49.659367 IP 131.120.9.15.49284 > 131.120.9.16.49162:	DP, length 45
16:25:49.662143 IP 131.120.9.16.49162 > 131.120.9.15.49284:	DP, length 45
16:25:49.679254 IP 131.120.9.15.49284 > 131.120.9.16.49162:	DP, length 45
16:25:49.682173 IP 131.120.9.16.49162 > 131.120.9.15.49284:	DP, length 45
16:25:49.699316 IP 131.120.9.15.49284 > 131.120.9.16.49162:	DP, length 45
16:25:49.702296 IP 131.120.9.16.49162 > 131.120.9.15.49284:	DP, length 45
16:25:49.719246 IP 131.120.9.15.49284 > 131.120.9.16.49162:	DP, length 45
16:25:49.722171 IP 131.120.9.16.49162 > 131.120.9.15.49284:	DP, length 45
16:25:49.739302 IP 131.120.9.15.49284 > 131.120.9.16.49162:	
16:25:49.742157 IP 131.120.9.16.49162 > 131.120.9.15.49284:	DP, length 45
16:25:49.759326 IP 131.120.9.15.49284 > 131.120.9.16.49162:	
16:25:49.762154 IP 131.120.9.16.49162 > 131.120.9.15.49284:	
16:25:49.779284 IP 131.120.9.15.49284 > 131.120.9.16.49162:	
16:25:49.782164 IP 131.120.9.16.49162 > 131.120.9.15.49284:	
16:25:49.799300 IP 131.120.9.15.49284 > 131.120.9.16.49162:	
16:25:49.802151 IP 131.120.9.16.49162 > 131.120.9.15.49284:	
16:25:49.819233 IP 131.120.9.15.49284 > 131.120.9.16.49162:	
16:25:49.822164 IP 131.120.9.16.49162 > 131.120.9.15.49284:	
16:25:49.839311 IP 131.120.9.15.49284 > 131.120.9.16.49162:	
16:25:49.842186 IP 131.120.9.16.49162 > 131.120.9.15.49284:	
16:25:49.859399 IP 131.120.9.15.49284 > 131.120.9.16.49162:	
16:25:49.862166 IP 131.120.9.16.49162 > 131.120.9.15.49284:	
16:25:49.879374 IP 131.120.9.15.49284 > 131.120.9.16.49162:	
16.25.49.882136 IP $131.120.9.16.49162 > 131.120.9.15.49284$:	
16:25:49.899275 IP 131.120.9.15.49284 > 131.120.9.16.49162:	
16.25.49.902156 IP $131.120.9.16.49162 > 131.120.9.15.49284;$	
16:25:49.919290 IP 131.120.9.15.49284 > 131.120.9.16.49162;	
16:25:49.922157 IP 131.120.9.16.49162 > 131.120.9.15.49284:	
16:25:49.939367 IP 131.120.9.15.49284 > 131.120.9.16.49162;	
16:25:49.942159 IP 131.120.9.16.49162 > 131.120.9.15.49284:	
16:25:49.959288 IP 131.120.9.15.49284 > 131.120.9.16.49162:	
16:25:49.962159 IP 131.120.9.16.49162 > 131.120.9.15.49284:	
16:25:49.979303 IP 131.120.9.15.49284 > 131.120.9.16.49162:	
16:25:49.982129 IP 131.120.9.16.49162 > 131.120.9.15.49284:	
16:25:49.999288 IP 131.120.9.15.49284 > 131.120.9.16.49162:	
16:25:50.002150 IP 131.120.9.16.49162 > 131.120.9.15.49284:	
16:25:50.019301 IP 131.120.9.15.49284 > 131.120.9.16.49162:	DP, length 45

Figure 55. Test 5: Packet Capture on eth0 of NAT 1

E.13. NAT 1 Eth1

The following is a snapshot of the packets captured on the second interface (eth1)

of NAT 1.

NAT1_ETH1 - WordPad	
Edit View Insert Format Help	
☞ ■ ● □. 株 氷 階 亀 ∽ 喝	
6:25:48.159372 IP 192.168.202.11.49284 > 131.120.9.16.49162: UDP, length 45	
16:25:48.162765 IP 131.120.9.16.49162 > 192.168.202.11.49284: UDP, length 45	
l6:25:48.179344 IP 192.168.202.11.49284 > 131.120.9.16.49162: UDP, length 45	
16:25:48.182812 IP 131.120.9.16.49162 > 192.168.202.11.49284: UDP, length 45	
16:25:48.199353 IP 192.168.202.11.49284 > 131.120.9.16.49162: UDP, length 45	
16:25:48.202647 IP 131.120.9.16.49162 > 192.168.202.11.49284: UDP, length 45	
L6:25:48.219377 IP 192.168.202.11.49284 > 131.120.9.16.49162: UDP, length 45	
16:25:48.222740 IP 131.120.9.16.49162 > 192.168.202.11.49284: UDP, length 45	
.6:25:48.239346 IP 192.168.202.11.49284 > 131.120.9.16.49162: UDP, length 45	
16:25:48.242644 IP 131.120.9.16.49162 > 192.168.202.11.49284: UDP, length 45	
.6:25:48.259403 IP 192.168.202.11.49284 > 131.120.9.16.49162: UDP, length 45	
6:25:48.263320 IP 131.120.9.16.49162 > 192.168.202.11.49284: UDP, length 45	
6:25:48.279326 IP 192.168.202.11.49284 > 131.120.9.16.49162: UDP, length 45	
6:25:48.282712 IP 131.120.9.16.49162 > 192.168.202.11.49284: UDP, length 45	
.6:25:48.299348 IP 192.168.202.11.49284 > 131.120.9.16.49162: UDP, length 45	
.6:25:48.302642 IP 131.120.9.16.49162 > 192.168.202.11.49284: UDP, length 45	
.6:25:48.319350 IP 192.168.202.11.49284 > 131.120.9.16.49162: UDP, length 45	
6:25:48.322634 IP 131.120.9.16.49162 > 192.168.202.11.49284: UDP, length 45	
.6:25:48.339343 IP 192.168.202.11.49284 > 131.120.9.16.49162: UDP, length 45	
.6:25:48.342645 IP 131.120.9.16.49162 > 192.168.202.11.49284: UDP, length 45	
6:25:48.359360 IP 192.168.202.11.49284 > 131.120.9.16.49162: UDP, length 45	
6:25:48.362641 IP 131.120.9.16.49162 > 192.168.202.11.49284: UDP, length 45	
.6:25:48.379316 IP 192.168.202.11.49284 > 131.120.9.16.49162: UDP, length 45	
l6:25:48.382695 IP 131.120.9.16.49162 > 192.168.202.11.49284: UDP, length 45	
16:25:48.399359 IP 192.168.202.11.49284 > 131.120.9.16.49162: UDP, length 45	
.6:25:48.403356 IP 131.120.9.16.49162 > 192.168.202.11.49284: UDP, length 45	
l6:25:48.419355 IP 192.168.202.11.49284 > 131.120.9.16.49162: UDP, length 45	
l6:25:48.422659 IP 131.120.9.16.49162 > 192.168.202.11.49284: UDP, length 45	
.6:25:48.439336 IP 192.168.202.11.49284 > 131.120.9.16.49162: UDP, length 45	
.6:25:48.442635 IP 131.120.9.16.49162 > 192.168.202.11.49284: UDP, length 45	
.6:25:48.449382 IP 192.168.202.11.49284 > 131.120.9.16.49162: UDP, length 45	
6:25:48.462661 IP 131.120.9.16.49162 > 192.168.202.11.49284: UDP, length 45	
6:25:48.469315 IP 192.168.202.11.49284 > 131.120.9.16.49162: UDP, length 45	
6:25:48.482654 IP 131.120.9.16.49162 > 192.168.202.11.49284: UDP, length 45	
6:25:48.489296 IP 192.168.202.11.49284 > 131.120.9.16.49162: UDP, length 45	
6:25:48.502612 IP 131.120.9.16.49162 > 192.168.202.11.49284: UDP, length 45	
6:25:48.509316 IP 192.168.202.11.49284 > 131.120.9.16.49162: UDP, length 45	
6:25:48.522668 IP 131.120.9.16.49162 > 192.168.202.11.49284: UDP, length 45	
.6:25:48.529329 IP 192.168.202.11.49284 > 131.120.9.16.49162: UDP, length 45	
.6:25:48.543380 IP 131.120.9.16.49162 > 192.168.202.11.49284: UDP, length 45	
.6:25:48.549307 IP 192.168.202.11.49284 > 131.120.9.16.49162: UDP, length 45	
6:25:48.562650 IP 131.120.9.16.49162 > 192.168.202.11.49284: UDP, length 45	
6:25:48.569340 IP 192.168.202.11.49284 > 131.120.9.16.49162: UDP, length 45	
6:25:48.582640 IP 131.120.9.16.49162 > 192.168.202.11.49284: UDP, length 45	
6:25:48.589308 IP 192.168.202.11.49284 > 131.120.9.16.49162: UDP, length 45	
6:25:48.602628 IP 131.120.9.16.49162 > 192.168.202.11.49284; UDP, length 45	
.6:25:48.609392 IP 192.168.202.11.49284 > 131.120.9.16.49162: UDP, length 45	
.6:25:48.622643 IP 131.120.9.16.49162 > 192.168.202.11.49284: UDP, length 45	
6:25:48.629316 IP 192.168.202.11.49284 > 131.120.9.16.49162: UDP, length 45	
16:25:48.642640 IP 131.120.9.16.49162 > 192.168.202.11.49284: UDP, length 45	
6:25:48.649372 IP 192.168.202.11.49284 > 131.120.9.16.49162: UDP, length 45	
leb, press F1	

Figure 56. Test 5: Packet Capture on eth1 of NAT 1

E.14. Analysis

As soon as Client C dialed the IP address of A, Client C sent out an "INVITE" message to Client A (red outline in Figure 44). The message had embedded SDP information to inform Client A that Client C would be sending and receiving RTP packets at 192.168.3.11 on port 49284 (purple outline in Figure 45). To acknowledge the invitation, Client A sent a "200 OK" packet to Client B with embedded SDP information indicating that it would send and receive RTP packets at 131.120.9.16 on port 49284 (green outline in Figure 44). The exchange of the "INVITE" and "200 OK" messages also occurred for the communication between Clients B and D. Client D informed Client B that it would send and receive RTP packets at 192.168.3.11 on 49162. On the other hand, Client B sent and received RTP packets at 131.120.9.17 on 49128. Figures 44 shows that Client A sent and received RTP packet directly to/from the public IP address of NAT 1. As explained in Appendix C, SJPhone will first attempt to send RTP media packets to the IP address indicated in the SDP messages (or the private IP address of Clients C and D). Since the firewall rules on Client A and Client B were configured to drop packets destined to the private IP address of Clients C and D, none of the initial packets sent out by Clients A or B could reach Clients C or D. Therefore, Clients A and B sent subsequent RTP packets to the IP address where it received Client C and D's RTP media packets from (blue outline in Figure 44). The packet captures on Clients C indicate that the first RTP packet in the communication was sent by Client C. Even though NAT 1 was not explicitly configured to rewrite the destination IP address of incoming packets to 192.168.1.2 (public IP address of NAT 2), NAT 1 was able to intelligently determine this because *iptables* has a mechanism to maintain connection states of packets that are initiated from the local network. In our scenario, when the first RTP packet sent by Client C reached NAT 1, the packet was processed get changed from 192.168.202.11 to 192.168.120.9. At the same time, NAT 1 created an entry in its connection tracking table to store essential information (such as source and destination IP addresses and ports) that would allow it to associate incoming packets with Client C. This was also true for the communication between Clients D and B (refer to Figures 49 through 54).

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX G. TEST 6: MYSEA VOIP CONFIGURATION

The objective of Test 6 is to confirm that the MYSEA server could support simultaneous VoIP sessions from multiple MLS LAN clients. As described in Chapter IV, each network interface on the MLS server, currently an XTS-400, currently can only have one static route entry. However, two different static routes are needed to route packets destined for Client C and Client D. The test scenarios described here were intended to be workarounds to the XTS-400 routing problem. The goal was to forward packets to the Router if the packets were received on the single-level interface of the MLS server or forward packets to the NAT 1 if the packets were received on the MLS LAN interface of the MLS server. In other words, the goal was to configure XTS-400 to forward packets to its adjacent components, namely NAT 1 and Router, based on the network interface it receives the packets. Table 9 lists network configurations that were applied to the MLS server for the four test scenarios.

Test Scenario	Dev
1	/d
	/d
2	/d
	/d
3	/d
	/d
4	/d
	/d
	/d

 Table 9.
 Test 6: Test Scenario Configurations

After each set of network configurations was applied to the MLS server, the Unix network utility *ping* was used to confirm the correctness of the network routing. In particular, each of the four IP addresses listed in Table 10 was pinged sequentially for four times from both the Router and NAT 1. Packets were captured using Ethereal at the MLS LAN interface of the Router (eth0, 192.168.0.27) and the single-level interface of NAT 1 (eth1, 192.168.100.88) for post-test analysis.

[Interface	
	MLS LAN (eth0)	
	single-level (eth1)	
	single-level (eth1)	
[public (ethO)	

Table 10. Test 6: Ping Operations

None of the four tests was completed successfully, i.e., there was at least one interface on the MLS server and/or the public NAT that the Router or NAT 1 was unable to ping. See the next four sections for the results.

A. Network Topology

Refer to Figure 14 and Figure 15 for the physical and logical network topology. Note that the clients and NAT 3 were not used in the test scenarios.

- B. Equipment Requirements
 - B.1. NAT 1, NAT 2 and Router
 - B.1.1. Linux Operating System (Fedora Core 4)
 - B.1.2. netfilter and iptables
 - B.1.3. Ethereal
 - B.1.4. Two network cards (for NAT 1 and NAT 2)
 - B.1.5. Three network cards (for Router only)
 - B.2. MLS Server
 - B.2.1. XTS-400
 - B.3. Additional Equipment
 - B.3.1. Cross-over cables and a switch or hub to implement the network architecture illustrated in Figure 14.
- C. Installation and Configuration
 - C.1. MLS Server
 - C.1.1. Configure two network interfaces to be at the same level as the MLS LAN by entering:

min as the security level

max as the integrity level

- C.2. Router
 - C.2.1. Configure eth0 by editing /etc/sysconfig/network-scripts/ifcfg-eth0 to include the following:

DEVICE=eth0 BOOTPROTO=NONE IPADDR=192.168.0.27 NETMASK=255.255.255.0 GATEWAY=192.168.0.130

- C.2.2. Activate eth0 by running: ifup eth0
- C.2.3. Configure eth1 by editing /etc/sysconfig/network-scripts/ifcfg-eth1 to include the following:

DEVICE=eth1 BOOTPROTO=NONE IPADDR=192.168.202.1 NETMASK=255.255.255.0

- C.2.4. Activate eth1 by running: ifup eth1
- C.2.5. Configure eth2 by editing and saving /etc/sysconfig/network-

scripts/ifcfg-eth2 to include the following:

DEVICE=eth2

BOOTPROTO=NONE

IPADDR=192.168.2.1

NETMASK=255.255.255.0

- C.2.6. Activate eth2 by running: ifup eth2
- C.2.7. Enable IP Forwarding by running: echo 1 > /proc/sys/net/ipv4/ip_forward
- C.2.8. Flush any existing firewall and NAT rules by running: iptables -F

iptables -t nat -F

C.3. NAT 1

C.3.1. Configure eth0 by editing /etc/sysconfig/network-scripts/ifcfg-eth0 to include the following:

DEVICE=eth0 BOOTPROTO=NONE IPADDR=131.120.9.15 NETMASK=255.255.255.0 GATEWAY=131.120.9.17

- C.3.2. Activate eth0 by running: ifup eth0
- C.3.3. Configure eth1 by editing and saving /etc/sysconfig/network-

scripts/ifcfg-eth1 to include the following:

DEVICE=eth1

BOOTPROTO=NONE

IPADDR=192.168.100.88

NETMASK=255.255.255.0

- C.3.4. Activate eth1 by running: ifup eth1
- C.3.5. Configure static routes by running:

route add –net 192.168.202.0 netmask 255.255.255.0 gw 192.168.100.130 eth1 route add –net 192.168.2.0 netmask 255.255.255.0 gw 192.168.100.130 eth1 route add –net 192.168.0.0 netmask 255.255.255.0 gw 192.168.100.130 eth1

C.3.6. Enable IP Forwarding by running:

echo 1 > /proc/sys/net/ipv4/ip_forward

C.3.7. Flush any existing firewall and NAT rules by running: iptables -F

iptables -t nat -F

C.3.8. Configure NAT rule by running: iptables -t nat -A POSTROUTING -o eth0 -j SNAT --to 131.120.9.15

C.4. NAT 2

C.4.1. Configure eth0 by editing and saving /etc/sysconfig/networkscripts/ifcfg-eth0 to include the following:

> DEVICE=eth0 BOOTPROTO=NONE IPADDR=196.168.202.11 NETMASK=255.255.255.0 GATEWAY=198.168.202.1

C.4.2. Activate eth0 by running:

ifup eth0

C.4.3. Configure eth1 by editing and saving /etc/sysconfig/networkscripts/ifcfg-eth1 to include the following:

> DEVICE=eth1 BOOTPROTO=NONE

> IPADDR=192.168.3.1

NETMASK=255.255.255.0

- C.4.4. Activate eth1 by running: ifup eth1
- C.4.5. Enable IP Forwarding by running: echo 1 > /proc/sys/net/ipv4/ip_forward
- C.4.6. Flush any existing firewall and NAT rules by running:

iptables -F

iptables -t nat -F

- C.4.7. Configure NAT rules by running: iptables -t nat -A POSTROUTING -o eth0 -j SNAT --to 192.168.202.11 iptables -t nat -A PREROUTING -i eth0 -j DNAT --to 192.168.3.11
- D. Scenario 1
 - D.1. Description

The MLS server is configured in order as follows: any packets received on its MLS LAN (eth0, 192.168.0.130) is forwarded to the MLS LAN interface (eth0, 192.168.0.27) of the Router and any packets received on its single-level (eth1,

192.168.100.130) is forwarded to the single-level interface (eth1, 192.168.100.88) of NAT 1.

