en-firewall

H.323 and firewalls/NATs

Intended for firewall administrators. If you have further comments on this document, please let us know at video-admin@niif.hu.

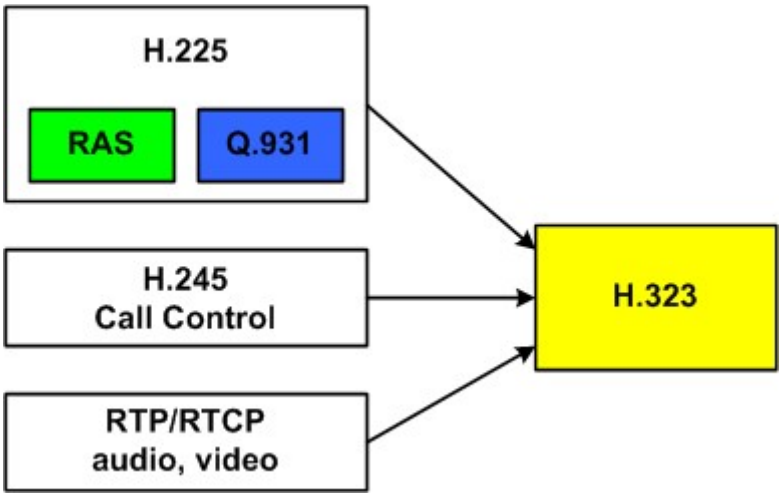
Why is it so difficult to get a H.323 terminal working with a firewall?

- H.323 is an extremely complex protocol system (set of protocols). Protocol messages are all ASN.1 encoded, which is demanding and complicated to decode for firewall/NAT systems in real-time.
- Several fix and dynamically allocated TCP and UDP ports are used (H.245, RTP/RTCP for audio and video streams).
- In case of using NAT address translation, most NAT system does not even speak the H.323 protocol, that makes impossible to change application layer carried IP addresses depending on NAT address allocation.

What are relevant parts of the H.323 protocol system?

Most important protocols used by H.323:

- H.225:
  - RAS (Registration, Admission and Status): endpoint and gatekeeper signalling (registration, call admission, etc.).
  - Q.931: call setup signalling.
- H.245: call control protocol (endpoint capability negotiation, appling changes during calls, etc.).
- RTP/RTCP: audio and video stream transport and its control protocol.



What ports are used by H.323?

Elements of H.323 (H.225, H.245 and RTP/RTCP) use the following ports:

H.323 protocol	Protocol	Port(s)	Direction and scope of communication
H.225	-	-	-
RAS	UDP	1719	bidirectional, endpoint-gatekeeper
Q.931	TCP	1720	bidirectional, endpoint-gatekeeper
H.245	TCP	dynamic (1024-65535)	bidirectional, endpoint-endpoint
RTP/RTCP	UDP	dynamic (1024-65535)	bidirectional, endpoint-endpoint

Allocation of dynamic ports (1024-65535) is done by the protocol used for communication in prior to the actual protocol (ie. in case of H.245 by Q.931, in case of RTP by H.245 messages).

What should I do with my firewall?

The following ports should be opened to get it working:

- RAS and Q.931 ports in both directions,
- RTP ports: Since RTP ports are allocated dynamically, it is very difficult to cope with. Usually, videoconference terminals allow usage of fix port intervalls, stretching to 4-8 ports only. The most secure is to require your users to enable fix port interval usage at the videoconference terminal (see examples below).

When using fix port intervals, H.245 messages are tunneled in the Q.931 connection, so it is not required to open up a bunch of TCP ports at the firewall.

Examples

Polycom ViewStation FX videoconference endpoints (admin setup menü):

```
System Info
 Admin Setup (enter admin password, if exists)
   LAN/H.323
     LAN/Intranet
       Firewall/LAN Connection

Use Fixed Ports: (check, add start of fixed port interval both with TCP and UDP, by default it
is 3230 (do not change it if it is not necessary))
```

Polycom VSX 7000 videoconference endpoint:

```
System
  Admin Settings (enter admin password, if exists)
    Network
      IP
        Firewall

Fixed ports (check, with TCP 3230-3235, in case of UDP 3230-3253 are the default values)
```

