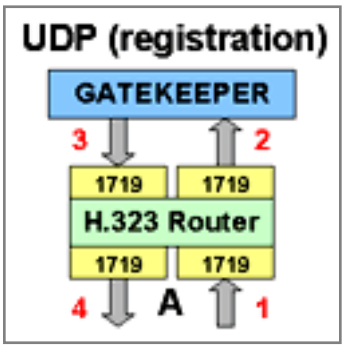
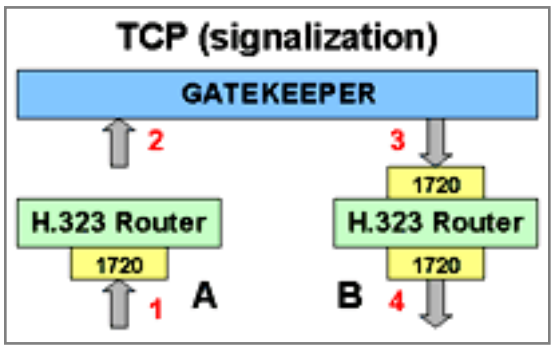
Voipac H323 Router Firewall Settings

Fayn client registration/unregistration



1. Fayn Client PC sends **UDP** packets to registrate on H323 Router to port usually **1719** (this is custom on H323 Router, say East for example)
2. H323 Router process packets and sends a bit modificated **UDP** packets from port **1719** (again customized, but for other site, say West) on GateKeeper port **1719**
3. GateKeeper answers with **UDP 1719** to H323 Router West **1719**
4. H323 Router sends answer from East **1719** to Fayn Client PC

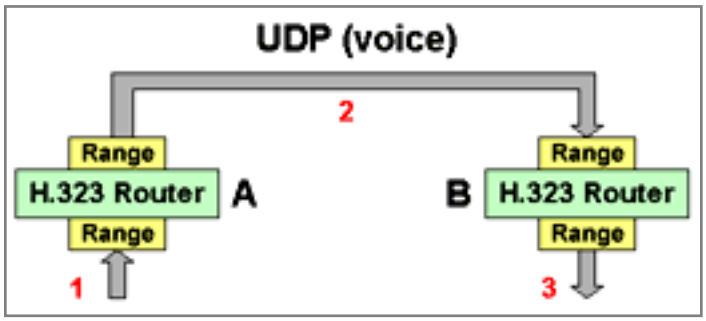
Starting call (signalization)



Say user A make a call to user B

1. Users A PC creates **TCP** connection to H323Router_A to port **1720**
2. H323 Router_A process packets and creates **TCP** connection from system free port to GateKeeper
3. Gate Keeper creates **TCP** conection and sends signalling packets to H323 Router_B port **1720**
4. H323 Router_B process packets and creates **TCP** connection from system free port to users B PC port **1720**

Voice



Voice = **UDP** (RTP) packets. You can customize on H323 Router range **UDP** ports, then call looks like:

1. From user A PC system free **UDP** port to H323 Router_A **UDP** port from set range
2. From set range H323 Router_A **UDP** port to set range H323 Router_B **UDP** port
3. From set range H323 Router_B **UDP** port to user B PC system free **UDP** port

These steps are made at the same time in both directions depending on speach.

Firewall examples

```
WAN= #set your wan interface IP address
IF= #set interface name (eth0, e.g.)
RANGE= #set range UDP ports set on H323Router (example 15000:15100)
GKP1= #set GateKeeper1 IP address
GKP2= #set GateKeeper2 IP address
```

IPCHAINS

```
# registration/unregistration
ipchains -A input -s $GKP1 1719:1719 -d $WAN 1719:1719 -i $IF -p udp -j ACCEPT
ipchains -A input -s $GKP2 1719:1719 -d $WAN 1719:1719 -i $IF -p udp -j ACCEPT
# signalization
ipchains -A input -s $GKP1 -d $WAN 1720:1720 -i $IF -p tcp -j ACCEPT
ipchains -A input -s $GKP2 -d $WAN 1720:1720 -i $IF -p tcp -j ACCEPT
# what is it ?
ipchains -A input -s 0.0.0.0/0 -d $WAN $RANGE -i $IF -p udp -j ACCEPT
# voice
ipchains -A input -s $GKP1 -d $WAN 1024: -p tcp -j ACCEPT
ipchains -A input -s $GKP2 -d $WAN 1024: -p tcp -j ACCEPT
```

IPTABLES

```
# registration/unregistration
iptables -t filter -A INPUT -i $IF -s $GKP1 -d $WAN -p udp -m udp --dport 1719 -j ACCEPT
iptables -t filter -A INPUT -i $IF -s $GKP2 -d $WAN -p udp -m udp --dport 1719 -j ACCEPT
# signalization
iptables -t filter -A INPUT -i $IF -s $GKP1 -d $WAN -p tcp -m tcp --dport 1720 -j ACCEPT
iptables -t filter -A INPUT -i $IF -s $GKP2 -d $WAN -p tcp -m tcp --dport 1720 -j ACCEPT
# what is it ?
iptables -t filter -A INPUT -i $IF -d $WAN -p udp -m udp --dport $RANGE -j ACCEPT
# voice
iptables -t filter -A INPUT -i $IF -s $GKP1 -d $WAN -p tcp -m tcp --dport 1024: -j ACCEPT
iptables -t filter -A INPUT -i $IF -s $GKP2 -d $WAN -p tcp -m tcp --dport 1024: -j ACCEPT
```

Voipac H323 Router

Voipac H323 Router works like proxy listening on one or two interfaces, processing voice packets and exchanging them from private network behind router with NAT to the public network (Internet) and backward. Solves problematic voice routing into private subnet. It does not depend on IP Routing enabled.