D.2. Operations

First, NAT 2 pings:

- 1. eth0 of MLS server
- 2. eth1 of MLS server
- 3. eth1 of NAT 1
- 4. eth0 of NAT 1

Then, Router pings:

- 5. eth0 of MLS server
- 6. eth1 of MLS server
- 7. eth1 of NAT 1
- 8. eth0 of NAT 1

D.3. Network Configuration on MLS Server

D.3.1. Type the following answers when prompted:

SAK

Enter command? tcpip_edit				
Enter editor request?	add			
Enter TCP/IP daemon name?	tcpip_ml	S		
Enter TCPIP/IP daemon description?	TCP/IP	for	MLS	LAN
network				
Enter domain name?	cisrlabm	lstest	bed1.cc	m
Enter host name?	mlsserve	er		
Enable the subnets local flag?	n			
Enable the IP forwarding flag?	у			
Enable the IP send redirect flag?	у			
Enable the shutdown on failure flag?	n			
Use default TCP maximum retransmission?	у			
Add the network interface configuration?	у			
Enter TCP/IP device name?	/dev/ethe	er0		
Enter interface address?	192.168	0.130)	

Enter destination address?	0.0.0.0
Enter broadcast address?	192.168.0.255
Enter network mask?	255.255.255.0
Add another network interface entry?	у
Enter TCP/IP device name?	/dev/ether1
Enter interface address?	192.168.100.130
Enter destination address?	0.0.0.0
Enter broadcast address?	192.168.100.255
Enter network mask?	255.255.255.0
Add another network interface entry?	n
Add the route configuration?	У
Enter TCP/IP device name	/dev/ether0
Is this route a default route	n
Enter destination address	0.0.0.0
Is destination address a host	n
Enter gateway address	192.168.0.27
Enter route metric	1
Add another network route entry	У
Enter TCP/IP device name	/dev/ether1
Is this route a default route	n
Enter destination address	0.0.0.0
Is destination address a host	n
Enter gateway address	192.168.100.88
Enter route metric	1
Add another network route entry	n
Add the resolver configuration?	n

D.4. Preparation and Testing

D.4.1. On NAT 1,

- D.4.1.2. Go to the Capture menu
- D.4.1.3. Go to Interfaces

D.4.1.4. Click on Capture 192.168.100.88

D.4.2. On Router,

- D.4.2.1. Launch Ethereal
- D.4.2.2. Go to the Capture menu
- D.4.2.3. Go to Interfaces
- D.4.2.4. Click on Capture 192.168.0.27
- D.4.3. On NAT 2,
 - D.4.3.1. Run the following commands:
 - ping –c 4 192.168.0.130

ping -c 4 192.168.100.130

ping -c 4 192.168.100.88

ping –c 4 131.120.9.15

D.4.4. Repeat the above commands on the Router

D.4.5. Stop Ethereal captures on both NAT 1 and Router

D.5.Result

Table 11 lists the result of the Scenario 1. The first column shows where the ping was initiated and the first row shows what hosts/IP addresses were pinged. Neither NAT 2 nor the Router was able to ping the public interface of the Public NAT.

to	192.168.0.130	
	(eth0, MLS LAI	
from	interface of MLS	
	server)	
NAT 2	Successful	
Router	Successful	

Table 11.Test 6: Scenario 1 Result

D.6. Packet Capture when pinged from NAT 2

D.6.1. Router

The following two figures are snapshots of the packets captured on eth0 of Router when the four interfaces were pinged from NAT 2.

Ele	Ē00	. We	W §	20	⊆aphu	re	<u>A</u> na)	28 3	(8050	CS [β¢																								
	-					1	6	6) >	6	96	3	9	4	-	Q	7	1	Ł			110	Ð	Q	0			X	Y		X		0		
Elter:	C														Eq	pressio	n (jear	Apply	1															
No	2	Tine			Sou	rce					estina				Pro	stocol	Info	8		_													-1	•	
			0051				8.20				31.1				IC				ing)																
-			0051					2.11			31.1				IC				ing)																
	19.15	0.00	0052	-			1000	2,11			31.1				IC				ing)																
	-		0052	-			8.20	2.11			31.1				10				ing)																
	-		0053					2.11		-	31.1		CALC: NO		IC				ing) ing)																
-	70	101		50			0.20			- 1	/1.1			-	R				ing)	_	_	-	-	-	-	-	-	-	-	-	-	_	-	+	1]
	79	18,	0054	56	192	.16	8.20	2,11		1	31.1	80.9	.15		10	MP	Ech	D (p)	ing)	req	Jest														Jì
	81	18.	0055	64	192	.16	8.20	2.11		1	31.1	20.9	15		IC	мр	Ech	0 (0)	1197 110g)	real	Jest													T)
		(*****	0056	-			8.20				31.1				IC				ing)																
		1000	0056				8.20				31.1				IC				ing)																
			0057		192		8.20				31.1				IC				ing)																
-			0057				8.20				31.1				IC				ing) ing)																
			0058				8.20				31.1				IC				ing)																
			0059				8.20				31.1				IC				ing)																
1	89	18.	0059	98			8.20			_	31.1				IC		1000		ing)										000	-					
	91	19.	0039	80				2.11			31.1				IC			1.25	ing)			-			NG.		919		915	5.)					
		1	-									14	14				• •	1		-													_		
E Fr				Cer.	. 10	3 10	10 A	37 /	00	n. 42	1.0.1				03.14	16 A	130 (200.00	0.05		07.20		1										4	1	
S Iu															22.14	00.0.	130 1	00.0	.0.93	.07.	07.50	2	1	(ora	nge	9								
		sion					***			** 1													J												
				th:	20	byte	6																												
						1.0		ield:	: 0.0	0) (0	SCP (0x00	: Def	ault;	ECN	: 0x0	(0)																		
	Tot	al L	engt	h: 1	84																														
	Ide	ntif	icat	ion	: 0x	0000	0) (0)																											
					on't		agre	t)																											
		-			+ . 0	٦	ŀ		IFO	00																									
			liv				J	5	re	en																									
					(0)																														
	-	per	cnec	K5U	m: 0	x364	be [torne	cc1																								1	4	
0000					7 30						08.0						E.	2		-		-	-	-	-		-		-				-7		
0010								58 6						.T	ę	Xn.,	X																		
0020								00 0							0		+/C																		
0040	16	17	18 1	9 1	a 1b	10	1d	1e 1	If a	21	22 2	3 24	25				*#\$%																		
0050	-			-		_	_	2e i		_	32 3	3 34	35				12345	2															3	1	
	a la		ake se	visa	Hinn	4.6	D: 25	4 D: 2	OA M-	0																								1	

Figure 57. Test 6: Scenario 1 Packet Capture on Router (pinged from NAT 2), Part 1

)	X	Ø	2	q	4	•) 7	1		0	Q	0		X		X	0		
Eilter:									•	<u>E</u> xpressi	m Ø	ear Appl	Y										
Nio	Time		ource			Destin				Protocol	0.000											^	
	72 18.005		92.168.				120.9.1			ICMP	Echo	(ping)	request										
	73 18.005						120.9.1			ICMP			request										
	74 18,005		92.168.				120.9.1			ICMP			request										
	75 18.005		92.168.				120.9.1			ICMP			request										
	76 18.005 77 18.005		92.168. 92.168.				120.9.1			ICMP			request										
	78 18.005		92.168.				120.9.1			ICMP			request										
	70 19 005	156 1	1.0	11.60		171	100.0	ſ		TCMD	Esha	laina	nequest								_)
	80 18.005		92.168.	02.11			120.9.1			IONP	Echo	(ping)	request										1
	200 01 10		100.100	12.44	-	-	20.0		-	1000	-Gene	-	request		-	-	-	-	-	-		-	J
	82 18.005 83 18.005		92.168.				120.9.1			ICMP ICMP			request										
	63 18.005 84 18.005		92.168.				120.9.1			ICMP			request										
	85 18.005		92.168.				120.9.1			ICMP			request										
	86 18.005		92.168.	02.11		131.	120.9.1	15		ICMP			request										
	87 18.005	892 1	92.168.	02.11		131.	120.9.1	15		ICMP			request										
	88 18.005		92.168.				120.9.1			ICMP			request										1
	89 18.005	998 1	92.168.	02.11		131.	120.9.1	15		ICMP	Erito	[6160]	request										
			CONTRACTOR	a state		tion 1	tield and	1.11		1.000				and the second		and some						-	Ļ
	91 19.003						120.9.1			ICAN	Tine	-to-lity	request	d (Inte	to II	Vê lexo	eeded 1	n trans	It)				}
. Fra	91 19.003 me 80 (\$18	908 1 bytes	92.168. an wire	, 98 b		131.	120.9.1 ed)	15	+. 1	ICAN	Echo	-to-liv (ping)	request		to II	VE EKC	eded 1	n trans	itj)	}
e Fra	91 19.003 me 80 (98 ernet 42,	908 1 "bytes Snc: 1	92.168. on wire 92.168.	, 98 b 0.130	(00:cl	131. apturi	ed) 9:07:30	15 D) Ds		ICMP ICMP	Echo	(ping) (ping)	request	0 }		orang	ge	n trans	10)			Ŷ	}
≣ Fra W€th ∃ Int	91 19.003 me 80 (98 ernet 14, ernet Pico	bytes Src: 1 tocol,	92.168. on wire 92.168.	, 98 b 0.130	(00:cl	131. apturi	ed) 9:07:30	15 D) Ds		ICMP ICMP	Echo	(ping) (ping)	request	0 }		prang	ge	n trans	it)			^	}
≣ Fra Ry≨th ∃ Int V	91 19.003 me 80 (98 ernet 42,	bytes Src: 1 tocol,	on wire 92.168. 92.168. Src: 15	, 98 b 0.130	(00:cl	131. apturi	ed) 9:07:30	15 D) Ds		ICMP ICMP	Echo	(ping) (ping)	request	0 }		ve exc	ge	n trans	15)			•	}
≣ Fra ¥vÆth 3 Int V H	ernet 40 (98 ernet 44, ernet Pag ersion: 4 eader len	908 1 Src: 1 tocol, gth: 2	92.168. an wire 92.168. Src: 19	, 98 b 0.130 2.168.	(00:cl 202.11	131. aptur 9:95:ci 1 (192	ed) 9:07:30	15 0) Ds 02.11)	, Dst	ICMP 92.168.0	Echo 0.27 (0	(ping) (ping)	request	0 }		prang	ge	n trans	15)			•	}
E Fra ¥w≨th ∃ Int V H E D	91 19.003 me 80 (98 ernet 12, ernet Pto ersion: 4	908 1 Src: 1 tocol, gth: 20 ated Si	92.168. an wire 92.168. Src: 19	, 98 b 0.130 2.168.	(00:cl 202.11	131. aptur 9:95:ci 1 (192	ed) 9:07:30	15 0) Ds 02.11)	, Dst	ICMP 92.168.0	Echo 0.27 (0	(ping) (ping)	request	0 }		prang	ge	n trans	15)			•	}
E Fra WEth ∃ Int V H E D T	91 19.003 me 80 (96 ernet IC, ernet Pro ersion: 4 eader len ifferenti	908 1 Src: 1 tocol, gth: 20 ated So th: 84	92.168. 92.168. 92.168. Src: 19 bytes ervices	02.11 , 98 b 0.130 2.168. Field:	(00:cl 202.11	131. aptur 9:95:ci 1 (192	ed) 9:07:30	15 0) Ds 02.11)	, Dst	ICMP 92.168.0	Echo 0.27 (0	(ping) (ping)	request	0 }		prang	ge	n trans					}
≣ Fra ¥w≨th B Int V H ⊞ D T I	91 19.003 me 80 (96 ernet 12, ernet Peo ersion: 4 eader len ifferenti otal Leng	908 1 Src: 1 tocol, ated Si th: 84 tion: (92.168. on wire 92.168. Src: 19 bytes ervices	02.11 , 98 b 0.130 2.168. Field: 0)	(00:cl 202.11	131. aptur 9:95:ci 1 (192	ed) 9:07:30	15 0) Ds 02.11)	, Dst	ICMP 92.168.0	Echo 0.27 (0	(ping) (ping)	request	0 }		prang	ge	n trans			_		}
E Fra Xwith S Int V H E D T I S F	91 19.003 me 80 (96 ernet IZ, ernet Pag ersion: 4 eader len ifferenti otal Leng dentifica	908 1 5rc: 1 tocol, ated Si th: 84 tion: (4 (Don	92.168. on wire 92.168. Src: 19 bytes ervices bx0000 't Frag	02.11 , 98 b 0.130 2.168. Field: 0)	(00:cl 202.11	131. aptur 9:95:ci 1 (192	ed) 9:07:30	15 0) Ds 02.11)	, Dst	ICMP 92.168.0	Echo 0.27 (0	(ping) (ping)	request	0 }		prang	ge	n trans	15)				}
E Fra Ryfth B Int B D H B D T I I F F	91 19.003 me 80 (96 ernet II, ernet Pag ersion: 4 eader len ifferenti otal Leng dentifica lags: Dx0	908 1 Src: 1 tocol, gth: 20 ated So th: 84 tion: (4 (Don ffset:	92.168. on wire 92.168. Src: 19 bytes ervices bx0000 't Frag	02.11 , 98 b 0.130 2.168. Field: 0) went)	(00:cl 202.11 0x00	131. aptur 0:95:cl 1 (192 (DSCP	ed) 9:07:30	15 0) Ds 02.11)	, Dst	ICMP 92.168.0	Echo 0.27 (0	(ping) (ping)	request	0 }		ve exc	ge	n trans	15)			~	}
₩ Fra With Int U H H F T I T	91 19.003 me 80 (98 ernet Id, ernet Pag ersion: 4 eader len ifferenti otal Leng dentifica lags: 0x0 ragment o	908 1 Src: 1 tocol, ated Se th: 84 tion: (4 (Don ffset: ve: 10	92.168. on wire 92.168. Src: 19) bytes ervices bx0000 (t Frage 0	02.11 , 98 b 0.130 2.168. Field: 0) went)	(00:cl 202.11	131. aptur 0:95:cl 1 (192 (DSCP	ed) 9:07:30	15 0) Ds 02.11)	, Dst	ICMP 92.168.0	Echo 0.27 (0	(ping) (ping)	request	0 }		ve exc	ge	n trans	it)		_		}
E Fra Evjeth U D E Int E D T I E P	91 19.003 me 80 (%6 ernet I2, ernet Pho ersion: 4 eader len ifferenti otal Leng dentifica lags: 0x0 ragment o ime to li	908 1 bytes Src: 1 tocol, ated Si th: 84 tion: (0 ffset: IOMP (0	92.168. on wire 92.168. Src: 19 bytes ervices bx0000 't Frage 0 bx010	02.11 , 98 b 0.130 2.168. Field: 0) ent)	(00:cd 202.11 0x00 gree	131. aptur 0:95:cl 1 (192 (DSCP	ed) 9:07:30	15 0) Ds 02.11)	, Dst	ICMP 92.168.0	Echo 0.27 (0	(ping) (ping)	request	0 }		ve exc	ge	n trans	it)				}
H Fra Ryfth B Int H H B D T I I F F P H	91 19.003 me 80 (96 ernet I, ernet Pog ersion: 4 eader len ifferenti otal Leng dentifica lags: 0x0 ragment o ime to li rotocol: eader che	908 1 bytes Src: 1 tocol, gth: 2 tated Si th: 84 th: 84 (Don ffset: ve: 10 ICMP (i cksum:	92.168. on wire 92.168. Src: 19) bytes ervices bx0000 (t Frag 0 0 0 0 0 0 0 0 0 0 0 0 0	<pre>02.11 , 98 b 0.130 2.168. Field: 0) ent) } [corre</pre>	(00:d 202.11 0x00 gree ct]	131. :apturi):95:cl (DSCP en	ed) 9:07:30 .168.20	15 0) Ds 02.11) Defa	, Dst	LCV2 ICMP 922.168.0 1: 131.1 EECN: Cod	0.27 ((20.9.1)	(ping) (ping)	request	0 }		ve exc	ge	n trans	it)				}
E Fra EvEth B Int B Int B D T I B F F F F F H H 0000	91 19.003 me 80 (96 ernet 12, ernet Pag ersion: 4 eader len iifferenti otal Leng dentifica lags: 0x0 ragment o ime to li rotocol: eader che	bytes Src: 1 tocol, gth: 2/ th: 84 tion: (4 (Don ffset: ICMP (cksum: 1c 7d	92.168. on wire: 92.168. Src: 19) bytes ervices bx0000 (t Fragmond) 0 0 0 0 0 0 0 0 0 0 0 0 0	<pre>02.11 , 98 b 0.130 2.168. Field: 0) hent) [corre</pre>	(00:d 202.11 0x00 gree ct]	131. apturn):95:cl (DSCP PDT 30:08	20,9,1 ed) 9:07:30 168.20 0x00:	0) Ds 02.11) Defa	, Dsf	10/2 ICMP 32.168.0 1: 131.1	0.27 (0 20.9.1) 00)	(ping) (ping)	request	0 }		ve exc	ge		it)				}
E Fra ExyEth Int E Int U E D T I E F F P H 0000 0010 0020	91 19.003 me 80 (96 ernet 42, ernet Pag ersion: 4 eader len ifferenti otal Leng dentifica lags: 0x0 ragment o ime to li rotocol: eader che 00 a0 d2 00 54 00 00 54 00	908 1 bytes frc: 1 tocol, gth: 2/ ated Si ated Si th: 84 tian: (4 (Don ffset: ve: 10 ICMP (i cksum: 1c 7d (00 40) 00 55	92.168. on wire 92.168. Src: 19 bytes srvices bx0000 t Frage 0 0x596e 24 00 cl 10 0a 0 92 f8 0	02.11 , 98 b 0.130 2.168. Field: 0) ment) [correction of the second seco	(00:cd 202.11 0x00 gree ct] 9 07 e c0 0 d5	131. apturi 1955:cl 1 (192 (DSCP en 30 08 a8 ca 26 2f	ed) 9:07:30 168.20 0x00: 0x00:	0) Ds 02.11) Defai 00 78 ef	, Dsf ilt; I }	LCV2 ICMP 922.168.0 1: 131.1 EECN: Cod	0.27 (0 20.9.1) 00)	(ping) (ping)	request	0 }		ve exc	ge						}
E Fra ExyEth Int E Int U E D T I I F F P H 0000 0010 0020 0030	91 19.003 me 80 (96 ernet 42, ernet Pag ersion: 4 eader len ifferenti otal Leng dentifica lags: 0x0 ragment o ime to li rotocol: eader che 00 a0 d2 00 9 0f 08 03 00 08	908 1 bytes frc: 1 tocol, gth: 2/ ated Si tth: 84 ttian: (4 (Don ffset: ve: 10 ICMP (i Ccksum: 1c 7d ICMP (0 00 40 00 05 09 0a	92.168. on wire 92.168. Src: 19 bytes prvic	<pre>02.11 , 98 b 0.130 2.168. Field: 0) ent) [corre 59 6 00 0 0 00 0 0 00 0 0 00 0 0 00 0 0 00 0</pre>	(00:cd 202.11 0x00 gree ct] 9 07 e c0 0 d5 f 10	131. apturi 1955:cl 1 (192 (DSCP en 30 08 a8 ca 26 2f 11 12	ed) 9:07:30 .168.20 0x00: 0x00: 0x00:	0) Ds 02.11) Defai 00 78 ef 15	, Ds1 , lt; l ,lt; l }	109 IOMP 92.168.0 1: 131.1 ECN: 0xi	0.27 ((20.9.1) 00)	(ping) (ping)	request	0 }		prang	ge						}
₽ Fra 2006 1 mt 1 mt 1 mt 1 mt 1 mt 1 mt 1 mt 1 mt	91 19.003 me 80 (96 ernet 42, ernet Pag ersion: 4 eader len ifferenti otal Leng dentifica lags: 0x0 ragment o ime to li rotocol: eader che 00 a0 d2 00 54 00 00 54 00	908 1 'bytes Src: 1 tocol, gth: 2 ated Si th: 84 tion: (4 (Don ffset: 10 76 1 100 40 00 55 19 1a	92.168. on wire 92.168. Src: 19 bytes prvices bytes	02.11 , 98 b 0.130 2.168. Field: 0) ent) (correction of the second secon	(00:cd 202.11 0x00 0x00 gree ct] 9 07 e c0 0 d5 f 10 f 20	131. aptur: 1955:c (DSCP 0008 as ca 26 2f 11 12 21 22	200 45 1 00 45 0 00 45 1 00 43 1 13 14 23 24	0) Ds 02.11) Defai 00 78 ef 15 25	, Ds1 , lt; ,}	10/2 ICMP 22.168.0 1: 131.1 ECN: 0xl	0.27 (t 20.9.1) 00)	(ping) (ping)	request	0 }		pran	ge		11				}

Figure 58. Test 6: Scenario 1 Packet Capture on Router (pinged from NAT 2), Part 2

D.6.2. NAT 1

The following is a snapshot of the packets captured on the eth1 of NAT 1 when the four interfaces were pinged from NAT 2.

