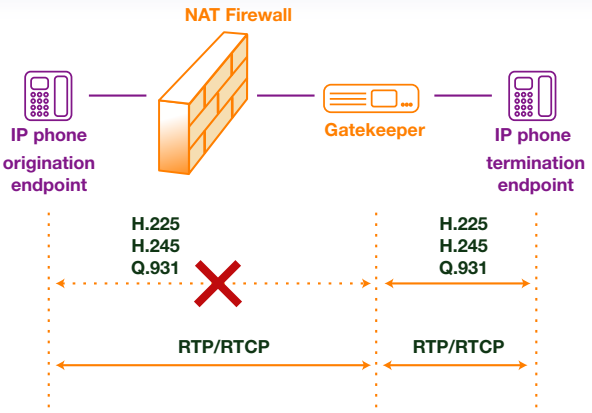
SysMaster™

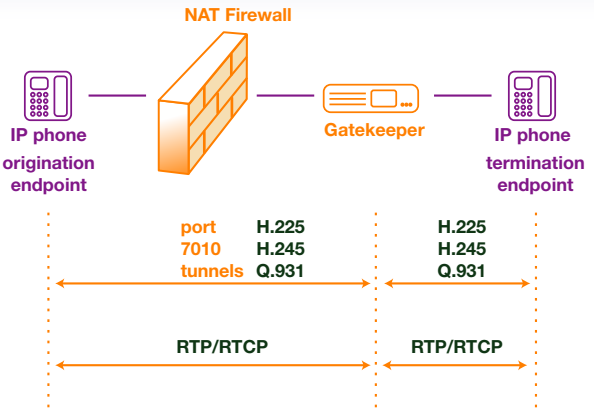
NAT TRAVERSAL SOLUTION

H.323 NAT Technology

problem



solution



problems

- Usage of private IP addresses and NAT firewall to prevent connections to be established to devices behind the NAT firewall.
- H.323 protocol uses three types of network connections for a VoIP call. Any problem that causes the loss or inability to establish any of these three connections will result in H.323 call failure.
- Call Signal (Q.931/H.245) is a TCP network connection that can not be established from outside the NAT firewall.
- Call Setup (RAS) is a UDP network connection that may have different send and receive ports.
- Call Voice Data (RTP/RTCP) is a UDP network connection that may have different send and receive ports.

solution

There are two call scenarios:

- **Outbound Calls**

In this scenario, the call origination party is behind NAT. For outbound calls to support two-way audio, the following conditions must be met:

1. The H.323 origination endpoint (IP Phone, Soft Phone, etc.) must use the same port to send and receive RAS messages. The default port for RAS communication is 1719.
2. The H.323 origination endpoint (IP Phone, Soft Phone, etc.) must use the same port to send and receive RTP/RTCP voice data packets. If the send and receive ports are different - the connection will support one-way audio only.

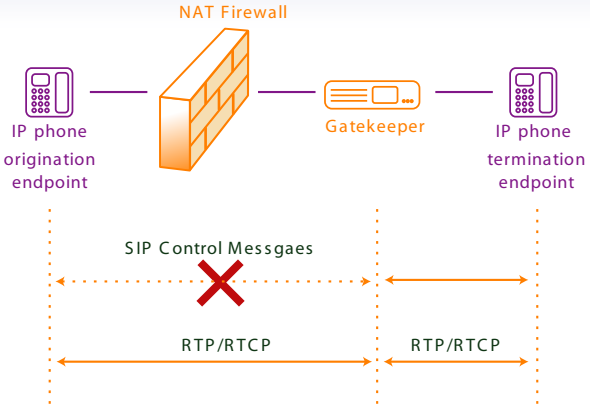
- **Inbound Calls**

In this scenario, the calls are originated from outside the NAT firewall and terminated into the endpoint which is behind the NAT firewall. Unfortunately, due to the fact that the call must be established outside the NAT firewall it will be dropped by the firewall unless one of the following methods is used:

