Internet Engineering Task Force MIDCOM WG
Internet Draft Y.Takeda
draft-takeda-symmetric-nat-traversal-00.txt Panasonic Communications
Category: Informational Research Laboratory

Symmetric NAT Traversal using STUN

<draft-takeda-symmetric-nat-traversal-00.txt>

Status of this Memo

Abstract

It is generally known that the binding acquisition for symmetric NATs with STUN (Simple Traversal of UDP through NATs) protocol will not yield a usable address for traversing symmetric NAT. The use of symmetric RTP allows you to accompolish symmetric NAT traversal only in situations where the other end is open to the Internet, or has a full-cone or a restricted-cone NAT. This document proposes an analytical method for symmetric NATs to obtain more detailed characteristics of the symmetric NAT using STUN, and describes how we can establish a peer-to-peer UDP connection even in situations where NATs (including symmetric NATs) are present at both ends.

1 Introduction

STUN is a useful tool to discover the presence and characteristics of Network Address Translators (NATs). (It does not support 'traversal' by itself.) It is generally known that the binding acquisition for symmetric NATs, with STUN, will not yield a usable address, and in cases that the other end also has a port restricted-cone NAT or symmetric NAT, there is no possible way to traverse these NATs.

We have discovered in our NAT characteristics research, that the number of symmetric NATs deployed in the market is significant even in the residential market. This is a significant issue, especially for service providers or manufacturers who are seriously looking for a solution to the actual NAT issues they have.

TURN (Traversal Using Relay NAT)[2] has been proposed to complement the limitation of STUN, however, this type of solution requires a relay server somewhere on the public network, which is an additional cost for service providers. It is important that service providers reduce the amount of server deployments as much as possible.

This document proposes an analytical method for symmetric NATs to obtain more detailed characteristics of symmetric NATs using STUN, and describes how we can establish a peer-to-peer UDP connection even in situations where the NATs (including symmetric NATs) are present at both ends. The operation is based upon a prediction of a set of IP address and port that a symmetric NAT will allocate. However, the discovery processes proposed in this document, using STUN, produce a fairly good success rate of symmetric NAT traversal. As a result, it will significantly reduce the requirement for relay servers.

This document does not provide any specific protocol, nor a proposal for any modifications to current STUN protocol. In order to incorporate the method described in this document into existing protocols (e.g. SDP), those protocols will need to be modified. It is expected that this method be appropriately examined in this public community to yield improvements and as motivation for applying it to both old and new protocols.

2 Terminology

NAT - Network Address Translation
RTP - Real-time Transfer Protocol
SDP - Session Description Protocol

STUN - Simple Traversal of UDP through NATs
TURN - Traversal Using Relay NATs
UDP - User Datagram Protocol

3 Network Configuration

The assumption in this document is based upon what is shown in Figure 3.1, in that there are one or more NATs at both endpoints(EP-a and EP-b) that wish to communicate to each other directly through the NATs. In order to get information about the NATs, each endpoint uses a STUN server located on the public network.

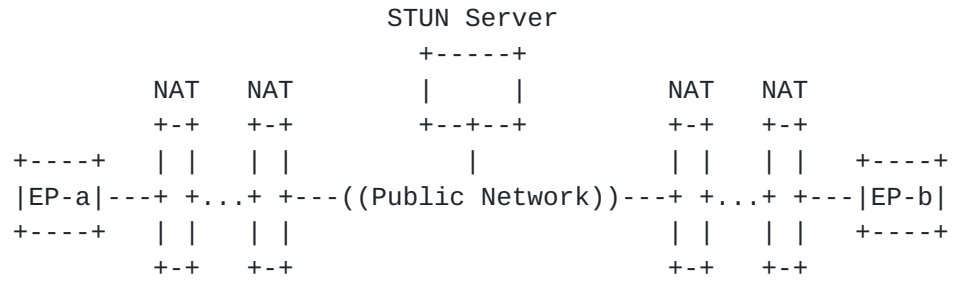


Figure 3.1 Network Configuration

4 NAT Behavior Analogy

An analogy is provided here to aid in the explanation of how the various NATs operate. It is assumed that readers of this document are familiar with STUN protocol[1] and have a good understanding of NAT behaviors.

The analogy is presented in terms of a doorman to a building (corresponding to a private network) in which a tenant (an endpoint device) is present. A NAT acts just like a wall of the building. Until the tenant sends a packet to the outside, there are no doors on the wall of the building. When the tenant in the building sends a packet, a door on the wall will be created with a doorman. The NAT behavior can be characterized in different ways depending on the doorman's role and the rules that created the door.

Full-cone NAT:

A door will be created when a tenant(endpoint) in a building

sends a packet for the first time. In the case of a full-cone NAT, the doorman standing at the door checks if each packet trying to come in is visiting the tenant who created this door. The doorman, however, does not check where each packet originates.

Restricted-cone NAT:

A door will be created when a tenant(endpoint) in a building sends an invitation letter (a packet) for the first time to another building. In this case, the doorman will check if each person (packet) trying to come in is visiting the tenant who created this door. The doorman also checks if visitors came from the building that received the invitation letter from the tenant.

Port restricted-cone NAT:

A door will be created when a tenant(endpoint) in a building sends an invitation letter (a packet) for the first time to a tenant in another building. The doorman will check if each person trying to enter is visiting the tenant who created the door. The doorman also checks if they have received the invitation letter from the tenant.

Symmetric NAT:

A door will be created every time when a tenant(endpoint) in a building sends an invitation letter (a packet) to a new tenant in another building. The doorman will check if each one trying to come in is visiting the tenant who created the door. The doorman also checks if they have received the invitation letter sent from him through this door.