Frame 1 (60 bytes on wire, 40 bytes captured) Frame 1 (60 bytes on wire, 40 bytes captured)	K			-		0	1	x	R	8	9	4	φ.	1	2			6	Ð	Q	Q	1		M	8	X	0
I 01000000 192.168.100.88 192.168.100.108 192.168.100.108 192.168.100.100.81 192.168.100.100.81 192.168.100.100.100 192.168.100.100 192.168.100.100 192.168.100.100.81 192.168.100.100.100 192.168.100.100.100 192.168.100.100.100 192.168.100.100.100 192.168.100.100.100 192.168.100.100.100 192.168.100.100.100 192.168.100.100.100 192.168.100.100.100 192.168.100.100.100 192.168.100.100.81 192.168.100.110 192.168.100.100.81 192.168.100.110 192.168.100.100.81 192.168.100.110 192.168.100.100.81 192.168.100.110 192.168.100.100.81 192.168.100.110 192.168.100.100.81 192.168.100.110 192.168.100.100.100 192.168.100.110				-		U men				-		1										-					
I 01000000 192.168.100.88 192.168.100.108 192.168.100.108 192.168.100.100.81 192.168.100.100.81 192.168.100.100.100 192.168.100.100 192.168.100.100 192.168.100.100.81 192.168.100.100.100 192.168.100.100.100 192.168.100.100.100 192.168.100.100.100 192.168.100.100.100 192.168.100.100.100 192.168.100.100.100 192.168.100.100.100 192.168.100.100.100 192.168.100.100.100 192.168.100.100.81 192.168.100.110 192.168.100.100.81 192.168.100.110 192.168.100.100.81 192.168.100.110 192.168.100.100.81 192.168.100.110 192.168.100.100.81 192.168.100.110 192.168.100.100.81 192.168.100.110 192.168.100.100.100 192.168.100.110	10		Terra	_	· · · · ·	8		-	Deat			-	Dashar	ed take		_		-	-	-	-			-	_	-	
<pre>2 0.000084 192.168.100.88 192.168.100.130 AP 192.168.100.88 is at 0010c141:f1:f1:f1:f1:f1:f1:f1:f1:f1:f1:f1:f1:f1</pre>									1		-	_			has 1	No.	NIM I		01	10	35723	100.1	18	_	_	_	_
4 0.000168 192.168.100.88 192.168.202.11 IOMP Echo (ping) reply 5 1.000749 192.168.202.11 192.168.202.11 IOMP Echo (ping) reply 7 1.000579 192.168.202.11 192.168.202.11 IOMP Echo (ping) reply 7 1.000579 192.168.202.11 192.168.202.11 IOMP Echo (ping) reply 7 1.000548 192.168.202.11 192.168.202.11 IOMP Echo (ping) reply 9 1.000448 192.168.202.11 192.168.202.11 IOMP Echo (ping) reply 9 1.000448 192.168.202.11 192.168.202.11 IOMP Echo (ping) reply 10 1.000514 192.168.100.88 192.168.202.11 IOMP Echo (ping) reply 11 4.990951 192.168.100.88 192.168.100.130 ARP Who has 192.168.100.1307 Tell 192.168.100.88 12 4.999043 192.168.100.130 192.168.100.88 ARP 192.168.100.130 is at 00:c0:95:c9:07:11 Frame 1 (60 bytes on wire, 60 bytes captured) Ethorem till, irc: 192.168.100.0310 (00:c0:95:c9:07:31), 0st: Broadcast (ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:		2	0,0000	184	192.1	68.10	0,88		192	168.1	00.130	2	ARP	192	168.10	0.88	15 at										
\$ 1.000749 192.168.202.11 192.168.00.88 IOMP Echo (ping) reguest 6 1.000841 192.168.100.88 192.168.202.11 IOMP Echo (ping) regly 7 2.000597 192.168.100.88 192.168.202.11 192.168.100.88 IOMP Echo (ping) regly 8 2.000642 192.168.100.88 192.168.202.11 192.168.100.88 IOMP Echo (ping) reguest 8 2.000642 192.168.100.88 192.168.202.11 IOMP Echo (ping) reguest 10 3.000514 192.168.100.88 192.168.02.11 IOMP Echo (ping) reguest 10 3.000514 192.168.100.88 192.168.00.130 ARP Who has 192.168.100.1307 Tell 192.168.100.88 12 4.999043 192.168.100.130 192.168.100.88 ARP 192.168.100.110 is at 00:c0:95:c9:07:31 Frame 1 (60 bytes on wire, 60 bytes captured) Ethernet II, 5rc: 192.168.00.0130 (00:c0:95:c9:07:31), 0st: broadcast (ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:													-														
6 1.000041 192.168.100.88 192.168.202.11 1000 Echo (ping) reply 7 2.000597 192.168.202.11 192.168.202.88 1000 Echo (ping) reply 8 2.000662 192.168.202.11 192.168.202.11 IOMP Echo (ping) reply 9 3.000514 192.168.202.11 192.168.202.11 IOMP Echo (ping) reply 9 3.000534 192.168.202.11 1000 RE Cho (ping) reply 10 3.000534 192.168.202.11 IOMP Echo (ping) reply 11 4.998951 192.168.100.88 192.168.100.38 192.168.100.30 12 4.999043 192.168.100.130 192.168.100.88 ARP 192.168.100.130 is at 00:c0:95:c9:07:31																											
7 2.000597 192.168.202.11 192.168.202.11 1000 Echo (ping) request 8 2.000682 192.168.202.11 192.168.202.11 1000 Echo (ping) request 9 3.000488 192.168.202.11 192.168.202.11 1000 Echo (ping) request 10 3.000548 192.168.200.88 192.168.202.11 1000 Echo (ping) request 11 4.998951 192.168.100.88 192.168.202.11 1000 Echo (ping) request 12 4.999043 192.168.100.130 192.168.100.88 ARP 192.168.100.130 Tell 192.168.100.88 12 4.999043 192.168.100.130 192.168.100.88 ARP 192.168.100.130 is at 00:c0:95:c9:07:31																											
9 3.000448 192.168.202.11 192.168.202.11 100P Echo (ping) reput 10 3.000534 192.168.100.88 192.168.202.11 IOMP Echo (ping) reply 11 4.998951 192.168.100.88 192.168.100.130 ARP Who has 192.168.100.1307 Tell 192.168.100.88 12 4.999043 192.168.100.130 192.168.100.88 ARP 192.168.100.130 is at 00:0195:09:07:31														Ech	(pin) req	uest										
10 3.000514 192.168.100.88 192.168.202.11 ICMP Echo (ping) reply 11 4.998951 192.168.100.88 192.168.100.130 ARP Who has 192.168.100.1307 Tell 192.168.100.88 12 4.999043 192.168.100.130 192.168.100.88 ARP 192.168.100.130 is at 00:c0:95:c9:07:31 Frame 1 (60 bytes on wire, 60 bytes captured) Ethernet II, Src: 192.168.00.030 00:c0:95:c9:07:31), Dst: Broadcast (ff:ff:ff:ff:ff:ff:ff:ff)														Ech) (pin	i) rep	ly										
11 4.998951 192.168.100.88 192.168.100.130 ARP Who has 192.168.100.1307 Tell 192.168.100.88 12 4.999043 192.168.100.130 192.168.100.88 ARP 192.168.100.130 is at 00:c0:95:c9:07:31																											
12 4.999043 192.168.100.130 192.168.100.88 ARP 192.168.100.130 is at 00:c0:95:c9:07:31 Frame 1 (60 bytes on wire, 60 bytes captured) Ethernet II, 5rc: 192.168.100.130 (00:c0:95:c9:07:31), Dst: Broadcast (ff:ff:ff:ff:ff:ff:ff)															(pin	i) rep	lly.										
Frame 1 (60 bytes on wire, 60 bytes captured) Ethernet II, Src: 192.168.100.130 (00:c0:95:c9:07:31), Dst: Broadcast (ff:ff:ff:ff:ff:ff)										168.1	00.130			- Mbo	has 1	12.168	.100.1	382	Tel	1.14	12.16	8,100.	882				
Ethernet II, Src: 192.168.100.130 (00:c0:95:c9:07:31), Ost: Broadcast (ff:ff:ff:ff:ff:ff)		12	4,999	¥)										who 192	has 1 168,1	0.130	15 a1	307	Te1 c0:9	1 15	92.16	8,100.	88				
		12	4,999	543										who 192	has 1 168,1	0.110	. 100.1	307	Te1 c0:9	1 15	92.16	8.100.	8				
		ame	1 (60	bytes	192.1 5 ON W	68.10	0.130 00 byt		192 192	ed)	00.88		ARP	192	168.1	0.110) is at	307 00:0	Te1 c0:9	1 15	9:07:	8,100.	88				
	£t)	ame	1 (60 Het II.	bytes	192.1 s on w : 192.	68.10 ire. 1	0 byt 0.130	(00	192 192	ed)	00.88		ARP	192	168.1	0.110) is at	307 0010	Te1 c0:9	1 19	9:07:	8.100.					
	Add	ame hern dres	1 (60 Het II. SS Reso	bytes src: olutio	192.1 s on w : 192. on Pro	1re, 1 168.10 168.10	0.130 0.byt 0.130 (requ	(00 est)	192 aptur c0:9	ed) 5:c9:0	7:31),	Dst:	Broad	192	168.1	0.110) is at	307 00 : c	Te1 c0:9	1 15 16	9:07:	8.100.					
10 08 00 06 04 00 01 00 c0 95 c9 07 31 c0 a8 64 82	Add	ame hern dres	1 (60 het II. 55 Reso 77 Ff	bytes Srcs Slutic	s on w : 192.1 : 192. : 192. : an Pro	1re, 1 168.10 168.10	0.130 0.5yt 0.130 (requ	(00 est)	192 aptur: c0:9	ed) 5 : c 9 : 0 a8 64	7:31),	Dst:	Broad	192	168.1	0.110) is at	307	Te1 c0:9	1 15 165	9:07:	8,100.					



D.6.3. Analysis

NAT 2 was able to ping 192.168.0.130 and 192.168.100.130 because the MLS server shared a peer-to-peer relationship with the Router and the Router had logic to route packets between the MLS server and NAT 2. It was also able to ping 192.168.100.88 because XTS-400 was capable of routing the Echo requests and replies to its immediate peers that in turn, routed the packets to the destination. Pinging 131.120.9.15 was unsuccessful from NAT 2. The Router saw ICMP requests when NAT 2 pinged 131.120.9.15 (red outline in Figure 57). The ICMP requests were routed from 192.168.0.27 (yellow outline in Figure 57) to 192.168.0.130 (orange outline in Figure 57). As soon as the MLS server received the requests, the XTS-400 bounced them back to the IP address from which they came (yellow and orange outlines in Figure 58). Note that the time-to-live field was decremented from 11 (green outline in Figure 57) to 10 (green outline in Figure 58) indicating that the two requests seen in the packet capture were, in fact, the same packet. This sequence of events continued until the time-to-live was exceeded in transit (blue outline in Figure 57). Thus, the ICMP was never able to reach NAT 1 as shown in Figure 59.

D.7. Packet Capture when pinged from Router

D.7.1. Router

The following two pictures are snapshots of the packets captured on eth0 of the Router when the four interfaces were pinged from Router.

	57	9		6	8	x	¢	8	9	4		07	1		0	Θ	Q	••				×	1			
Elter:										•	Expres	sion	jear Ar	ply												
No	Te	*	Souro				Destr	ation		-	Protoco	i Info	i.										-	-		
19		1/1/123/	176.	100.10			176.	100.V.			IUNY	ELF	U (pin	jį repty												
		169992		168.0.7				168.100			ICMP) request												
		170105		168.100				168.0.			ICMP			 reply request 												
		169957		168.100				168.0.1			ICMP) reply												
		. 604015						168.100			ICMP) request												
20) 11	1.604475	192.	168.100	0.88		192.	168.0.3	27		ICMP) reply												
		2.604378		168.0.2				168.100			ICMP) request												
				168.100				168.0.			ICMP) reply												
		3.604169 3.604476		168.0.7				168.100			ICMP			<pre>p) request p) reply</pre>												
		1.604015		168.0.2	10777			168.100			ICMP) request												
	-	604333	103	100.10	- 00-	_	103	100.0		_	1/10	- Cal	200	hand	_	_	_	_	_	_	_	_	_)
		.009871		168.0.2				120.9.			ICMP	Ech) request												ł
_		010000		169.0.3		-	and shares	130.9.1			T(NO		n (nin	and the second second											\mathbf{r}	
		2.009888		168.0.2				120.9.1			ICMP) request)
		2.010001		168.0.2	-			120.9.1			ICMP			p) requestp) request												
		8.009851						120.9.1			ICMP) request												
		1.009584		168.0.2				120.9.1			ICMP) request												
34	1 24	1.009697	192.	168.0.7	27		131.	120.9.1	15		ICMP) request										v		
Ver	rfet ader ffer	t Protoco en: 4 r length: rentiated Length: ification	20 , 500 20 by d Servi 84 n: 0x00	t: 192. ytes ices Fi	108.0. ield: () nt)	.21	192.1 (DSCP	od.0.2	J , US	FC: 1)1,12J.	9.15		95:c9:07:0 0.9.15)] 0	rang	le							100		
Tot Ide	ags: me t otoc ader 0 ct	to live: col: IOMF r checksu 0 95 c9 0 4 00 00 4 f 08 00 0	P (0x0) um: 0x8 07 30 0 40 00 4	ed5e [c	d2 1c ed 5e	70 0	8 00 84	00 45 1 1b 83	78	.T0	0 .e^	X					_	_					_	- ^		

Figure 60. Test 6: Scenario 1 Packet Capture on Router (pinged from Router), Part 1