Management

H323 Router service is represented as a set of attributes organized in a hierarchical naming structure. There is a command line utility called `vpacadm` with a set of shell-like commands, that can be used to access the attributes. The attributes are described in the following tables.

Root node attributes:

Under the running service, several instances of H323 Router can be created. In the management tree, these instances are represented by a subtree called configuration. The first table shows the attributes common for all configurations.

Attribute	Description	Type	Default Value
/CreateConfig	Creates new configuration subtree for an instance of H323Router.	STRING	none
/DeleteConfig	Deletes the specified configuration subtree and destroys the associated instance of H323Router.	STRING	none
/RTPPortMax	The maximum port number of the UDP socket that is used for RTP channels.	NUMERIC	0
/RTPPortMin	The minimum port number of the UDP socket that is used for RTP channels.	NUMERIC	0
/VACAddr	Voipac Alert Center IP address.	IPADDRESS	0.0.0.0
/VACPort	Voipac Alert Center port number.	NUMERIC	0

Attributes in the configuration subtree:
These attributes are specific to an instance of service. The configuration attribute names are specified relative to the <configuration name> node. Since the configuration nodes are placed in the root node they must not be assigned names from one of attributes specified in the above table.

Attribute	Description	Type	Default Value
ServiceStatus	This attribute is used to start and stop the instance of service. [Running, Stopped]	ENUM	Stopped
Interfaces/East/CLIR	When set to TRUE, all calls originating from east interface to west side will not have a caller information. (Calling Line Identification Restriction)	BOOLEAN	FALSE
Interfaces/East/FwProxyAddr	When not set to default value, router uses this address instead of interface address in RAS messages. This can enable the router to operate from behind a firewall. Firewall should forward RAS and call signaling port to H323 router.	IPADDR	0.0.0.0
Interfaces/East/GkpAddr	Just one side of H323 router can have this value set to valid IP address of gatekeeper, where RAS messages and call signaling should be forwarded.	IPADDR	0.0.0.0
Interfaces/East/IFaceAddr	Specifies the interface of router side.	ENUM	depends on host system
Interfaces/East/NetMask	Updated according to selected IFaceAddr.	IPADDR	none

Interfaces/East/RasPort	Specifies RAS port for RAS channel as defined in H323 standard.	NUMERIC	1719
Interfaces/East/SetupPolicy	Incoming call can be eliminated before any processing, [PassAll = no filter, CheckAddr = checks peer address to be equal to GkpAddr, (e.g just gatekeeper can originate a call), RefuseAll = all connection are refused].	ENUM	PassAll
Interfaces/West	This node contains attributes of the west interface. They are the same as the east interface attributes.	NODE	
Logs/CDRFile	The path to call detail record file.	STRING	exgateway.cdr
Logs/LogFile	The path to H323 protocol log file.	STRING	exgateway.log
Logs/LogLevel	Verbosity of log file. [None,Trace]	ENUM	None
Logs/TruncateLog	By setting this attribute to TRUE, the log specified by the LogLevel attribute is truncated.	BOOLEAN	FALSE
Settings/GRQTimeout	Timeout for gatekeeper request message.	NUMERIC	5
Settings/MaxCalls	The maximum number of calls a router can route. If the value is less than zero the number of calls is unlimited.	NUMERIC	-1
Settings/RTPFrameSize	When a value grater than zero is specified, all RTP frames are retranslated to fulfil the minimum size specified. This attribute has no effect when RouteRTP is set to FALSE. [bytes]	NUMERIC	0
Settings/RasRetryCount	Number of times a RAS message is resent in a case of no response from destination.	NUMERIC	2
Settings/RasTimeout	RAS message timeout as defined by H323. [seconds]	NUMERIC	3
Settings/RejTimeout	Timeout after a rejection was received. [seconds]	NUMERIC	15
Settings/RouteH245	Whether to route H.245 signaling.	BOOLEAN	TRUE
Settings/RouteRAS	Specifies the mode of application. (read only, always TRUE, TRUE = H323 router)	BOOLEAN	TRUE
Settings/RouteRTP	Specifies whether to route RTP channels.	BOOLEAN	FALSE

Settings/SetupTimeout	How long should router wait for Q.931 Setup message after admission was granted.	NUMERIC	60
Settings/TOS	All RTP packets leaving the router will have Type of Service set to this value. [0 = not changed]	NUMERIC	0