Media Gateway Unit, MGU2

DESCRIPTION

NOTICE

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Networks™ Corporation (MITEL®). Mitel makes no warranty of any kind with regards to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes.

TRADEMARKS

1 INTRODUCTION

This document describes the functions, performance and limitations in the MX-ONE Media Gateway Unit (MGU2).

The MGU2 is a device board to be inserted in a dedicated board position in a 1U, 3U or 7U chassis/subrack. Unlike other device boards, this board is required in the Media Gateway subrack, and only one can be inserted at its dedicated board position.

The key features of MGU2 includes:

- **Device Board Interface**. MGU2 intermediates all communication between device boards in the 3U/7U chassi and the MX-ONE Service Node.
- **Digital trunks.** MGU2 provides layer 1 and layer 2 for E1/T1.
- **VoIP**. MGU2 provides RTP/SRTP including DTMF detection, DTMF relay and facsimile tones over RTP. The VoIP channel also includes configurable echo canceler.
- **Fax relay T.38**. MGU2 provides relaying T.30 facsimiles (G3 fax) to/from Internet Aware Faxes or Gateways using T.38 protocol.
- **Keycode Receiver**. MGU2 provides Keycode Receivers (DTMF and MFC receivers), intended for mobile extensions (DTMF) and CAS E1 trunks (MFC).
- **Keycode Sender**. MGU2 provides Keycode Senders (DTMF and MFC senders), intended for mobile extensions (DTMF) and CAS E1 trunks (MFC).
- **Tone Sender**. MGU2 provides Tone Senders for call progress tones, e.g. dial-tone, according to market specifications.
- **Multi Party**. MGU2 provides Multi Party resources for e.g. conference and intrusion call cases.
- **Recorded Voice Announcements**. MGU2 provides play out of pre-recorded, locally stored, media files over TDM switch.
- **TDM switch**. MGU2 provides a non-blocking TDM switch with attenuation support for interconnection of circuit switched media.
- **Network Redundancy**. MGU2 supports redundant networks.
- **External Alarms**. MGU2 supports inputs in backplane for external alarms.

1.1 SCOPE

This document provides a description of the MGU2 board, provided functions, their performance and limitations. The document does not cover details of end-user and administrator commands, etc. provided by MX-ONE Service Node and/or MX-ONE Manager for initiating or using these functions.

1.2 GLOSSARY

For a complete list of abbreviations and a glossary, see the description for *ACRONYMS, ABBREVIATIONS AND GLOSSARY*.

AES
Advanced Encryption Standard

AH
Authentication Header

CAS
Channel Associated Signaling (for E1 trunk interface).

CBC
Cipher Block Chaining

CNG
Comfort Noise Generation. Used to generate background noise when no RTP packets are received or when NLP is engaged.

DBS
Device Board Server. This is a MGU2 subsystem, running in a linux process for device board communication, and also implementing virtual device boards (ISDN).

ESP
Encapsulating Security Payload

IKE
Internet Key Exchange

ISAKMP
Internet Security Association and Key Management Protocol

IPsec
Internet Protocol Security

LFO
Link Fail Over. Redundancy with switched network.

NLP
Non-Linear Processor. Removes the residual echo that the linear echo canceler couldn’t remove. It is idle at double-talk.

DFE
Dual-Filter Echo Canceler. This is an optional echo canceler in MGU2 that improves echo canceling significantly, but also decreases capacity.

DP
Device Processor. This is the main control and supervision processor, running a linux operating system, on MGU2 board.

DSP
Digital Signal Processor.

MCA
Media Control Application. This is a MGU2 subsystem, running in a linux process for Media related tasks (VoIP and TDM switch management).

MSP
Media Stream Processor. System-on-Chip module with DSP capabilites for voice and media processing.

OMA
Operation & Maintenance Application. This is a MGU2 subsystem running in a linux process for O&M related tasks.

PCM
Pulse Code Modulation. Digital representation of analog signals in e.g. circuit switched (TDM) systems. In TDM systems, usually 8000 Hz sampling rate and A-law or mu-law encoding is used.

PRI
Primary Rate Interface (2048 kbit/s E1, or 1544 kbit/s T1).

PTS
Proceed To Send.

