



IP-IP



Itamar Leser – January 2008

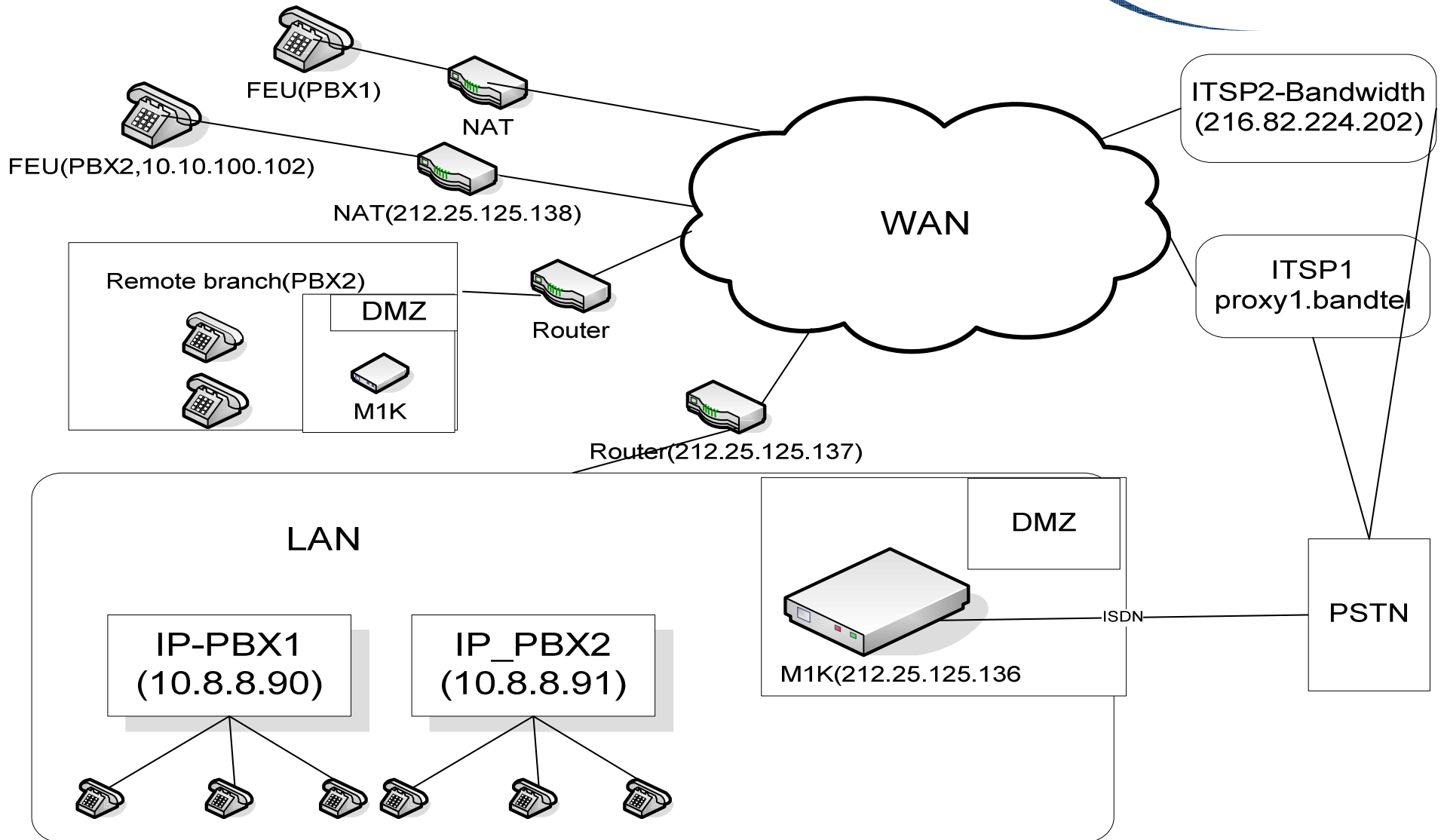


© 2006 AudioCodes Ltd.
All rights reserved.
AudioCodes Confidential Proprietary



AudioCodes
Your Gateway to VoIP

Architecture example



Why do we need SBC?



