Packetizer®

Building the H.323 Global Network

Paul E. Jones
Rapporteur, ITU-T Q2/16

H.323 Global Network

Overview

- The H.323 Global Network is an initiative to help individuals, organizations, and government agencies to interconnect using the ITU-T Standard H.323
- Successful interconnection requires adoption of certain standards and procedures
- Support available in both open source and commercial products
- The “network” is not owned by any entity, as it operates over the public Internet in order to enable a globally-connected, fully federated audio and video communication

Technologies At Work

- Base system protocols – H.323, H.225.0, and H.245
- NAT/FW traversal standards – H.460.18, H.460.19, H.460.23, and H.460.24
- Security – H.235-series
- Audio – Any audio codec may be used, but all devices must support G.711 and G.729
- Video – Any video codec may be used, but H.263 is mandatory and H.264 is recommended

Deployment Scenarios

- There are multiple deployment scenarios that one may utilize
- Different options exist, because different users prefer to place equipment inside the DMZ, behind a NAT/FW, or in the public Internet
- Further, some older devices do not support required features, requiring the insertion of devices to facilitate NAT/FW traversal

Deployment Scenarios (cont.)

- Positioning the Gatekeeper
  - Gatekeeper behind a NAT/FW
  - Gatekeeper in the DMZ
  - Gatekeeper in the public Internet
  - One Gatekeeper behind a NAT/FW and another in the public Internet or DMZ
- Alternatively, users may utilize services offered by a public H.323 service provider

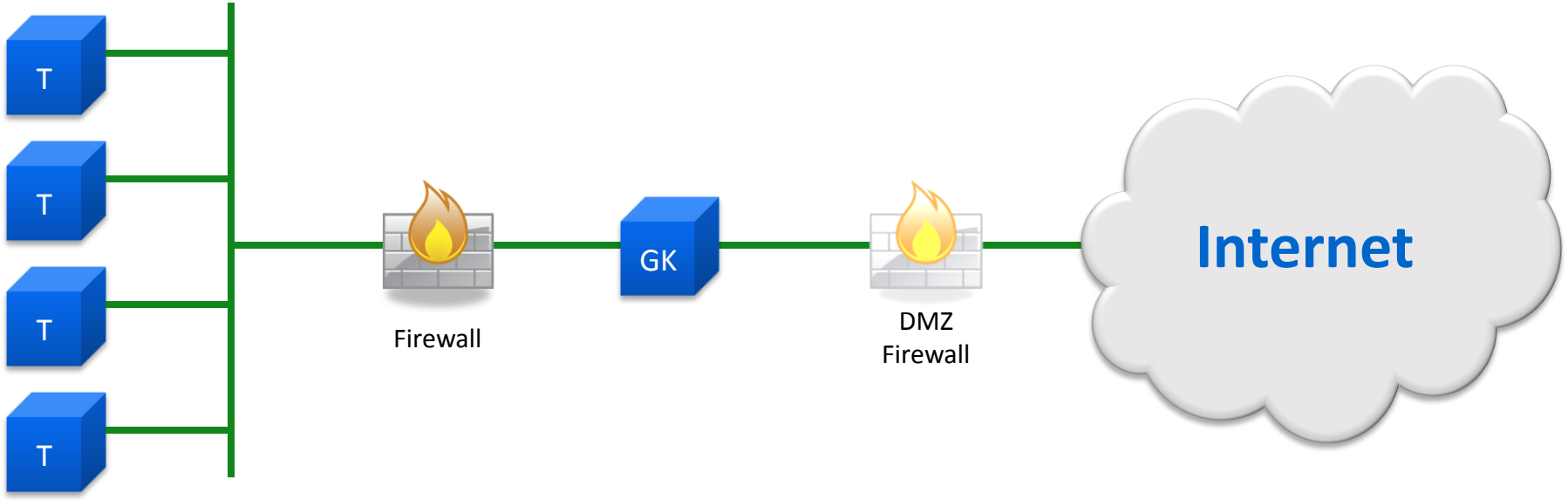
Signaling and Media Flows

- In cases where H.460.23 and H.460.24 are used, media flows directly between devices on the Internet, even when devices are behind a NAT/FW device (called “Point-to-Point Media”)
- When H.460.18 and H.460.19 are used, media flows to a “proxy” server behind the firewall, and then forwarded to the Gatekeeper in the DMZ (internal device called “Client Proxy”)
- In all cases, the Global H.323 Network enables users to communicate without requiring on Peer-to-Peer technology
- Signaling must be proxied by the Gatekeepers in order to get through the NAT/FW devices that protect the endpoints

