STUN Protocol

bintec-Dm 769-I

Legal Notice

Warranty

This publication is subject to change.

bintec offers no warranty whatsoever for information contained in this manual.

bintec is not liable for any direct, indirect, collateral, consequential or any other damage connected to the delivery, supply or use of this manual.

Table of Contents

Chapter 1 Introduction

1.1 Introduction

1.1.1 NAT and its problems in VoIP

Network Address Translators (NATs), while providing many benefits, also come with many drawbacks. The most troublesome of those drawbacks is the fact that many existing IP applications cease to function. Examples of such applications include almost all peer-to-peer protocols, such as multimedia applications where we find VoIP.

The reason why VoIP stops working through NAT is that in the VOIP packets explicit reference is made to IPs and ports where the device expects to receive both the voice and signaling packets. These addresses and ports are subsequently modified by NAT, but NAT does not modify the content of the VOIP messages where reference to said addresses and ports is made and therefore the conversation does not actually establish.

1.1.2 Types of NAT

There are four types of NAT, classified according to their behavior:

Full Cone: A full cone NAT is one where all requests from the same internal IP address and port are mapped to the same external IP address and port. Any external host can send a packet to the internal host, simply by sending packets to the external IP and port.

Restricted Cone: A restricted cone NAT is one where all requests from the same internal IP address and port are mapped to the same external IP address and port. Unlike a full cone NAT, an external host can send a packet to the internal host only if the internal host had previously sent a packet to said host's IP address.

Port Restricted Cone: A port restricted cone NAT is like a restricted cone NAT, but the restriction includes port numbers. Specifically, an external host can send a packet to the internal host only if the internal host had previously sent a packet to said external host's IP address and port.

Symmetric: A symmetric NAT is one where all requests from the same internal IP address and port, to a specific destination IP address and port, are mapped to the same external IP address and port. If the same host sends a packet with the same source address and port, but to a different destination, a different mapping is used. Furthermore, only the external host that receives the UDP packet can send packets back to the internal host.

Neither SIP nor H323 protocols can operate through a symmetric NAT although the STUN protocol is supported.

1.1.3 Hairpin:

If an internal host sends a packet to the public IP address and port of an already established association and the NAT correctly undoes this association and forwards the packet to the private IP address and ports of said association, then NAT supports Hairpin.

Hairpin is required so that two STUN clients behind the same NAT can communicate with each other.

1.1.4 A solution: STUN

The typical configuration is shown below: a STUN client connected to a private network through a NAT known as NAT 1. Public network where the STUN server resides connects to Internet via NAT 2.

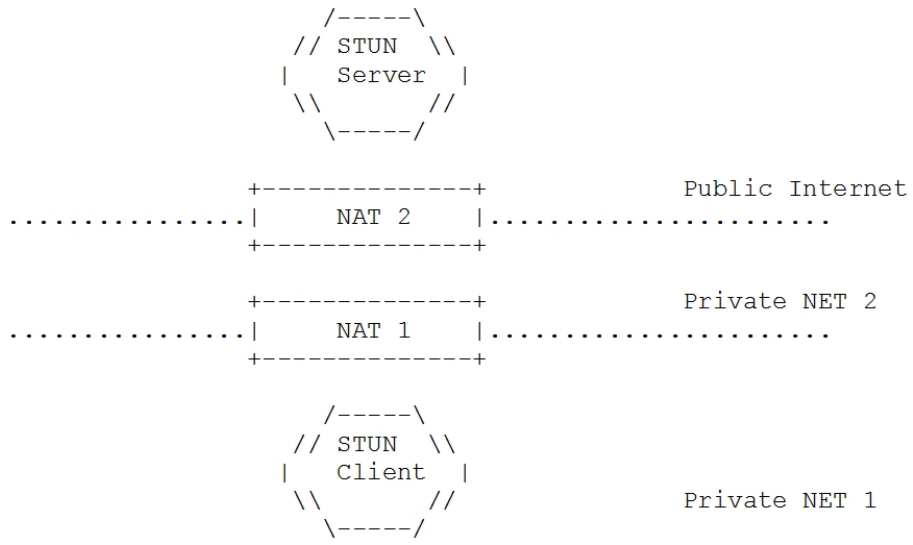

Fig. 1: STUN Configuration

STUN is a simple client-server protocol. A client sends a request to a server, and the server returns a response. These requests are used to determine the private IP port/public IP port associations established by the NATs.