SA
Security Association

SLIP
A standardized procedure to take care of different clock rates between two digital systems by either skipping or repeating a frame of data

TDM
Time Division Multiplexing. A way to transfer several channels, containing PCM samples (timeslots), on a single wire.

VAD
Voice Activity Detect. Used to stop RTP packet encoding and transmission during silence periods in received PCM stream, resulting in reduced DSP and network load.

Virtual Board
A native application on MGU2 that simulates a legacy physical (“real”) board. From a management point of view it is configured and behaves like a real board.

Virtual Magazine
The virtual magazine is the equipment range in MGU2 that holds the virtual boards and the MSP resources that are mapped to equipment numbers.

2 BOARD DESCRIPTION

This chapter gives a high-level description of the Media Gateway Unit (MGU2) board.

2.1 BOARD LAYOUT AND FRONT CONNECTORS

Figure below shows the MGU2 front and the external connectors in the front. For further description of these, refer to section 2.2 Interfaces on page 7. The MGU2 hardware architecture and its external interfaces
(connectors) is outlined in the figures below. The board has connectors in the front and to the backplane. The backplane is mainly the interface to other device boards, alarm signals and power to the board.

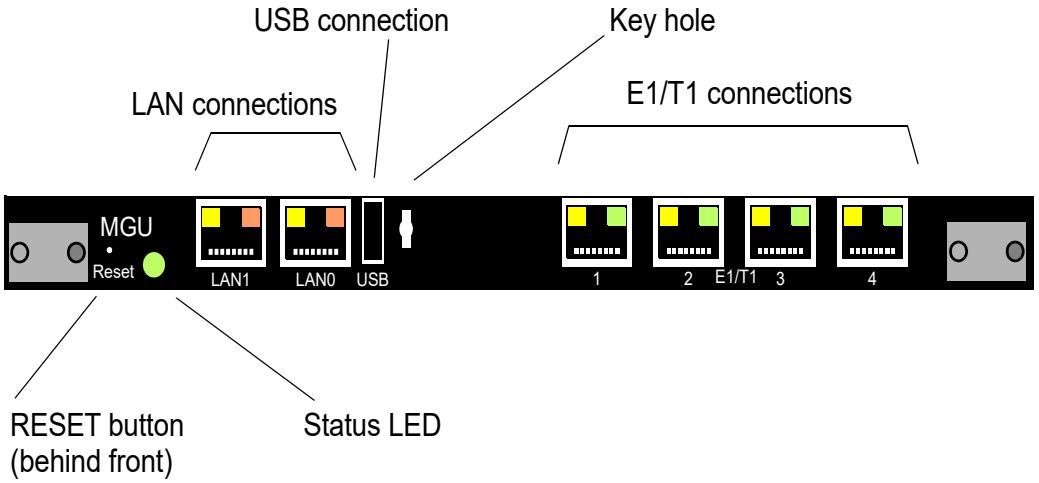


Figure 1: MGU2 front and connectors

Figure below shows interfaces on the MGU's PCB.

