Firewall and Network Address Translation (NAT) Support

On this Page

Figure Reference

Overview

When a user on the internal network initiates a request to the Internet, their private IP address is translated to the public IP address when the request goes through the firewall/Network Address Translation (NAT) to the Internet. This is so the destination site knows the IP address to which it should return the information. The firewall/NAT maintains a log of which endpoints requested what destinations, and when a response is received from a destination site, the firewall/NAT directs it to the endpoint that made the original request.

When the VX is on a private network and needs to establish a call to a SIP UA in the public network, the call goes through a NAT server. The NAT translates the IP address in the IP header, but generally, it is not able to translate the IP Address in the SIP and SDP Headers.

This feature enables VX's signaling and audio stream NAT traversal assuming that the VX is placed behind a NAT on the Private Network side. The VX uses the Public IP of the NAT behind which it is placed, in all SIP and SDP messages for making SIP calls to/receiving SIP calls from devices on the public internet.

In the following sections, the call direction is referred as follows:

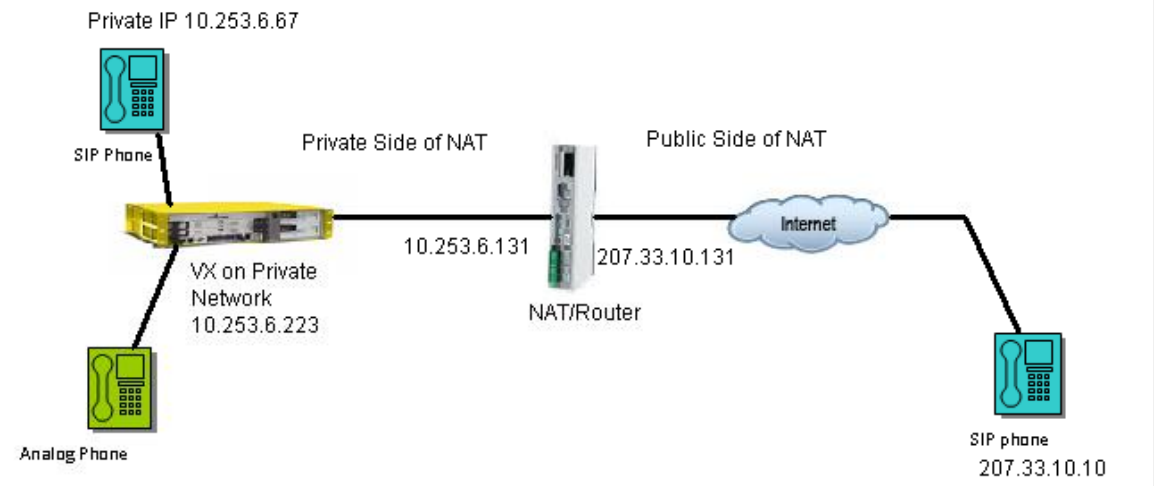
Forward Direction Call: Call initiated from inside the Private side of the NAT to the Public side.
Reverse Direction Call: Call initiated from Public side of the NAT to the Private side

In addition to the SIP calls, this feature works for other SIP messages like Subscribe, Register, etc.

Network Layout

A Network Diagram showing VX behind a NAT is shown in Figure 1.