The client sends a Binding Request to the server, over UDP. The server examines the source IP address and port of the request, and copies them into a response that is sent back to the client. There are some parameters in the request that allow the client to ask that the response be sent elsewhere, or that the server send the response from a different address and port.

The trick is using STUN to discover the presence of NAT, and to learn and use the bindings they allocate.

The STUN client is typically embedded in an application which needs to obtain a public IP address and port that can be used to receive data, this is the case for both the SIP protocol and the H323 protocol.

The STUN Request is used to discover the presence of a NAT, and to discover the public IP address and port generated by NAT which correspond to the private IP address and port. The Requests are sent to the STUN server using UDP. When a Request arrives at the STUN server, it copies the source IP address and port in the STUN response. For all possible types of NAT, this response will arrive at the client.

When the STUN client receives the Response, it compares the IP address and port in the packet with the IP address and port that was used to send the request. If these do not match, the STUN client is behind one or more NATs. In the case of a full-cone NAT, the IP address and port in the body of the STUN response are public, and can be used by any client to receive messages from the public network.

Of course, the client may not be behind a full-cone NAT. To determine that, the client sends another STUN Request. This second request is sent to a different server IP address, but from the same source IP address and port. If the IP address and port in the response are different from those in the first response, the client knows it is behind a symmetric NAT. To determine if it's behind a full-cone NAT, the client can send a STUN Request with a flag that tells the STUN server to send a response from a different IP address and port than the request was received on. If the client receives this response, it knows it is behind a full cone NAT.

STUN also allows the client to ask the server to send the Response from the same IP address the request was received on, but with a different port. This can be used to detect whether the client is behind a port restricted cone NAT or just a restricted cone NAT.

Chapter 2 Configuration

2.1 Accessing the configuration menu

The STUN protocol configuration commands must be entered in the configuration menu associated with the STUN (*STUN Client Config*>). To access this menu, use the **feature stun client** command found in the general configuration menu (*Config*>).

```
Config>feature stun client
STUN Client Config$
```

If you want the commands to take immediate effect, without needing to restart the router, you need to access the configuration through the dynamic general configuration menu (*Config$*).

```
Config$feature stun client
STUN Client Config$
```

2.2 STUN menu configuration commands

2.2.1 [NO] ADDRESS-SPACE

Through this command you can configure an address space and associate it with one or more STUN servers. You can configure various address spaces for a hypothetical scenario where the device could have IP connectivity for two NATs with different address spaces, although the most common situation would be only one NAT with an address space.

An address space can have various STUN servers associated with it. In this case we have only used the first of the configured servers which is active, with the rest behaving as backup should the first one fail.

Syntax:

```
STUN Client Config$[no] address-space <space-id>
  description    Description of this item
  server         Add a server to this address space
```

description	Description for this address space, for information purposes only.
server	Aggregates a previously defined STUN server to this address space.

2.2.2 [NO] SERVER

Defines a STUN server. Subsequently, the STUN servers are associated with an address space.

Syntax:

```
STUN Client Config$[no] server <server-id>
  description    Description of this item
  ip             Ip address of this server
  keep-alive     Seconds between bindings refresh
  local-ip       Local ip to use
  port           Port of this server
```

description	Description for this address space, for information purposes only.
ip	Server IP address
keep-alive	Time between bind refreshes for this server
local-ip	Local IP address to be used in the STUN packets addressed to this server.
port	Server UDP port. Default is 3478.

2.2.3 [NO] SHUTDOWN

Enables or disables the STUN protocol. Default is disabled.

Syntax:

```
STUN Client Config$[no] shutdown
```

2.2.4 [NO] EXIT

Permits you to return to the general configuration menu.

Syntax:

```
STUN Client Config$exit
```

Chapter 3 Monitoring

3.1 Accessing the Monitoring Menu

The STUN protocol monitoring commands must be entered in the monitoring menu associated with the STUN (STUN Client Mon+). To access this menu, use the **FEATURE STUN CLIENT** command found in the general monitoring menu (+).

```
+feature stun client
STUN Client Monitor
STUN Client Mon+
```

Once you have accessed the STUN protocol monitoring menu, you can enter the commands described below.

3.1.1 LIST

3.1.1.1 LIST REQUESTS

Displays information on all the STUN requests in process.

