Gigaset VoIP telephones behind various routers with Network Address Translation (NAT)

NAT constitutes a basic obstacle to VoIP telephony. Typical error patterns caused by NAT are:

1. Absence of speech paths, sometimes partial paths
2. Incoming calls not possible
3. Outgoing calls unsuccessful

Preferred Port- and Router-Configuration in case of NAT Problems

Usually there is no special router configuration required to run Gigaset VoIP phones behind NAT. But if there are error patterns, such as described above, they often could be fixed by selecting exclusive SIP and RTP port numbers in the Gigaset VoIP phone. In some cases it might additionally be necessary to program Port forwarding rules for these ports in the router:

1. Use exclusive Port Numbers for SIP and RTP in the Gigaset VoIP phone: Especially if there are additional VoIP phones in the LAN, it might help to choose port numbers, which are not used by any other host or application in the LAN and which are far away from the default SIP and RTP ports (e.g. random numbers from 1024 up to 49152). You need to know, that RTP protocol uses the preconfigured RTP base port number (e.g. 5004) and the next two even port numbers (e.g. 5006 and 5008). In the latest software releases you can configure a range of RTP ports. As you need to remember these port numbers for router configuration, you could choose numbers, which are quiet similar to the default settings, e.g.:
   SIP: 49060 instead of 5060
   RTP: 49004 (up to 49008) instead of 5004 (up to 5008)

   Recommended procedure to change SIP and RTP ports:
   1. Change SIP and RTP ports.
   2. Wait until active SIP accounts are registered again.

2. **Port forwarding (or Port-mapping)**
   For these port numbers of the Gigaset VoIP phones you need to program port forwarding rules in the router, to ensure, that these port numbers are also you used at the WAN interface with the public IP address.
   e.g.:

Protocol	public Port	local Port	Host (IP-address)	
UDP	49060	49060	192.168.2.10	for SIP
UDP	49004-49008	49004-49008	192.168.2.10	for RTP

   In the latest software releases of Gigaset VoIP phones you can configure a range of RTP ports. Then you also have to program port forwarding rules for this range of RTP ports. To allow for such port forwarding rules, the DHCP settings of the router must ensure, that the Gigaset VoIP phone always gets the same local IP address.

Background Information

Following you find further details about NAT traversal of VoIP traffic.

STUN

The STUN protocol is the preferred instrument of Gigaset VoIP telephones for overcoming NAT. And in many cases it is sufficient. If the problems described above arise even though the STUN protocol is activated, the deactivation of the STUN protocol is a useful test for troubleshooting. This measure enables any "helpers" that are available in the router (SIP Application Layer Gateway) or with the provider (SIP Proxy and RTP Proxy) to intervene and support NAT traversal.

symmetric NAT

There is a so-called symmetric NAT, on which the STUN protocol does not work adequately. If a Gigaset VoIP phone is connected behind a symmetric NAT, although it can correctly ascertain the public IP address used for the VoIP protocols, it nevertheless cannot ascertain the public port mappings that the NAT will assign to the VoIP protocols. The Gigaset VoIP phone then assumes that the local ports set up for SIP and RTP also correspond to their public mapping. But this is not necessarily the case. The user can make sure that it is, however, with the following options.

1. Option: Port Forwarding Rules:
   The user can generally program so-called Port Forwarding Rules in the router, which ensure that the VoIP ports used locally in the Gigaset (e.g. 5060 for SIP and 5004 and ff. for RTP) are mapped on the WAN side to the same port numbers. Only the base port can be set up for the RTP port on the Gigaset VoIP phone. Depending on the number of parallel VoIP calls supported, the subsequent even port numbers are used for RTP: 2 for devices that support one VoIP call, 3 for those that support two VoIP calls simultaneously. For example: 5004 is set up as the RTP port. Two

parallel VoIP calls are supported. So 5004, 5006 and 5008 are used as RTP ports

2. Option: Use of exclusive ports for VoIP protocols
   The user can set up the VoIP ports used locally in the Gigaset (for SIP and RTP) in such a way that no other subscriber in the LAN can use the same ports. With many routers, although by no means all, the ports are not re-mapped by the NAT in such cases, which means they meet the requirement that the locally set port numbers are also used on the WAN side.

Ambiguous Port Numbers within the LAN

Some NAT implementations have problems with forwarding traffic returning to the LAN to the correct LAN subscriber if multiple LAN subscribers are using the same port numbers for this. So for Gigaset VoIP telephones this behavior results in problems when further subscribers in the LAN, especially VoIP telephones or VoIP clients on connected PCs, are also using the port numbers set up on the Gigaset phone for SIP and port number ranges for RTP. In this case it is necessary to set up in the Gigaset VoIP phone exclusive port numbers (or port number ranges) for SIP and RTP, which no other LAN subscriber uses. It would also be possible to use the option of "random port numbers" for this, if latest firmware release is installed. For random port numbers it is not possible to program port forwarding rules in router.

SIP-Application Layer Gateway (SIP-ALG)

Often there might be SIP-ALGs implemented in routers, which try to correct the effect of network address translation in the SIP protocol. But SIP-ALGs can also be troublesome in certain cases. This can be the case when older implementations modify the SIP protocol in a way that does not comply with RFC3261. It can then be helpful to deactivate a SIP-ALG in the router/gateway (rarely possible) or to circumvent the SIP-ALG. Circumventing the SIP-ALG is sometimes possible by setting up a local SIP server port for the Gigaset VoIP phone that is far removed from the conventional SIP ports (5060, 5062, …).

Gigaset VoIP phones with integrated Router

Gigaset VoIP phones with integrated Router (CE450 IP R and AM variant) are somewhat different from the other Gigaset VoIP telephones as far as NAT traversal strategy is concerned. Depending on firewall settings, the integrated router implements symmetric NAT. So STUN is not particularly suitable for NAT traversal. Instead, the integrated router implements a SIP Application Layer Gateway which helps the SIP and SDP protocol to overcome the influences of NAT. This works very well as long as the NAT of the integrated router is the only NAT that needs to be overcome (e.g. if the CE450 IP R is connected directly to a DSL modem). Should the CE450 IP R be installed behind another NAT (router/gateway) however, this strategy no longer works.

The following measures are then required:

1. Activate STUN
2. Circumvent SIP-ALG in the CE450 IP R router. This is possible by setting up a SIP port outside the range of 5056-5071 in the telephony part of Gigaset CE450 IP R.
3. Enable Firewall.
4. Ensure, in accordance with the preceding sections on symmetric NAT, that the ports set up locally in CE450 IP R for SIP and RTP are used on the "public" side (WAN side) of the router in question. For this it may be necessary to program Port Forwarding Rules in both routers (CE450 IP R and upstream router).

Incoming request from other than the preconfigured SIP-Proxy

In order to pass through the NAT, incoming requests to the Gigaset VoIP phone must always be originiated by that communication endpoint, which the Gigaset VoIP phone expects requests to come from, because only to these endpoints a NAT binding is opened and maintained. Usually, this is the preconfigured SIP-Proxy. There are provider, which might send requests to the Gigaset VoIP phones via other SIP servers. Such requests will probably not pass through a NAT. For these providers, it is necessary to open the SIP listen port even at the WAN-interface by programming a port forwarding rule in the router.