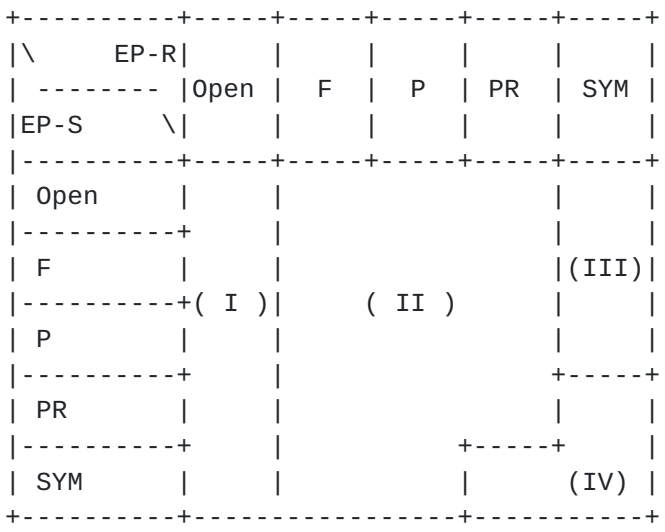
What makes NAT traversal difficult with symmetric NAT is the door creation rule. In other (non-symmetric) cases, the same door will be used whenever the same tenant in a building sends an invitation packet to a different destination. In symmetric NAT , a new door will be always created every time the tenant in the building sends an invitation packet. Therefore, when you want to talk to Mr.A and Mr.B at the same time, for example, the door to let Mr.A enter is always different from the one to let Mr.B enter. With STUN, the tenant sends an invitation packet to the STUN server (binding request) and the STUN server sends back a reply with the location of the door (MAPPED-ADDRESS) used to send the invitation, so that the tenant will know which door on the NAT can be used for other parties to enter. However, if the NAT is symmetric, the door obtained from the STUN server is not

the same as the door that will be used for other parties to enter.

In this analogy, a 'tenant' is used to represent a local UDP port. It should be noted that several tenants comprise a 'company'. The IP address represents a company in the 'building'. To recap, each building (LAN behind a NAT) has multiple companies (IP addresses) made up of many tentants (UDP ports). The trick to traverse NAT with UDP is to utilize the 'invitation letter (packet)". This will create a door for visitors outside the building to come in. The invitation packet is not necessarily a 'special' invitation packet. The first part of data transmission works as an invitation because it creates a door and a doorman as a result. STUN protocol provides us with a way to ascertain the doorman's role and the door creation rule.

5 NAT Combination Classification & Current Approach

The following chart shows combinations of NATs at each endpoint with the current NAT type definitions in STUN. The combinations are classified into 4 groups: Class I, II, III and IV.



Note:
EP-S: Sending endpoint.
EP-R: Receiving endpoint.
(In full-duplex, both EP-a and EP-b in Figure 3.1 will have both EP-S and EP-R)
Open: Open to public network (no NAT)
F : Full-cone NAT
R : Restricted-cone NAT
PR : Port restricted-cone NAT

SYM : Symmetric NAT

Figure 5.1 NAT Combination Classification

Class I is a case in which the receiver does not have a NAT. There is no actual NAT issue here because receiver side has no NAT and has a routable IP address to receive packets.

Class II is a case in which the receiver has a non-symmetric NAT and the sender has no NAT or any type of NATs except the case in which the receiver has a port restricted symmetric NAT and sender has a symmetric NAT. In order to traverse the NAT in this case, the receiver sends an invitation packet to the sender so that the doorman will not block any packets sent from the receiver of the invitation packet.

Class III involves a symmetric NAT at the receiver. There is a full-cone or restricted-cone NAT at the sender side. The problem in this case is that STUN is not able to provide a valid MAPPED-ADDRESS of the symmetric NAT for EP-S to send packet. EP-S can send an invitation packet to the MAPPED-ADDRESS on EP-R side NAT. This will cause an existing allocated port on EP-S side NAT to accept incoming packets sent from the MAPPED-ADDRESS on the EP-R side NAT. EP-R will also send an invitation packet to EP-S and the EP-S can record the source IP address and port number of the received packet to send packets back to the recorded address/port. This source address recording technique is known as "symmetric RTP"[3],[4].

Class IV is the case that this document addresses. The problem here is that STUN is not able to provide a valid MAPPED-ADDRESS for the symmetric NAT. Therefore, the other endpoint cannot send an invitation packet to the symmetric NAT. As a result, the symmetric RTP solution is not applicable here either. A key solution to this class IV traversal is to do further analysis on the symmetric NAT and make the invalid MAPPED-ADDRESS useful. The details are described in the following sections.

6 More About Symmetric NAT Behavior

6.1 Port Allocation Behavior

A symmetric NAT allocates different mapping (MAPPED-ADDRESS) when a new request is sent to a different destination, although it is sent from the same internal IP address and port. In the non-symmetric case, the same MAPPED-ADDRESS is always used. The following is a

typical example of the port assignment behavior of the symmetric NAT. In this example, 4 packets (TRY-1 thru -4) are sent to a different destination from the same internal IP address and port. TRY-1 and 2 send a packet to different port numbers of the same IP address. TRY-3 and -4 do so but to a different IP address from the one in TRY-1 and -2.