The state, associated server and address space are displayed for each request.

Three requests with 0 address spaces are automatically generated for each server which monitor the server state.

Syntax:

```
STUN Client Mon+LIST REQUESTS
```

Example:

```
STUN Client Mon+ LIST REQUESTS
Request id 31fd040032fd040033fd040034fd0400, state BINDED, server 2, address space 1
External address 172.26.1.1:32770
Socket Id 3, Retransmits number 0
Request id 35fd040036fd040037fd040038fd0400, state BINDED, server 2, address space 1
External address 172.26.1.1:32771
Socket Id 2, Retransmits number 0
Request id 39fd04003afd04003bfd04003cfd0400, state BINDING, server 2, address space 0
External address 0.0.0.0:0
Socket Id 2, Retransmits number 6
Retransmits 6, next retransmit 1600
Request id 95fa040096fa040097fa040098fa0400, state BINDED, server 2, address space 0
External address 172.26.1.1:32768
Socket Id 2, Retransmits number 0
Request id 99fa04009afa04009bfa04009cfa0400, state BINDED, server 2, address space 0
External address 172.26.1.1:32768
Socket Id 2, Retransmits number 0
Request id 89fe04008afe04008bfe04008cfe0400, state ERROR, server 1, address space 0
External address 0.0.0.0:0
Socket Id 1, Retransmits number 0
Request id 19f604001af604001bf604001cf60400, state ERROR, server 1, address space 0
External address 0.0.0.0:0
Socket Id 1, Retransmits number 0
Request id 1df604001ef604001ff6040020f60400, state ERROR, server 1, address space 0
External address 0.0.0.0:0
Socket Id 1, Retransmits number 0
STUN Client Mon+
```

3.1.1.2 LIST SERVERS

Permits you to view the status of the configured servers, if there is connectivity or not and the type of NAT through which the device has to pass in order to access them.

Syntax:

```
STUN Client Mon+LIST SERVERS
```

Example:

```
STUN Client Mon+LIST SERVERS
Server 172.25.1.32:3478
Nat Type No UDP connectivity, Hairpin: No

Server 172.25.1.2:3478
Nat Type Full cone, Hairpin: No

stun-client STUN Client Mon+
```

3.1.2 EXIT

Returns to the general monitoring menu.

Syntax:

```
STUN Client Mon+exit
```

Chapter 4 Example

4.1 Example: STUN protocol with SIP

A business with two voice gateways is connected to the Internet through a router which executes full-cone NAT. In order for the office to be able to make calls to and receive calls from a central office, the STUN protocol is used in both voice gateways.

The STUN server is located in the company's central office as well as the router which in turn acts as the registrar.

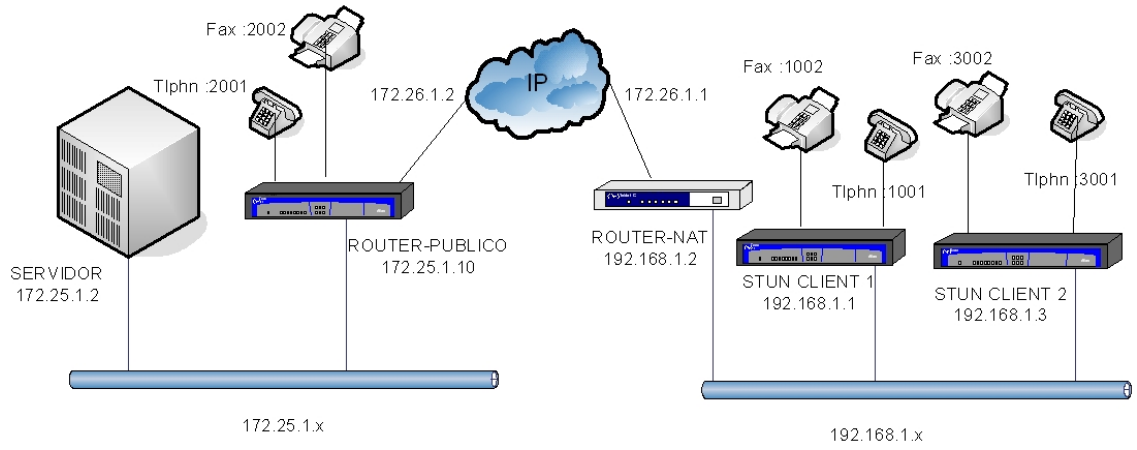

Fig. 2: Example: STUN protocol with SIP

As the branch router does not support hairpin, the calls between clients 1 and 2 must be executed without using the STUN protocol. Therefore the protocol is disabled in the corresponding dial-peer. If the NAT does support hairpin, then the STUN does not have to be disabled for calls between the two voice gateways.