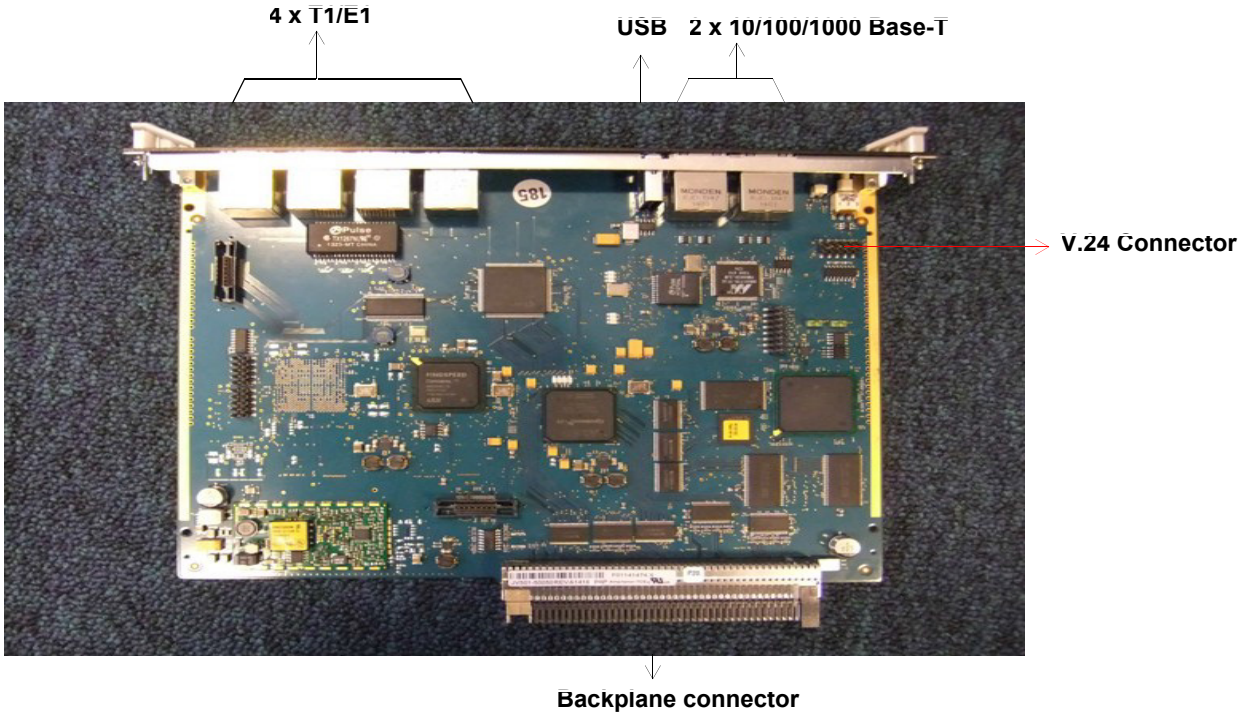


Figure 2: MGU2 board layout

2.2 INTERFACES

- **LAN0 and LAN1**. Primary (LAN0) and Secondary (LAN1) LAN ports. These two ports provides support to connect to redundant networks. See also 3.11 IP Network Redundancy and Security on page 23 for more information how to connect these.
- **Device Board Interface** (Backplane Interface). This is the interface towards all device boards. Up to 16 device boards can be accessed. It includes TDM buses (including frame sync input and output) and HDLC/UART signaling buses to all device boards.
- **E1/T1**. 4 Primary Rate Interface (PRI) for ISDN, CAS trunks and CAS extension.
- **Visual Indicators** (front LED). The LED shows the operating status of the MGU2 board. There are also indicators on the LAN and E1/T1 connectors, see further 3.12 Visual Indications on page 28.
- **Reset button**. The Reset button is connected via the FPGA to HW reset of the Device Processor (DP) to be able to reset the board.
  This button can also be used to clear settings to the factory default IP values.
- **USB**. Management and service interface (linux console) which support USB to serial (V.24) bridge (USB serial dongle).
  A TSR 899 135/1 cable can be connected from this interface to for example a PC with terminal program. The terminal program shall be configured for 9600 baud, no parity, 1 stop bit to connect to this interface. Other USB serial dongles that uses a PL2303 chip might work as well.

Note: All management that can be done from the USB interface can also be done through SSH login.

- **V.24**. The V.24 interface located on the PCB is mainly intended for debug purposes, but can be used as a “fall back” Management interface if USB access is not possible. Same terminal configuration as for USB applies. A TSR 43 297/1000 cable can be connected to this interface.

2.3 KEY COMPONENTS

2.3.1 TDM SWITCH

The TDM (Time-Division Multiplexing) switch on MGU2 has a very central function, since all media interconnections between trunks, extensions, and auxiliary functions are made through this switch. An exception to this is when media is setup between two IP extensions where media can be setup direct between these extensions on the LAN. However, there are also such cases when IP extensions are forced connected via the MGU2 and thus through the TDM switch as well.

The TDM switch is a non-blocking Time-Space-Time switch handling cross connections for up to 2048 64kbps timeslots. Of these, only 896 are connected and used, as shown in figure 3 below.

The switch provides a multi-cast feature (a.k.a. sunfan) to connect one timeslot to many other (there is no restrictions how many).