[TRY]	[FROM]	[TO]	[MAPPED-ADDRESS]
1	192.168.1.2:4136	65.12.66.10:3478	67.105.12.10:49152
2	192.168.1.2:4136	65.12.66.10:3479	67.105.12.10:49153 (49152+1)
3	192.168.1.2:4136	65.12.66.11:3478	67.105.12.10:49154 (49153+1)
4	192.168.1.2:4136	65.12.66.11:3479	67.105.12.10:49155 (49154+1)

The symmetric NAT allocates a new MAPPED-ADDRESS, however the increment size of its port number, called 'delta p', is, in most cases constant. In the example above, the delta p value is '+1'. It is known that delta p takes on another value other than '+1', as in the example below.

[TRY]	[FROM]	[TO]	[MAPPED-ADDRESS]
1	192.168.1.2:4136	65.12.66.10:3478	67.105.12.10:49152
2	192.168.1.2:4136	65.12.66.10:3479	67.105.12.10:49154 (49152+2)
3	192.168.1.2:4136	65.12.66.11:3478	67.105.12.10:49156 (49154+2)
4	192.168.1.2:4136	65.12.66.11:3479	67.105.12.10:49158 (49156+2)

With regard to port allocation behavior, since the symmetric NAT shown above allocates a new MAPPED-ADDRESS every time a packet is sent to a different IP address or port, this allocation behavior is called 'port sensitive' allocation.

It is also known that there is another type of port allocation behavior as follows.

[TRY]	[FROM]	[TO]	[MAPPED-ADDRESS]
1	192.168.1.2:4136	65.12.66.10:3478	67.105.12.10:49152
2	192.168.1.2:4136	65.12.66.10:3479	67.105.12.10:49152
3	192.168.1.2:4136	65.12.66.11:3478	67.105.12.10:49153 (49152+1)
4	192.168.1.2:4136	65.12.66.11:3479	67.105.12.10:49153
5	192.168.1.2:4136	65.12.66.12:3478	67.105.12.10:49154 (49153+1)
6	192.168.1.2:4136	65.12.66.12:3479	67.105.12.10:49154
7	192.168.1.2:4136	65.12.66.13:3478	67.105.12.10:49155 (49154+1)
8	192.168.1.2:4136	65.12.66.13:3479	67.105.12.10:49155

This symmetric NAT behaves, in terms of port allocation rule, like a cone (non-symmetric) NAT when packets are sent to different ports of the same IP address. But when the packets are sent to the different IP addresses for the first time, it will assign a new MAPPED-ADDRESS.

This port allocation rule is called 'address sensitive' allocation. Even in this case the port increment size, delta p, is likely to be constant.

The consistency of delta p is very important in order to traverse symmetric NAT. If an IP device behind a symmetric NAT knows the value of delta p and its consistency, the IP device can predict the next port number to be assigned by the symmetric NAT from the MAPPED-ADDRESS. The prediction, however, can fail.

One of the scenarios for prediction failure would be that another PC behind the same symmetric NAT created a new binding during the prediction process. Specifically, if there are multiple network applications running behind the same symmetric NAT, ap1 and ap2 shown in Figure 6.1 for example, ap1 first obtains a MAPPED-ADDRESS from STUN server (t0). Right after, ap2 starts talking to a remote host with UDP that causes another binding creation on the NAT (t1). The ap1 makes a prediction from the obtained MAPPED-ADDRESS but the predicted port number has just been taken by ap2. Eventually, ap1 sends a packet to a remote host (at t2) but the allocated port by the NAT for this transmission is not the one that the ap1 has predicted.

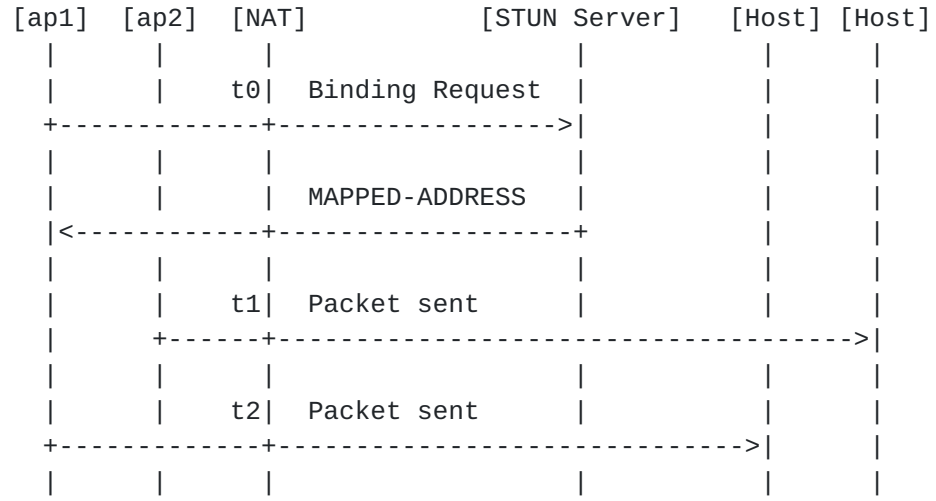


Figure 6.1 Prediction Failure Case A

The critical time period for the correct prediction is between t0 and t2. Prediction failure rate is determined by binding occurrence probability by another application behind the same NAT during the time period. Success rate can be maximized by minimizing the length of the time period.

Typically, a symmetric NAT allocates a port for a new binding from a specific range of ports. (e.g. 0xC000 - 0xCFFF) In most cases, the allocation starts from the beginning of the port range and when it

hits the bottom of the range, it will start over from the beginning.

This port assignment method of NAT is called "incremental allocation". With the incremental allocation, there usually is a table that keeps the status of each port in the NAT. The table has a status flag that shows whether or not the associated port is in use. The symmetric NAT, when a new binding is being created, looks for the next available port number by looking at the status flag. If it is in use, it will skip the port and look at the next port. If the prediction is made right before the skip occurs, the prediction will fail. This may happen if there are a number of IP devices connected behind the same NAT and noticeable amounts of UDP transactions are being made.