10		Yew G	io <u>C</u> apture	e <u>A</u> nalyze	e Satis	tics Hy	þ	101101					-						0.007			_
				6	;	(6		9	4	•	07	5 1			Q	Q	•••			X	0	
ter:									•	[ppres	sion	çlear Ap	hy									
0. +	1	ine	Source			De	stination	9		Protoc	ol Info	1										^
		. 1/923		100.100.			2.100.1			LURP			y reply									
		.16999		168.0.2/			2.168.1 2.168.0			ICMP) request) reply									
		.16984		168.0.27			2.168.1			IONP) request									
		.16995		168.100.			2.168.0			ICMP) reply									
		1.6040		168.0.27	7	19	2.168.1	88.00		ICMP) request									
		1.6044		168.100.			2.168.0			IOMP	Ech	io (ping) reply									
		2.6043		168.0.2			2.168.1			ICMP) request									
		2.6046		168.100.			2.168.0			ICMP) reply									
		3.6041 3.6044		168.0.2/			2.168.1 2.168.0			ICMP) request) reply									
		4.6040		168.0.27	10.01		2.168.1			IONP) request									
	100110	4.6043		168,100.			2.168.0			ICMP) reply									
-	0.00	1.0098	a la sub de la sub d	168.0.27		13	1.120.9	.15		TCMP	Fre	n (nin) request							_		
			09 192.			-	1.120.5			IONP) request	1								
			88 192.	168.0.2			1.120.9		_	TOMP) request		_				_		_	-
		2.0100		168.0.2/			1.120.9			ICMP) request) request									
		3.0098		168.0.27			1.120.9			IONP) request									
		4.0095		168.0.27			1.120.9			ICMP) request									
			97 192.				1.120.9			ICMP) request									v
														-				_	_		_	~
9¥ 1 1 1	lerne Versi Head Diffe Tota Idem	t Plot ion: 4 ir leng irentia Lengt ificat	th: 20 by th: 20 by ted Serv h: 84 ion: 0x0	(; 192.1 ytes ices Fie 000 (0)	100.0.2 21d: 0x	, (195	.105.0.	<i>ü</i>], U	5t: 1	31.120	.9,15	(00:a0:	d2:1c:7d:0	4) }	- oi	ang	le					10.1
	Vers Head Diffi Idem Flag Frag Time	t Prot on: 4 r leng rentia Lengt cificat cont of to liv con: 1	th: 20 b) th: 20 b) ted Serv h: 84 ion: 0x00 (Don't) fset: 0 e: 63 OMP (0x0)	ct 192.1 ytes ices Fie 000 (0) Fragment	:00.0.2 :1d: 0x :) }	gre/	.165.U.	<i>ü</i>], U	5t: 1	31.120	.9,15	(00:a0:	d2:1c:7d:0	4) }	• or	ang	le					11 10 10 11 12 12 12 12 12 12 12 12 12 12 12 12
	Vers Head Diffi Idem Flag Frag Time	t Prot on: 4 r leng rentia Lengt cificat cont of to liv con: 1	th: 20 b) th: 20 b) ted Serv h: 84 ion: 0x00 (Don't 1 fset: 0 e: 63	ct 192.1 ytes ices Fie 000 (0) Fragment	:00.0.2 :1d: 0x :) }	gre/	.165.U.	<i>ü</i>], U	5t: 1	31.120	.9,15	(00:a0:	d2:1c:7d:0	4)	- or	rang	le					(×) 1 m m () ()
	Versi Head Diffi Tota Iden Flag: Frag Time Proto Head	t Proti on: 4 er leng rentia Lengt tificat to liv col: 1 er chec	th: 20 by ted Servi h: 84 ion: 0x00 (Don't 1 fset: 0 0XP (0x0 ksum: 0x0 c 7d 04	vtes ices Fie 000 (0) Fragment eeSe [co 00 c0 S	<pre>cos.u.2 eld: 0x t) forrect] forrect] forrect]</pre>	gree	.166.0. CP 0x00 en	2/), 0): Defa	st: 1 ult;	ECN: 0	.9,15 x00)	(00:a0: 131.12	d2:1c:7d:0	4) }	- or	rang	le					> 1(<) 1
	Vers Head Diffi Tota Ident Flag Frag Time Proto Head	t Plot ion: 4 ir leng irentia Lengt ificat i: 0x04 icol: 1 ir chec io 02 1 ir chec	th: 20 by ted Servine (Don't 1 fset: 0 e: 63 OMP (0x0) ksum: 0x0 c 7d 04 0 0 40 00	(; 192.1 ytes ices Fie 000 (0) Fragment p 1 eeSe [co 00 c0 S 3f 01 e	<pre>cos.u.2 cld: 0x c</pre>	gre 7 30 (0 30 0 (05	. 166. U. CP 0x00 en	27), 0 1: Defa 5 00 1 78	st: 1 ult;]	51.180 ECN: 0	.9,15 x00)	(00:a0:	d2:1c:7d:0	4) }	- or	rang	le					
Eth PM IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	Vers Head Diff Tota Idem Flag Frag Time Proto Head 00 00 00 00	t Plot ion: 4 ir leng irentia ificat ificat is: 0x04 if 0x04 if 0x04 if 0x04 if 0x04 if 0x04 if 0x04 if 0x04 if 0x04	th: 20 bj ted Serv h: 84 ion: 0x00 (Don't 1 fset: 0 e: 63 OMP (0x0) ksum: 0x0 c 7d 04 0 40 00 0 cf 7f	(; 192.1 ytes ices Fie 000 (0) Fragment p 1 00 c0 S 3f 01 e 86 0b 0	<pre>cld: 0x cld: 0x c</pre>	gree	. 166. U. CP 0x00 en 8 00 4 0 16 8 f 43 c	27), 0 1: Defa 1 78 7 2c	st: 1 ult;]	ECN: 0	.9,15 x00)	(00:a0:	d2:1c:7d:0	4) }	- or	rang	le					1. (1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1
Eth PM IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	Versi Head Diffi Total Ident Flag: Frag Frag Frag OO 00 00 00 00 00 00 00 00	t Plot ion: 4 ir leng irentia ificat ificat is: 0x04 if 0x04 if 0x04 if 0x00 if 0x00 0x000 if 0x00	th: 20 bj ted Servi h: 84 ion: 0x00 (Don't 1 fset: 0 e: 63 OMP (0x0) ksum: 0x0 c 7d 04 0 40 00 0 40 00 0 40 00	xtes ices Fie 000 (0) Fragment 00 c0 S 3f 01 e 86 0b 0 0c od 0	<pre>ces.u. 2 cld: 0xi cld: 0x</pre>	gree 7 30 0 6 0 12 7 30 0 6 0 12 0 11 1	.166.0. CP 0x00 en 8 00 4 0 16 8 f 43 c 2 13 1	27), 0 0: Defa 1 78 7 2c 4 15	st: 1 wlt;]	51.187 ECN: 0	.9.15 x00)	(00:a0:	d2:1c:7d:0	4) }	- or	rang	le					Transfer 14 mar 1/2 1/2
Eth 200 10 10 10 10 10	Versi Head Diffi Total Ident Flag: Frag Time Proto Head 00 00 00 00 00 00 00 00 00 00 00 00 00	t Plot ion: 4 ir leng irentia Lengt Lengt to liv col: 1 ir chec if 0 8 0 00 08 0 00 08 0 7 18 1	th: 20 bj ted Serv h: 84 ion: 0x00 (Don't 1 fset: 0 e: 63 OMP (0x0) ksum: 0x0 c 7d 04 0 40 00 0 cf 7f	192.1 ytes ices Fie 000 (0) Fragment 1) 2) 2) 2) 2) 2) 3) 2) 3) 2) 2) 2) 2) 2) 2) 2) 2) 2) 2) 2) 2) 2) 2) 2) 2) 2) 3) 2)	<pre>cld: 0xi cld: 0x</pre>	gree 7 30 0 6 6 0 1 2 0 1 1 1 0 21 2	-166.0. CP 0x00 en 6 00 4 6 15 8 7 43 c 2 13 1- 2 23 2	27], 0 0: Defa 1 78 7 2c 4 15 4 25	st: 1 wlt; .T.0	51.180 ECN: 0	.0E.	(00:a0: (151.12	d2:1c:7d:0	4) }	• or	rang	le					(c) 1 an ((s) 1(c) 1)
Eth 200 10 20 20 20 20 20 20 20 20 20 20 20 20 20	Versi Head Diffe Tota Ident Flag Frag Frag Frag OO 00 00 00 00 00 00 00 00 00 00 00 00	t Plot ion: 4 ir leng irentia ificat ificat ificat icon ion ion ion ion ion ion ion ion ion i	th: 20 by ted Serv h: 84 ion: 0x00 (Don't 1 fset: 0 04P (0x0 ksum: 0x0 c 7d 04 0 0 0 0 cf 7f 9 0a 0b 9 1a 1b	c: 192.1 ytes ices Fie 000 (0) Fragment 10 10 10 10 10 10 10 10 10 10	<pre>cld: 0x1 cld: 0x</pre>	gree 7 30 (0 0 48 (6 01 2 0 11 1 0 21 2 0 31 3	-166.0. CP 0x00 en 6 00 4 6 15 8 7 43 c 2 13 1- 2 23 2	27], 0 0: Defa 1 78 7 2c 4 15 4 25	st: 1 wlt; .T.0	91.120 ECN: 0	.0E.	(00:a0: (151.12	d2:1c:7d:0	4) }	- or	rang	le					1 (1) 1 (1) (1) (1) (1) (1) (1)

Part 2

D.7.2. NAT 1

The following is a snapshot of the packets captured on the NAT 1 when the four interfaces were pinged from Router.

- 12		0	0		B	2	x	ê	д		4		8 T	4			٢	Θ	Q	m	2		9	X	6
		-		-	-	ω		•₩	-						-	-	~	~	~	-	-		MC 0	19.1	a
Şker:	_	_				_	_			_	•	Express	ion Ø	w Boh	Y										_
W. +		ne	22.0	Source			_		sation				i info	and all		1000									
	nunu	.000	Address	192.1	68,100			-	268.1	00,130		ARP		168,100							0				_
	30	.000	124	192.1	68.0.2	1		192.	168.1	88.00		IOF	Lcho	(ping)	reque	tst.		1000	19922						
		.000		192.1					168.0			ICMP ICMP	Echo	(ping)	reply	0									
		,000			68.0.2 68.100				168.0			100	Echo	(ping) (ping)	reque	151									
	71	.999	646	192.1	68.0.2	7		192.	168,1	00,88		IONP	Echo	(ping)	reque	ist									
		,999 ,999		192.1	68.100				168.0			ICMP ICMP		(ping) (ping)											
		.999			68.100				168.0			IOW		(ping)											
	11 4	, 998	100	192.1	68.100	. 88		192.	168,1	00.130		ARP	Who	has 192	.168.3	100.13					8				
	12 4	.998	792	192.1	68.100	.130		192.	168.1	88.00		ARP	192.	168,100	.130 1	s at	0100	19510	91071	1					
				s on w						7:31).	Det:	Broade	ast (ff	didi		:#)						_	_	_	_
Eth D	erne esti	t II nati	, Src on: D	: 192.: roadca:	168.100 st (ff	.130	(00 f :ff	:c0:95	:c9:0)	7:31),	Dst:	Broado	ast (ff	iffiff	:#:#	:#)							_		_
Eth D S	erne esti ourc	t II nati e: 1	, Src on: 8 92.16	: 192.: roadca: 8.100.:	168.100 st (ff	.130	(00 f :ff	:c0:95	:c9:0)	7:31),	Dst:	Broado	ast (ff	iffiff	:11:11	:#)		_	_						
Eth D S T	erne esti ourc ype:	t II nati e: 1 ARP	, Src on: B 92.16 (0x0	: 192.: roadca: 8.100.: 806)	168.100 st (ff 130 (00).130 (ff:f):c01	(00 f :ff 95 :c	:c0:9! :ff:fi 9:07:	:::9:0 ?) 1)	7:31),	Dst:	Broadc	ast (ff	ittitt	:11:11	:#)									
Cth D S T T	erne esti corc ype: rail	t II nati e: 1 ARP er:	, Src on: 8 92.16 (0x0 00000	: 192.: roadca: 8.100.:	168.100 st (ff 130 (00).130 (ff:f):c0:	(00 f:ff 95:c	:c0:9! :ff:fi 9:07:	:::9:0 ?) 1)	7:31),	Dst:	Broadc	ast (ff	attatt	:11 :11	:ff)		_							
Cth D S T T	erne esti corc ype: rail	t II nati e: 1 ARP er:	, Src on: 8 92.16 (0x0 00000	: 192.: roadca: 8.100.: 806) 0000000	168.100 st (ff 130 (00).130 (ff:f):c0:	(00 f:ff 95:c	:c0:9! :ff:fi 9:07:	:::9:0 ?) 1)	7:31),	Dst:	Broadc	ast (ff	ittitt	:11 :11	:ff)									_
Cth D S T T	erne esti corc ype: rail	t II nati e: 1 ARP er:	, Src on: 8 92.16 (0x0 00000	: 192.: roadca: 8.100.: 806) 0000000	168.100 st (ff 130 (00).130 (ff:f):c0:	(00 f:ff 95:c	:c0:9! :ff:fi 9:07:	:::9:0 ?) 1)	7:31),	Dst:	Broadc	ast (ff	attatt	:11 :11	:ff)									
Eth D S T T E Add	erne esti ourc ype: rail ress	t II nati e: 1 ARP er: 1 Res	, Src on: 8 92.16 (0x0 00000 oluti	: 192.1 roadca: 8.100.1 806) 0000000 on Prot	168.100 st (ff 130 (00 1000000 tocol (0.130 iffif 01:00: 00000 (requ	(00 fiff 95ic 00000 est)	:c0:9 :ff:f 9:07: 000000	100000	01			1	uttutt	aff aff	:#f)									
Eth D S T T E Add	erne esti ourc ype: rail ress	t II nati e: 1 ARP er: Res	, Src on: 8 92.16 (0x0 00000 00000 010tin	: 192.; roadca: 8.100.; 8060 0000000 00 Prot	168.100 st (ff 130 (00 1000000 tocol (0 c0	0.130 iff if 0:c0: 00000 (requ 05 c3 95 c9	(00 fiff 951c 00000 est)	:c0:9 :ff:ff 9:07:: 000000	100000	01			1 1d.	uff aff	aff aff	:#)									_
Eth D S T T E Add	erne esti ourc ype: rail ress	t II nati e: 1 ARP er: Res	, Src on: 8 92.16 (0x0 00000 01utin	: 192.1 roadca: 8.100.1 806) 0000000 on Prot	168.100 st (ff 130 (00 1000000 tocol (0 c0 0 c0 0 a8	0.130 iff:f 0:c0: 000000 iff:f 0:c0: 000000 iff:f 0:c0:	(00 fiff 95ic 00000 est) 07 07	200 : 91 200	100000	01			1 1d.	uffuff	uff off	:#f)									
Eth D S T T E Add	erne esti ourc ype: rail ress	t II nati e: 1 ARP er: Res	, Src on: 8 92.16 (0x0 00000 01utin	: 192.; roadca: 8.100.; 806) 0000000 on Prot 6 ff 0 0 01 0 0 00 c	168.100 st (ff 130 (00 1000000 tocol (0 c0 0 c0 0 a8	0.130 iff:f 0:c0: 000000 iff:f 0:c0: 000000 iff:f 0:c0:	(00 fiff 95ic 00000 est) 07 07	200 : 91 200	100000	01		d(.	1 1d.	uff aff	aff aff	:#)									
Eth D S T T E Add	erne esti ouro ype: rail ress 08 0 00 0 00 0	t II nati e: 1 ARP er: 1 Res 0 06 0 00 0 00	, Src on: 8 92.16 (0x0 00000 blutin 04 0 00 0 00 0	: 192.; roadca: 8.100.; 806) 0000000 on Prot 6 ff 0 0 01 0 0 00 c	168.100 130 (00 130	0.130 cff :f 0:c0 : 0:0000 (required) 0:5 c3 0:5	(00 fiff 951c 00000 est) 07 00 00	200 : 91 200	100000	01		d(.	1 1d.	dfaff	df df	:#)									

Figure 62. Test 6: Scenario 1 Packet Capture on NAT 1 (pinged from Router)

D.7.3. Analysis

Figures 60 to 62 indicate similar behaviors when the four interfaces were pinged from the Router instead of NAT 2. The Router could ping 192.168.0.130, 192.168.100.130 and 192.168.100.88 for the reason explained in D.6.3. Pinging 131.120.9.15 from the Router had a different behavior than the one seen when it was pinged from NAT 2 such that the Echo requests never had their time-to-live exceeded. Each of the four Echo requests was routed between 192.168.0.27 and 192.168.0.130 twice (yellow and orange outlines in Figure 60 and Figure 61). Each request was routed from 192.168.0.27 first and then XTS-400 routed it back to 192.168.0.130 (Router) as soon as XTS-400 received it. The decrement in the time-to-live field indicated that the same request was routed back and forth (green outlines in Figure 60 and Figure 61). The request was not routed further when the Router received it because the Router recognized its own packet and thus, stopped routing it. As a result, NAT 1 never saw the Echo requests as shown in Figure 62.

E. Scenario 2

E.1. Description

The MLS server is configured in order as follows: any packets received on its MLS LAN interface (eth0, 192.168.0.130) is forwarded to the single-level interface of NAT 1 (eth1, 192.168.100.88) and any packets received on its single-level interface (eth1, 192.168.100.130) is forwarded to the public interface of Router (eth0, 192.168.0.27).

E.2. Operations

First, NAT 2 pings:

- 1. eth0 of MLS server
- 2. eth1 of MLS server
- 3. eth1 of NAT 1
- 4. eth0 of NAT 1

Then, Router pings:

- 5. eth0 of MLS server
- 6. eth1 of MLS server
- 7. eth1 of NAT 1

8. eth0 of NAT 1

E.3. Network Configuration on MLS Server

E.3.1. Type the following answers when prompted:

	SAK	
	Enter command?	tcpip_edit
	Enter editor request?	add
	Enter TCP/IP daemon name?	tcpip_mls
	Enter TCPIP/IP daemon description?	TCP/IP for MLS LAN
net	work	
	Enter domain name?	cisrlabmlstestbed1.com
	Enter host name?	mlsserver
	Enable the subnets local flag?	n
	Enable the IP forwarding flag?	У
	Enable the IP send redirect flag?	У
	Enable the shutdown on failure flag?	n
	Use default TCP maximum retransmission?	у
	Add the network interface configuration?	У
	Enter TCP/IP device name?	/dev/ether0
	Enter interface address?	192.168.0.130
	Enter destination address?	0.0.0.0
	Enter broadcast address?	192.168.0.255
	Enter network mask?	255.255.255.0
	Add another network interface entry?	У
	Enter TCP/IP device name?	/dev/ether1
	Enter interface address?	192.168.100.130
	Enter destination address?	0.0.0.0
	Enter broadcast address?	192.168.100.255
	Enter network mask?	255.255.255.0
	Add another network interface entry?	n
	Add the route configuration?	У
	Enter TCP/IP device name	/dev/ether0

Is this route a default route	n
Enter destination address	0.0.0.0
Is destination address a host	n
Enter gateway address	192.168.100.88
Enter route metric	1
Add another network route entry	У
Enter TCP/IP device name	/dev/ether1
Is this route a default route	n
Enter destination address	0.0.0.0
Is destination address a host	n
Enter gateway address	192.168.0.27
Enter route metric	1
Add another network route entry	n
Add the resolver configuration?	n

E.4. Preparation and Testing

E.4.1. On NAT 1,

E.4.1.1.	Launch	1 Ethe	real

- E.4.1.2. Go to the Capture menu
- E.4.1.3. Go to Interfaces
- E.4.1.4. Click on Capture 192.168.100.88

E.4.2. On Router,

- E.4.2.1. Launch Ethereal
- E.4.2.2. Go to the Capture menu
- E.4.2.3. Go to Interfaces
- E.4.2.4. Click on Capture 192.168.0.27

E.4.3. On NAT 2,

E.4.3.1. Run the following commands:

ping -c 4 192.168.0.130

- ping -c 4 192.168.100.130
- ping -c 4 192.168.100.88
- ping -c 4 131.120.9.15

E.4.4. Repeat the above commands on the Router

E.4.5. Stop Ethereal captures on both NAT 1 and Router

E.5. Result

Table 12 lists the result of the Scenario 2. The first column shows where the ping was initiated and the first row shows what hosts/IP addresses were pinged. NAT 2 was unable to ping any of the four IP addresses.



Table 12.Test 6: Scenario 2 Result

E.6. Packet Capture when pinged from NAT 2

E.6.1. Router

The following is a snapshot of the packets captured on the Router when the four interfaces were pinged from NAT 2.

a F		(from NAT 2) - Etheres Capture Analyze Statist			
-					
er:				 Expression 	n Geer Apply
4	Time	Source	Destination	Protocol	
-0	2 2.514332	192.168.0.27 192.168.0.130	224.0.0.251 Broadcast	ARP	Standard query response A 192.168.0.27 PTR localhost.local Who has 192.168.0.1307 Gratuitous ARP
	3 6.224379	192.168.0.27	Broadcast	ARP	Who has 192.168.0.130? Tell 192.168.0.27
	4 6.224487	192.168.0.130	192.168.0.27	ARP	192.168.0.130 is at 00:c0:95:c9:07:30
	5 6.224497	192.168.202.11	192.168.0.130	TONP	Echo (ping) request
	6 7.223589	192.168.202.11	192.168.0.130	IONP	Echo (ping) request
	7 8.223442	192.168.202.11	192.168.0.130	IOMP	Echo (ping) request
	8 9.223295	192.168.202.11	192.168.0.130	ICMP	Echo (ping) request
		192.168.202.11 192.168.202.11	192.168.100.130 192.168.100.130	ICMP	Echo (ping) request
		192.168.202.11	192.168.100.130	IONP	Echo (ping) request Echo (ping) request
		192.168.202.11	192.168.100.130	ICMP	Echo (ping) request
		192.168.202.11	192.168.100.88	ICMP	Echo (ping) request
-		192.168.202.11	192.168.100.88	ICMP	Echo (ping) request
		192.168.202.11	192.168.100.88	ICMP	Echo (ping) request
		192.168.202.11	192.168.100.88	ICMP	Echo (ping) request
		192.168.0.27	192.168.0.130	ARP	Who has 192.168.0.1307 Tell 192.168.0.27
1	18 44.461658	192.168.0.130	192.168.0.27	ARP	192.168.0.130 is at 00:c0:95:c9:07:30
1	19 55.189197	192.168.202.11	131.120.9.15	ICMP	Echo (ping) request
		192.168.202.11	131.120.9.15	ICMP	Echo (ping) request
100		192.168.202.11 s on wire, 98 bytes	131.120.9.15 cantured)	TCMP	Frho (nina) request
Ethe	ernet II, Src	: 192.168.0.27 (00:8	0:d2:1c:7d:04), Dst: 1		130 (00:c0:95:c9:07:30)
		1, Src: 192.168.202.	.11 (192.168.202.11), 0)st: 192.1	58.0.130 (192.168.0.130)
V	ersion: 4				
H	eader length:	20 bytes			
E D	ifferentiated	Services Field: 0x	00 (DSCP 0x00: Default:	ECN: 0x0	0)
To	otal Length:	84			
I	dentification	: 0x0000 (0)			
	lags: 0x04 (0	on't Fragment)			
¥ F	ragment offse				
	ime to live:				
Fr					
Fr		(0,01)			
Fr T Pr	rotocol: ICMP				
Fr T Pr	rotocol: ICMP	(0x01) m: 0xefca [correct]			
Fi Ti Pi Hi	rotocol: IOMP eader checksu	m: Oxefca [correct]	4 04 08 00 45 00		
Fi T Pi Hi 20 (rotocol: ICMP	m: Oxefca [correct]		0}. .8.?	
Fr T Pr Hi 20 (rotocol: ICMP eader checksu 00 c0 95 c9 0 00 54 00 00 4 00 82 08 00 8	m: Oxefca [correct] 7 30 00 a0 d2 1c 7 10 00 3f 01 ef ca cl 5 ba 16 0c 00 00 b	0 a8 ca 0b c0 a8 .T. 1 2c 2f 43 56 c6		
Fr Pr Hi 10 0	rotocol: IOMP eader checksu 00 c0 95 c9 0 00 54 00 00 4 00 82 08 00 8 Da 00 08 09 0	m: Oxefca [correct] 7 30 00 a0 d2 1c 7 10 00 3f 01 ef ca cl 15 ba 16 0c 00 00 b 1a 0b 0c 0d 0e 0f 10	0 a8 ca 0b c0 a8 .T. 1 2c 2f 43 56 c6 0 11 12 13 14 15		/cv.
Fi Pi Hi 0 0	rotocol: IOMP eader checksu 00 c0 95 c9 0 00 54 00 00 4 00 82 08 00 8 0a 00 08 09 0 16 17 18 19 1	m: Oxefca [correct] 7 30 00 a0 d2 lc 7 0 00 3f 01 ef ca c 5 ba 16 0c 00 00 b va 0b 0c 0d 0e 0f 1 a 1b 1c 1d 1e 1f 2	0 a8 ca 0b c0 a8 .T. 1 2c 2f 43 56 c6 0 11 12 13 14 15 0 21 22 23 24 25	.0.?	/Cv. *#\$%
FI T P H	rotocol: IOMP eader checksu 00 c0 95 c9 0 00 54 00 00 4 00 82 08 00 8 0a 00 08 09 0 16 17 18 19 1 26 27 28 29 2	m: Oxefca [correct] 7 30 00 a0 d2 1c 7 10 00 3f 01 ef ca cl 15 ba 16 0c 00 00 b 1a 0b 0c 0d 0e 0f 10	0 a8 ca 0b c0 a8 .T. 1 2c 2f 43 56 c6 0 11 12 13 14 15 0 21 22 23 24 25		/Cv. *#\$%
FI T P H O O O O	rotocol: IOMP eader checksu 00 c0 95 c9 0 00 54 00 00 4 00 82 08 00 8 0a 00 08 09 0 16 17 18 19 1 26 27 28 29 2	m: Oxefca [correct] 7 30 00 a0 d2 1c 7 6 00 3f 01 ef ca cl 5 ba 16 0c 00 00 b a 0b 0c 0d 0e 0f 11 a 1b 1c 1d 1e 1f 2 a 2b 2c 2d 2e 2f 3	0 a8 ca 0b c0 a8 .T. 1 2c 2f 43 56 c6 0 11 12 13 14 15 0 21 22 23 24 25	.0.?	/Cv. *#\$%