Figure 3 below shows the TDM switch and interconnection of TDM devices on MGU2. The figure shows the physical (HW) timeslot numbers. These numbers can be mapped to logical timeslot numbers (multiple numbers) and EQU (Equipment) positions as shown in table See “TDM Switch Timeslots to Equipment/Resource mapping” on page 9..

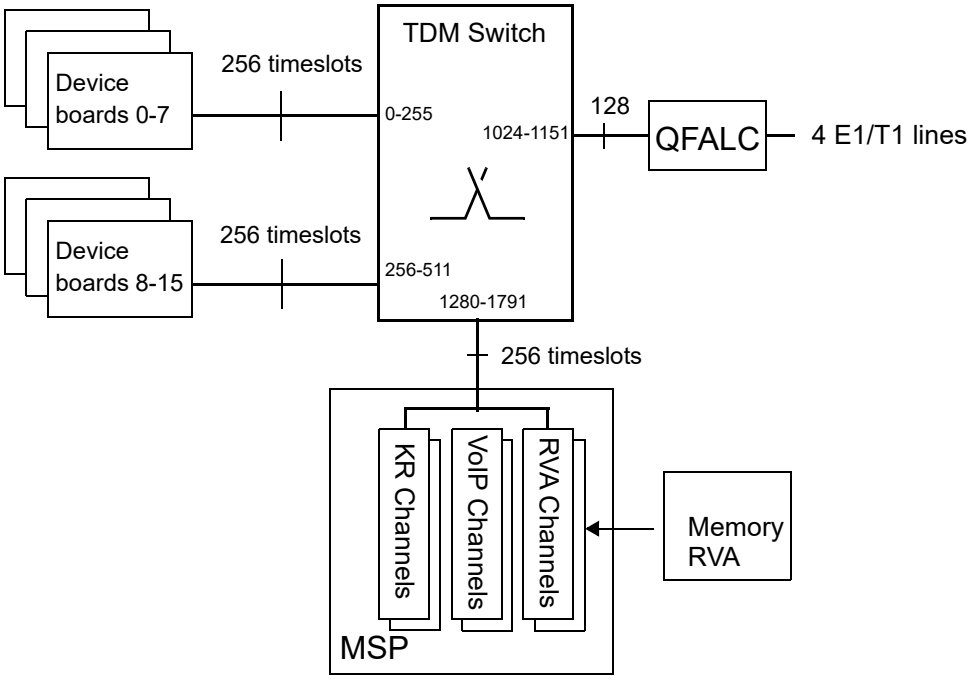


Figure 3: TDM switch and interconnection to TDM devices

For each device connected to TDM switch, the number of 64kbps timeslots is stated, and the physical timeslot number (0-2047) in the switch (note: not all timeslots are used, see table See “TDM Switch Timeslots to Equipment/Resource mapping” on page 9.).

The TDM switch provide functionality to select attenuation level on each connection individually. Attenuation values are pre-configured at MGU2 startup according to selected market. See market characteristics for attenuation levels used per market.

Table 1 TDM Switch Timeslots to Equipment/Resource mapping

TDM switch range	Equipment / Resource type		Multiple Number range (decimal / hex)		EQU range *) (within Media GW) **)
0..511	Device Boards (16 positions)	3U and 7U	0..31	000..01F	0-00-0 .. 0-00-31
			32..63	020..03F	0-10-0 .. 0-10-31
			64..95	040..05F	0-20-0 .. 0-20-31
			96..127	060..07F	0-30-0 .. 0-30-31
		3U and 7U	128..159	080..09F	0-40-0 .. 0-40-31
		7U only	160..191	0A0..0BF	0-50-0 .. 0-50-31
			192..223	0C0..0DF	0-60-0 .. 0-60-31
			224..255	0E0..0FF	0-70-0 .. 0-70-31
			256..287	100..11F	1-00-0 .. 1-00-31
			288..319	120..13F	1-10-0 .. 1-10-31
			320..351	140..15F	1-20-0 .. 1-20-31
			352..383	160..17F	1-30-0 .. 1-30-31
			384..415	180..19F	1-40-0 .. 1-40-31
			416..447	1A0..1BF	1-50-0 .. 1-50-31
			448..479	1C0..1DF	1-60-0 .. 1-60-31
			480..511	1E0..1FF	1-70-0 .. 1-70-31
512..1023	*Unused*				
1024..1151	E1/T1 Links (4 virtual boards)	Link 1	512..543	200..21F	2-00-0 .. 2-00-31
		Link 2	544..575	220..23F	2-10-0 .. 2-10-31
		Link 3	576..607	240..25F	2-20-0 .. 2-20-31
		Link 4	608..639	260..27F	2-30-0 .. 2-30-31
1280..1535	Dynamic Resources in MSP (e.g. VoIP channels and Keycode Receivers)		768..1023	300..3FF	3-00-0 .. 3-70-31
1536..2047	*Unused*				