In contrast to the incremental allocation, there is another allocation method, called "queued resource allocation". In this method, a predetermined range of port numbers are stored in a queue (FIFO) in an orderly fashion at the initial phase. When a binding occurs, a port number will be read from the queue to be allocated for the binding. After the binding is released, the port number will be returned back into the queue. Since the length of the binding life-time varies, the order of the returned port numbers will not be continuous. That means, the order of the port numbers in the queue will be shuffled gradually and start losing continuity, which makes port prediction very difficult.

Here is a summary for possible reasons for port prediction failure:

(a) Another binding occurrence between t0 and t2.
(b) Hit the bottom of the port range. (incremental allocation)
(c) High UDP usage in the local network.
(d) Random port allocation (typically with queued resource allocation)

In order to prevent port prediction failure, the following solutions can be taken:

- Minimize the time length between t0 and t1. - for (a)
- Implement a retry process. - for (a), (b), (c)
- Multiple port prediction. (see 8.4) - for (a), (b), (c)

There is no practical solution for (d) at this moment. There might be a way to recover the port number continuity in the queue by manipulating allocation and release timings of the bindings of the NAT, however, it might have other disruptive factors caused by the non-norm NAT world.

6.2 Incoming Packet Filtering

Another factor that characterizes symmetric NAT behavior is the incoming packet filter type. Once a MAPPED-ADDRESS is allocated on the symmetric NAT for an internal device, the allocated port will accept incoming packets sent from an IP address and port to where the device has previously sent packets. There can be a symmetric NAT that accepts incoming packets sent from other external endpoints, just like a full-cone NAT or a restricted-cone NAT, in terms of incoming packet filtering.

The current STUN discovery process assumes that a symmetric NAT does not route incoming packets sent from other IP addresses and/or ports other than one to which an internal device previously sent a packet. In fact, with the STUN discovery process, a symmetric NAT that accepts packets from other IP addresses will result in a full-cone NAT.

The sensitivity, in terms of the incoming packet filter, to a source IP address and port number of the incoming packet needs to be evaluated as well as the port allocation rule. If the incoming packets are examined by the sender's IP address and port number, this is called 'port sensitive' filtering. If the packets are examined by the sender's IP address only, it is called, 'address sensitive' filtering.

6.3 NAT Characteristics Classification

As discussed in section 6.1 and 6.2, symmetric behavior can be characterized with two parameters as follows:

(1) Port Allocation Rule (door creation rule)
(2) Incoming Packet Filter (doorman's role)

These parameters can be applied to non-symmetric NATs, as well. The following chart shows all the possible NAT characteristics evaluated with the two parameters mentioned above.

Table 6.3.1 NAT Characteristics Classification

Port Allocation Rule	Cone	Incoming Packet Filter: No Filter	Incoming Packet Filter: AS Filter	Incoming Packet Filter: PS Filter
	Full-cone	Restricted-cone	Port restricted-cone	
AS Symmetric	Symmetric (a)	Symmetric (b)	Symmetric (c)	
PS Symmetric	Symmetric (d)	Symmetric (e)	Symmetric (f)	

(NOTE) AS: Address Sensitive, PS: Port Sensitive

All the non-symmetric NATs are categorized as 'cone' NAT. There are three types of cone NATs corresponding to the three incoming packet filter types.

The other six NAT types are members of a symmetric NAT defined in STUN except Symmetric (a) and symmetric (d). These symmetric types are classified as a full-cone NAT. It is assumed in the current STUN process that if a packet is received in Test II, it determines that the NAT is full-cone without evaluating its port allocation rule. The details of this issue are discussed in section 6.5.

In order to detect the six types of symmetric NATs shown in this table, current STUN message definition and its server can be used as is. This symmetric NAT discovery process is described in section 7.

6.4 Exceptional Behavior

A symmetric NAT has exceptional behavior on port allocation that might help NAT traversal. The symmetric NAT allocates a port as well as typical symmetric NAT behaviors but this symmetric NAT allocates the same port number as its local port number.

[TRY]	[FROM]	[TO]	[MAPPED-ADDRESS]
1	192.168.1.2:4136	65.12.66.10:3478	67.105.12.10:4136
2	192.168.1.2:4136	65.12.66.10:3479	67.105.12.10:49152
3	192.168.1.2:4136	65.12.66.11:3478	67.105.12.10:49153
4	192.168.1.2:4136	65.12.66.11:3479	67.105.12.10:49154
5	192.168.1.2:4137	65.12.66.10:3478	67.105.12.10:4137
6	192.168.1.2:4137	65.12.66.10:3479	67.105.12.10:49155
7	192.168.1.2:4137	65.12.66.11:3478	67.105.12.10:49156

8 192.168.1.2:4137 65.12.66.11:3479 67.105.12.10:49157

If a device behind this type of NAT knows its behavior, the device will be able to detect that the port number to be allocated by this symmetric NAT will have the same port number as the local port bound in a UDP socket of the device. In this case, once the device detects the type of NAT, it will not perform the binding request to the STUN server and use the local port as a global one with a previously obtained global IP address from the STUN server.

6.5 Symmetric (a) and (d) and Full-cone NAT

Symmetric (a) and (d) are types of symmetric NAT, but they behave like a full-cone NAT in terms of the incoming packet filtering. STUN discovery process with these types of NAT results in full-cone, which is fine but it might have a problem if the device (e.g. EP-a) behind the NAT needs to send a packet to the other endpoint (EP-b).