Figure 1: Network Diagram Showing VX Behind a NAT



Feature Details

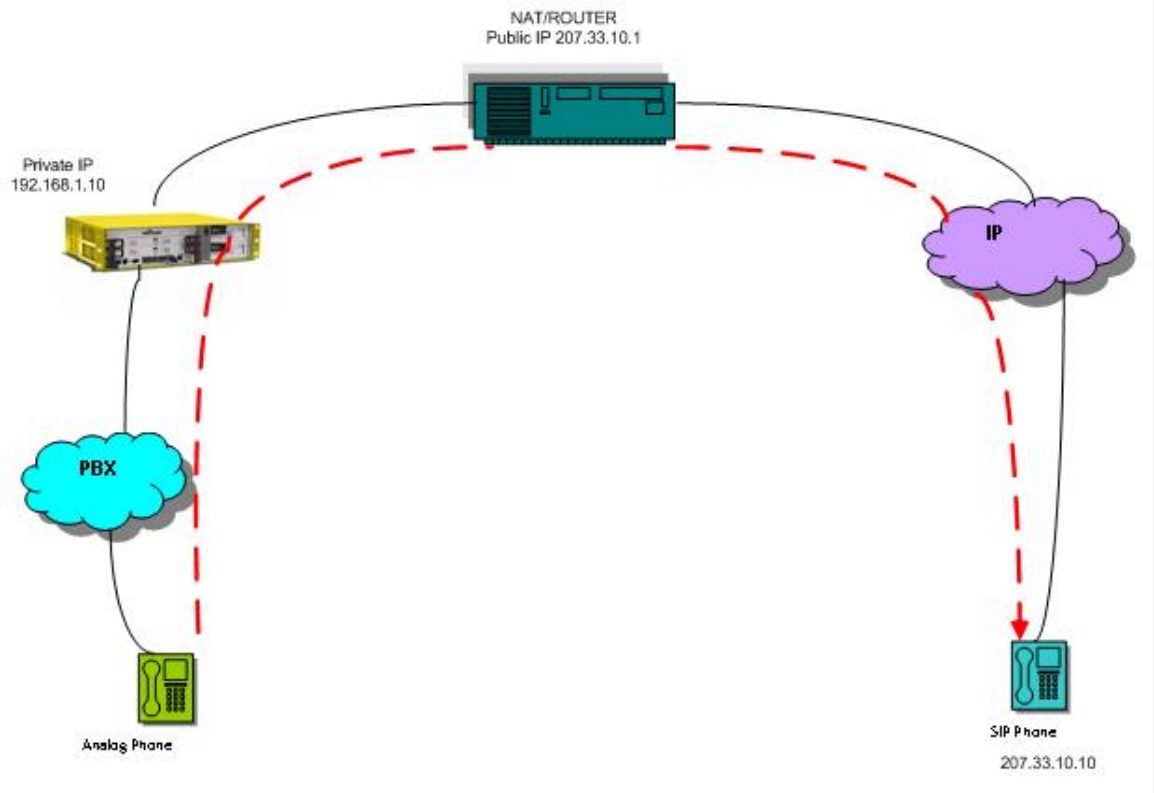
In VX, SIP messages are routed through Trunkgroups. If a Trunkgroup is configured with VX being behind a NAT, the SIP Signaling and Media Packets are populated with the Public IP of the NAT, which is a configurable item in the SIP Tab of the Trunkgroup.

This requirement is specific to the SIP protocol. None of the management protocols on the VX need to be aware of the Public IP Address even when behind a NAT. It is also assumed that the NAT will always use the same port for public and private IP Addresses with regard to SIP Signaling and RTP Media as used by the VX. The NAT IP set in the SIP tab of the Trunkgroup is assumed to have a static Public Address in dotted decimal IP format.

Examples

Forward Call Scenario

Figure 2: SIP Forward Direction Call Scenario



Note the following:

1. In this example, the PSTN Phone initiates a call that lands on the VX.(If it's a SIP entity that initiates the call, then it's assumed that the VX is acting as a B2BUA). In this setup, the VX is placed behind a NAT and has a private IP Address of 192.168.1.10.

2. The Machine performing the NAT has a Private Address of 192.168.1.1 on one side of the NAT and a Public Address of 207.33.10.1 on the other side of the NAT.

3. VX sends an INVITE to the SIP Phone in the Public domain. The IP of this phone(UAS) as shown in Figure 3 is 207.33.10.10.

4. In such a scenario, as per the current behavior, the VX generates an outbound SIP INVITE with the From, Call-ID, Via and the Contact fields in the SIP Header and the Owner and the Connection Information fields in the SDP Header with the Private IP of the VX (192.168.1.10 in this example).

