MIDCOM WG
Internet-Draft
Expires: April 24, 2005

C. Jennings
Cisco Systems

October 24, 2004

NAT Classification Results using STUN
draft-jennings-midcom-stun-results-02

Status of this Memo

Copyright Notice

Abstract

IETF has several groups that are considering the impact of NATs on various protocols. Having a classification of the types of NATs that are being developed and deployed is useful in gauging the impact of various solutions. This draft records the results of classifying NATs using the STUN protocol.

This work is being discussed on the ietf-behave@list.sipfoundry.org mailing list

1. Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC-2119 [2].

In this document, the term NAT means port address translation. This is an unfortunate use of the terminology but is what NAT has come to mean.

2. Introduction

A major issue in working with NAT traversal solutions for various protocols is that NATs behave in many different ways. RFC 3489 (STUN) classifies these and provides a method to test them. This draft describes the results of testing several residential style NATs.

Several NATs attempt to use the same external port number as the internal host used. This is referred to as port preservation. On the NATs that did this, some were found to have different characteristics depending on whether the port was already in use or not. This was tested by running the STUN tests from a particular port on one internal IP address and then running them again from the same port on a different internal IP address. The results from the first interface, where the port was preserved are referred to as the primary type while the results from the second interface, which did not manage to get the same external port because it was already in use, is referred to as the secondary type. On most NATs the secondary type is the same as the primary but on some it is different; these are referred to as nondeterministic NATs, since a client with a single internal IP address can not figure out what the type of the NAT is.

There are several NATs that would be detected as address restricted by the STUN tests but are not. These NATs always use the same external port as the internal port and store the IP address of the most recent internal host to send a packet on that port. The NATs then forward any traffic arriving to the external interface of the NAT on this port to the most recent internal host to use it. These NATs are labeled of type "Bad" in the result table since they do not meet the definitions of NAPT in RFC 3022. Interestingly, as long as the clients behind the NAT choose random port numbers, they often do work. STUN detects these NATs as address restricted although they are really not address restricted NATs. This type of NAT is easily detected by sending a STUN packet from the same port on two different internal IP addresses and looking at the mapped port in the return. If both packets were mapped to the same external port, the NAT is of

the Bad type.

Another important aspect of a NAT for some applications is whether it can send media from one internal host back to another host behind the same NAT. This is referred to as supporting hairpin media.

Some NATs were rumored to exist that looked in arbitrary packets for either the NATs' external IP address or for the internal host IP address - either in binary or dotted decimal form - and rewrote it to something else. STUN could be extended to test for exactly this type of behavior by echoing arbitrary client data and the mapped address but sending the bits inverted so these evil NATs did not mess with them. NATs that do this will break integrity detection on payloads.

To help organize the NATs by what types of applications they can support, the following groups are defined. The application of using a SIP phone with a TLS connection for signaling and using STUN for media ports is considered. It is assumed the RTP/RTCP media is on random port pairs as recommended for RTP.

Group A: NATs that are deterministic, not symmetric, and support hairpin media. These NATs would work with many phones behind them.
Group B: NATs that are not symmetric on the primary mapping. This group would work with many IP phones as long as the media ports did not conflict. This is unlikely to happen often but will occasionally happen. Because they may not support hairpin media, a call from one phone behind a NAT to another phone behind the same NAT may not work.
Group D: NATs of the type Bad. These have the same limitations of group B but when the ports conflict, media gets delivered to a random phone behind the NAT.
Group F: These NATs are symmetric and phones will not work.

3. Results

The following table shows the results from several NATs. This includes some random NATs the author had lying around as well as every NAT that could be purchased in February 2004 in the San Jose Fry's, Best Buy, CompUSA, and Circuit City. Clearly this is not a very good approximation to a random sample. It is clear that the NATs widely purchased in the US are different from what are available in Japan or in Europe.

In the following table the Prim column indicates the primary type of the NAT. A value of Port indicates port restricted, Cone is a full cone, Bad is described in the next section, Symm is Symmetric, and Addr is Address restricted. The Hair column value of Y or N

indicates whether the NAT will hairpin media. The Pres column indicates whether the NAT attempts to preserve port numbers. The Sec column indicates the secondary type of the NAT, and a value of Same indicates it is the same as the primary type. The Grp indicates the group that this NAT falls into.