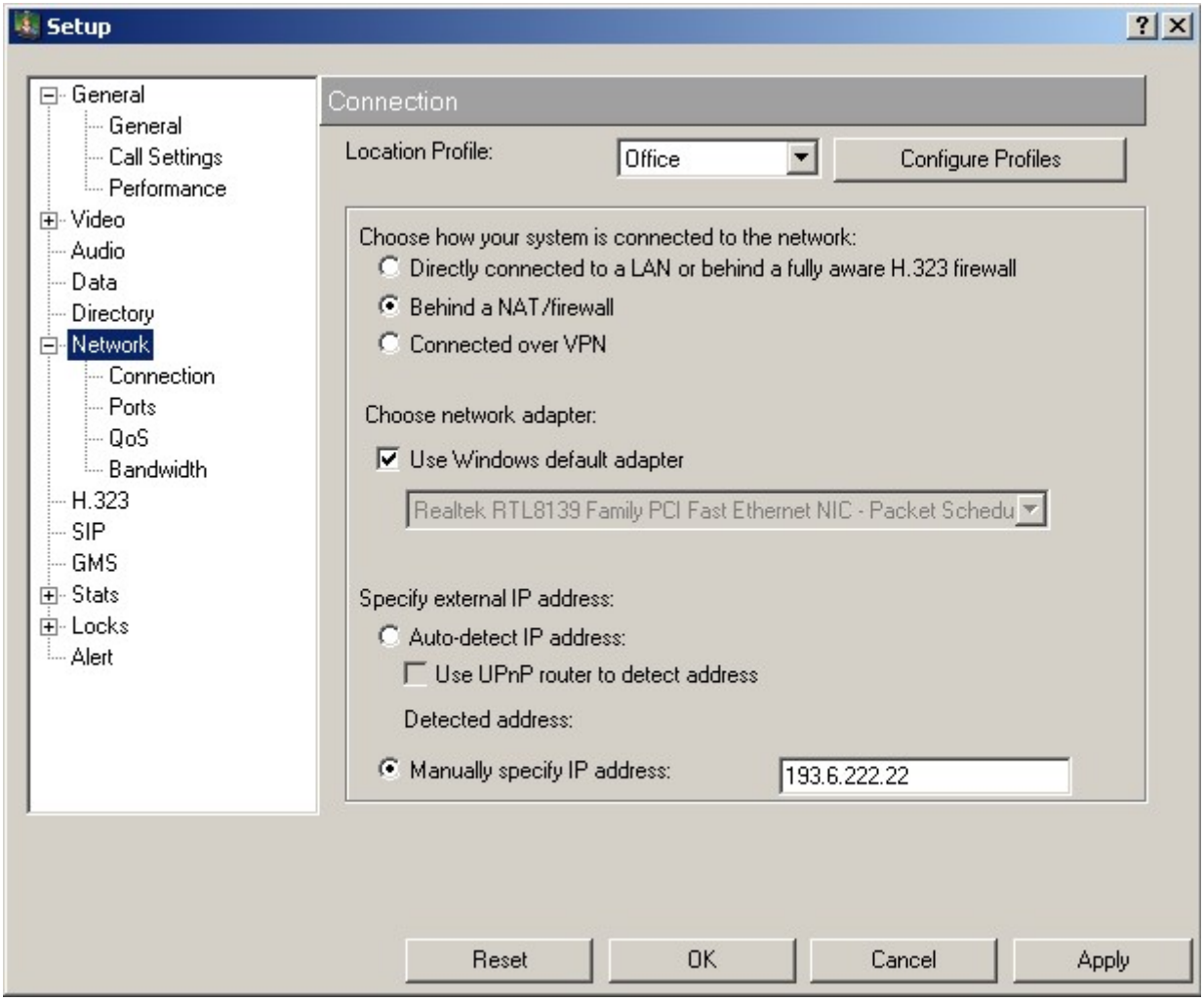
Hardware endpoints often feature an internal MCU (they can provide a simple shared screen multipoint functionality for max. 4-6 connected clients). When having a single pont-to-pont videoconference call, we need 8 RTP (UDP) ports (1-1 for audio and video, content and far-end camera control, and 4 additional RTCP ports). When operating the internal MCU, many more ports are required to open (connected clients x 8).

Polycom PVX software videoconference client (Preferences menu):

```
Network
  Behind a NAT/firewall
  Specify external IP address (use either autodetect (UPnP) or enter IP manualy)

Network
  Ports
    Media port range (UDP and TCP): (by default it is the 3230-3237 interval that is set, this
```

```
have to be opened on the firewall)
    Use UPnP port forwarding: (with UPnP)
```



What about NAT?

H.323 communication is bidirectional (outgoing and incoming calls), thus the following approach should be used:

- Fix address translation (one-to-one private/public IP allocation),
- Fix port translation (using fix port intervals by the endpoint is suggested, see above),
- Allocate a public address for the endpoint, and configure it on the videoconference terminal as external address or use UPnP if possible.

Tipical problems caused by firewalls

Below problems are tipically caused by wrong firewall configuration:

- The endpoint is not able to register at the gatekeeper: H.225 RAS port is not opened.

- The call rings (several times), but it is not established: the firewall does not allow traversing (in both direction) messages required for establishing the call (H.225 Q.931).
- The call is established, but audio and/or video is not delivered (could be asymmetric as well, in this case one end looks perfectly alright): RTP/RTCP ports are not opened correctly.

If your users are experiencing something similar to the above, please check your firewall/NAT configuration.

Proxy gatekeeper

Proxy gatekeeper is an elegent solution for firewall and NAT traversal. In this case a gatekeeper operating in proxy mode is deployed inside the organizational network (behind the firewall) maintaining and application level gateway functionality. This solution requires operating of an own gatekeeper (separate GDS numbering space is required). To implement a proxy gatekeeper we advise the open source GnuGk. More information and confiuration examples here.

Változat #1
document-uploader hozta létre 2025-08-07 11:59:51 CEST
document-uploader frissítette 2025-08-07 11:59:51 CEST