***)** The Media GW number has been omitted from the EQU numbers in this table. For example, if resource is in Media GW 1A, 1A- shall be added as a prefix to the EQUs listed here.

****)** As of MX-ONE 5.0 SP3, the following TMU functionality has been moved to the MGU2 software. Therefore, no TMU board is needed in a MGU2 based MGW chassis for a standard MX-ONE installation with IP/TDM users assuming that the InAttend operator is used:

- Extension conference
- Extension Intrusion
- DTMF send/receive
- Tone sending

The following functionality is not supported by the MGU2 based TMU software.

- Native MX-ONE operator
- Dial tone detection (use a Proceed to send, PTS timer instead)
- Specific market tones (e.g. morse)
- Analog MoH input, e.g. no live announcement for Emergency notification.

In the case that the above functionality is needed, then a TMU board must be present with the MGU2 based MGW chassis.

2.3.2 ETHERNET (LAYER 2) SWITCH

There are two standard 10/100/1000 Base-T LAN connection on the MGU2 board marked LAN 0 and LAN 1.

The Ethernet packets are via a layer 2 switch routed to the Device Processor (DP) or to the Media Stream Processor (MSP). See figure below.

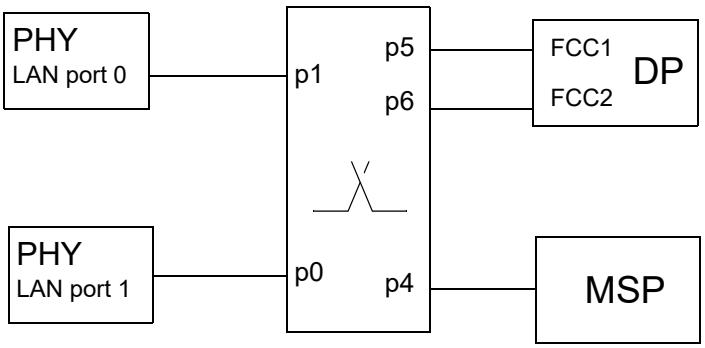


Figure 4: Ethernet switch (Ports for index 3 & 4 boards in parentheses)

Packets on the LAN can be of two kinds.

- Non-RTP packets, for signaling, are routed to the DP.
- RTP packets carrying media (VoIP), are routed to the DSP.

2.3.3 MEDIA STREAM PROCESSOR (MSP)

The M82349 is a System-on-chip for VoIP telephony applications.

The MSP is a common resource pool shared by all DSP-related functions provided by MGU2. Examples of functions are VoIP, T.38 and DTMF receivers. Depending on function used and configuration settings, the load on MSP differs (the load from a particular function might even vary over time) and thus the maximum density in MSP varies

depends on usage. See further section 6 Capacity and Limitations on page 40 that states MSP density for different functions and a few configurations.

The processor load is continuously supervised and reported to MX-ONE Service Node to indicate high-load conditions (high load conditions will be logged in MGU's syslog as well). High-load condition is also checked in run-time when orders to activate a new DSP function is received from MX-ONE Service Node. If too high load at that time, the order is rejected with information about the cause.

Note: The syslog is stored in the file /var/log/syslog in MGU's file system.

2.3.4 TDM SYNCHRONIZATION UNIT

A clock circuit is used to generate a system clock. The system clock is distributed to internal (on board) components and external resource boards in a magazine where applicable.

The clock source is user defined and is one of the following:

- The free running XO (Crystal Oscillator).
- One of the internal TDM trunks.
- Any board slot in a magazine (when a magazine is used) containing a TDM trunk board or other board that can provide PCM sync.