- In the example above the SBC is needed in order to add the following functionalities to the PBX
 - Connecting Far-End-Users (traveling PBX users) to the local PBX
 - Enable connectivity to ITSP's (Internet Telephone Service Provider)–(SIP trunks)
 - Enable connectivity between remote branches and the PBX
 - Enable Survivability for users located in remote branches (both IP and PSTN) in case of WAN failure.

The IP-PBX is located in the enterprise LAN and IP-PBX vendors prefer not to be exposed to the WAN and deal with Security\NAT\Firewall\ITSP-interoperability problems.

The SBC is the entity to solve all these problems.

Far End Users (FEU)



The main role of the SBC while working with FEU is to hide the fact that FEU are located in the WAN and this way cause the IP-PBX work with FEU seamlessly as if they were located in the LAN.

In order to do so the SBC should perform the following -

- The SBC should always keep track of the whereabouts of each FEU and have a pin hole opened (on the FEU firewall) in order to direct INVITES from the IP-PBX to the FEU.
- The SBC should overcome NAT\Firewall problems that may be caused due to the fact that the FEU\IP-PBX uses its local (behind NAT) IP-Address (SDP>Contact...).
- The SBC should make the necessary translations between the leg with the FEU and the IP-PBX (Tls->Udp, Rtp->Srtp, Coder transcoding...)

Connecting To SIP trunks (ITSP)



- In order to connect SIP trunks to the IP-PBX, the SBC should perform the following –
 - Register on behalf of the IP-PBX to the ITSP (in some cases there is a need to have a user password in order to authenticate)
 - Solve NAT\Firewall problems in connections between the IP-PBX and the ITSP (both of them may be located behind NAT)
 - Solve any SIP interoperability problem that may arise as a result of different SIP flavors used by the IP-PBX and the ITSP.
 - Make the necessary translations between the leg with the ITSP and the IP-PBX (Tls->Udp, Rtp->Srtp, Coder transcoding...)
 - Add routing rules in order to direct SIP sessions from the IP-PBX to a specific ITSP and from ITSP to a specific IP-PBX.
 - Perform PSTN fall back in case of ITSP failure.

Security



- As the SBC is exposed to the WAN (in order to allow Sip connectivity to FEU\ITSP\Remote branches), the SBC should perform a security mechanisms.
- Only RTP associated with a specific call will traverse the SBC.
- A set of allowed destinations for SIP traffic can be configured.
- Limits for SIP sessions per I destination can be configured

The solution - SETUP



- The SBC unit (TP or M1K) will be behind the router and connected to the DMZ.
- The SBC unit will have LAN access
- The SBC unit will have 1 global IP address.
- Far End Users\Remote branches
 - The SBC will be configured and function as an outbound proxy for each FEU\NEU.
 - Each Register\INVITE sent from FEU\NEU will be sent to the serving IP-PBX in a B2BUA manner and thus solve NAT\Firewall problems.
 - The contact in the leg to the IP-PBX will be the SBC's contact.
 - Any authentication (if needed) will be performed by the IP-PBX
 - In case of successful registrations the SBC will manage a dynamic data base that consists of the whereabouts of each FEU.
 - The SBC should cause the FEU to send registrations in a rapid rate in order to keep NAT binding open.

What is B2BUA?



- The SBC GW behaves as **B2BUA**
- Proxy has 1 call ID for both sides
- B2BUA has 2 legs – **2 call IDs**
- RTP is passing through the SBC GW.
- **Transcoding**: Coders, transport type (UDP, TCP, TLS), RTP\SRTP etc.
- Each call uses 2 DSP channels
- Disadvantage: The SBC is not fully transparent which may damage advanced SIP features while traversing the SBC.
- Currently only INVITES and Register are handled by the SBC (no support for subscribe\publish\...)