Gatekeeper in the Internet

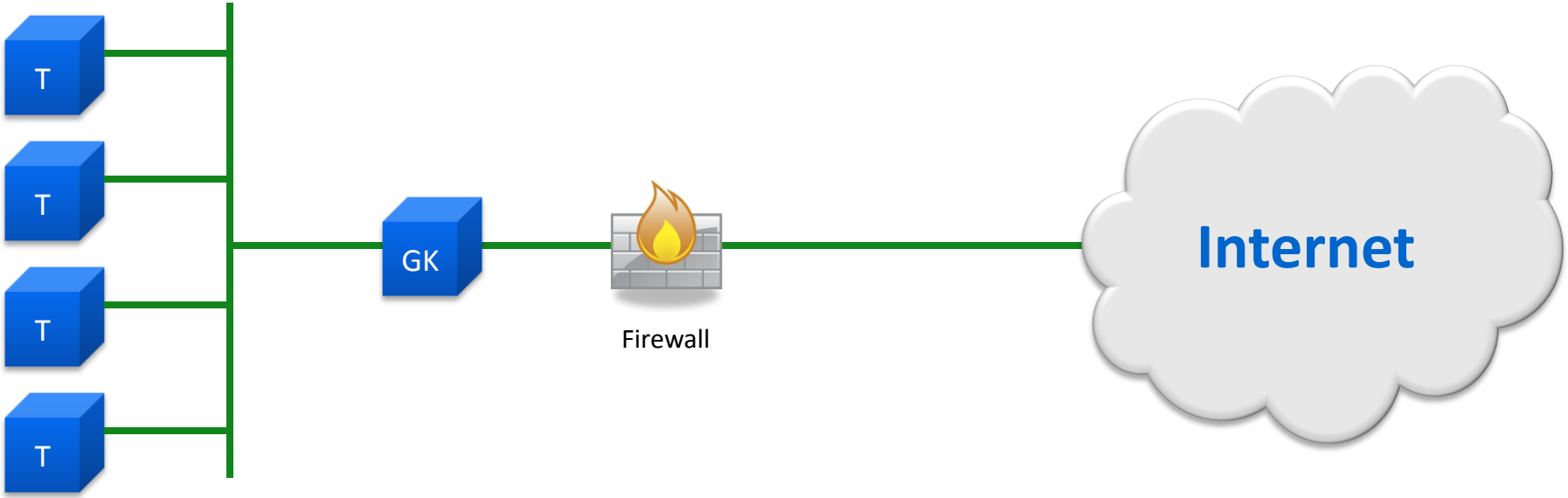
- Terminals (T) and Gatekeeper (GK) must support NAT/FW traversal standards