After obtaining a MAPPED-ADDRESS, EP-a tells EP-b the MAPPED-ADDRESS so that EP-b can send packets to EP-a via the MAPPED-ADDRESS. If EP-a wants to send a packet to EP-b, the packet transmission will cause a new port allocation on the NAT because the NAT is actually a symmetric NAT. Then EP-b will receive a packet from the new port. EP-b believes that it is sending packets to the MAPPED-ADDRESS to talk to EP-a, but the packet is coming from a different port than the MAPPED-ADDRESS. This might cause some confusion in EP-b.

7 NAT Characteristics Discovery using STUN

Current STUN message format and test definitions are used as is in order to detect the NAT types defined in Table 6.3.1.

Test I: The client sends a STUN Binding Request to a server, without any flags set in the CHANGE-REQUEST attribute, and without the RESPONSE-ADDRESS attribute. This causes the server to send the response back to the address and port that the request came from.

Test II: The client sends a Binding Request with both the "change IP" and "change port" flags from the CHANGE-REQUEST attribute set.

Test III: The client sends a Binding Request with only the "change port" flag set.

It does not require any modification to STUN server, either. The only

difference is the discovery process flow as described in the following sections.

7.1 Incoming Packet Filter Type Discovery

The client begins by initiating Test I. If this test yields no response, the client knows right away that it is not capable of UDP connectivity. If the test produces a response, the client examines the MAPPED-ADDRESS attribute. If this address and port are the same as the local IP address and port of the socket used to send the request, the client knows that it is not "natted". The client then executes Test II.

If a response is received during the Test II, the client knows that it has open access to the Internet (or, at least, its behind a firewall that behaves like a full-cone NAT, but without the translation). If no response is received, the client knows its behind a symmetric UDP firewall.

In the event that the IP address and port of the socket did not match the MAPPED-ADDRESS attribute in the response to Test I, the client knows that it is behind a NAT.

Specifically, the process up until this point is considered the NAT presence discovery process. The following process covers the incoming packet filter type discovery that is performed only in situations where the client is behind one or more NATs.

The client performs Test II. If a response is received, the client knows that the NAT that the client is behind has no port filter. If no response is received, the client performs Test III. If a response is received, the client is behind a NAT that has an address sensitive filter. If no response is received, the NAT has a port sensitive filter.