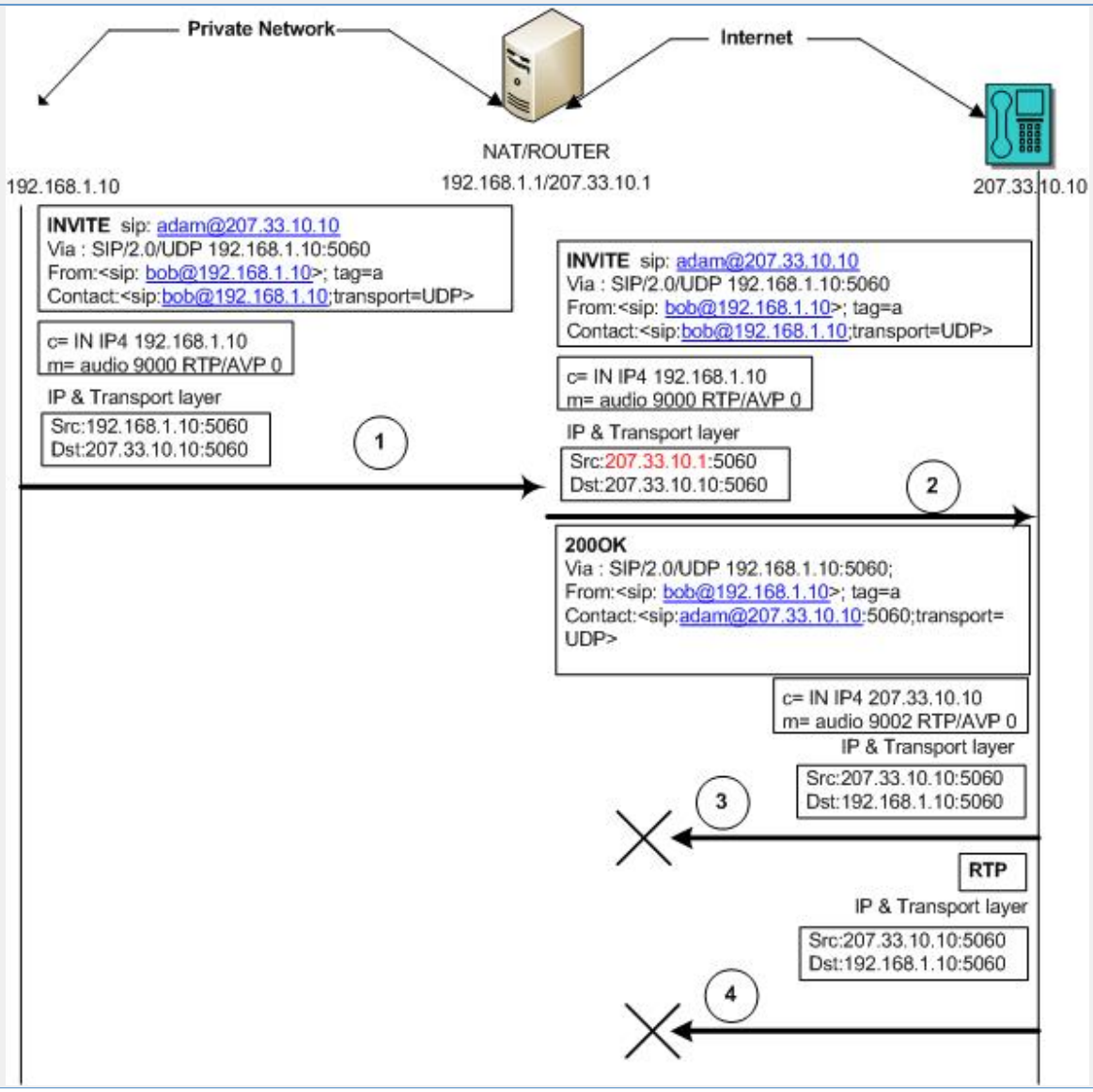
5. The INVITE Request intended for the SIP Phone in the Public Domain reaches the device performing NAT. The NAT device replaces the Private Address present in the Source IP (in the IP Header) of the outgoing INVITE with the Public Address of the NAT, which in this case is 207.33.10.1.

This INVITE reaches the SIP Phone in the Public Domain. The SIP Phone formulates a reply to this INVITE and tries to send it to the IP Address in the Via Header of the incoming INVITE, for example the Private IP is 192.168.1.10. Since this Private Address is not routable, the reply would not reach the VX and hence the SIP Signaling would not come up.

A similar issue is seen for the RTP Media. The Media Description carried in the SDP Header of the SIP INVITE generated by the VX behind NAT contains the Private IP Address (192.168.1.10 in our example). The SIP Phone in Public Domain tries to send the RTP to this Private Address. As the Private Address is not routable, RTP Media is unable to reach from the SIP Phone (207.33.10.10) in the public domain to the VX (192.168.10.10) in the private domain.

The call flow in Figure 3 depicts the problem.