New tables



- IP Group
- Proxy Set
- Account Table

IPGroup table



- The IPGroup table defines logical IP entities that may be either servers (IP-PBX, ITSP...) or users (FEU\NEU)
- Each call is associated with Source and Destination IPGroup (in case of no specific rule the default IPGroup is selected).
- IPGroup act as logical destinations we can route or register to (registrations can be made only to servers)
- In case of defining default proxy for all the gateway (IsProxyUsed) only one IPGroup will be defined (0-default) and working with multiple IPGroups will not be allowed.
- One can also define that one IPGroup registers to another.
- IPGroups may also be assigned with host names and other parameters that reflect parameters sent in SIP Request From\To these IPGroups.

Server IPGroup



- This kind of group may be a registrar a proxy a PBX or any other group that we know it's whereabouts.
- Each server group must be associated with a Proxy-set (as defined below) in order to know how to route requests to this group.
- This kind of group may be defined as a serving IPGroup for other IPGroups\TrunkGroups, in such case any requests arriving from these IP\Trunk group will be routed to the serving IPGroup.

User IPGroup



- This kind of group gather IP users that share the same functionality in terms of Registrations\Routing...(probably all Far\Near end users that belong to the same IP-PBX).
- This kind of Group can't be associated with a proxy set as it gather multiple users located in different addresses
- In order to know the locations of each user, registration must be sent from users belonging to these group to the SBC.
- Usually this kind of group will be associated with a serving IP-Group.
- The survivability flag can be turned on only for this kind of group

IP Group



- Example

IP Group Table

Basic Parameter Lis

	Type	Description	Proxy Set ID	SIP Group Name	Contact User	Serving IPGroup ID	Enable Survivability	Send Invite To Proxy	Always Use Route Table
1	SERVER	PBX1	1	10.8.8.90	1234		Disable	Disable	Disable
2	SERVER	ProxyBandtel	2	ProxyBandtel.com	5678		Disable	Disable	Disable
3	SERVER	BandWidth	3	BandWidth.com	777		Disable	Disable	Disable
4	USER	FEU_PBX1_Group	0	N/A	N/A	1	Disable	Disable	Disable
5						1	Disable	Disable	Disable

Proxy set



- Proxy set is a logical set of IP-Addresses group that is usually associated with an (server) IPGroup in order to know how to route SIP dialogs to this IPGroup.
- Can include 1 or more IP addresses or FQDN that can be resolved to IP address.
- All the multi-proxies functionality exists in each group (e.g. redundancy, hot swap, load balancing, DNS, SRV etc.)

Example – Proxy set 1



Proxy Sets Table

Proxy Set ID: 1

	Proxy Address	Transport Type
1	10.8.8.90	UDP
2		
3		
4		
5		

Enable Proxy Keep Alive: Disable

Proxy Keep Alive Time: 60

Proxy Load Balancing Method: Disable

Is Proxy Hot Swap: No

Example – Proxy set 2



Proxy Sets Table

Proxy Set ID: 2

	Proxy Address	Transport Type
1	proxy1.bandtel	UDP
2	proxy2.bandtel	UDP
3		
4		
5		

Enable Proxy Keep Alive: Disable

Proxy Keep Alive Time: 70

Proxy Load Balancing Method: Disable

Is Proxy Hot Swap: No

Example – Proxy set 3



Proxy Sets Table

Proxy Set ID: 3

	Proxy Address	Transport Type
1	216.82.225.203	UDP
2	216.82.225.202	
3		
4		
5		

Enable Proxy Keep Alive: Disable

Proxy Keep Alive Time: 70

Proxy Load Balancing Method: Disable

Is Proxy Hot Swap: No

Account Table



- This table defines account that served groups (either IP or Trunk) have in a serving IPGroup, for the sake of Registration\Authentication
- Defines the Username\Password used for the different registration\authentication options
- Each IPG\Trunk Group can register to more than 1 IPG (by defining different table entries)
- May be used for instance in order to register to ITSP on behalf of a IP-PBX

Example



Account Table

Note: Select row index to modify the relevant row.