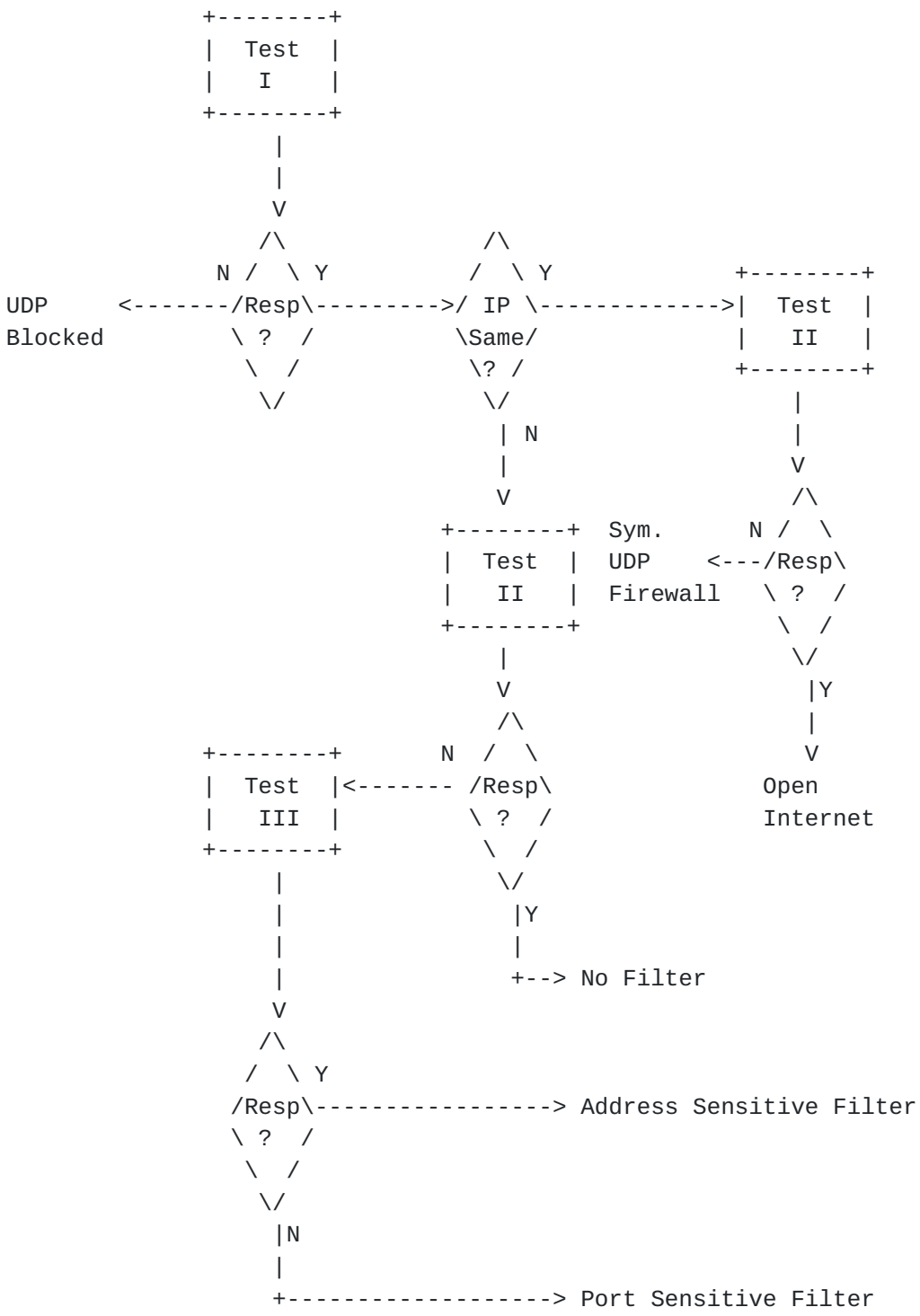


Figure 7.1 Incoming Filter Type Discovery Process Flow

7.2 Port Allocation Rule Discovery

The port allocation rule discovery process is performed only in

situations where the device is found "natted" with a previous NAT presence discovery process. The port allocation rule discovery process uses only Test I, but applies it to different combinations of IP addresses and ports in order to figure out the port allocation characteristics of the NAT. A STUN server uses 2 different IP addresses (Da and Ca) as shown in Table 7.1 and 2 different ports (Dp and Cp). This is the minimal set required to discover the allocation rule.

Table 7.1 Test I Destinations for Port Allocation Discovery Process

	Destinations		
	IP Address	Port	
TRY-1	Da	Dp	<= STUN client obtains Ca and Cp in CHANGED-ADDRESS attribute in the response.
TRY-2	Da	Cp	
TRY-3	Ca	Dp	
TRY-4	Ca	Cp	

Test I is performed 4 times (TRY-1 through TRY-4) per local port. Destinations to which the TRY-1 through TRY-4 are performed are shown in Table 7.1. This process can be done with the same local port that is used in the previous NAT discovery process. Since TRY-1 has already been done in Test I, it can be skipped and testing can begin from TRY-2. The client will obtain 4 MAPPED-ADDRESSes from the responses. The 4 MAPPED-ADDRESSes are analyzed to determine the port allocation rule, the delta p value, and to evaluate consistency.

To look for consistency, the process can be performed multiple times, however, each test should be done from a different local port which does not have a NAT binding associated with it.

The port allocation rule will be determined by looking at the port numbers obtained from MAPPED-ADDRESSes. If all port numbers are incremented at each test, the port allocation rule is 'Port Sensitive'.

If the port increment size from TRY-1 and TRY-2, and the ones from TRY-3 and TRY-4 are always 0, but the incremental size between the ones from TRY-2 and TRY-3 are not 0, the port allocation rule is 'Address Sensitive'.

The delta p value will be determined as follows:

Cone NAT:

If all port numbers of the obtained MAPPED-ADDRESSes are the same, the NAT is a 'Cone NAT'.

Address sensitive allocation:

The delta p is equal to a port increment size between TRY-2 and TRY-3. If the process is re-done one more time from another local port (TRY-5 to TRY-8 as shown in Figure 7.2), delta p should also equal to the port increment sizes between TRY-4 and TRY-5 and between TRY-6 and TRY-7.

Port sensitive allocation:

The delta p is the difference between adjoining port numbers of MAPPED-ADDRESSes obatained from testing (TRY-[N+1] and TRY-[N]).

```
[TRY] [MAPPED-ADDRESS]
  1   67.105.12.10:49152
  2   67.105.12.10:49152 (+0)----+
  3   67.105.12.10:49154 (+2)--+ |
  4   67.105.12.10:49154 (+0)--|-+
  5   67.105.12.10:49156 (+2)--+ |
  6   67.105.12.10:49156 (+0)--|-+
  7   67.105.12.10:49158 (+2)--+ |
  8   67.105.12.10:49158 (+0)--|-+
                               | +-> always 0: 'Address Sensitive'
                               +---> consistently 2: Delta p = 2
```

Figure 7.2 Allocation Discovery Result: Address Sensitive

Figure 7.2 shows the result of the allocation discovery process with a NAT that has an address sensitive allocation rule. TRY-5 through TRY-8 are performed from a different local port than the one used in TRY-1 through TRY-4.

In situations that the internal device could not find the consistency with the port increment size for delta p determination, the application needs to have an algorithm to determine the delta p value based on statistical observation, or to decide to give up obtaining a valid delta p. The device should be able to determine whether or not it is address sensitive or port sensitive. The device still has a chance to traverse the NAT if the NAT combination class is III as described in section 5.

8 Traversing Symmetric NAT

This section describes how the symmetric NAT traversal (specifically, class IV traversal) is accomplished. To aid in this explanation, the following network configuration is used.

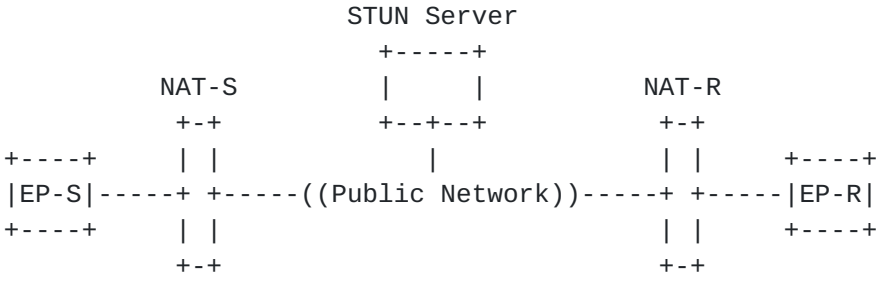


Figure 8.1 Network Configuration

There are two endpoints EP-S and EP-R, for example, that are located behind different NATs (NAT-S and NAT-R, respectively) and EP-R wants to receive UDP packets from EP-S.

Both EP-S and EP-R have performed NAT discovery processes and know the following attributes of the NAT obtained from the discovery processes described in the previous sections.