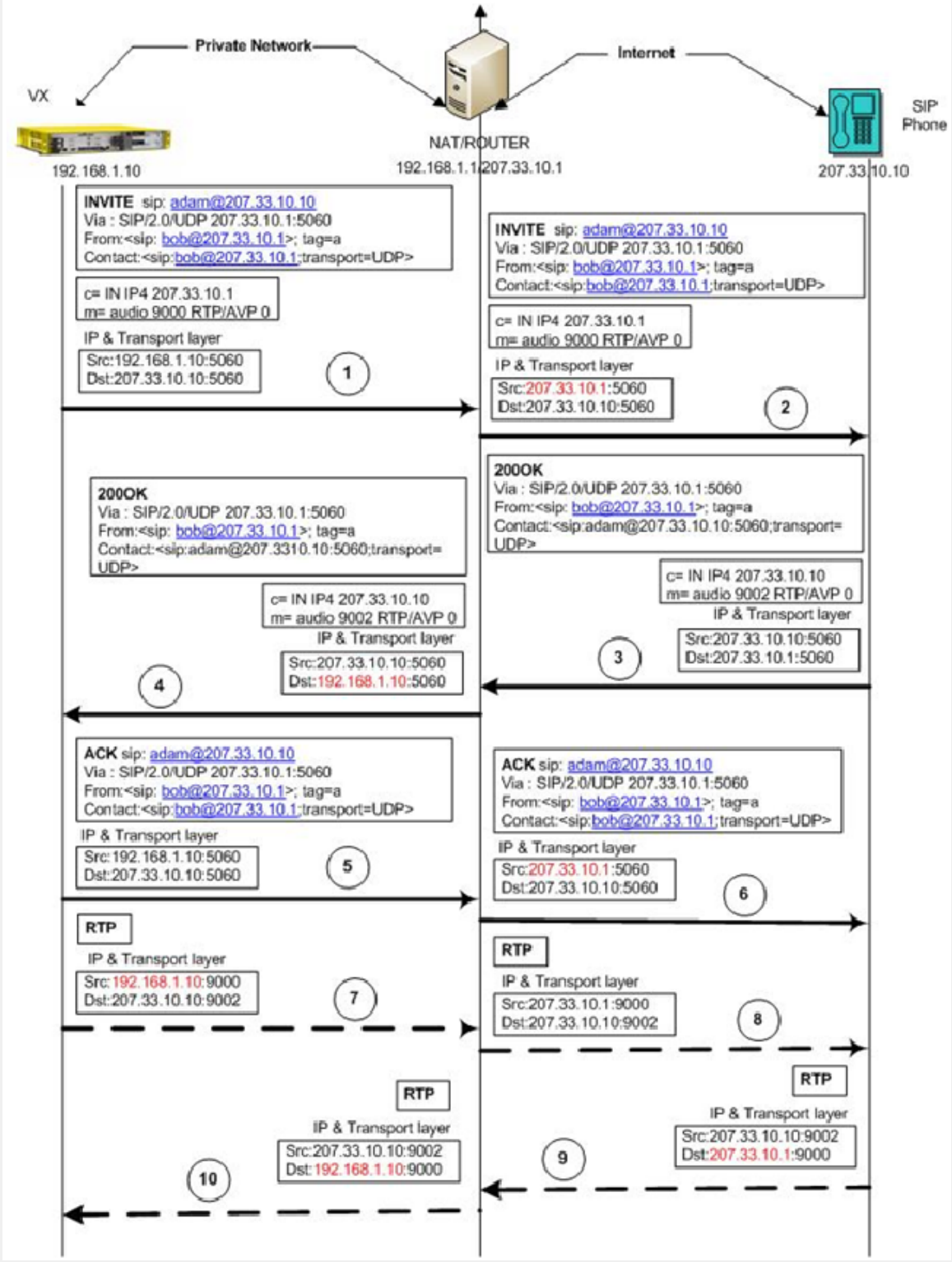
Figure 3: Call Flow as per Current VX Behavior



6. With the new feature in place, VX would populate the SIP Headers fields like From, Call-ID, Via and the Contact in the INVITE message with the Public IP of the NAT(207.33.10.1 in the example diagram) if this is configured. Also this Public IP will be populated in the SDP Header fields like Owner and Connection Info.