Vendor	Model	Firmware	Prim	Sec	Hair	Pres	Grp
Airlink	ASOHO4P	V1.01.0095	Port	Symm	N	Y	B
Apple	Air Base	V5.2	Cone	Same	Y	N	A
Belkin	F5D5321	V1.13	Port	Same	N	N	B
Cisco	IOS		Port	Symm			-
Cisco	PIX		Port	Same			-
Corega	BAR Pro2	R1.00 Feb 21 2003	Cone				-
DLink	DI-604	2.0 Jun 2002	Cone	Same	N	N	B
DLink	DI-704P	2.61 build 2	Cone	Same	Y	N	A
Dlink	DI-804	.30, Tue,Jun 24 20	Cone	Same	Y	N	A
Hawkings	FR24	6.26.02h Build 004	Bad	Same	Y	Y	D
Linksys	BEFSR11		Port				B
Linksys	BEFSR11 V2	1.42.7, Apr 02 200	Port				B
Linksys	BEFSR41	v1.44.2	Port				B
Linksys	BEFSR81	2.42.7.1 June 2002	Addr	Same	N	Y	B
Linksys	BEFSRU31		Port				B
Linksys	BEFSX41	1.44.3, Dec 24 200	Port				B
Linksys	BEFVP41	1.41.1, Sep 04 200	Port				B
Linksys	BEFW11S4	1.45.3, Jul 1 2003	Port				B
Linksys	WRT54G	1.42.2	Port	Symm	N	Y	B
Linksys	WRT55AG	1.04, Jun.30, 2003	Port				B
Linksys	WRV54G	2.03	Port	Same	N	Y	B
Microsoft	MN-700	02.00.07.0331	Cone	Same	N	N	B
Netgear	FVS318	V1.4 Jul. 15 2003	Port	Same	N	N	B
Netgear	RP114	3.26(CD.0) 8/17/20	Cone				-
Netgear	RP614	4.00 April 2002	Cone	Same	Y	N	A
NetworkEver	NR041	Version 1.0 Rel 10	Symm	Same	N	N	F
NetworkEver	NR041	Version 1.2 Rel 03	Bad	Same	Y	Y	D
SMC	2804WBRP-G	v1.00 Oct 14 2003	Port	Symm	Y	Y	B
SMC	7004ABR	V1.42.003	Port	Same	N	N	B
SMC	7004VBR	v1.03 Jun 12, 2002	Cone				-
Toshiba	WRC-1000	1.07.03a-C024a	Port	Cone	N	Y	B
umax	ugate-3000	2.06h	Port				-
US Robotics	USR8003	1.04 08	Cone	Same	N	N	B
ZOT	BR1014	Unknown	Bad	Same	N	Y	D

Since the time this testing was done, some addition testing and two shopping sprees in France and Taiwan, has provided the following results.

Vendor	Model	Firmware	Prim	Sec	Hair	Pres	Grp
Netgear	MR814v2	Version 5.01	Bad	Same	Y	Y	D
Cisco	PIX 515	6.3(3)	Port	Same	N	N	B
Dynex	DX-E401	1.03	Cone	Same	Y	N	A
Asante	FR1004	R1.13 V2	Cone	Same	N	N	B
Linksys	BEFSR81	2.42.7.1	Addr	Note 1	N	Y	B
Lanner	BRL-04FPU		Cone	Same	N	N	
AboCom	CAS3047		Port	Same	N	Y	
Lemmel	LM-IS6400B		Port	Same	N	Y	

The NAT with a secondary type of "Note 1" is particularly weird. The primary connection is address restricted. If a second host uses this same port, it also gets an Address Restricted but when a third host uses this same port, it get Symmetric.

Another good source of information for behavior of various NATs is the NATCECK [6] web page.

4. Discussion

It is clear from discussions with various vendors and watching how tests have changed over the years that symmetric is becoming less common. This change is being driven primarily by the desire to make online gaming work; many games use methods similar to STUN for NAT traversal. The only symmetric NAT found was an old device. More recent version of the software on the same device were not symmetric. It is clear that other symmetric NATs are deployed, but it is hard to find them.

5. Security Concerns

It is often assumed that symmetric NATs are more secure than port restricted NATs. This is not true - they are identical from a security point of view. They both only allow a packet to come inside the NAT if the host inside has previously sent to the exact same external IP and port. One can argue that cone is less secure than port restricted, but this is not true if the attacker can spoof the IP address, which is fairly easy to do in many cases. What level of security can be expected from NATs at all is a strange and curious topic. With all the NATs, if you allow packets out, packets can come in, so don't be surprised if NATs provide less security that anticipated.

6. Open Issues

The hairpin media tests were done by having a single host use STUN to find a public address on the NAT and then send media to itself and

see if it was received. It is possible that NATs might not hairpin media to the same host but would hairpin media to another host behind the same NAT. It is possible that because of this, the hairpin results reported here might be wrong.

This sample set of NATs is very US-centric: D-Link, Lynksys, and Netgear dominate the US consumer market. It would be good to get more results from other places.

These test results should be verified by another group. This has not been done yet.

This draft should be moved to be consistent with the classification in [7].

7. Acknowledgments

Many people and several mailing lists have contributed to the material on understanding NATs in this document. Many thanks to Larry Metzger, Dan Wing, and Rohan Mahy. The STUN server and client is open source and available at http://sourceforge.net/projects/stun and thank you to Jason Fischl who runs the public STUN server at larry.gloo.net. Thanks to Yutaka Takeda who tested and found bugs and Christian Stredicke for getting people thinking. Thanks to Francois AUDET for catching mistakes, verifying several results, and finding the very strange non-deterministic nature in the BEFSR81.

8. References

8.1 Normative References

[1] Rosenberg, J., Weinberger, J., Huitema, C. and R. Mahy, "STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)", RFC 3489, March 2003.

[2] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

8.2 Informative References

[3] Daigle, L. and IAB, "IAB Considerations for UNilateral Self-Address Fixing (UNSAF) Across Network Address Translation", RFC 3424, November 2002.

[4] Srisuresh, P. and K. Egevang, "Traditional IP Network Address Translator (Traditional NAT)", RFC 3022, January 2001.

[5] Srisuresh, P. and M. Holdrege, "IP Network Address Translator

(NAT) Terminology and Considerations", RFC 2663, August 1999.

[6] Ford, B. and D. Andersen, "Nat Check Web Site: http://midcom-p2p.sourceforge.net", June 2004.

[7] AUDET, F. and C. Jennings, "NAT/Firewall Behavioral Requirements", July 2004.

Author's Address

Cullen Jennings
Cisco Systems
170 West Tasman Drive
Mailstop SJC-21/2
San Jose, CA 95134
USA

Phone: +1 408 421 9990
EMail: fluffy@cisco.com

Intellectual Property Statement

Disclaimer of Validity

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Copyright Statement

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.