Figure 63. Test 6: Scenario 2 Packet Capture on Router (pinged from NAT 2)

E.6.2. NAT 1

The following four figures are snapshots of the packets captured on NAT 1 when the four interfaces were pinged from NAT 2.

	i		9(0	Â	¥.	6) (1	x	R	1	3	9	4		\$	0	Ŧ	1	ł		7	(Ð	Q	Q			7	Y		X		0			
Elter	.[-									-			•	Eppre	ssion	g	ear	Apply	017000				_				-						-		
No	2	In		-	0	urce	-	_	-	-	De	tinati					Proto	end i	Infa	<u>.</u>		-		-	-	-	-		-	-				-	_	^		
-	244		434		13	14.1					13			c. 11			LUNE		ELIN																-			
		3.				2.1								2.11			ICMP		Echo Echo																			
		3.				2.1								2.11			ICMP		Echo																			
		3.				2.1								2.11			ICMP		Echo																			
						2.1				-			_	2 11			T(MP		Echo					-	-	-	-	-	-	-	-	_	_		-	H	٦	1
		1				12 1								2.11		_	TCMD		Scho																		J	ł
		3.				2.1								2.11			ICMP		Echo																			,
		3.				2.1								2.11			ICMP		Echo Echo																			
		3.				2.1								2.11			ICMP		Echo																			
	256	3.	240	83	19	2.1	68.0	.130)		19	2.16	8.20	2.11		-	ICMP	ŝ.	Echo	(pi	ng)	repl	ÿ.															
		3.				2.1								2.11			ICMP ICMP		Echo Echo																			
		2.				2.1						10					CONP.		ECHO					16		0	ve e	NCER.		n t	àns:	Ð						
		4.				2.1								2.11			ICMP	ų –	Echo	(pi	ng)	repl	ÿ –															
	-	4.				2.1					-			2.11			ICMP		Echo																			
		4.	000	_	-	2.1	-	-						2.11			ICMP		Echo Echo																			
		4.				2.1								2.11			ICMP		Echo																	v		
3 I 3 8	Ver Hei Dif Tot Ide Fli Fri	net sio der fer al enti ags:	Pro n: 4 ler enti Leng fica OxC	took ateo th: tion 4 (C	20 5 20 84 1: 0 20 1: 0 20 1: 0	Src: byt rvic x2dt t Fr	tes tes	2.16 Fiel 1171	8.0 d: 1)	130 1×00	(19 (D9	2.16	8.0.		, D5	t: 1	92.1	68.	202.1				:ef:a 202.1		']	. (ora	nge	*							The second		
	Pro Hei	otoc ader	che	ICMF cksu) (0 .m:	0xf8	ob.		rec		**	0.00	47	~~					-																	1		
000 010 020 030 040	00	54 a 0b a 00 5 17	2d 00 08 18	00 8 09 0 19 1	40 0 bd b Da 0	0 09 a 16 b 00 b 10	9 01 5 00 5 00 5 00	f8 00 06 16	00 00 0f	c0 b1 10 20	a8 (2c 2 11 1 21 2	8 00 0 82 f 43 2 13 2 23 2 33	c0 56 14 24	a8 c6 15 25		.e.		,/	CV.																	< minute (>		

Figure 64. Test 6: Scenario 2 Packet Capture on NAT 1 (pinged from NAT 2), Part 1

	čor	Yew	Ã0	^z ahinis	- 20	ay <i>u</i> o	2(4)5	ocs	Ωeh																						_		
		01			6	•		X (31	9	9	4	-	Ŕ) 7	5 1	Ł			0		20	2	**					K	0			
Eiter:												•	Ē¢	ressio	n (gear	Apply	r															
No	I	ine i		Souro	ė				Destina	tion			Pro	tocol	Info).															٨		
		.7234		192.					192.1				10					repl															
_		.7235		192.					192.1	227.00	No. of Pr		IC	qp	Ech	0 (p	ing)	repl	y												a		
		.7235		192.					92.1				10 10					repl													-		
_		.7236		192.					192.1				10					rep]															1
_		.1231									12.11		10		ECN	0 (p	1 <i>ng)</i>	repl	ý –												T	1	Ł
		.7230		192. 192.					92.1		2.11		10 10					repl													-	1	J
		.7238		192.					192.1				10					repl															
	254 3	.7239	74	192.	168.0	.130			192.1	68.2	2.11		IC	ΝP	Ech	0 (p	ing)	repl	ý –														
_		.7239		192.					192.1 192.1				10					repl repl															
1 million (1997)		.7240		192.					192.1				10					repl															
		124	<u>%</u>	1927	1001	111	_	-	<u>, 11</u>	0012	1.11		10	1		1		1 4	5			191						-				1]
_		17242				00.8		_	192.1		130		10		_	_	_		eeded	(Tia	ie to	TV	e exc	eede	d tr	tre	isit)					J	ł
		.7091		192.					192.1				10					repl)
		.7092		192.	1000	0000					2.11		10		Ech	0 (p	ing)	repl	y .														
		.7092		192.					192.1		2.11		10 10					repl															
е е С	Versi Heade Diffe Total Ident Flags Frage Time Proto Heade	er ler erenti Leng tifica s: OxC ment c to li to li to li to li to 20 54 2d	agth: ated offse we: IOMP ecksu	20 by Servi 34 : 0x2i 34 : 0x2i 34 : 0x2i 34 : 0x2i 34 : 0x2i 34 : 0x2i 33 : 0x0i 33 : 0x0i 33 : 0x0i 33 : 0x0i 34 : 0x2i 34 : 0x2i 35 : 0x2i 34 : 0x2i 35 : 0x2i : 0x2i 35 : 0x2i 35 : 0x2i 35 : 0x2i 35 : 0x2i : 0x2: 0 : 0x2: 0 : 0x2: 0 : 0x2: 0 : 0x2: 0 : 0 : 0 : 0 :	vtes ices dbf (Fragn 1) f90b 	Field (11711 (corr (corr (f9	i: 0x () ree ef a	00 (n	05CP	0x00	00 a8	ault;		: 0x0	0)			100.				ora									1. (> 1< 1.		
0030 0040 0050	16 1 26 1	17 18	19 1 29 2	a 16 : a 26 :	1c 10 2c 20	1e 2e	1f 2 2f 3	0 21	22 2	3 24	25		 *+,-	1	*#\$\$																1		
	un Mil	Ci Ola	010.00	milal	6 J Ci	-0010	1000	niv						_										_	_	_					11		

Capture on NAT 1 (pinged from NAT 2), Part 2 Test 6: Scenari 2 Pac

			♦ ♥ ₹ ½ ■ ■ Q Q Q ™ ₩ M ₩ % Ø	
ijker:			Expression Gear Apply	
io Time	Source	Destination	Protocol Info	
2049 23.216374	192.168.100.130	192.168.202.11	IOMP Echo (ping) reply	
2050 23.216473	192.168.100.130	192.168.202.11	ICMP Echo (ping) reply	
2051 23.216485 2052 23.216584		192.168.202.11 192.168.202.11	ICMP Echo (ping) reply ICMP Echo (ping) reply	
	192.100.100.150	192.169.100.130	IONP Time-to-live exceeded (Time to live exceeded in transit)	
2054 29.968321		192.168.100.130	ARP Who has 192.168.100.1307 Tell 192.168.100.88	
2055 29.968414	192.168.100.130	192.168.100.88	ARP 192.168.100.130 is at 00:c0:95:c9:07:31	
	192.105.202.11	192.105.100.00	zow Ecit (ping) repose	٦
2057 36.948651	192.168.100.88	192.168.202.11	IONP Echo (ping) reply Ione Echo (ping) reply	J
2059 37.947973	192.168.202.11	192.168.100.88	IONP Echo (ping) request	
2060 37.948058	192.168.100.88	192.168.202.11	IOMP Echo (ping) reply	
	192.168.100.88	192.168.202.11	ICMP Echo (ping) reply	
	192.168.202.11	192.168.100.88	ICMP Echo (ping) request	
	192.168.100.88 192.168.100.88	192.168.202.11 192.168.202.11	ICMP Echo (ping) reply ICMP Echo (ping) reply	
	192.168.202.11	192.168.100.88	IOMP Echo (ping) request	
	192.168.100.88	192.168.202.11	IOMP Echo (ping) reply	
	192.168.100.88	192.168.202.11	ICMP Echo (ping) reply	
2068 52.674292 2069 52.674413	192.168.202.11	131.120.9.15 192.168.202.11	IOMP Echo (ping) request IOMP Echo (ping) regly	
	wtes on wire, 98 hvt			
y Internet Protoco VersioN+ 4 Header length Differentiate Total Length: Identificatio ■ Flags: 0x00 Ecoment offs Time to live: Protocol: ION Header checks 000 00 c0 95 c9 010 00 54 cc ac 200 ca 0b 00 00 030 0e 00 08 09	<pre>>1, SrC: 192.108.100. 20 bytes d Services Field: 0x0 84 n: 0xecac (60588) et: 0 64 9 (0x01) gre 10; 0xde47 [correct] 07 31 00 0c 41 ef a</pre>	en 10 (DSCP 0x00: Default; en 5 eb 08 00 45 00 2 2c 2f 43 50 6c 11 12 13 14 15	192.168.100.130 (00:00:95:c9:07:31) orange t: 192.168.202.11 (192.168.202.11) ECN: 0.00) 1AE. ,(PP1 ,(PP1 ,(P1)	

Figure 66. Test 6: Scenario 2 Packet Capture on NAT 1 (pinged from NAT 2), Part 3

IJ	-		1	¥		1	3		1	X	R) {		[9	4	-	\$	0	3	ł	1			ļ	1	0	Q	0			X	¥		X	2	0		
jter:].		Dore	ssion	h., (lear	App	hj																
ib. +		Ine			Sourc	8	_	_	_		De	stina	tion			-	1	Proto	col	Info		_		_	_		_	_	_	_	_	_	_	_	_	_		٨	
2	349	23.2	1637	4	192.	168	.10	0.1	0		19	2.1	58.2	02.	11		3	ICMP		Ech	0 (ping)) re	eply															
	00150		1647	5	25.27	000	0.000	1000	25-0				58.2					IONP				ping																	
			1648 1658		192. 192.								58.2					ICMP				ping																	
-	152	0.0	1020	-	192.	223		1.00	-			1111	58.2	-		-	_	ICHP			-	ping)	-	pry	ener	16	144	to	tvé	e de la	515		rans	a.					
2	054	29.9	6832	1	192.	168	.10	0.8	}				58.1			10		ARP		Who	hà	5 19	2.16	68.1	00.1	30?	Te	11 1	92.1	68.10	0.88	8						1	
			6841		192.								58.1					ARP				8.100				00	:c0:	95:0	9:07	:31									
2	256	36.9	4853	1	192.	168	.20	2.1			19	2.1	58.1	00.	88		_	IONP		Ech	0 ()	ping) 11	eque	st														
3	613	6.9	1875	i	192	113	51				10	2.1		02				IONP	8	Ech	i	0100	1 re	in lu															
			17.97	-		-			_		-						_	C.	-	1000	-	ping	-	1	st		-									-		-	-
			4805		192.								58.2					ICMP		Ech	0 (ping) re	eply															
	1000	2000	4815	2	192.		-	2000					58.2					IONP				ping																	
			4781 4790		192.								58.1 58.2					ICMP ICMP				ping) ping																	
			4800										58.2					ICMP				ping																	
2	065	39.9	4766	7	192.	168	.20	2.1					58.1					ICMP		Ech	0 (ping) 1	eque	st														
			4775										58.2					ICMP				ping																	
			4785 7429										58.2 20.9					IONP				ping																	
			7441						•				58.2					ICMP				ping) ping																v	
	110	110	198		1922		112	1	R k	iter	. 63	ntu	(har		19.5	_	-	0-m	-		010	50610		10.09	_	-	7	_	_	_	_	_	_	_	_	_	-		
3 In 8 8	tern Vers Head Diff Tota Iden Flag Frag Time	et F ion: erer l Le tifi s: (ment to ocol	roto 4 engt tiat ngth cati	col h: ed on: set : 6	, Sr 20 b Serv 4 0xe : 0 3	c: yte ice cac	192 s F (6	.168 ield 0588	.10 :: 0)).88 400 gre	(DS	92. CP (168.	100	.88), D	st:	192	2.16	8.20		(00: 11 (1						0	ran	ge								 10 10 	
020 030 040	00 ca 0e 16	54 8 06 0 00 0	1 ef c ac 0 00 8 09 8 19 8 29	00 99 0a 1a	00 14 05 1b	3f 1c 0c 1c	01 0c 0d 1d 2d	00 0e 1e 2e	47 00 of 1f 2f	c0 d2 10 20	ht 1 11 1 21 1	45 f4 21 22	3 14) 88) 60 15 25	:	.T)(50 /	dx /CP1																		(se) tertained (se)	

Figure 67. Test 6: Scenario 2 Packet Capture on NAT 1 (pinged from NAT 2), Part 4

E.6.3. Analysis

NAT 2 failed to ping 192.168.0.130 and 192.168.100.130. Figure 63 show that the Router did not see any Echo replies from 192.168.0.130 or 192.168.100.130. However, it is evident that 192.168.0.130 and 192.168.100.130 replied since NAT 1 saw them (red outline in Figure 64). If routing was done correctly, the Echo replies should have been sent to the Router and then to NAT 2 instead of to NAT 1. Instead, MLS server sent the Echo replies to NAT 1. Figure 65 indicated that when NAT 1 received the Echo replies, it sent them to next hop (192.168.100.130) based on its routing table (yellow and orange outlines in Figure 65). However, XTS-400 forwarded the replies back NAT 1 at 192.168.100.88 (yellow and orange outlines in Figure 64). Hence, Echo replies were bounced back and forth between 192.168.100.130 and 192.168.100.88 until the time-to-live field reached zero (blue outline in Figure 65). This sequence of events also occurred for the Echo requests from 192.168.202.11 to 192.168.100.130.

NAT 2 also failed to ping 192.168.100.88 and 131.120.9.15. Figures 66 and 67 show that there exists two Echo replies for each Echo request destined for 192.168.100.88 and 131.120.9.15. For each Echo request destined for 192.168.100.88, NAT 1 responded with an Echo reply which is sent to its next hop at 192.168.100.130 (orange outline in Figure 66). However, the same Echo reply was bounced back by XTS-400 to where it came from when XTS-400 received it (yellow and orange outline in Figure 67). NAT 1 stopped routing the Echo reply further since it recognized its own packet. This explains why NAT 2 was never able to receive any replies. The same was true when NAT 2 pinged 131.120.9.15.

E.7. Packet Capture when pinged from Router

E.7.1. Router

The following is a snapshot of the packets captured on the Router when the four interfaces were pinged from the Router.

	4			B		x	(2)	д		4		Ð 3	4			•	Θ	0		7	M	88	X	0
			en.	-	w)	200		-		1										-	-			u.
ker:				_	_	_			_		Ĉ/txes	son S	lear Bop	Y	_	_	_	_			_	_	_	_
0. +	Ter	e	Source				Dest	sation				ol Info												
		000000		68.0.2				168.0			ICMP		(ping)			7.11	103		410					
		000147 000177	192.1					dcast 168.0			ARP		has 19. 168.0.						.130					
		000.00				-		161.0		-	100		(ping)			100 100	**!.*!	9.04		-	-	-	-	-
		999625	192.1	68.0.1	27		192.	168.0	.130		IONP	Ech	(ping)	reque	est									
		999738	192.1					168.0			100		(ping)											
		999474 999589	192.1					168.0			ICMP		(ping) (ping)											
		999318	192.1	2000000				168.0			ICMP		(ping)											
		999444	192.1					168.0			IOP		(ping											
		934383	192.1						00.130		ICMP		(ping)											
		934499	192.1					168.0			IONP.		(ping)											
		934567 934680	192.1				10001	168.0	00.130		TON5		(ping) (ping)											
		934414	192.1						00.130		ICMP		(eing)											
		934527	192.1					168.0			IOP		(ping)											
		934260	192.1						00.130		IOP		(ping)											
		934373	192.1					168.0			IOP		(p1ng											
		.149493	192.1					168.1			100P		(ping) (ping)											
			192.1					168.1			ICMP		(ping											
			192.1					168.0			ICMP		(ping)											
			192.1					168.1			ION		(ping)											
			192,1					168.0			IONP		(ping											
2	5 15	.149468	192,1	68.0.7	17		192.	168.1	88.00		IONP	Ech	(p1ng)	reque	est									
Ethe De Sc Ty Inte	innet istin Surce /pe; innet	(98 byte II, Src ation: 1 : 192.16 IP (0x01 Protoco Control	: 192.: 92.168 8.0.130 00) 1, Src	168.0. .0.27 0 (00: 192.	130 (0 (00:a) c0:95	0:0) ;d2 ;c9:(195:0 10:17 10:17 10:17 10:17	9:07: 1:04)							11.70*									

Figure 68. Test 6: Scenario 2 Packet Capture on Router (pinged from Router)

E.7.2. NAT 1

The following is a snapshot of the packets captured on NAT 1 when the four interfaces were pinged from the Router.