7. When the SIP Phone on the Public IP 207.33.10.10 receives this SIP INVITE, it sends back the SIP Responses and RTP Packets to the Public IP of NAT(207.33.10.1). The NAT Machine performs Reverse NAT on all the incoming packets and hence forwards these packets to the VX which in turn relays the media back to the originator. And hence the signaling and media path flows properly as shown in Figure 4.

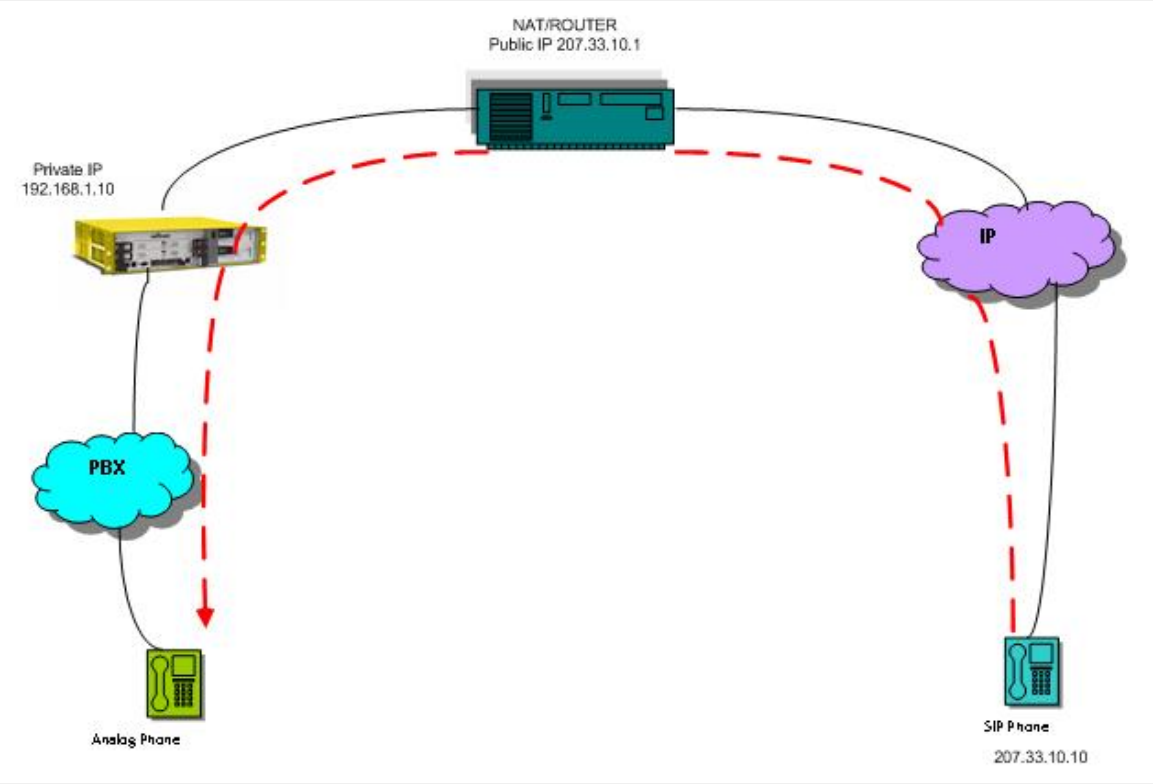
Figure 4: SIP Forward Direction Call Flow



Reverse Call Scenario

Figure 5 and 6 depict a Reverse Call Scenario.