Add Duplicate Compact

x	ServedTrunkGroup	ServedIPGroup	ServingIPGroup	Username	Password	HostName	Register
0	-1	1	2	2062700001	swilla		0
0	-1	1	3	58986989	ac		1

Routing and association of Source\Dest groups to SIP sessions



- From our perspective a call has two legs that define its type, IP<->IP has two IP legs, and IP<->TEL has one IP and one TEL legs
- Each call (either IP<->IP or Tel<->IP) has two associated groups, one is the source group and the other is Destination group
- Each established call must be associated with these two groups, the association to a destination Group also define where to route the call (in case of IPGroup, to the assigned ProxySet or DB and in case of trunk group the this Trunk group)

Associating & routing of Incoming IP calls



- Incoming INVITE will be processed in the IP to Trunk Group routing table.
- This table has now a new role that is very important in case of IP->IP calls (but may also be relevant for IP->Tel calls), the new role is to set the source IPGroup
- Added columns -
 - Input: Source and destination host names (addresses) taken from the request URI and the From\P-asserted\RPI
 - Output: Source IP group
- If destination Trunk Group is other than -1 the call is IP->Tel call and the destination group is the specific trunk group
- In case the Trunk group is -1, this call is IP->IP call that has a source IPGroup but doesn't have a destination IPGroup yet
- In order to set the destination IPGroup we must visit the Tel->IP routing table as described in the next slide.
- In case the source IPGroup is not configured, the associated IPGroup will be the default (0) one

Example



Inbound IP Routing Table

Basic Parameter List ▲

Routing Index: 1-12

IP To Tel Routing Mode: Route calls before manipulation

	Dest. Host Prefix	Source Host Prefix	Dest. Phone Prefix	Source Phone Prefix	Source IP Address	Trunk Group ID	IP Profile ID	Source IPGroup
1			*	*	10.8.8.90	-1	0	1
2		ProxyBandtel.com	*	*	*	-1	0	2
3		BandWidth	*	*	*	-1	0	3
4	PBX1		*	*	*	-1	0	4

Associating & routing of Outgoing (to IP) calls



- Each outgoing (to IP) call has a source Group (either IP or Trunk) but doesn't have a destination group yet.
- In case the Source Group has a serving IPGroup the routing and Dest group association is set to the the serving IPGroup.
- If not we must visit the Tel->IP routing table.
- This table has now a few new columns in order to help us route –
 - (Input) Source IPGroup (in case of IP-IP)
 - (input) Source TrunkGroup (in case of IP-TEL)
 - (input) Source and dest hosts (in case of IP-IP)
 - (output) Dest IPGroup.
- In case the Dest IPGroup is not configured, the routing will be to the specified IP-Address and the associated IPGroup will be the default (0) one.
- After setting Dest IPGroup the routing will be done to this IPGroup.

Example



Outbound IP Routing Table

B

▼

Routing Index: 1-10 ▼

Tel To IP Routing Mode: Route calls before manipulation ▼

	Src. IPGroupID	Src. Host Prefix	Dest Host Prefix	Src. Trunk Group ID	Dest. Phone Prefix	Source Phone Prefix	->	Dest. IP Address	Dest. IP Group ID
1	1 ▼				1800	*	*		3 ▼
2	1 ▼				1919	*	*		2 ▼
3	2 ▼				0200	*	*		1 ▼
4	1 ▼				FEU5	*	*		4 ▼

Far\Near end users



- Far\Near end users should be gathered into logical IPGroups (probably all users belonging to a specific IP-PBX belong to the same group)
- This IPGroup should be defined as a user IPGroup
- By default register\invite requests arriving from Users that belong to a user IPGroup are handled and sent to the serving IPGroup (other registrations requests will be rejected)
- In case of successful response the FEU details will be added to a dynamic DB.
- INVITES arriving from IP-PBX and destined to FEU group (rules in the routing table should define which requests to route to FEU group) will be routed according to the dynamic DB.

FEU NAT\Firewall problems



- In many cases the FEU will be behind NAT – in this case we will respond to the address we receive packets from
- In UDP the source port = destination port
- In TCP we will keep the same connection
- The FEU opened a pin hole in the firewall – to maintain it we will reduce the registration time between the FEU and the SBC.

Questions?