T/	far.	Yen	ø	Çaphire	<u>k</u> olyze	2.ststx	s theb																	
*		0	0		6	X	1	8	9	\$	¢ 4	0 T	뢒			0	Q	Q	•		7	5	X	0
ter:										•	Express	ion Ø	nar Bop	H										
١.,	1	Time	-	Source	_	_	Dect	sation	-	-	Protoco	l Info		-	-	-	-	_	_	_	-	_	-	-
		Roto			ii.100.	W.		SHEET	-	-	The state		nas 19	-	10m	100	thesto	NT1 B	TANK B	<u>6</u>	-	-	-	-
		0,000			68,100,		-	168.10	0,130		APP	192.	168,100	0,88 1	is at i	10:00	41 tef 1	af teb						
		0.000			68.0.27	2		168.10			IOP		(ping)				100120	1000						
		0,000		192.1	68,100.	10	192.	168.0.	27		IONP		(ping)											
	5	1,0001	181	192.1	68.0.27		192.	168.10	88.0		IONP	Echo	(ping)	requ	vest									
	6	1.0001	267	192.1	68.100.	86	192.	168.0.	27		IOP	Echo	(ping)	(rep)	ly.									
		2,0000			68.0.27			168.10			ION		(ping)											
		2.000			68,100,	38		168.0.			ICMP		(ping)											
		2.999	200		68.0.27	0		168.10			ICMP		(ping)											
		2,999		100000	68,100,			168.0.			ICMP		(ping)			24,112		100-613	1.0					
		4,999			68,100,			168,10			ARP		has 197							18				
		4.9993			68.100.	130		168.10			ARP		168.10			00100	195105	10713	1					
		5.068			68.0.27			120.9.	C		100		(ping)											
	-	5.0690			20.9.15			168.0.			ICMP ICMP		(ping)											
		6.069			68.0.27 20.9.15			120.9.			IOP		(ping) (ping)											
		7.070			60.0.27			120.9.			IOIP	Licho Licho	(ping)	rep)	in at									
		7.070			20.9.15			168.0.			ION	Echo	(ping)	ren	lu lu									
		8.070		192.1				120.9.			IOP		(ping)											
		1.070			20.9.15			168.0.			IOP		(ping)											
		1 (60	, Sec	: 192.1	re, 60	130 (00	:0:99	:c9:07	':31),	Dst:	Broade	ast (ff	:ff:ff	iffit	1:11)						_		_	
[1]	hern Dest Sour Type Trai	et II inati ce: 1 : ARP ler: 0	92.16 (0x0 00000	806) 0000000	rt (ffr: 130 (00 10000000 10000000	000000	91071	1)																
Add	hern Dest Sour Type Trai dres	et II inatio ce: 1 : ARP ler: 1 s Reso ff ff 00 06 00 00	92.16 (0x0 00000 oluti 04 0 00 0	8,100,1 806) 0000000 on Prot 0 01 00 0 00 c0	130 (00 10000000 10000 (r	c01951 c000000 equest) c9 07 58 00	9:07:3 000000 31 08 31 c0 00 00	00000 06 00 48 64	82		dx	1												

Figure 69. Test 6: Scenario 2 Packet Capture on NAT 1 (pinged from Router)

E.7.3. Analysis

The Router was able to ping all four interfaces described in D.2. The Router could ping 192.168.0.130 because it shares a peer-to-peer relationship with the MLS server. It was also able to ping 192.168.100.130 because XTS-400 knew its interfaces. The same logic applied to the case when the Router pinged 192.168.100.88. The Router successfully pinged 131.120.9.15 in this scenario but not in Scenario 1. In order for this to occur, XTS-400 would have to send the Echo requests to 192.168.100.88 in order for the requests to reach 131.120.9.15. When 131.120.9.15 received the requests, it sent Echo replies to the Router by routing the packet to the next hop or the MLS server. XTS-400 had the logic to route the replies to the Router since it knew its peers.

F. Scenario 3

F.1. Description

The MLS server is configured in order as follows: any packets received on its single-level interface (eth1, 192.168.100.130) is forwarded to the single-level interface of NAT 1 (192.168.100.88) and any packets received on its MLS LAN interface (192.168.0.130) is forwarded to the public interface of the Router (192.168.0.27).

F.2. Operations

First, NAT 2 pings:

- 1. eth0 of MLS server
- 2. eth1 of MLS server
- 3. eth1 of NAT 1
- 4. eth0 of NAT 1

Then, Router pings:

- 5. eth0 of MLS server
- 6. eth1 of MLS server
- 7. eth1 of NAT 1
- 8. eth0 of NAT 1

F.3. Network Configuration on MLS Server

F.3.1. Type the following answers when prompted:

SAK

Enter command?	tcpip_edit												
Enter editor request?	add												
Enter TCP/IP daemon name?	tcpip_mls												
Enter TCPIP/IP daemon description?	TCP/IP for MLS LAN												
network													
Enter domain name?	cisrlabmlstestbed1.com												
Enter host name?	mlsserver												
Enable the subnets local flag?	n												
Enable the IP forwarding flag?	у												
Enable the IP send redirect flag?	у												
Enable the shutdown on failure flag?	n												
Use default TCP maximum retransmission?	у												
Add the network interface configuration?	у												
Enter TCP/IP device name?	/dev/ether0												
Enter interface address?	192.168.0.130												
Enter destination address?	0.0.0.0												
Enter broadcast address?	192.168.0.255												
Enter network mask?	255.255.255.0												
Add another network interface entry?	У												
Enter TCP/IP device name?	/dev/ether1												
Enter interface address?	192.168.100.130												
Enter destination address?	0.0.0.0												
Enter broadcast address?	192.168.100.255												
Enter network mask?	255.255.255.0												
Add another network interface entry?	n												
Add the route configuration?	У												
Enter TCP/IP device name	/dev/ether1												
Is this route a default route	n												
Enter destination address	0.0.0.0												
Is destination address a host	n												

Enter gateway address	192.168.100.88
Enter route metric	1
Add another network route entry	у
Enter TCP/IP device name	/dev/ether0
Is this route a default route	n
Enter destination address	0.0.0.0
Is destination address a host	n
Enter gateway address	192.168.0.27
Enter route metric	1
Add another network route entry	n
Add the resolver configuration?	n
F.4. Preparation and Testing	
F.4.1. On NAT 1,	
F.4.1.1. Launch Ethereal	
F.4.1.2. Go to the Capture menu	
F.4.1.3. Go to Interfaces	
F.4.1.4. Click on Capture 192.168.100).88
F.4.2. On Router,	
F.4.2.1. Launch Ethereal	
F.4.2.2. Go to the Capture menu	
F.4.2.3. Go to Interfaces	
F.4.2.4. Click on Capture 192.168.0.2	7
F.4.3. On NAT 2.	

F.4.3. On NAT 2,

- F.4.3.1. Run the following commands:
 - ping -c 4 192.168.0.130
 - ping -c 4 192.168.100.130
 - ping -c 4 192.168.100.88

ping -c 4 131.120.9.15

- F.4.4. Repeat the above commands on the Router
- F.4.5. Stop Ethereal captures on both NAT 1 and Router

F.5. Result

Table 13 lists the result of the Scenario 3. The first column shows where the ping was initiated and the first row shows what hosts/IP addresses were pinged. The result is exactly the same as the result obtained in Scenario 2.



Table 13.

Test 6: Scenario 3 Result

F.6. Packet Capture when pinged from NAT 2

F.6.1. Router

The following is a snapshot of the packets captured on the Router when the four interfaces were pinged from NAT 2.

ile i		cenario 3 Jew Go	Çapture				9eb																			. 6
K			-	6	6	×	96	3	9	4	ŵ I	0	Ŧ	ł				Ð,	Q,	Q	•		Y		X	0
Rer:		11. -	2.01		0.07					•	Expres	ision	Gear	Asol	Y											
0. •	Te	e	Source			(estina	tion			Protoc	al Ir	10				-		1107				_	-	-	
	1 0.	000000	192.10	8.0.1	50	1	road	cast			ARP	W	to ha	\$ 192	.168	.0.13	107	Grat	uito	is AR	P					
		407812	192.16				road		0		ARP					.0.13					0.27					
		407919	192.16					68.0.2			ARP			10017		s at	0010	0195	1091	17:30	Sale Der					
_	-	407929	192.10			_		65.0.1			LUNP	_	ha (100 C	_											
		407062 407092	192.16					68.0.1 68.0.1			ICMP		the (
		407372	192.16					68.0.1			ICMP		tho () tho ()													
			192.16					68.100			TOMP		tho (
			192.16				10000	68.100			ICMP		tho (
			192.16					68.100			ICMP		ho (
	11 22	.266449	192.16	8.202.	.11	3	92.16	68.100	.130		ICMP		:ho ()													
			192.10					68,100			ICMP		:ho ()													
			192.16					68.100			ICMP		tho (
			192.16					68.100			ICMP		:ho (
		.443091				-	1.2	68.100	000		ICMP		ho (7-11	103							
		,442183 ,442281	192.10					68.0.1			ARP					.0.1) s at					9.0					
		.508810						20.9.1			ICHP		:ho ()				wit	N 199	10.211	17 134						
		.508040						20.9.1			TOMP		tho (_											
	200.20		192.16		17.5			20.9.1			ICMP		tho (
		\$07747	197.16	R, 202	.11	1	11.12	20,9,1	5		TOMP		hn fi													
Int H C H C H C H C H C H C H C H C H C H C	ernet Versio Versio Versio Versional	II, Src Protoco n: 4 length: entiated Length: fication 0x04 (D nt offse o live: ol: ICMP checksu	1, Src: 20 byt Servic 84 : 0x000 on't Fr t: 0 63 (0x01) m: 0xef	192.1 es es Fie 0 (0) agnent	:)	.11 (192.1	168.20	2.11)	, Dst	t 192	. 168.														
00	00 2	95 c9 0		10	0 10 1	1.14	08 A	0 45 0	20			1	-	_	_	_	_	_	_	_		_		_	_	_
	00 54	00 00 4	0 00 3	01				b c0 a	18	T0.																
20	00 82	08 00 c	4 49 75	0c 0	0 00 3	14 2f	2f 4	0 61 3	14 ,																	
		0 08 09 0						3 14 1				****	-													
40		18 19 1 28 29 2						3 24 2		104																
0.2					N 81 1		46.4	1 14 1	14 14	• M. 1																
-	Route	(scenario 3	from NA	P: 30 D	: 30 M; 0)					-															

Figure 70. Test 6: Scenario 3 Packet Capture on Router (pinged from NAT 2)
F.6.2. NAT 1

The following three figures are snapshots of the packets captured on NAT 1 when the four interfaces were pinged from NAT 2.

1		Yew										-		_									1						_		174				12			
	į.	0	0		N.	6	5	6)		Ì			9	4	1	•	0	Ŧ	1					0	e	20	2	•••	è				K	0			
Elter:															•	Ę	pres	sion	. g	a A	pply																	
No. •	1	Time		s	urce	C.					Desti	nation	R.			P	rotoco	ol 1	nfo															_		^		
		0.000			- CO.	~~~		.130				idcas idcas	<u> </u>				RP RP			185 1 185 1		70.73						- C - C - C	RP 100.1	30								
	7	7.407 1.407	0.90	1		100. [6]]	200				.74	100.	100			-	en CXP		7411	(p1)		00	5 0	-											_			ľ
	7	7.400	040	4		.00.	w.	30	-	_	-	100.	-			-	Unit -	_		(pin	1.1		-	-		-	_	-	_		_	_	_			-	μ	
		3.408			100.00	168.						168.					CMP			(pin																		
		3.408 3.408				168. 168.						168.					CMP			(pin																		
		3.408				168.						168.					CMP			(pin (pin																		
		3.408				168.						168.					CMP			(pin																		
	11	3.408	385	1	92.1	168.	0.1	30			192.	168.	202	.11		1	CMP	8	cho	(pir	19)	repl	ly .															
		3.408		1								168.					CMP			(pin																		
		3.408				68.						168.					CMP			(pin																		
		3.408 3.408		1		168.						168.					OMP			(pin (pin																		
		3.408		1								168.					ONP			(pin																		
		3.408				168.						168.	_				CMP			(pin																		
		3.408				168.					-	168.		-			CMP			(pin																		
		3.408				168.						168.					CMP			(pin																		
		3,408				68.						168.					CMP			(pin																v		
B 1 C 0000 0010 0020	tern Vers Head Diff Tota Ider Flag Erar Prot Head 00 00 ca	et (r ion: ler le ierent il Ler stific (s: 0) ment i to 1 ler ch 0c 41 54 30 0b 00	otoc 4 ingth iate offs ive: IOM vecks ive: 04 (04 (04 (04 (04 (04 (04 (04 (255 eff (C 255 eff (C 255 eff (C 255 eff (C 255 eff (C 255 eff (C 255 eff (C 255 eff (C 255 eff (C 255 eff (C) 255 eff (C) 256	570 by rvi k30 t F 0 bx01 0xf 0 bx01 0xf 19 7	: 1 tes ces 42 rag) f87 f 0 c 0 f 0 c 5 0	(12 mer (12 (12 mer	eld: 354) t) 95 c ff 8 00 0	0.1: 0xi eei ct] 900 7 c0	0 (0 (1 31 31 32	050 050 00 2f	00 4 82 0 43 0	0.1 0:1 5 0 0 a	0), Defa 0 8 4	ult;	EC	92 . 11	×00)	E.	1 (1	92	.00.	202.	11)	~ĵ		anç	Je						_		and (2) (6) 1		
0030	0f 16	00 00	09	0a (1a 1	b 0	ic 0	ld .d	0e 0 1e 1	f 1 f 2	21	12 22	13 1	4 1	5			· · ·	17	ŝŝ																	*		
	-	ument	and t			1		-	2070	0.4	1					-				-	-	-	-	-	-	-	-	-	-	-	-		-	_	-	-		

Figure 71. Test 6: Scenario 3 Packet Capture on NAT 1 (pinged from NAT 2), Part 1

	ų	0			6	5	2	X	R		1	9	4	-	¢) 7	1	Ł		;	0	Q	0				Y	5	X	0	
Elker:		10100											•	£φ	ressio	n Ç	lear	Apply													
No. +	1	ine		Source	e	_	_	_	De	tination	í.	_		Pro	tocol	Info				_	_		_			_		_			^
		.0000		-	168.		-			adca				ARS					168.10												
		.4078		-	168.					adca:		.130		ARS					168.10 88 is						,130						
	4.)	.4079	11	192.	100.	1.13	V.		19	.100	eve	.11		10	۳.	ECR	, (p)	ngj	герту												
	-	.4080			168.		-			. 168	-	-		10			-		reply	_			_	_						_	
	73	.4081	52	192.	168.	0.13	0		19	2.168	202	.11		10	NP .	Echo) (pi	ng)	reply												
		.4082			168.					2.168				10					reply reply												
		.4083		2000	168.	2022				2.168				10					reply												
1	13	.4083	35	192.	168.	0.13	0			2.168				10		Echo	(pi	ng)	reply												
		.4084			168.					2.168				10					reply												
		.4084			168.					2.168				10					reply reply												
		.4086			168.					2.168				10					reply												
		.4087			168.					2.168				10		Echo	(p1	ng)	reply												
		.4087			168.					2.168				10		Echo) (pi	ng)	reply												
		.4088			168.					2.168				10					reply												
		.4088			168.					2.168				10					reply reply												
		.4089			168.					.168				TO					renly		~										۷
He Di To Id Fr Fr Ti Pr	rne sade ffe tal aps an me oto		tocol gth: ated th: 8 tion: 4 (Do ffset ve: 2 ICMP	, Sr 20 b Serv 4 : 0x3 : 0x3 : 0x3 : 0x3 : 0x3 : 0x0	c: 19 ytes ices 042 (Frage	(123 Fie (123 rent	68.0 1d: 54))	130 0×00	(19	2.168 CP Oxi	.0.1	30),	Dst:	192	.168	.202.						0	aı	ige							and the state of t
•	23			• •		÷.								_		_														_	-
010 0 020 0 030 0 040 1	10 1 (a ()f (16 1	00 d0	42 40 00 cm 09 04 19 14	00 49 00 10	fe 0: 75 0: 0c 0: 1c 1:		0 88 0 00 e 0f e 1f	c0 34 10 20	a8 0 2f 2 11 1 21 2	0 82 f 43 2 13 2 23	c0 a 61 3 14 1 24 2	8455	.TOBR	Iu.	4/	/Ca4															<
							D: 20				1.1	1	- u		11.11		_											_			122

Figure 72. Test 6: Scenario 3 Packet Capture on NAT 1 (pinged from NAT 2), Part 2

				6		X			ये (R) 7	1				Ð (Q		++	¥.	¥	X	C			
iter:										▼Đ	pressio	n (j	ear App	λy													
0, +	Time		Source			(estinatio	n		Pr	otocol	Info		_										_	^		
205	55 35.	443399		68.100				3.202.			MP	Echo	(ping) re	eply .												
		443300						. 202.		1	.nr		Chind													h	
		443052 443137	100,000	68.202 68.100	0.000			8.100. 8.202.			IMP Imp		(ping (ping													Ł	
205	59 36.	443237	192.1	68.100	.88	- 1	92.16	3.202.	11	I(MP	Echo	(ping)) re	ply	_	_	_	_	_	_	_					
		443490						100			MD		(nina													1	
		443576 443676						8.202. 8.202.			IMP Imp		(ping (ping														
		442740						3.100.			MP	Echo	(ping) re	quest												
		442825						8.202.			MP	Echo	(ping) re	ply												
		442933					0.00000	3.202.	2/201		CMP RP		(ping		ply 58,100.	1202	Tal	1 10	1.0	100.0	00						
		299353 299445						8.100. 8.100.			RP RP	1000			0 15 8						00						
		508358						.9.15			MP	Echo	(ping) re	quest												
		508484						3.202.			MP		(ping														
		508585 507578					000000	3.202.	50) - C		CMP CMP		(ping (ping														
		507661						3.202.			MP		(ping														
207	73 52.	507761	131.1	20.9.1	5			3.202.		I	MP	Echo	(ping) re	ply												
		507422						0.9.15			MP		(ping														
		507508 507620						3.202. 3.202.			CMP CMP		(ping (ping														
				68.202			0.0000000	.9.15	_	-	MP		(ping														
		507355						8.202.			CMP		(ping														
		507454 19 (98 h		70 0 1				5 202	11	1/	'ND	Coho	Inino) re	nlv										<u> </u>		
Si Si Tj Inte	ource: ype:] ernet	II, Src atio 11 : 192.16 IP (0x08) Protoco	8.100. 00) 1, Src	130 (00 : 192.1	0:c0:95	:c9:(7:31)	:eo)										nge									
100	ernet	Control	NCSSG	ye rrol	.0001																						
		41 ef a ec b9 0								A													 		^		
20	ca Ob	00 00 9	7 ff 7	b Oc (00 01 5	6 2f	2f 43	7c 7d		····{																	
30	00 00	08 09 0	a Ob O	c Od (Oe Of 1	0 11	12 13	14 15																	2		
	16 17	18 19 1	a 1b 1	c 1d .	le 1† 2	20 21	22 23	24 25 34 35			./01																

Figure 73. Test 6: Scenario 3 Packet Capture on NAT 1 (pinged from NAT 2), Part 3

F.6.3. Analysis

NAT 2 failed to ping all four interfaces. The behaviors seen in the packet captures in this section are identical to the behaviors seen in section E.5. All the Echo replies (red outline in Figure 71) from 192.168.0.130 and 192.168.100.130 were bounced between 192.168.100.130 and 192.168.100.88 (yellow and orange outlines in Figure 71 and Figure 72). As a result, the replies never reached the Router (Figure 70). As described in F.5, every Echo request destined for 192.168.100.88 and 131.120.9.15 had two Echo replies (red outline in Figure 72). The first reply went from 192.168.100.88 to 192.168.100.130. When the MLS server received the reply, the XTS-400 routed it back to 192.168.100.88. This was the reason for seeing two Echo replies per request. Refer to E.6.3 for more detail explanation.