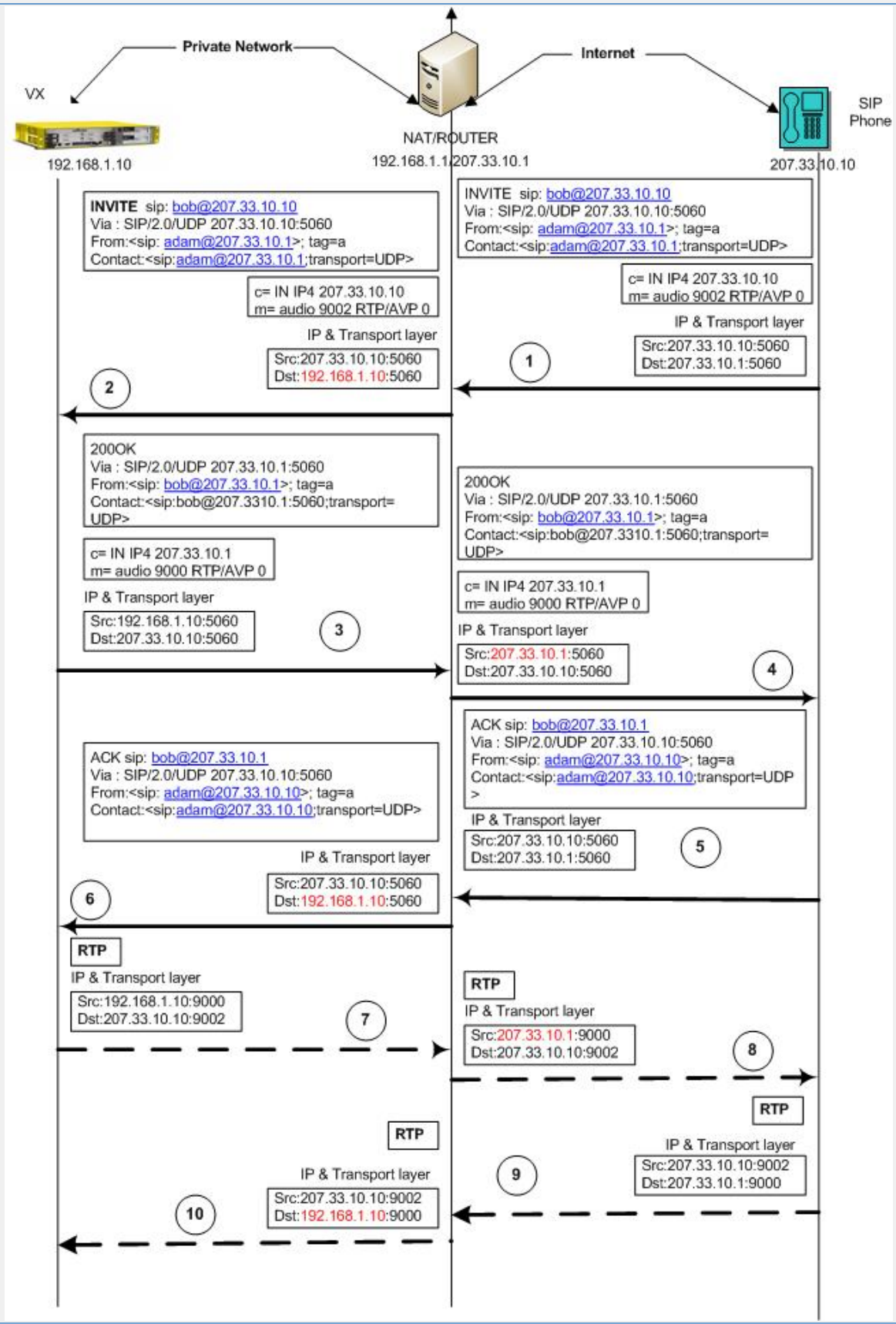
Figure 5: SIP Reverse Direction Call Scenario



Assumption: The NAT just statically maps the Public IP and the Private IP and vice versa keeping the port same.

1. For the calls in the Reverse direction, from public side of the NAT to the private side, the SIP requests should be destined to the Public IP Address of the NAT Machine (207.33.10.1 in our example). The SIP Headers fields To and Request-URI should thus contain this public Address.
2. When the SIP Request reached the NAT machine, it will perform reverse NAT and replace the Destination Address in the IP Header with the Private Address of VX.
3. The VX, acting as a B2BUA, on receiving this request should then generate a new INVITE to the local endpoint if it is a SIP UA or perform appropriate action like Ringing, if it's a PSTN phone.
4. The SIP Responses from the VX destined to the UAC (SIP Phone with IP 207.33.10.10 on the public side in our case) should contain the Public IP of the NAT in the SIP Header fields From, Call-ID, Via and the Contact and the SDP Header fields Owner and Connection-Info as shown in the call flow in Figure 6.