Gatekeeper in the DMZ



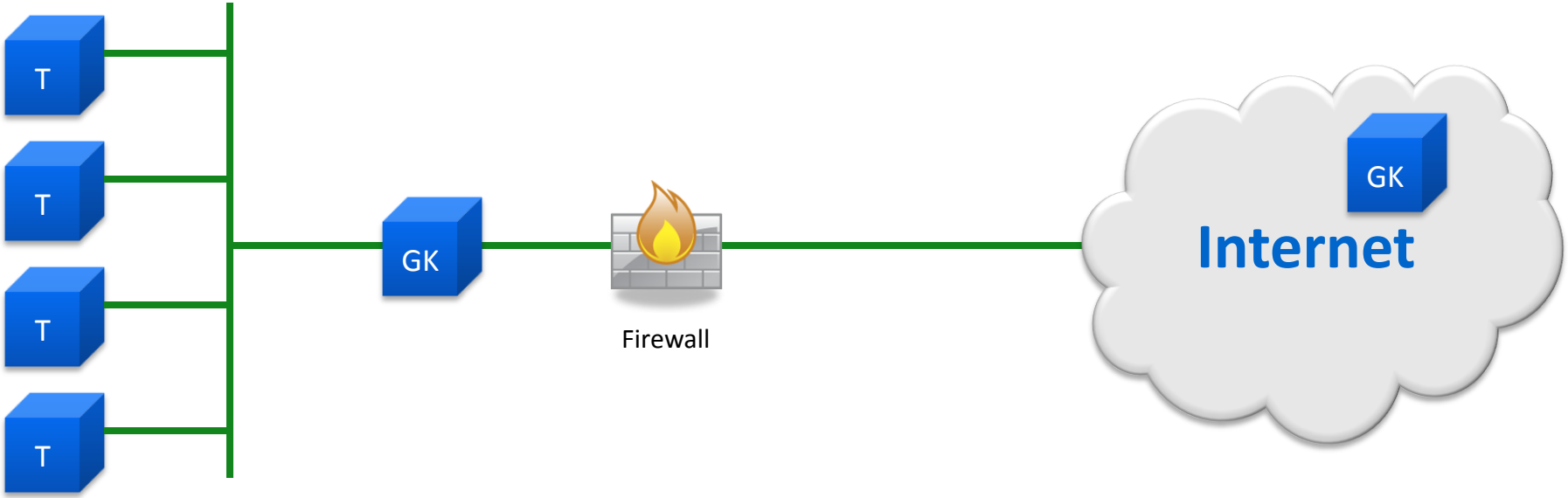
- Terminals (T) and Gatekeeper (GK) must support NAT/FW traversal standards
- Ports on the DMZ firewall (on the right) must be open so that the GK is fully accessible from the Internet

Gatekeeper Behind the NAT/FW (option 1)



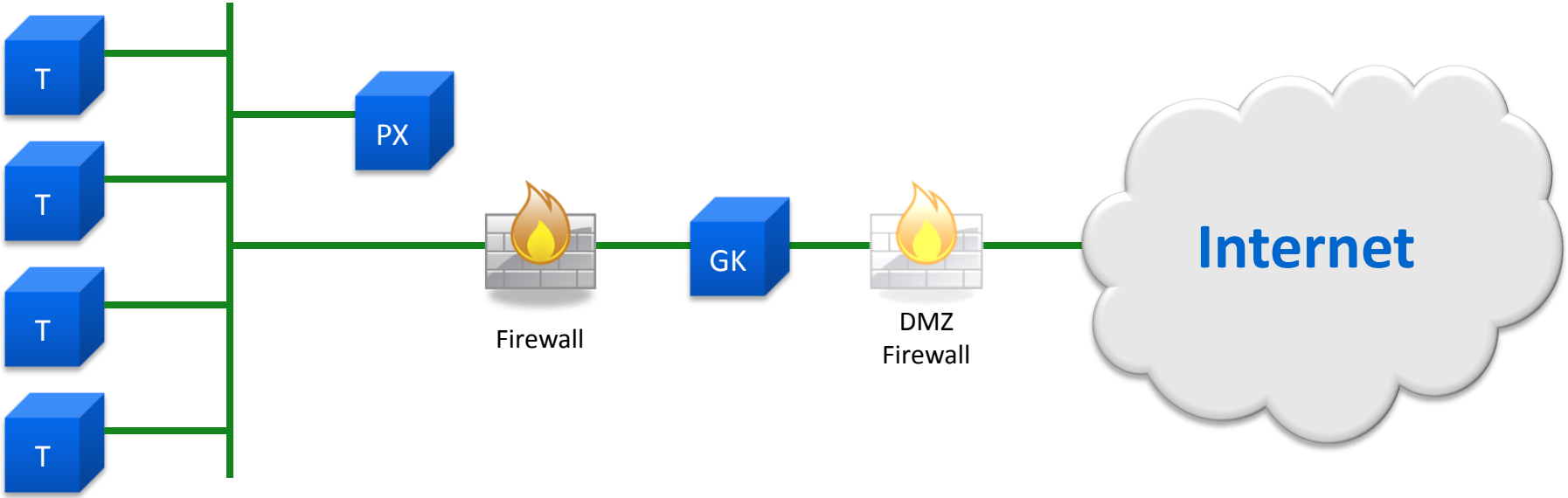
- Gatekeeper must proxy signaling and media on behalf of endpoints
- To enable media and signaling flows through the firewall
  - Gatekeeper must implement NAT/FW traversal standards
  - Holes must be opened in the firewall for the Gatekeeper for signaling