F.7. Packet Capture when pinged from Router

F.7.1. Router

The following is a snapshot of the packets captured on the Router when the four interfaces were pinged from Router.

				8	6) x	(1)	8		4		0 7	2			0	0	0	•		Y		×	0
n. [•	Epres	ision S	har Boo	W	111									
	Ter	ie i	Source		_	-	Des	tination	_	-	Protoc	ol Info		_		_	_	_	_	_	_	_	_	
	τυ.		192.	141.07	27	-	20	.0.0.2	51.	_	NIS	Star	ndard q	Jery I	respon	58 A 1	12710	1.0.1	PIR.	locali	ost.	ocal		
		580759	-	168.0.				.168.0			1009		(ping)							199811	2010	es ils		
		580905		168.0.				adcast			ARP		has 19.						.130					
		500936 581027		168.0. 168.0.				.168.0			IOP		168.0.			100105	1101/	0104						
		589482		168.0.				.168.0			IOW		(ping)											
		589604		168.0.				.168.0			IONP	Ech	(ping)	rep	ly									
		598882		168.0				.168.0			ICMP		(ping											
		599002		168.0.	000			.168.0			IONP IONP		(ping											
_		608388 608508		168.0. 168.0.	100			.168.0			ICMP		(ping) (ping)											
		215655		168.0.				.168.1)	ICMP		(ping)											
		215771		168.10		0	192	.168.0	.27		ICMP		(ping)											
		,215229	192.					,168.1)	IONP		(ping)											
		.215343				0		.168.0			ICMP		(ping											
		.215077		168.0.		6		.168.1			IOP		(ping) (ping)											
		214926				¥.		.168.1)	IONP		(0100)											
		.215040				0		.168.0			IONP		(ping)											
20	14	,777204	192.	168.0.	27		192	.168.1	00.88		IOP		(ping)											
		777642						.168.0	0.000		IONP		(ping											
		.777385						.168.1			ICMP ICMP		(ping) (ping)											
		.777231	192.					.168.1			TOND		(ping											
		.777551						.168.0			IONP		(6110)											
ther Des Sou Typ Inter Iser Iser Iser 0 00	rnet stin urce pe: Dat in N	(124 by II, Sri ation: 1 192.1 IP (0x0 Protoco agram Pr ame Syst Se 60 0 0 0a	c: 192. 01:00: 68.0.2) 000) al, Sro natocol tem (re 00 fb (40 00 fb (168.0 169.0 100 100 100 100 100 100 100 1	.27 (00:fi a0:d): .168. Port e)	(00:a) b (01 211c: 0.27 1: 53	0:82:1 :00:56 76:04) (192. 53 (53	c:7d:0 ::00:00 168.0. 53), D	27), C st Por	ost: 2 t: 53	24.0.0	.251 (2 53) }E.			100100):fb)								
0 00	0 ft 0 01	14 e9	14 e9 (00 5a 09 6c	62 (2a 00 63 61	00 Bi 6c 6i	00 00 6f 73 00 f0	00 74		1.1 00													

Figure 74. Test 6: Scenario 3 Packet Capture on Router (pinged from Router)

F.7.2. NAT 1

The following is a snapshot of the packets captured on NAT 1 when the four interfaces were pinged from Router.

W.		-		Bole	2.8	0473	Date																		
		0		0	6	x	¢	8	9	4	\$	0	Ŧ	2				0	Q	Q	•		Y	X	Ø
jker:										٠	(). ().	ssion	QN	w 650	Y										
W. +	Time		Source				Destin	ation	_		Protoc	col 1	No												
	1 0.000	ALC: NOT THE OWNER		61.100			100.00	stast			ALP										100.1	6			
	2 0.0000			68.100					0,130		ARP			68,100		10.000	001	Oc 143	Lief 1	aftel)				
	3 0.000			68.0.2				168.1			IOP			(ping)											
	4 0.000			68.100 68.0.2				168.0			IONP IONP			(ping) (ping)											
	6 1.0000		192.1					168.0			100			(ping)											
	7 1.999			68.0.2				168.1			IOUP			(ping)											
	8 1,999			68,100				168.0			ICMP			(ping)											
	9 2.999			68.0.2				168.1			ICMP			(ping)											
	10 2.999	744	192.1	68.100	88		192.	168.0	.27		ICMP			(ping)											
	11 4,998			68,100					0.130		ARP										.100.8	18			
	12 4.998			68,100				168.1			ARP			68.100			it 00	10015	95109	10713	1				
	13 5.246			68.0.2				120.9			ICHP	_		(ping)											
	14 5.246			20.9.1				168.0			IOP			(ping)											
	15 6.247		192.1					120.9			ICMP			(p1ng)											
	16 6.247		131.1					168.0			IOP			(ping)											
	17 7.246		192.1	68.0.2				120.9			IOP			(p1ng) (p1ng)											
	19 8.246			68.0.2				120.9			IOW			(ping)											
	20 0.246		131.1					168.0			IOP			(ping)											
											Acc.		MIM.	ALC: NO											
. (t	ame 1 (60 hernet II Destinati Source: 1 Type: ARP Trailer: dress Res	, Src on; 8 92.16 (0x0 00000	: 192.: roadca: 8.100.: 806) 000000	168.100 st (ff: 130 (00	.130 ff:ff 1:c0:9	(00: :ff: 5:c9	pture c0:95 ff:ff :07:3	:c9:0) 1)	7:31),	Dst:)								
E Ad	hernet II Destinatio Source: 1 Type: ARP Trailer:	, Src on: 1 92.16 (0x0 oluti 5 04 0 0 00 0	: 192.1 Prosdca: 8.100.1 (06) 0000000 on Prot 0 01 0 0 01 0 0 00 0	168.100 st (ff: 130 (00 0000000 toccol (0 c0 : 0 a8 : 0 0 : 0 0 :	130 ffiff 11:019 000000 reque 5 : c9 5 : c9	(00: 1ff: 5:c9 00000 st) 07 3 00 0 00 0 00 0	pture c0:95 ff:ff :07:3 00000 1 08 1 c0 0 00	269:00) 1) 00000 06 00 85 64	01 82			icast	(ff :)							 	

Figure 75. Test 6: Scenario 3 Packet Capture on NAT 1 (pinged from Router)

F.7.3. Analysis

The Router was able to ping all four interfaces as described in F.2. The behavior of this scenario is identical to the one in E.7. Refer to E.7.3 for a more detail analysis.

G. Scenario 4

G.1. Description

The MLS server is configured as follows in order: any packets received on its single-level interface (eth1, 192.168.100.130) is forwarded to the single-level interface of the Router (eth0, 192.168.0.27) and any packets received on its MLS LAN interface (eth0, 192.168.0.130) is forwarded to the single-level interface of the NAT 1 (eth1, 192.168.100.88).

G.2. Operations

First, NAT 2 pings:

- 1. eth0 of MLS server
- 2. eth1 of MLS server
- 3. eth1 of NAT 1
- 4. eth0 of NAT 1

Then, Router pings:

- 5. eth0 of MLS server
- 6. eth1 of MLS server
- 7. eth1 of NAT 1
- 8. eth0 of NAT 1

G.3. Network Configuration on MLS Server.

G.3.1. Type the following answers when prompted:

	SAK				
	Enter command?	tcpip_ed	it		
	Enter editor request?	add			
	Enter TCP/IP daemon name?	tcpip_ml	S		
	Enter TCPIP/IP daemon description?	TCP/IP	for	MLS	LAN
netwo	ork				
	Enter domain name?	cisrlabm	lstestl	bed1.co	m

Enter host name?	mlsserver
Enable the subnets local flag?	n
Enable the IP forwarding flag?	у
Enable the IP send redirect flag?	у
Enable the shutdown on failure flag?	n
Use default TCP maximum retransmission?	у
Add the network interface configuration?	у
Enter TCP/IP device name?	/dev/ether0
Enter interface address?	192.168.0.130
Enter destination address?	0.0.0.0
Enter broadcast address?	192.168.0.255
Enter network mask?	255.255.255.0
Add another network interface entry?	у
Enter TCP/IP device name?	/dev/ether1
Enter interface address?	192.168.100.130
Enter destination address?	0.0.0.0
Enter broadcast address?	192.168.100.255
Enter network mask?	255.255.255.0
Add another network interface entry?	n
Add the route configuration?	У
Enter TCP/IP device name	/dev/ether1
Is this route a default route	n
Enter destination address	0.0.0.0
Is destination address a host	n
Enter gateway address	192.168.0.27
Enter route metric	1
Add another network route entry	У
Enter TCP/IP device name	/dev/ether0
Is this route a default route	n
Enter destination address	0.0.0.0
Is destination address a host	n

Enter gateway address	192.168.100.88
Enter route metric	1
Add another network route entry	n
Add the resolver configuration?	n

- G.4. Preparation and Testing
 - G.4.1. On NAT 1,
 - G.4.1.1. Launch Ethereal
 - G.4.1.2. Go to the Capture menu
 - G.4.1.3. Go to Interfaces
 - G.4.1.4. Click on Capture 192.168.100.88

G.4.2. On Router,

- G.4.2.1. Launch Ethereal
- G.4.2.2. Go to the Capture menu
- G.4.2.3. Go to Interfaces
- G.4.2.4. Click on Capture 192.168.0.27

G.4.3. On NAT 2,

- G.4.3.1. Run the following commands:
 - ping -c 4 192.168.0.130
 - ping -c 4 192.168.100.130
 - ping -c 4 192.168.100.88

ping –c 4 131.120.9.15

- G.4.4. Repeat the above commands on the Router
- G.4.5. Stop Ethereal captures on both NAT 1 and Router

G.5.Result

Table 14 lists the result of the Scenario 4. The first column shows where the ping was initiated and the first row shows what hosts/IP addresses were pinged. The result from Scenario 4 is exactly the same as the result obtained in Scenario 1.

to	192.168.0.130	Ū laita lait
	(eth0, MLS LA	4
from	interface of ML	_
	server)	
NAT 2	Successful	
Router	Successful	

Table 14.

Test 6: Scenario 4 Result

G.6. Packet Capture when pinged from NAT 2

G.6.1. Router

The following is a snapshot of the packets captured on the Router when the four interfaces were pinged from NAT 2.



Figure 76. Test 6: Scenario 4 Packet Capture on Router (pinged from NAT 2), Part 1

B	ചചച	61 0	5 M	. 6			4	a 4	7	л	A		0	0			m	N	R
			- 6	× c	20	9	4	44	1	T		a a	4	4			Ю	N	U
Eilter:							•	Expressio	n (je	ar Asph	1								
No	Tine	Source		D	estination			Protocol	Info										4
	95 56.103943	192.168.			31.120.9			ICMP			request								
	96 56.103947 97 56.104048	192.168.			31.120.9 31.120.9			ICMP			request								
	98 56.104052	192.168.			31.120.9			ICMP			request								
	99 56.104158				31.120.9			ICMP			request								
	00 56.104162 01 56.104267	192.168.			31.120.9 31.120.9			ICMP			request								
	02 56 104221	102 169			71 120 0			TOND		(ping)									
1	03 56.104371	192.168.	202.11	1	31.120.5	9.15		IONP	Echo	(ping)	request								
	04 30.104374				1.120.			TONP			request								
	05 56.104474 06 56.104478	192.168.			31.120.9 31.120.9			ICMP			request								
	07 56.104577	192.168.			31.120.9			ICMP			request								
	08 56.104581	192.168.			31.120.9			ICMP	Echo	(ping)	request								
	09 56.104684 10 56.104688	192.168.			31.120.9 31.120.9			ICMP			request								
		192.100.			920182			101			request	d (Time	tolli	/e exce	eded in	trans	t)		
	12 57.102529				31.120.9			ICMP			request		an luncio		a haaraan	- COLORINA			
	13 57.102640				31.120.9			ICMP			request								
	14 57,102646 15 57,102759	192.168.			31.120.9			ICMP			request								
						** * *	_	IN MP	ermi.	THURST	trought	<u> </u>					_	_	_
	ame 103 (98 by: Ternet 11, Src					300 1	ct · 10	A 168 D	27.10	(Partne	Plev/c M	ł							-
	ernet Protoco					_						y ora	inge						
	Version: 4																		
Н	leader length:	20 bytes																	
€D)ifferentiated	Services	Field: (0x00 (D	SCP 0x0	D: Defa	ult; l	ECN: 0x0	0)										
T	iotal Length:	84																	
	Identification																		
	lags: 0x04 (0	11111111111111	ment)																
	ragment offse	the second s		gre	en														
	Time to live: Protocol: ICMP		J	9.0	011														
	leader checksu		fcorrect	+1															
-				·															1
000	00 a0 d2 1c 7							0											1
	00 54 00 00 4 09 0f 08 00 6						·14	[n SP	1. ×										
	Oc 00 08 09 0	a Ob Oc O	d Oe Of	10 11	12 13 1	4 15													
020 030		a 16 1c 1	d 1e 1f	20 21	22 23 2	4 25			"#\$%										
020 030 040	16 17 18 19 1 26 27 28 29 2	a 10 10 1	1 3. 36	30.34		4 30	41734	+,/01	33.45										

Figure 77. Test 6: Scenario 4 Packet Capture on Router (pinged from NAT 2), Part 2

G.6.2. NAT 1

The following is a snapshot of the packets captured on the NAT 1 when the four interfaces were pinged from NAT 2.

					-	2.ststx																	
K	ų		0		0	X	ø	8		4	¢ ¢	0 T	2	E		0	Q	9			7	X	0
er:										•	Express	ion Ø	har Ba	phy									
	j	ine .		Source			Dest	nation			Protocol	i Info							_	_		_	
	14			192.10	4.100.	30	linoi	scast	-		ALP	who i	nas Il	2.100	100.11	UT UT	atuito	ous Aki		2		_	_
		7.57			8.100.			idcast	ione.		ARP	Who I	has 19	2.168.	100.88	7 Tel	1 192	.168.1		N.			
		7.57		192.16	10.012.00				00.130		ARP				is at 0	0:00:14	1:ef:	af :eb					
				192.10				168.10			ICMP :	Echo	(ping) req	lest								
				192.16				168.2			10%P 10%P	Echo	(ping) rep	ly unit								
				192.10				168.2			IOP		(ping (ping										
				192.16				168.1			ICMP		(ping										
				192.10				168.2			ICMP		(6100										
	10 4	0.57	2656	192.10	8.202.	1	192.	168.1	88.00		IONP		(ping										
				192.16				168.2			TOND		(ping										
				192.16					00.130		ARP				.100.13				100.88	<u>(</u>			
		13.67					192.																
		12.57	1023		in hidd			kerde	(1994) (1994)		ARP							:07:31					
		12.57	1023								AX.P				1.2111								
											ALP												
Eth C S T	me 1 erne esti	1 (60 et II inati ce: 1 : ARP	byte , Src on: 8 92.16	s on wi : 192.1 roadcas 8.100.1	re, 60 68.100. t (ff:1	bytes (130 (00 fiffifi c01951(1:00:95 1ff:ff 19:07:1	(d) (c9:0) (f) (11)				ast (ff											
Eth S T T	me 1 erne vesti ouro ype: ype:	t (60 et II inati ce: 1 : ARP ler:	byte , Src 0n: 8 92.16 (0x0 00000	s on wi : 192.1 roadcas 8.100.1	re, 60 68.100. t (ff:1 30 (00	bytes (130 (00 fifififi 0000000	1:c0:95 1ff:ff (9:07:1) 000000	(d) (c9:0) (f) (11) 000000	7:31),														
Eth C S T Add	me 3 erne setti ouro ype: rail ress	1 (60 et II inati cer 1 : ARP ler: s Res	byte , Src (0x0 00000 oluti	s on wi : 192.1 nosdcas 8.100.1 806) 0000000 00 Prot	re, 60 68.100. t (ff:t 30 (00 0000000 0000000 00001 (r	bytes (130 (00 6:051:0 0000000 equest, c9 07	1:00:99 1:ff:ff 9:07:1 0000000 (gratu) 31:08	(d) (c) (c) (c) (c) (c) (c) (c) (c) (c) (c)	7:31), ARP)		broadc	ast (ff											
Eth C S T Add	rest vype: vail rest 08 (00 0	1 (60 et II inati ce: 1 ler: s Res FF FF 00 06 00 00	byte , Src (0x0 00000 oluti 04 0 00 0	s on wi : 192.1 roadcas 8.100.1 806) 0000000 pn Prot	re, 60 68.100. t (ff: 30 (00 0000000 0000 (r c0 9 c0 9 c0 9	bytes (130 (00 fiffifi c01951) 0000000 equest, c9 07 c9 07 c9 07	1::01:95 5::07:: 9::07:: 0000000 (gratu) 31:08 31:00 00:00	d) :::9:0 () 11) 00000 a8 64	7:31), ARP) 01 82 00	Dst: H	troadc	ast (ff											

Figure 78. Test 6: Scenario 4 Packet Capture on NAT 1 (pinged from NAT 2)

G.6.3. Analysis

Scenario 4 had the same result as Scenario 1. In other words, NAT 2 was able to ping 192.168.0.130, 192.168.100.130, and 192.168.100.88 only. It failed to ping 131.120.9.15. The Echo request destined for 131.120.9.15 was routed from 192.168.0.27 to 192.168.0.130 (yellow and orange outlines in Figure 76). However, XTS-400 forwarded the packet back to 192.168.0.27. This sequence of events occurred until the time-to-live exceeded. As a result, the Echo requests never reached NAT 1 (Figure 77). Refer to D.6.3 for more details.

- G.7. Packet Capture when pinged from Router
 - G.7.1. Router

The following is a snapshot of the packets captured on the Router when the four interfaces were pinged from Router.