Configurations:

The configuration for the "STUN CLIENT 1" router is displayed below:

```
; Showing System Configuration ...
; XXX Router 2 156 Version 10.7.0

log-command-errors
no configuration
set hostname stun-client1
set data-link x25 serial0/0
set data-link x25 serial0/1
set data-link x25 serial0/2
telephony
; -- Telephony configuration --
   dial-peer 1 voice-port
      destination-pattern 1001
      target voice-port voip1/0 1
   exit
;
   dial-peer 5 sip
      destination-pattern 300.
      destination-pattern 800.
      target ipv4 192.168.1.3
   exit
;
   dial-peer 4 sip
      destination-pattern 3...
      target ipv4 192.168.1.3
   exit
;
   dial-peer 2 sip
      destination-pattern 2...
      fax mode t38-detect
```

```
      fax t38 redundancy 2
      target ipv4 172.25.1.12
   exit
;
   dial-peer 6 voice-port
      destination-pattern 1002
      target voice-port voip1/0 2
   exit
;
exit
;
network voip1/0
; -- VoIP interface Configuration --
   line 1 no suspend-mode
;
exit
;
feature stun client
   no shutdown
   server 1 ip 172.25.1.32
;
   server 2 ip 172.25.1.2
;
   address-space 1 server 1
   address-space 1 server 2
;
;
exit
;
event
; -- ELS Config --
   enable trace subsystem VOIP ALL
   enable trace subsystem TLPHY ALL
   enable trace subsystem H323 ALL
   enable trace subsystem STUN ALL
exit
;
protocol ip
; -- Internet protocol user configuration --
   internal-ip-address 192.168.1.1
;
   address ethernet0/0 192.168.1.1 255.255.255.0
;
;
   route 0.0.0.0 0.0.0.0 192.168.1.2
;
;
;
exit
;

protocol sip
   application address 192.168.1.1
   application gateway
   application server
   proxy 172.25.1.12 default
;
   realm bcn.bintec.es
   stun 1
exit
;
dump-command-errors
end
; --- end ---
```

The “STUN CLIENT 2” router configuration is shown below:

```
; Showing System Configuration ...
```

```
; XXX Router 2 156 Version 10.7.0

log-command-errors
no configuration
set hostname stun-client2
set data-link x25 serial0/0
set data-link x25 serial0/1
set data-link x25 serial0/2
telephony
; -- Telephony configuration --
   dial-peer 1 voice-port
      destination-pattern 3001
      target voice-port voip1/0 1
   exit
;
   dial-peer 2 sip
      destination-pattern ....
      target sip-proxy
   exit
;
   dial-peer 3 sip
      destination-pattern 1...
      no stun
      target ipv4 192.168.1.1
   exit
;
   dial-peer 4 voice-port
      destination-pattern 3002
      target voice-port voip1/0 2
   exit
;
exit
;
feature stun client
   no shutdown
   server 1 ip 172.25.1.2
   server 1 local-ip 192.168.1.3
;
   address-space 1 server 1
;
;
exit
;
protocol ip
; -- Internet protocol user configuration --
   internal-ip-address 192.168.1.3
;
   address ethernet3/0 192.168.1.3 255.255.255.0
;
;
   route 0.0.0.0 0.0.0.0 192.168.1.2
;
;
;
exit
;
protocol sip
   application gateway
   proxy 192.168.1.1 default
;
   realm bcn.bintec.es
   stun 1
exit
;
dump-command-errors
end
; --- end ---
```

4.2 Example: STUN protocol with H323

A company wishes two of its branches to be able to execute calls using the H323 protocol. The connection to Internet for both branches is carried out through two routers with NAT, therefore the STUN protocol must be enabled in the voice gateways of both branches.

The central headquarters have a STUN server, a voice gateway and a gatekeeper where both branches are registered and the central's voice gateway.