Gatekeeper Behind the NAT/FW (option 2)



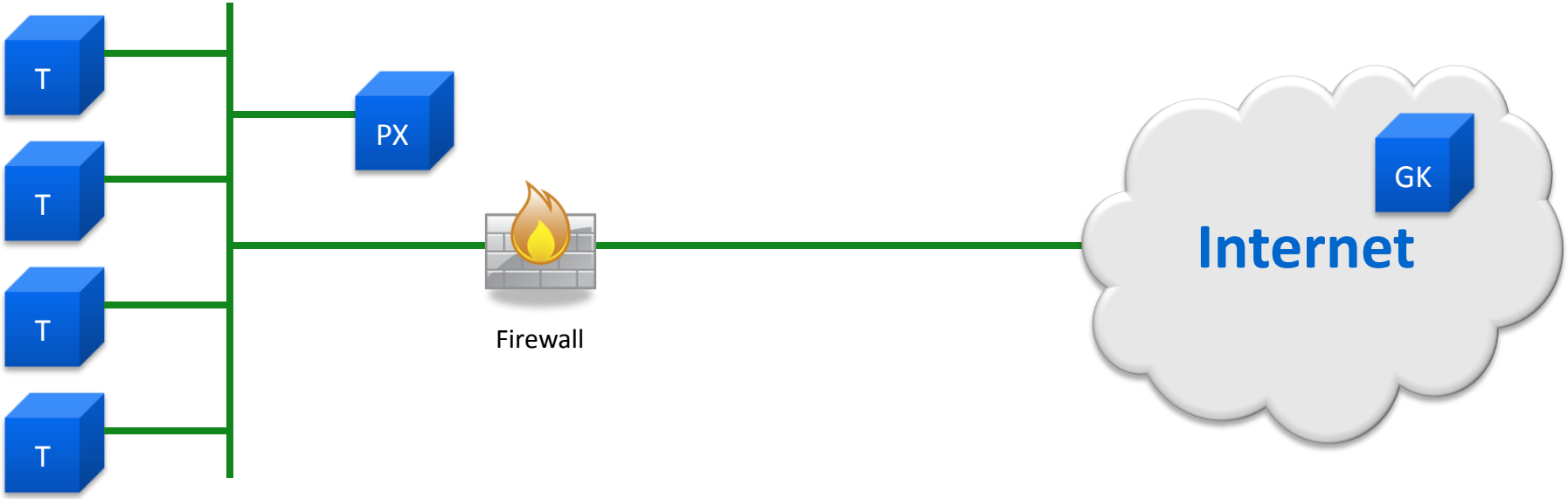
- Gatekeeper must proxy signaling and media on behalf of endpoints
- To enable media and signaling flows through the firewall
  - Gatekeeper must implement NAT/FW traversal standards
  - Gatekeeper in the enterprise registers like an endpoint to the Gatekeeper in the cloud (i.e., acts as a Session Border Controller)