- Incoming Packet Filter Type
- Port Allocation Rule
- Delta p

8.1 Information To Be Exchanged

Incoming packet filter type attribute is used to determine whether or not an endpoint device needs to send an invitation packet. This attribute is not necessary for the other endpoint and need not be exchanged.

When it comes to sending packets (including invitation packets), the endpoint needs to know the destination address for the packets. If the port allocation rule of the other endpoint is a symmetric type, the endpoint needs either to record the source port number of an incoming packet or to predict a port number that the symmetric NAT will assign, with a MAPPED-ADDRESS obtained from the other endpoint.

The following items are the required information to be exchanged between the endpoints (EP-S and EP-R) in order to traverse NAT (including the class IV case).

- o MAPPED-ADDRESS (from Binding Request with STUN server)
- o Port Allocation Rule
- o Delta p (required if port allocation rule is either address sensitive or port sensitive)

8.2 EP-R Behavior

Soon after the information exchange is complete EP-R decides, using the obtained information, the following items with regard to an invitation packet transmission.

(1) If an invitation packet needs to be sent.
(2) Requirement for its repetition.

(1) is to be decided with port allocation rule of EP-S and incoming packet filter type of EP-R as shown in Table 8.1.

Table 8.1 Invitation Packet Determination Chart for EP-R

		NAT-R Incoming Packet Filter Type		
		No Filter	Address Sensitive	Port Sensitive
NAT-S Port Allocation Rule	Open Cone		YES	
	Address Sensitive	NO	YES (*1)	YES (*2)
	Port Sensitive			

(*1) in Table 8.1 is the case that EP-R mentioned in Figure 8.1 has a NAT that has an address sensitive filter. Although NAT-S is a symmetric NAT (the port shown in MAPPED-ADDRESS is invalid), EP-R can send a packet to any port of the IP address in the MAPPED-ADDRESS. This can be done because the NAT-R's incoming packet filter is not sensitive to its source port.

(*2) If NAT-R has a port sensitive filter and NAT-S is a symmetric NAT, EP-R needs to predict a specific port that will be allocated by NAT-S later on so that EP-R can send the invitation packet to the port.

The invitation packet is required to be sent repeatedly in case the other endpoint (EP-S shown in Figure 8.1) needs to capture the invitation packet to record its source port to which EP-S can send packets afterwards.

The reason for the repetition is that when the first invitation packet is sent from EP-R, NAT-S might not be ready to route the packet to EP-S because EP-S hasn't sent an invitation packet yet. Since EP-S needs to capture the packet to record its source port number, EP-R has to make sure that EP-S receives the invitation packet.

The condition that EP-R is required to send invitation packets repeatedly is when NAT-R follows either address sensitive allocation rule or port sensitive allocation rule.

The retransmission should stop when EP-R starts to receive packets from EP-S successfully, or a time-out event set up for error handling occurred.

NOTE: Even if NAT-R has no filter, EP-R has to send the invitation packets repeatedly because the purpose of the invitation packet in this case is not only for opening the filter on NAT-R for the destination but also for informing EP-S of the source port number allocated by NAT-R.

8.3 EP-S Behavior

Soon after the information exchange is complete, EP-S decides, with the obtained information, the following items with regard to invitation packet transmission:

(1) If an invitation packet needs to be sent.
(2) If source port recording is required.

EP-S only needs to send an invitation packet to EP-R when source port recording is required and NAT-S has either address sensitive filter or port sensitive filter (Table 8.2). By sending an invitation packet, it opens up the filter (door) at NAT-S to NAT-R so that the invitation packet coming from EP-R will be received at EP-S.

Source port recording is required if and only if NAT-S has either address sensitive allocation rule or port sensitive allocation rule.

Table 8.2 Invitation Packet Determination Chart for EP-S

		NAT-S Incoming Packet Filter Type		
		No Filter	Address Sensitive	Port Sensitive
NAT-R Port Allocation Rule	Open Cone	NO	YES	YES
	Address Sensitive		YES (*3)	YES (*4)
	Port Sensitive			

(*3) in Table 8.2 is the case in which EP-S mentioned in Figure 8.1 has a NAT that has an address sensitive filter. Although NAT-R is a symmetric NAT (the port shown in MAPPED-ADDRESS is invalid), EP-S can send a packet to any port of the IP address in the MAPPED-ADDRESS. This can be done because the incoming packet filter for NAT-S is not sensitive to its source port.

(*4) If NAT-S has a port sensitive filter and NAT-R is a symmetric NAT, EP-S needs to predict a specific port that will be allocated by NAT-R later on so that EP-S can send the invitation packet to the port.

8.4 Increasing Prediction Success Rate

In order to increase success rate of the port prediction for symmetric NATs, invitation packets can be sent to multiple destinations that are possible next ports to be allocated by symmetric NATs.

For example, NAT-R has a port sensitive filter and a port sensitive allocation rule. NAT-S has a port sensitive filter and an address allocation rule. In this case, source port recording is required. In order for EP-S to capture an invitation packet from EP-R, EP-S sends an invitation packet to a predicted port on NAT-R. The prediction is typically made by adding delta p to the port number of the MAPPED-ADDRESS obtained from EP-R earlier.

As mentioned in section 6.1, a symmetric NAT might not allocate the predicted port number because the port might be in use and skipped to

the next one (+2 * delta p). For that reason, EP-S can send invitation packets not only to +delta p, but also to the next possible ports such as +2*delta p, +3*delta p,...as shown below.