The clock circuit will automatically change to Holdover mode when the input signal is invalid, i.e. the input is off by more than capture range which is more than +-280 ppm or when the input signal is "gone" (steady high or low).

The locking time for the clock circuit is typically 50 seconds.

The on board FPGA routes the synchronization clock from one of the trunks to the clock circuit unless the XO is used. The on board components and resource boards are then fed by the clock circuit and distributed by the FPGA.

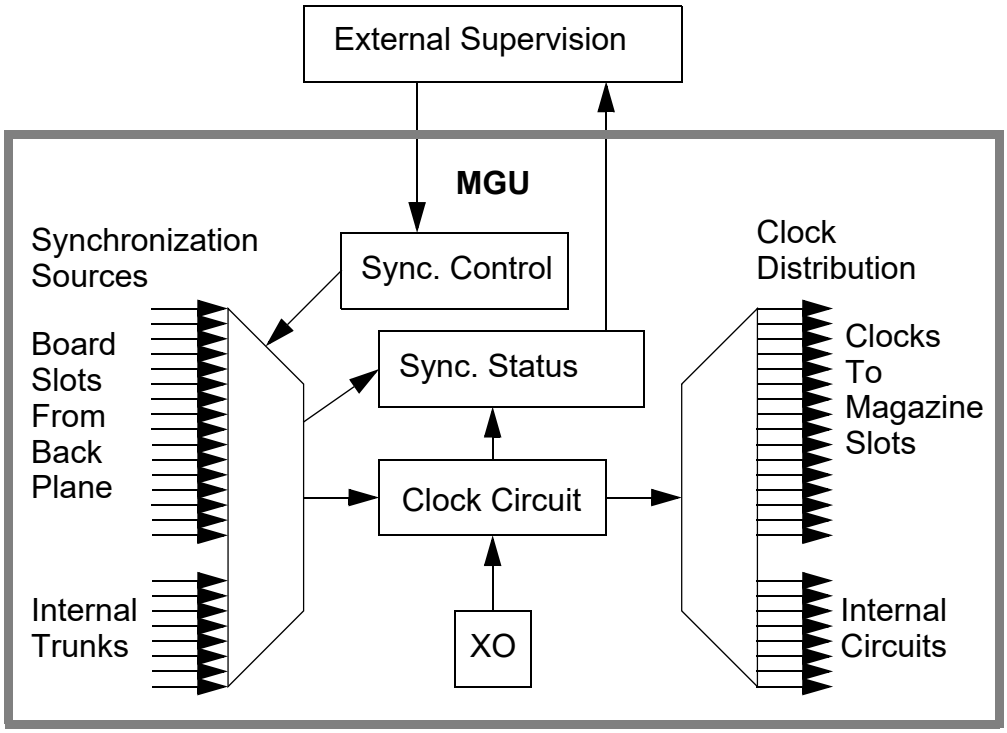


Figure 5: Clock synchronization sources and distribution

3 FUNCTIONALITY

3.1 RESTART & FACTORY RESET

The MGU2 can be restarted by different sources:

- HW Reset Button.
- HW Reset Button factory reset mode.
- HW Watchdog
- MX-ONE Service Node

The MGU2 has an external button (hole in the front) to make a HW reset of the board.

When the reset button is pressed and released, the reset line to the Device Processor (DP) is pulled which causes an immediate restart of the DP and reboot of SW.

Pressing the Reset button on the front of the Media Gateway for 5 seconds will reset your Media Gateway to its factory default factory settings. When the reset button is pressed the Ethernet's LAN port LEDs are starting to flash and after 5 seconds the LEDs are changing to fixed green light, to give the operator a hint when the factory reset takes place.
Any earlier settings on the Media Gateway will be erased.
For default parameters settings, see section 6.11 table 27.

Note: Using HW reset on a running live system reset should only be used as a last resort, since there is a risk of corrupting flash file system and/or configuration data.

During normal operation, the Device processor regularly restarts the watchdog timer to prevent it from elapsing, or "timing out".

If, due to a hardware fault or program error, the DP fails to restart the watchdog, the timer will elapse and generate a Hardware reset (restarting the HW) to try to get the MGU2 in a reset state and restoring normal system operation.

A watchdog indication in the NOR Flash (NV-parameters) shows the latest state of the watchdog after a HW restart.