As the STUN protocol only allows the UDP ports to open, the TCP 1720 port (H323 signaling) must be configured as a visible port in the routers executing NAT at both branches. Additionally the calls must be carried out through the fast-start procedure to avoid negotiating the TCP H245 ports.

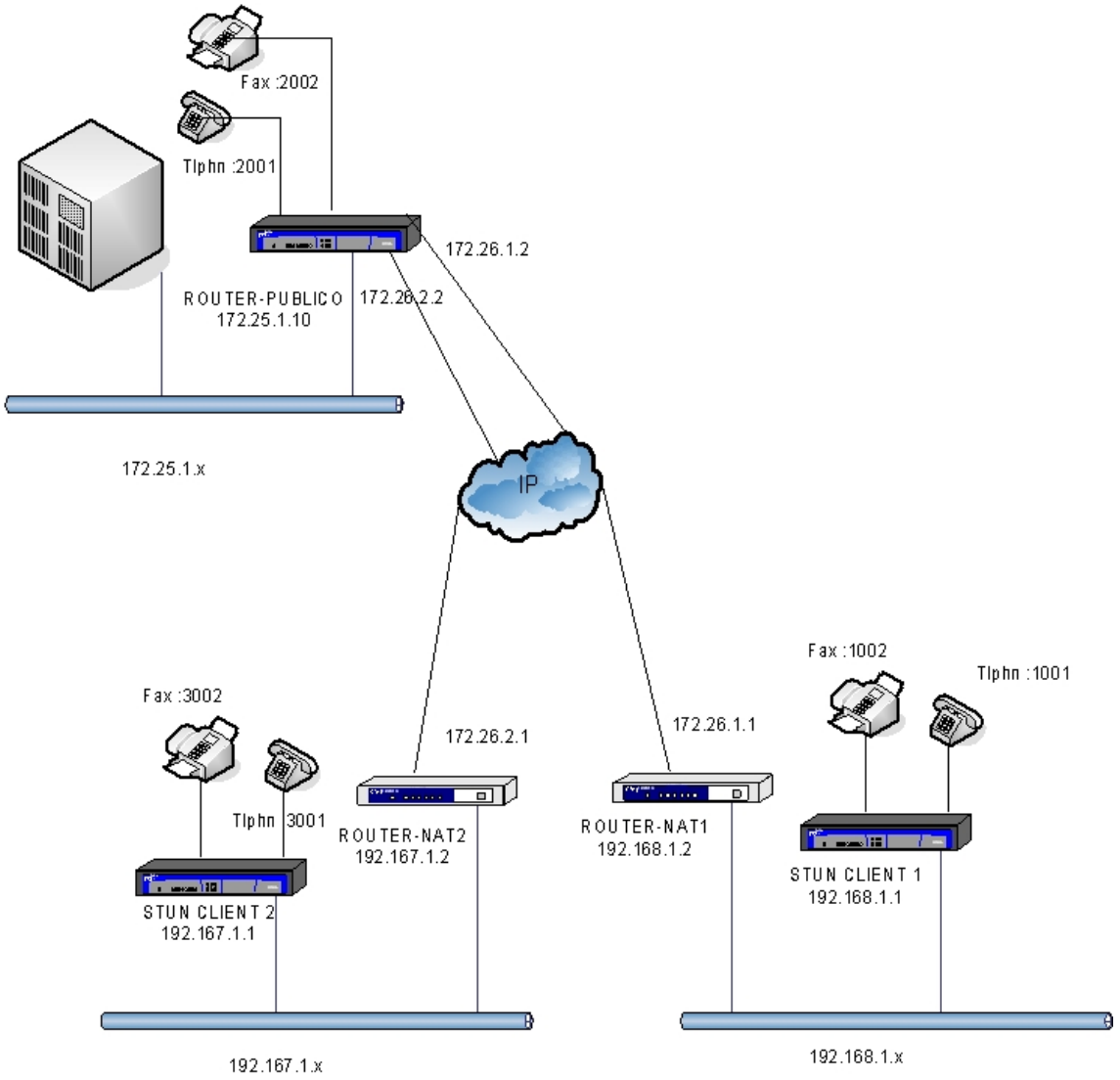

Fig. 3: Example: STUN protocol with H323

Configurations:

Below you can see the "STUN CLIENT1" and the "ROUTER-NAT1" router configurations together with the central router. The configurations for the second branch have not been presented as they are identical to the first branch with the exception of the IP addresses.

