# *No. 31 – WTL Built-In SBC Functions*

An essential part of a well-designed VoIP network is a Session Border Controller (SBC). In order to make network architecture and deployment easier, WTL have designed extensive SBC features into our switches and gateways, instead of offering a standalone SBC device.
The benefits of the WTL approach include:

- Fewer boxes in the network (means less cost, easier deployment)
- Single point of administration
- Same policies/rules can be applied to both VoIP and TDM traffic

## What is a Session Border Controller?

The following definition is from Wikipedia:
*A **Session Border Controller** is a device used in some VoIP networks to exert control over the signaling and usually also the media streams involved in setting up, conducting, and tearing down calls. Within the context of VoIP, the word **Session** in Session Border Controller refers to a call.*
*The word **Border** in Session Border Controller refers to a point of demarcation between one part of a network and another. It is the job of a Session Border Controller to assist policy administrators in managing the flow of session data across these borders.*
*The word **Controller** in Session Border Controller refers to the influence that Session Border Controllers have on the data streams that comprise Sessions, as they traverse borders between one part of a network and another. Additionally, Session Border Controllers often provide measurement, access control, and data conversion facilities for the calls they control.*

## WTL SBC operation

WTL products are able to act as switches and gateways for VoIP and TDM calls. As such they are inserted into the signaling and media paths between calling and called parties using SIP, H.323, and NOP call/session handling protocols.
The WTL switch acts as if it were the called VoIP phone and then places a second call to the actual called party. In technical terms, when used within the SIP protocol, this is defined as being a Back-to-Back User-Agent, or B2BUA. The effect of this behaviour is that the WTL switch can control not only the signaling traffic, but also the media traffic (voice). The switch can also redirect media traffic to a completely different element elsewhere in the network, perhaps for recording, generation of music-on-hold, or other media-related purposes.
The WTL SBC allows the network operator to control the kinds of calls that can be placed through the network on which it resides, to fix or change protocols and protocol syntax to achieve interoperability, and also to overcome some of the problems that firewalls and NAT (Network Address Translation) cause for VoIP calls.
SBCs are often used by corporations along with firewalls to enable VoIP calls to and from a protected enterprise network. VoIP service providers use SBCs to allow the use of VoIP protocols from private networks with internet connections using NAT, and also to implement strong security measures that are necessary to maintain a high quality of service.
Additionally, the WTL SBC can allow VoIP calls to be set up between two devices using different VoIP signaling protocols (SIP, H.323, NOP) as well as performing transcoding of the media stream when different codecs are in use*. The WTL SBC also provides certain firewall features for VoIP traffic (denial of service protection, call filtering, bandwidth management, etc...).

## Business Models Supported

The WTL SBC function allows operators to offer multiple different business models in complete safety:

- Carrier-to-carrier
  - Bilateral or multilateral
  - Domestic and international
  - Interconnect and peering
- Carrier to enterprise
  - SIP trunking
  - Hosted IP PBX and IP Centrex
  - SIP Application services (conferencing, IVR etc)
  - Number manipulation
  - Correct 'Nature of Address' handling
  - Privacy/anonymous CLI
  - Call throttling
  - PABX environment (WTL acts as pseudo-local exchange)
- Carrier to Subscriber
  - VoBB (Voice over Broadband)
  - SIP registration
  - Call transfer
  - Voice mail support – redirect on no answer, on busy, unconditional, call forwarding
  - Pre-Paid services
  - Combined voice and data services

For all models a generic set of features provide protection for the operator's network:

- Overload protection (inbound, outbound or total call limits can be imposed)
- Call usage / Rate limiting
- Per session authentication and authorisation
- Call rating and mediation

## Security

WTL equipment provides a wide range of features to keep the operator's network secure from threats to operational service (DoS attacks) or to revenues (fraud attacks). The WTL SBC adds the following features:

- '**Anti-spoofing' techniques** confirm that a source IP address is genuine. The WTL call control uses the source IP address not the IP address 'claimed' in the message.
- **Flood attack prevention:** SIP sessions may be limited based on source IP address. WTL implement the concept of a 'Max Users' field per account. An account can be tied to a source IP address.
- **NAT traversal** is supported by use of a callers' source IP address.
- **2 levels of IP filtering** are implemented to allow only known/trusted source IP addresses into the network. This filtering is flexible and works with a) specific approved addresses or b) ranges of addresses. In addition, IP address may be associated with an account. Accounts can in turn be validated by CLI or using Digest Authentication.