The are 2 states:

- **Watchdog normal**
  A normal reset has occurred on the MGU2 which means that the software or an operator has invoked the reset. The restart is logged (for trace analysis) in the linux syslog if the restart is ordered by the MX-ONE Service Node.
- **Watchdog timed out**
  The watchdog timer has elapsed causing a HW reset.

In order to supervise SW and HW execution there is a HW Watchdog on the MGU2.

- **MX-ONE Service Node**
  The MX-ONE Service Node can send media gateway restart message which will cause a HW reset on the MGU2.

3.2 DEVICE BOARD INTERFACE

The Device Board Interface provides a signaling and restart interface between MX-ONE Service Node and the Device boards in the 3U/7U subracks, and a PCM interface between Device boards and the TDM switch on MGU2. This interface is also used for on-board provided functions that are implemented as “virtual boards”, like the Digital E1/T1 Trunk (see next section). Virtual boards is a way to emulate older Device boards but with new Hardware.

The MGU2 supports a propriety device board interface using 2Mbit HDLC and/or 128Kbit UART for signaling, and 2Mbit PCM for circuit switched media (32 x 64kbps timeslots) per device board position. Up to 16 device boards can be supported. The older UART protocol with slow signaling supported by DSU is not supported by MGU2.

3.3 DIGITAL TRUNK E1 AND T1 INTERFACE

MGU2 provides 4 digital trunk interfaces (PRI:s) of type E1 and T1.

Each PRI is implemented as a “virtual board” in the “virtual magazine 2” (i.e. EQU range 2-0-00 to 2-30-31) and can be configured and run independently of each other.The configuration of E1 resp T1 framing of each interface is done during “board” activation. Each interface can be configured as either:

- E1 with ISDN protocol (corresponding to a TLU76/11 board)
- E1 with CAS protocol (corresponds to a TLU76/13 board)
- T1 with ISDN protocol (corresponding to a TLU77/11 board)

MGU2 ISDN/PRI interface has been verified to comply with ETSI TBR004 (EU), TIA-968-A 47 CFR Part 68 (US), CS-03 Issue 9 Part VI (CA), AS/ACIF S038 (AU) and Newsletter No 125 (NZ).

MGU's ISDN Layer 1 and 2 supports ETS 300 011 and ETS 300 125 respectively.

When an E1 interface is configured as CAS trunk the ISDN Layer 2 protocol in time slot 16 is replaced by a CAS multi frame structure and signaling according to ITU-T G.732 for 2048 kbit/s. MGU2 supports MFC R1 and R2 signaling, replacing similar functionality in the MFU board.

Configuration parameters per PRI are set in run-time in the MX-ONE Service Node SW.

- Application = E1 or T1
- Network Termination = User side or Network side (for ISDN)
- A set of parameters unique for CAS trunk

Note: The E1 interface can as well be used for CAS Extension. In this configuration 30 logical extensions can be represented at each E1 port.

3.3.1 LIMITATIONS

E1 CAS

MGU does not support all features and tones supported by the MFU board. MFU board(s) are therefore required where non standard MFC R1/R2 is used.

T1

Some of the counters and timers for error statistics reporting provided by TLU77/1 are not supported by the T1-PRI:s at MGU2.

Also the Facility Data Link (FDL) provided by TLU77/1 is not supported by the T1 PRI at MGU2.

3.3.2 LAYER 1 - PHYSICAL INTERFACE

The Layer 1 physical interface supports ISO 10173, and RJ45 connectors with wiring according to USOC RJ-48C.

The electrical connection is twisted pair 120 ohm for E1 and 100 ohm for T1.

MGU2 supports both European E1 and the North-American T1 TDM interface standard.

For E1 MGU2 provides automatic adaptation to "CRC-4 multi-frame structure" or "Double frame structure" for E1 and is specified in ETS 300 167, (based on ITU-T recommendations G704/G706).

For T1 or DS-1 MGU2 supports Super Frame (SF) or Extended Super Frame (ESF) framing scheme, bipolar with eight-zero substitution (B8ZS) or zero code suppression (ZCS).