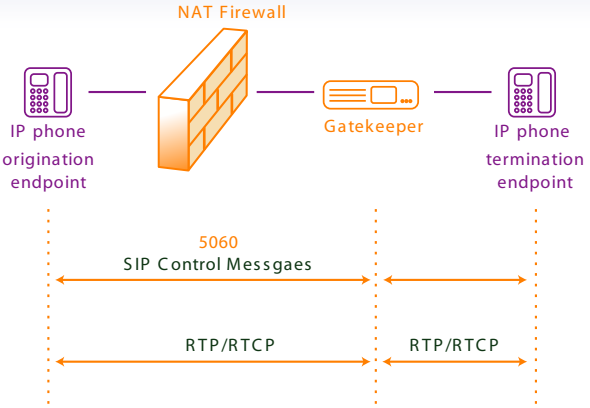
1. **NAT Traversal** - this is special software that runs on the endpoint and on the gatekeeper that supports permanent socket connection between them to transfer call data. Since the socket is established and supported from the endpoint (behind NAT) to the gatekeeper (outside the NAT) this connection is constantly available and can be used to make a successful inbound call.
2. **Bi-directional NAT Firewall** - this is a special NAT firewall that will translate outside connection into inside port number or IP address.
3. **DMZ NAT Firewall** - some firewall allow DMZ settings that allow direct packet routing to particular IP address that represents the endpoint behind the NAT firewall.

SIP NAT Technology

problem



solution



problems

- Usage of private IP addresses and NAT firewall to prevent connections to be established to devices behind the NAT firewall.
- SIP protocol uses two types of network connections to complete a VoIP call. Any problem that causes the loss or inability to establish any of these two connections will result in SIP call failure.
- Call Message is a TCP or UDP network connection that can not be established from outside the NAT firewall.
- Call Voice Data (RTP/RTCP) is a UDP network connection that may have different send and receive ports.
- Some companies use STUN servers to facilitate connections of endpoints behind NAT, but these servers are usually used for endpoints that do not comply with universal requirements. However, most contemporary endpoints including all Cisco SIP Phones allow TTL and port setting to accommodate the NAT.

solution

Outbound Calls

In this scenario, the call origination party is behind NAT. For outbound calls to support two-way audio, the following conditions must be met:

1 The SIP origination endpoint (IP Phone, Soft Phone, etc.) must use the same port to send and receive Call Messages. The default port for Call Message communication is 5060.

2 The SIP origination endpoint (IP Phone, Soft Phone, etc.) must use the same port to send and receive RTP/RTCP voice data packets. If the send and receive ports are different then the connection will support one-way audio only.

solution

Inbound Calls

In this scenario, the calls are originated from outside the NAT firewall and terminated into the endpoint which is behind the NAT firewall. Due to the nature of the SIP protocol, inbound calls behind NAT are possible if the following conditions are met:

1 The Registrar and the proxy SIP Server must reside on the same network server (have the same IP address). The fact that the endpoint sends UDP registration call messages according to its TTL (time-to-live) parameter to the SIP Registrar, allows the NAT firewall to maintain an open port from the internal endpoint (IP Phone, Soft Phone, etc.) to the SIP Registrar/Proxy. This open firewall port is used by the Proxy to send inbound Call Messages to the endpoint (usually on port 5060).

2 Low TTL (time-to-live) setting on the endpoint (usually 60 seconds) needs to be less than the corresponding TTL parameter for connection persistency on the NAT firewall.

3 The endpoint must send and received Call Messages on the same port (default 5060).

4 The endpoint must send and receive RTP voice data on the same port (other than 5060). Once the Call Message is received by the endpoints, it opens an UDP session to the SIP Proxy to allow RTP voice data transfer.

SysMaster
2700 Ygnacio Valley Rd, Suite 210
Walnut Creek, CA 94598
United States of America

Email: sales@sysmaster.com
Web site: www.sysmaster.com