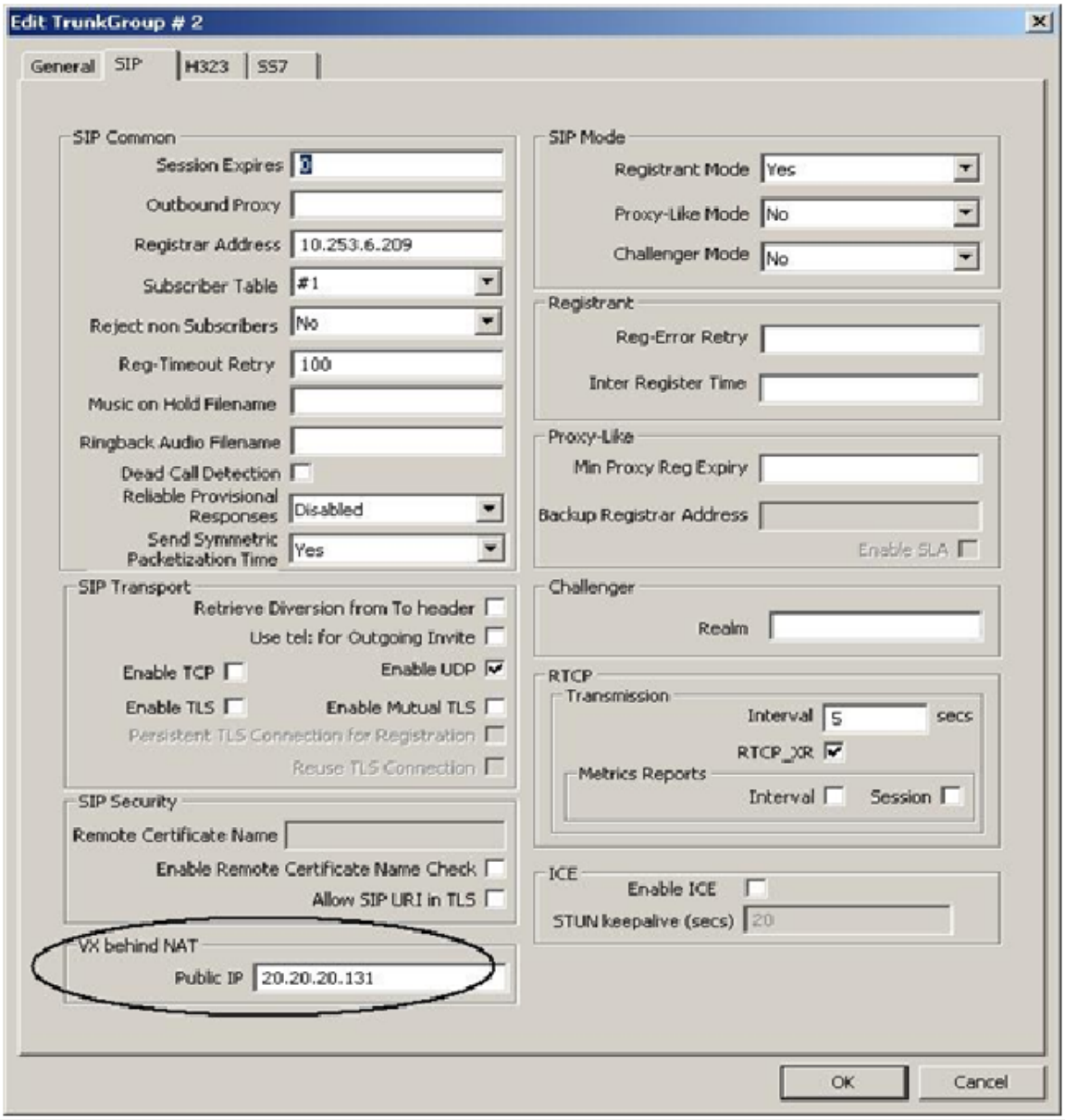
Figure 6: SIP Reverse Direction Call Flow



Configuring Support for VX Behind NAT Using VXbuilder

You can use VXbuilder to configure Support for VX behind NAT support. Access the **Edit TrunkGroup>SIP** tab view and enter a dotted decimal IP Address for the Public IP of the NAT in the **VX Behind NAT** section, as shown in Figure 7. The enabling/disabling of this feature takes effect for new SIP calls only, and a value of 0.0.0.0 or a blank entry in the Public IP field means that the Public IP of the NAT is not configured for this particular Trunk Group.

Figure 7: Network Diagram Showing VX Behind a NAT



Configuring the NAT IP Address using the CLI

You can set the NAT IP Address using the CLI by entering **nat-public-ip** and the IP Address. An Access Level 15 is required to perform this action.