"STUN-CLIENT 1":

```
; Showing System Configuration ...
; XXX Router 2 156 Version 10.7.0

log-command-errors
no configuration
set hostname stun-client1
set data-link x25 serial0/0
set data-link x25 serial0/1
set data-link x25 serial0/2
```

```
telephony
; -- Telephony configuration --
   dial-peer 1 voice-port
      destination-pattern 1001
      target voice-port voip1/0 1
   exit
;
   dial-peer 2 voice-port
      destination-pattern 1002
      target voice-port voip1/0 2
   exit
;
   dial-peer 3 h323
      destination-pattern ....
      incoming called number ....
      target gatekeeper
   exit
;
exit
;
feature stun client
   no shutdown
   server 1 ip 172.25.1.2
;
   address-space 1 server 1
;
exit
;
event
; -- ELS Config --
   enable trace subsystem VOIP ALL
   enable trace subsystem TLPHY ALL
   enable trace subsystem H323 ALL
   enable trace subsystem STUN ALL
exit
;
protocol ip
; -- Internet protocol user configuration --
   internal-ip-address 192.168.1.1
;
   address ethernet0/0 192.168.1.1 255.255.255.0
;
;
   route 0.0.0.0 0.0.0.0 192.168.1.2
;
;
;
exit
;
protocol h323
   application gateway
   gatekeeper address 172.25.1.2
   gatekeeper zone RVGK
   stun 1
exit
;
dump-command-errors
end
; --- end ---
```

“ROUTER-NAT1”:

```
; Showing System Configuration ...
; C4i SNA IPSec VoIP CR Router 1 125 Version 10.6.5-SIP-Beta TM

log-command-errors
no configuration
set hostname router-nat1
```

```
add device ppp 1
set data-link sync serial0/0
network serial0/0
; -- Interface Synchronous Serial Line. Configuration --
   speed 256000
exit
;
network ppp1
; -- Generic PPP User Configuration --
   base-interface
; -- Base Interface Configuration --
      base-interface serial0/0 link
;
   exit
;
exit
;
event
; -- ELS Config --
   enable trace subsystem NAPT ALL
exit
;
;
protocol ip
; -- Internet protocol user configuration --
   address ethernet0/0 192.168.1.2 255.255.255.0
   address ppp1 172.26.1.1 255.255.255.0
;
;
   route 0.0.0.0 0.0.0.0 172.26.1.2
;
   rule 1 default
   rule 1 local-ip 172.26.1.1
   rule 1 napt translation
;
nat pat
; -- NAPT configuration --
      visible-port 1720 rule 1 default
      visible-port 1720 rule 1 port 1720
      visible-port 1720 rule 1 ip 192.168.1.1
;
   exit
;
exit
;
dump-command-errors
end
; --- end ---
```

“ROUTER-PUBLIC”:

```
; Showing System Configuration ...
; XXX Router 2 156 Version 10.7.0

log-command-errors
no configuration
set hostname router-public
add device ppp 1
add device ppp 2
set data-link sync serial0/0
set data-link sync serial0/1
telephony
; -- Telephony configuration --
   dial-peer 2 voice-port
      destination-pattern 2001
      target voice-port voip2/0 1
   exit
;
```

```
   dial-peer 3 h323
      destination-pattern ....
      target gatekeeper
   exit
;
   dial-peer 1 voice-port
      destination-pattern 2002
      target voice-port voip2/0 2
   exit
exit
;
network serial0/1
; -- Interface Synchronous Serial Line. Configuration --
   speed 256000
exit
;
network ppp2
; -- Generic PPP User Configuration --
   base-interface
; -- Base Interface Configuration --
      base-interface serial0/1 link
;
   exit
;
exit
;
protocol ip
; -- Internet protocol user configuration --
   internal-ip-address 172.25.1.12
;
   address ethernet0/0 172.25.1.12 255.255.255.0
   address ethernet0/0 172.24.100.132 255.255.255.248
   address ppp1 172.26.2.2 255.255.255.0
   address ppp2 172.26.1.2 255.255.255.0
;
;
;
exit
;
protocol h323
   application gateway
   gatekeeper address 172.25.1.2
   gatekeeper zone RVGK
exit
;
dump-command-errors
end
; --- end ---
```