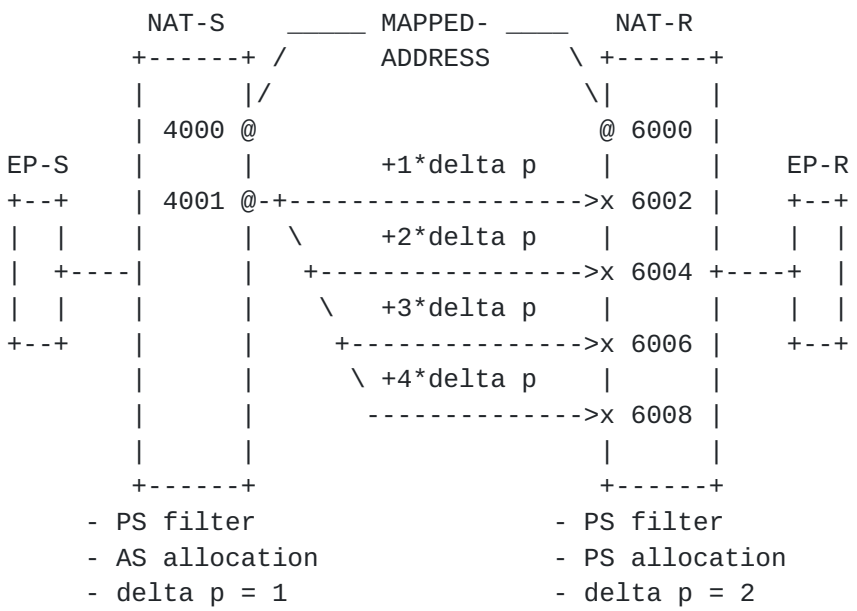


Figure 8.2 Invitation Packets To Multiple Predicted Ports

Sending invitation packets to multiple predicted ports is possible because NAT-S will not create a new port each time it sends an invitation packet to NAT-R. This means that if NAT-S is a port restricted-cone NAT, the method will still work.

If NAT-S has a port sensitive allocation rule and a port sensitive filter, this additional invitation packet does not help increase the success rate. Each time EP-S sends an invitation packet to a different port, EP-S allocates another port. The whole purpose of sending invitation packets to multiple ports on NAT-R is to have one specific port accept incoming packets from the multiple ports on NAT-R. New allocations on NAT-S defeat this purpose.

In Figure 8.3, EP-S is sending an invitation packet to multiple ports on NAT-R, assuming that when EP-R sends an invitation packet to NAT-S, NAT-R will allocate one of these ports (6000 through 6008) for the packet. If NAT-R allocated 6004 when EP-R sends an invitation packet to 4001 on NAT-S, for example, as NAT-S has port sensitive filter and 4001 never sent a packet to 6004, it blocks the incoming packet.

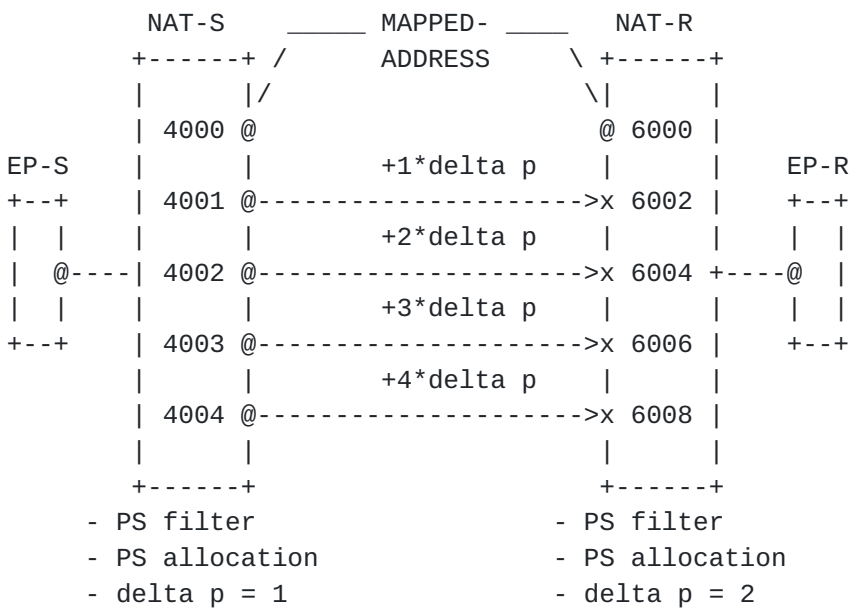


Figure 8.3 Invitation Packets To Multiple Predicted Ports

The benefit of knowing which allocation rule (address sensitive or port sensitive) a symmetric NAT has is that the discovery of the address sensitive allocation rule will increase the success rate of the port prediction.

9 Normative Reference

[1] Rosenberg, et al. "STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)" RFC 3489, March 2003.

[2] Rosenberg, J., "Traversal Using Relay NAT (TURN)", draft-rosenberg-midcom-turn-00.txt, November 2001.

[3] D. Yon, "Connection-oriented media transport in SDP," Internet Draft, Internet Engineering Task Force, May 2002. Work in progress.

[4] Rosenberg, et al. "NAT and Firewall Scenario and Solutions for SIP", draft-ietf-sipping-nat-scenarios-00.txt, IETF, June 24, 2002.

[5] M. Handley, V. Jacobson, "Session Description Protocol (SDP)", IETF RFC 2327, April 1998.

[6] P. Srisuresh, K. Egevang, "Traditional IP Network Address Translator (Traditional NAT)," RFC 3022, Internet Engineering Task Force, January 2001.

[7] J. Postel, "internet protocol", RFC 791, Internet Engineering Task Force, September 1981.

10 Author's Address

Yutaka Takeda
Panasonic Communications Research Laboratory
10993 Via Frontera
San Diego, CA 92127

EMail: takeday@kmerl.com