Gatekeeper in DMZ with a Client Proxy Inside



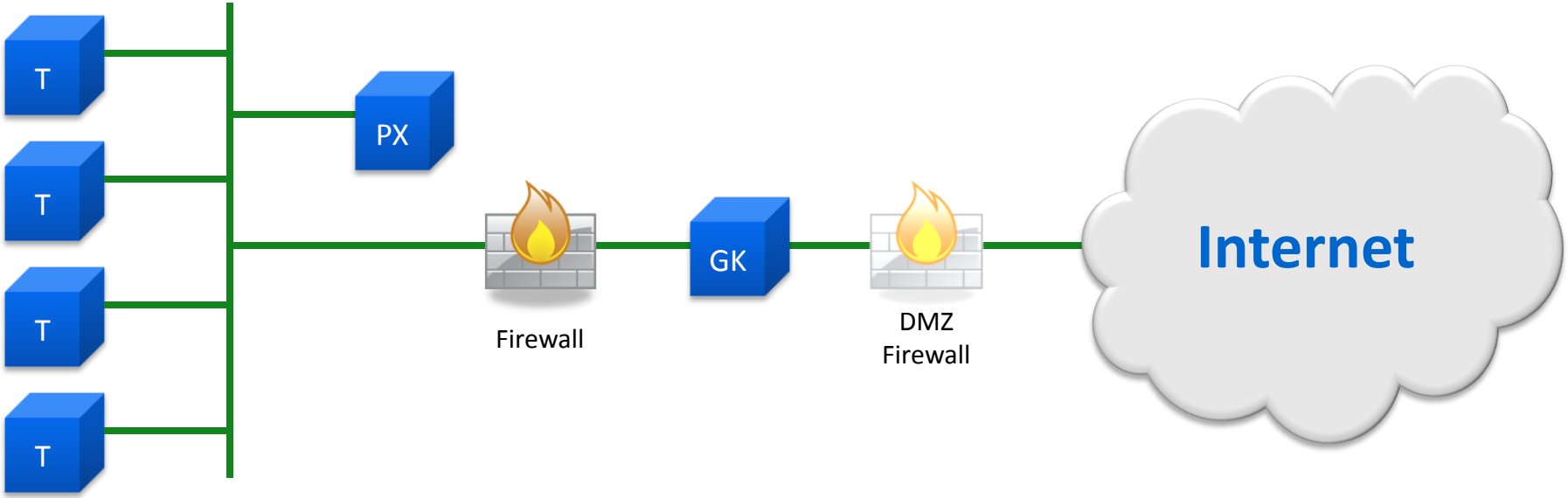
- No particular requirements on the terminals
- A Client Proxy (PX) must be deployed behind the firewall
- The Gatekeeper must be able to communicate with the traversal server to proxy media
- Ports on the DMZ firewall (on the right) must be open so that the GK is fully accessible from the Internet – NAT is not supported

Gatekeeper in the Internet with a Client Proxy Inside



- No particular requirements on the terminals
- A Client Proxy (PX) must be deployed behind the firewall
- The Gatekeeper must be able to communicate with the traversal server to proxy media
- Ports on the DMZ firewall (on the right) must be open so that the GK is fully accessible from the Internet – NAT is not supported

Use of Traversal Server and Point-to-Point Media



- No particular requirements on the terminals
- A Client Proxy (PX) must be deployed behind the firewall
- The Gatekeeper must be able to communicate with the traversal server to proxy media
- Ports on the DMZ firewall (on the right) must be open so that the GK is accessible from the Internet and NAT may be employed
- Gatekeeper must support NAT/FW traversal standards to enable proper communication out to the public Internet

Addressing in the Global H.323 Network

- DNS may be used to call other users and is the preferred addressing scheme (e.g., h323:user@h323.net)
  - Requires DNS records for the domain as described in H.323 Annex O
  - Presently the preferred and recommended record is _h323ls
  - No dependency other than DNS required to route calls directly between two users
- ENUM services are provided by NREN (https://www.nrenum.net/) for those who may wish to register and use their existing phone numbers
- Calls may be placed to any H.323 endpoint on the Internet that utilized the Global Dialing Scheme (GDS) by prefixing the number with 00 (the “International Access Code”) followed by the GDS number
  - http://www.vide.net/cookbook/cookbook.en/list_page.php?url=GDS.html
  - http://www.vide.net/help/gdsintro.shtml
  - http://en.wikipedia.org/wiki/Global_Dialing_Scheme
  - H323.net will provide address resolution into and from the GDS network
- H323.net will allocate numbers to individuals and organization from the Universal Personal Telecommunications (UPT) range with prefix +87840 and resolved via ENUM or LRQ messages transmitted to gk.h323.net.


Packetizer®