믭	1000	1	0	1	N			2	5	3	x	(3	9		9	4		\$	Ċ	7		ł			44	Đ	2	Q	0		•	N			5	×	1	0			
Elter:	Ē		-			-			-			_	-			_	7				- ۱ (-				•					-									
Ower.	L	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	-	Poble		nu 3	ea.	044			_	_	_	_	_	_	_	_	_	_	_	_	_	_			
No. +		1.11	10			Sou							estin								Info																			1		
						192				130						.130)		ICMP				(iny)		quest	6																
	17	12	2.0	1517	49	192	.16	8.1	00.	130			92.	168.	0.2	7			ICMP	2	Echt	()	ing)	re	ply																	
						192										.130)		ICMP						quest	(
						192				130			92. 92.		~~~~				ICMP ICMP				(ing)		quest																	
						192				88			92.						ICMP				(ing)																			
	2	1	6.1	5970	55	192	.16	8.0	.27			1	92.	168.	100	.88			IONP	•	Ech) (0	(ing)	re	quest	5																
						192				88			92.						ICMP				(ing)																			
						192			-	22		_	92. 92.		-	2.7.7.			ICMP ICMP				(pnro)		quest	-																
						192							92.						ICMP						quest																1	
	U	1	3.0	1970	157	192	. 10	8.1	ω.	58			92.	.66.	0.2	1	-	-	IUMP		ECRO	, U	ing,	re	piy	-	-		-	-	-	-	-	-	-	-	-	-			h	
	2	-1	Û.:	1000	34	192	.16	8.0	.27				31.	20.	9.1	5	_		108	7					quest									_								
	20		1	175.0	41	192	16	8.0	37				31.	20	9 1	ĉ			ICMP	2	Erbe	i'	inal	p.e	quest																1	-
						192							31.						ION						quest																	
		1000				192							31.						ICMP						quest																	
	3	1	2.5	9857	37	192	.16	8.0	.27				31.						ICMP		Echo	0 (0	(gnrd	re	quest																	
						192							31.						10%						quest																	
	35	1	5.5	1898	29	192	.16	5.0	.0			12	31.	120.	9.1	>			ICMP	2	ECRO	(p	ning)	re	quest	2	1	-												۲		
E In	ter Ve He Di To Id Fl. Fr.	ade fe tal	: Pr pn: ren Le ifi : O ent	4 eng tia ngti cat xD4 off	th: ted (De fset e: f	, 51 20 1 Ser 14 : 0x1 : 0x1 :: 0	vic vic Fr	19, 55 55 () 50 19	Fiel ()) ent)	8.0 Id:	.2/ 0x0	(1)	2.1	99.0	.27), 1	sti	13		0.9.	.15 (_	-		9:07:	10	J			, a	ng	3								× 1		
0000	000	0 5 9 0 1 0 5 1	4 0 6 0 7 1	0 0 8 0 8 0 8 1	0 40 0 85 9 04 9 14	30 00 12 00 12	40 ec 0c	01 0b 0d 1d	00	5 5 6 00	c0 60 10 20	68 04 11 21	12 22	1b 8 43 0 13 1 23 2	33 7 0b 9	18	.T.		e	····	/C																			< 11 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1		

Figure 79. Test 6: Scenario 4 Packet Capture on Router (pinged from Router), Part 1

	(🕍 🕒 🖁 🗙	: @ 🔒 🖻 ♦		¥ ¥		0,0	Q 🖻			XØ
jter:			 Expression. 	Gear Appl						
lo. • Time	Source	Destination	Protocol							^
	3 192.100.100.130	192.100.0.2/		ELINU (ping)						
	8 192.168.0.27 9 192.168.100.130	192.168.100.130 192.168.0.27		Echo (ping) Echo (ping)						
	5 192.168.0.27	192.168.100.130		Echo (ping)						
19 123.06116	5 192.168.100.130	192.168.0.27	ICMP	Echo (ping)	reply					
	9 192.168.0.27	192.168.100.88		Echo (ping)						
	0 192.168.100.88	192.168.0.27		Echo (ping)						
	5 192.168.0.27 3 192.168.100.88	192.168.100.88 192.168.0.27		Echo (ping) Echo (ping)						
	6 192.168.0.27	192.168.100.88		Echo (ping) Echo (ping)						
	5 192.168.100.88	192.168.0.27	ICMP	Echo (ping)	reply					
	0 192.168.0.27	192.168.100.88	ICMP	Echo (ping)	request					
	7 192.168.100.88	192.168.0.27		Echo (ping)						
	4 192,168.0.27 1 192.168.0.27	131.120.9.15 131.120.9.15		Echo (pina) Echo (pina)		_	_	_	_	_
	1 192.168.0.27	131,120,9,15	and the second se	Echo (ping) Echo (ping)	the fight and an or other					_
	0 192.168.0.27	131.120.9.15		Echo (ping)						
32 132.98561	7 192.168.0.27	131.120.9.15		Echo (ping)						
	7 192.168.0.27	131.120.9.15		Echo (ping)						
	5 192.168.0.27 9 192.168.0.27	131.120.9.15 131.120.9.15		Echo (ping) Echo (ping)						
Frame 29 (98 by	tes on wire, 98 bytes	; captured))					^
Internet Protoco Version: 4 Header length Differentiate Total Length: Identificatio ⊮ Flags: 0x04 (Fragment offs Time to live: Protocol: ION Header checks	01, SFC: 192.100.0.27 1: 20 bytes 1: 20 by		191.120.9.)	3.137					

Figure 80. Test 6: Scenario 4 Packet Capture on Router (pinged from Router), Part 2

G.7.2. Router

The following is a snapshot of the packets captured on the NAT 1 when the four interfaces were pinged from Router.

W																										
Å		0				3	1,	: 6	9	8	9	4	¢ 4	0 7	2			0	10	10			Y		X	0
ker:												•	Express	sion g	kar Bre	ł										
Ø. +		Time		50.					estin		_			ohi info												
		0.00	0085			100.8				KAST 68.10	0,130	-	ARP		nas 19 168,10						eh	10	-	-	-	
	3	0.00	0125	19.	.168	.0.27				68.10			IOP	Lcho	(ping) requ	est	1010%								
			0171			.100.1	8			68.0.			IONP		(ping											
			0351			.0.27	A			68.0.			1049 1049		(ping) (ping)											
		2102	0194			.0.27		_		68.10			IOP		(ping											
			0283			100.8	8			68.0.			ICMP	Echo	(ping) repl	y.									
			0031			.0.27				68.10			ICMP		(ping											
			0117 8437			.100.8				68.0.	0.130		ICMP ARP		(ping			107	Tall	192.1	68,100.	88				
			8529			.100.1				68.10			ARP		168.10											
						., 60																				
ít.	hern	et 1	I, Sr	e: 19	2.16	.100.	130 (0::0	:95 :	c9:07	':31),	Dst:	Broade	ast (f	f aff aff	uffuff	1:11)									
Et.	hern Dest	et 1 ingt	I, Sr ion:	e: 19 Broad	2.16 cast		130 () f:ff:	0:c0 f;ff	:95 : ;ff)	:c9:07	':31),	Dst:	Broade	cast (f	1.11.11	uff aff	1:11)									
[t	hern Dest Sour	inat ce:	I, Sr ion:	c: 19 Broad 68.10	2.16 cast 0.13	.100. (ff;f	130 () f:ff:	0:c0 f;ff	:95 : ;ff)	:c9:07	1:31),	Dst:	Broade	cast (f	t dt dt	uffaf	1:11)									
[E t	hern Dest Sour Type Trai	inat inat ice: AF ler:	I, Sr ion: 192.1 P (0x	c: 19 Broad 68.10 0806) 00000	2.16 cast 0.13). 100. (ff:f) (00:	130 () fiffi c0:95	0:00 f;ff 10:0000	:95 : :ff) 7:31	(9:07) 1)	':31),	Dst:	Broade	cast (f	1.111.111	utut	(111)									
[E t	hern Dest Sour Type Trai	inat inat ice: AF ler:	I, Sr ion: 192.1 P (0x	c: 19 Broad 68.10 0806) 00000	2.16 cast 0.13	(ff:f (00:	130 () fiffi c0:95	0:00 f;ff 10:0000	:95 : :ff) 7:31	(9:07) 1)	':31),	Dst:	Broadd	cast (f	1.11.11	uffaf	(:#)									
[E t	hern Dest Sour Type Trai	inat inat ice: I: AF ler:	I, Sr ion: 192.1 P (0x	c: 19 Broad 68.10 0806) 00000	2.16 cast 0.13). 100. (ff:f) (00:	130 () fiffi c0:95	0:00 f;ff 10:0000	:95 : :ff) 7:31	(9:07) 1)	·:31),	Dst:	Broadd	cast (f	1.11.11	uttat	(:#)									
[E t	hern Dest Sour Type Trai	inat inat ice: I: AF ler:	I, Sr ion: 192.1 P (0x	c: 19 Broad 68.10 0806) 00000	2.16 cast 0.13). 100. (ff:f) (00:	130 () fiffi c0:95	0:00 f;ff 10:0000	:95 : :ff) 7:31	(9:07) 1)	':31),	Dst:	Broadd	cast (f	1.11.11	uffaf	1:11)									
E Ad	hern Dest Sour Type Trai dres	inat inat ice: N ler: s Re	I, Sr ion: 192.1 P (0x 0000 solut	c: 19 Broad 68.10 0806) 00000 ion F	2.16 cast 0.13 0000 roto	1.100. (ff:f) (00: 000000 col (r	130 (fiffi c0:95 00000 tques	0:c0 f;ff cc9:0 00000	:95 : :ff) 7:31 0000	(9:07)))))))))))))))))))	01				1.11.11	affaf	(:#)									
E Ad	hern Dest Sour Type Trai dres	et I inat ce: A ler: s Re 00 (00 (I, Sr ion: 192.1 P (0x solut f ff 06 04	c: 19 Brosc 68.10 0806) 00000 ion F Ff Ff 00 0: 00 00	2.16 cast 0.13 0000 roto	1.100. (ff:f) (00: 000000 col (r col 95 s8 64	25 0 25 0 25 0 25 0 58 0	0::0 f;ff ::00000 000000 :) 7 31 7 31 0 00	195 : 195 :	269:207) 1.) 0000 56:00 88:64	01 82			.1	11111	uff af	1:11)									
Ad	hern Dest Sour Type Trai dres	et I inat ce: A ler: s Re 00 (00 (I, Sr ion: 192.1 192.1 P (0x solut f ff 6 04 0 00	c: 19 Brosc 68.10 0806) 00000 ion F Ff Ff 00 0: 00 00	2.16 cast 0.13 0000 roto	1.100. (ff:f) (00: 000000 col (r)	25 0 25 0 25 0 25 0 58 0	0::0 f;ff ::00000 000000 :) 7 31 7 31 0 00	195 : 195 :	269:207) 1.) 0000 56:00 88:64	01 82 00			.1 .1d.	1.11.11	uff af	1:11)				11 - 11					

Figure 81. Test 6: Scenario 4 Packet Capture on NAT 1 (pinged from Router)

G.7.3. Analysis

The Router could ping both interfaces of the MLS server because the Router and the MLS server share a peer-to-peer relationship. The Router was also able to ping NAT 1 since XTS-400 has routing capabilities to route packets to its immediate peers. However, pinging 131.120.9.15 was unsuccessful. Echo requests destined (red outline in Figure 79) for 131.129.9.15 were sent out by the Router (yellow and orange outlines in Figure 79). However, XTS-400 sent those requests back to the Router when it received them (yellow and orange outlines in Figure 80). The Router stopped routing the requests further as it recognized them. Therefore, the Echo requests never reached NAT 1 (Figure 81).

H. Observation

A number of observations can be made from analyzing the results and packet captures for the four scenarios. First, there were two different sets of results from running the four test scenarios. Scenarios 1 and 4 generated the first set and scenarios 2 and 3 have generated the other set of results (refer to sections D.5, E.5, F.5, and G.5). Second, each scenario that shared the same gateway address sequence in its routing configuration yielded identical results. In other words, the results were dependent on the order of the gateway address and were independent of the device name in the routing configuration (refer to Table 9). Third, XTS-400 seemed to always forward packets destined for unknown networks to the gateway indicated in the first static route in its routing table. In scenarios 1 and 4, XTS-400 bounced Echo requests it received from 131.120.9.15 to 192.168.0.27 instead of forwarding them onto NAT 1. Also in scenarios 1 and 4, similar behavior of XTS-400 forwarding packets to 192.168.0.27 was seen when the Router pinged 131.120.9.15. In both cases, the XTS-400 did not have routing information for the 131.120.9.x network and the gateway for its first static route is 192.168.0.27. The XTS-400 always routed packets destined for unknown networks to 192.168.100.88 instead in scenarios 2 and 3 where the 192.168.100.88 was the gateway in its first static route.

LIST OF REFERENCES

[1] T. Richardson, "US to embrace VoIP", 2005.

http://www.theregister.co.uk/2005/04/04/idc_voip_research/, Accessed: April 2005.

[2] ZDNet Research. "Corporate VOIP spending to reach \$903 mln in 2005" 2005 Available: <u>http://blogs.zdnet.com/ITFacts/index.php?id=P2656</u>, Accessed: April 2005.

[3] VOIP-info.org, "VOIP Phones", 2005, <u>http://www.voip-info.org/wiki-</u> VOIP+Phones#id892699, Accessed: April 2005.

[4] P. C. Mehta and S. Udani, "Overview of Voice over IP", Technical Report MS-CIS-01-31, Department of Computer Information Science, University of Pennsylvania, February 2001.

[5] D. R. Kuhn, T. J. Walsh, and S. Fires, "Security Consideration for Voice over IP Systems, Recommendations of the National Institute of Standards and Technology", Special Publication 800-85, 2005.

[6] "netfilter", 2005, http://www.netfilter.org/, Accessed: August 2005.

[7] C. E. Irvine, T. E. Levin, T. D. Nguyen, D. Shifflett, J. Khosalim, P. C. Clark, A. Wong, F. Afinidad, D. Bibighaus, J. Sears, "Overview of a High Assurance Architecture for Distributed Multilevel Security," Proceedings of the 5th IEEE Systems, Man and Cybernetics Information Assurance Workshop, United States Military Academy, West Point, NY, pg 38-45, June 10-11, 2004.

[8] T. D. Nguyen, T. E. Levin , and C. E. Irvine, "MYSEA Testbed", Proceedings from the 6th IEEE Systems, Man and Cybernetics Information Assurance Workshop, West Point, NY, June 2005, pp. 438-439.

[9] J. Glasmann, W. Kellerer, and H. M^{*}uller, "Service Architectures in H.323 and SIP: A Comparison", IEEE Communications Society Survey and Tutorials, Vol. 5, No. 2, 2003.

[10] H. Schulzrinne and J. Rosenberg, "A Comparison of SIP and H.323 for Internet Telephony", Proceedings of the 8th International Workshop on Network and Operating System Support for Digit Audio and Video (NOSSDAV 98), Cambridge, England, Jul. 1998, pp. 83-86.

[11] Javvin Technologies, Inc., "H.323: ITU-T VOIP Protocols Overview", 2005, http://www.javvin.com/protocolH323.html, Accessed: June 2005.

[12] N. Networks, "A Comparison of H.323v4 and SIP", 3GPP S2, Tokyo, Japan, Technical Report S2-000505, January 2000.

[13] S. Niccolini, R. G. Garroppo, J. Ott, S. Prelle, J. Kuthan, S. Ubik, M. Brandl, D. Daskopoulos, E. Verharen, E. Dobbelsteijn, "IP Telephony Cookbook", pp. 76,

TERENA, 2004. Available at:

http://www.terena.nl/library/IPTELEPHONYCOOKBOOK/chapters/IPTELEPHONYCO OKBOOK.pdf, Accessed August 2005.

[14] J. Winters, "IP Videoconferencing: ITU's H.323 and IETF's SIP", 2003 http://www.eng.mu.edu/rehab/Rehab167/Mod3/teleconf/h323-sip.htm, Accessed: April 2005.

[15] "SJ Labs", 2005, http://www.sjlabs.com, Accessed: August 2005.

[16] "Ethereal", 2005, http://www.ethereal.com, Accessed: August 2005.

[17] "Zone Labs" 2005 <u>http://www.zonelabs.com/store/content/home.jsp</u>, Accessed August 2005.

[18] John G. Ata, private email, 16 September 2005.

[19] J. Stephens, "Connection tracking", 2001,

http://kalamazoolinux.org/presentations/20010417/conntrack.html, Accessed: September 2005.

INITIAL DISTRIBUTION LIST

- 1. Defense Technical Information Center Ft. Belvoir, VA
- 2. Dudley Knox Library Naval Postgraduate School Monterey, CA
- 3. Hugo A. Badillo NSA Fort Meade, MD
- 4. George Bieber OSD Washington, DC
- 5. RADM Joseph Burns Fort George Meade, MD
- 6. John Campbell National Security Agency Fort Meade, MD
- 7. Deborah Cooper DC Associates, LLC Roslyn, VA
- CDR Daniel L. Currie PMW 161 San Diego, CA
- 9. Louise Davidson National Geospatial Agency Bethesda, MD
- 10. Vincent J. DiMaria National Security Agency Fort Meade, MD
- 11. LCDR James Downey NAVSEA Washington, DC

- 12. Dr. Diana Gant National Science Foundation Arlington, VA
- 13. Jennifer Guild SPAWAR Charleston, SC
- 14. Richard Hale DISA Falls Church, VA
- 15. LCDR Scott D. Heller SPAWAR San Diego, CA
- 16. Wiley Jones OSD Washington, DC
- 17. Russell Jones N641 Arlington, VA
- David Ladd Microsoft Corporation Redmond, WA
- Dr. Carl Landwehr National Science Foundation Arlington, VA
- 20. Steve LaFountain NSA Fort Meade, MD
- 21. Dr. Greg Larson IDA Alexandria, VA
- 22. Penny Lehtola NSA Fort Meade, MD

- 23. Ernest Lucier Federal Aviation Administration Washington, DC
- 24. CAPT Deborah McGhee Headquarters U.S. Navy Arlington, VA
- 25. Dr. Vic Maconachy NSA Fort Meade, MD
- 26. Doug Maughan Department of Homeland Security Washington, DC
- 27. Dr. John Monastra Aerospace Corporation Chantilly, VA
- 28. John Mildner SPAWAR Charleston, SC
- 29. Jim Roberts Central Intelligence Agency Reston, VA
- 30. Charles Sherupski Sherassoc Round Hill, VA
- 31. Dr. Ralph Wachter ONR Arlington, VA
- 32. David Wirth N641 Arlington, VA
- 33. Daniel Wolf NSA Fort Meade, MD

- 34. Jim Yerovi NRO Chantilly, VA
- 35. CAPT Robert Zellmann CNO Staff N614 Arlington, VA
- Dr. Cynthia E. Irvine Naval Postgraduate School Monterey, CA
- 37. Thuy D. Nguyen Naval Postgraduate School Monterey, CA
- CAPT Deborah McGhee Naval Postgraduate School Monterey, CA
- Lily Tse Naval Postgraduate School Monterey, CA