- **DOS attacks** are limited by using a first level of IP filtering which prevents an attack entering the higher levels of the application. Thus they are rejected with minimal resource utilisation.
- **CLI Spoofing:** a double level of verification is offered by WTL switches to ensure that an incoming CLI matches the IP address that it is supposed to come from.
- **Intelligent access lists**
- **IP address and port translation**: The WTL SBC provides access control and private-to-public IP network and port address translation.
- **Topology hiding** is supported. SIP message transiting WTL switches have all 'via lines' removed.
- **Traffic separation:** All equipment supports 2 Ethernet interfaces allowing the separation of administration and user traffic.
- **SIP signaling attacks** are dealt with using the 2 level IP filtering described above.
- **Blacklisting of endpoints:** the equipment contains tables of IP address / CLIs that are not allowed to call.
- **Malformed SIP messages** are efficiently dealt with and discarded.
- **Alarms** are recorded in the WTL equipment log files for audit or diagnostic purposes.

## Call Routing & Numbering Management

At the core of all WTL products is a robust, high capacity, intelligent Call Routing Engine. This allows a very flexible system of dial plans based on dialed E.164 digits.
Numbering features include the following:

- Called number translation
- Calling number verification/manipulation
- Trunk capacity limits
- Hunt groups
- Flexible Dial plans
- Day & time based routing
- Release cause based routing
- Calling number translation
- Call load sharing
- Session (Call) Detail Reporting
- LCR
- Registration-based routing
- Traffic type based routing
- Destination grouping

Sophisticated Least Cost Routing (LCR) models may be created with multi-level fallback to up to 5 alternate carriers per destination dialling code (or code group).
The WTL routing engine also supports a 'trusted' mode to be set up for simple IP exchange applications. In this case, traffic comes from 'trusted' sources and authentication rules may be relaxed.
Session (Call) Detail Reporting includes protocol information, QoS metrics, release causes, actual route taken etc.

## Protocol Matching

WTL switches are built around a central core which uses a standard representation of a call or session – and all the attributes associated with it – regardless of the protocol or media used by the

call. This makes WTL switches ideal in a 'transit' environment, since they are able to support multiple simultaneous protocols and route calls between them with no limitations.
VoIP calls may be made seamlessly between SIP and H,323, and also to WTL's own bandwidth optimisation protocol, NOP. Since SIP is an open and extensible protocol, many different variations exist which may, at times, be incompatible. WTL's SBC function addresses this and 'normalises' the signalling variations so that calls may be successfully connected between different vendors' equipment and amongst many operator networks.
The SoIP gateway is also capable of performing the same service for VoIP to TDM (SS7, ISDN and R2) calls.

## Interoperability and Interworking

The WTL switch allows the creation of multi-vendor, multi-protocol networks, as required. In order to achieve this, the WTL SBC must be able to smooth out the incompatibilities between the different entities. These problems may arise in the areas of codec mismatches, DTMF support, fax handling, ANI/DNIS or elsewhere – but wherever they occur, the WTL SBC will deal with them.
Over almost 10 years, WTL has built up extensive experience of interconnecting with a wide range of VoIP equipment on both the subscriber and network sides. WTL continues to run many interconnect tests to ensure maximum SIP compatibility.

## IP Addressing & Port Management

The WTL SBC allows a range of operations using the IP address of inbound calls. These include caller authentication, address translation, and call routing.
To improve security, the following SIP-specific method is supported: if a call is received via a known SIP proxy the WTL SBC will detect that the calls come from the proxy's IP address, and will look in the second via line for the actual customer IP address. Also, to counter CLI spoofing, an incoming CLI may be checked to ensure that the IP address is the one that ought to be associated with it.
In common with other gateways, WTL will allow the SIP port to be configurable. However, WTL can also support multiple SIP ports being used simultaneously. Different ports can have different settings: different proxies, forms of verification, choice of codecs etc because each SIP trunk has its own independent SIP signaling stack.
In order to overcome blocking of SIP by NAT devices, the WTL SBC can map SIP traffic to a non-standard IP port if required.
The WTL SBC supports IP address resolution for outbound calls according to DNS standards. This can be configured to be with or without external DNS, or to friendly DNS servers only. This means that the switch can route using a host name which can be useful for load sharing.

## WTL SBC Feature List

- Firewall Traversal
- NAT Traversal
- Topology hiding
- IP Address Resolution/Management
- SIP to H.323 conversion
- RTP termination and regeneration
- SSL tunnels
- H.323 V2 & 3 ( + partial V4 support)
- Voice codec conversion*
- Built-in firewall
- Authenticate VoIP calls and callers
- Session Admission Control
- Prevention of DoS attacks
- CDR generation
- G.711 / T.38 Fax relay for SIP and H.323
- RADIUS Support

- H.323 Fast Start & Slow Start
- H.323 ToS support
- Qos Marking, DiffServe support
- SIP transaction rate limiting (limit number of SIP Iknvites)
- Detect and drop malformed packets
- Per trunk bandwidth RTP policing
- Digit matching/manipulation
- Deep packet inspection
- H.245 tunnelling support
- H.225 RAS messages for alternative gatekeeper functionality
- Source and destination trunk group support
- Simultaneous peering with multiple gatekeepers and gateways

* Codec conversion requires hardware-based voice resources