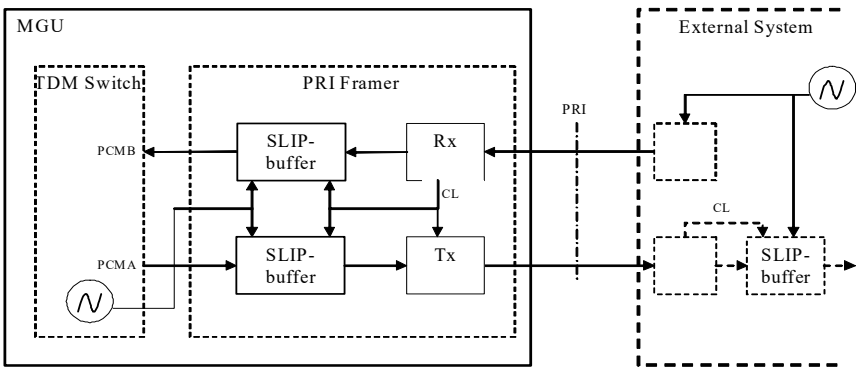
Facility Data Link (FDL) is not supported and it is assumed that external equipment can be used, providing the FDL functionality.

3.3.2.1 Transmit Slip buffer

Each PRI interface contains “elastic” buffers (aka Slip buffers) in order to handle situations with different clock frequencies between MGU2 and an external telephony system. Slip buffers are always active in the receive path, but in the transmit path (towards the external system) it is optional to use.

In most scenarios when clock synchronization is properly administrated slip does not occur. However in some (temporary) scenarios, for instance when the DECT sync ring is used for PCM clock distribution there are certain situations when it is preferred to use a free running MGU2 oscillator as PCM sync "master". In such situations to avoid SLIP alarms on “external systems” an activation of a Slip buffer in the transmit path of the E1/T1 Framer of MGU2 is needed.

The activation is made by setting the TX_Slipbuffer parameter (see ISDN parameters for details).



Block diagram showing the Slip buffers at the PRI interface

3.3.3 LAYER 2 - DATA LINK PROTOCOL

The PRI supports data link layer protocol ETS 300 125 (ITU-T ISDN user-network interface - Data link layer specification Q.921/I.441).

The PRI support point-to-point data link with non-automatic TEI assignment procedure.

3.3.4 PERFORMANCE

The PRI signal capacity with an ISDN call rate of 5 calls/seconds generates less than 20% CPU load in net contribution from the ISDN traffic alone. The capacity figure is based on a ten Q.931 Layer 3 messages per call and one Layer 2 RR frame per message.

3.4 VOICE OVER IP

The MGU2 provides Voice over IP according to the RTP and SRTP (secure VoIP) protocols. MGU2 also supports DTMF relay in VoIP channels according to RFC 2833/RFC 4733.

VoIP channels are obviously used to convert media between SIP/H.323 terminals and circuit switched devices, but also to interconnect media gateways, known as “inter-GW calls”. Thus, a “circuit switched” call between e.g. two analoge phones in two different gateways may take a path over some VoIP channels, causing an additional round-trip delay of about 100 ms that might need to be considered.

The VoIP channels in MGU2 are dynamic resources in MSP and the amount of available resources depends on the actual MSP load and the configuration of particular channel. The MSP load for a particular VoIP channel varies very much depending on choice of codec, packetization interval, VAD/CNG, echo canceler settings, crypto-suite, etc. For instance, use of VAD/CNG significantly reduce DSP load (and network bandwidth) and use of crypto-suite significantly increases load.

Furthermore, the selection of codec, packetization interval and crypto-suite also have great impact on the speech latency (especially packetization size). In general, latency sensitive installations should consider smaller packetization interval. Note that latency affects audio quality perception as well, especially when there is an echo situation.

Note: VoIP channels is also used for inter-GW media (links between Media Gateways) and that configuration means of these is not same as configuring e.g. SIP/H.323 endpoints.

3.4.1 RTP

The Media Stream Processor encodes the PCM audio data from TDM timeslots (from TDM switch) into packets to the streaming interfaces, and decodes packets from the streaming interfaces to output PCM TDM line.

The audio coding (codec) standard is used for both the encoder and the decoder.

MGU2 supports Voice Activity Detection (VAD) and Comfort Noise Generation for all supported codecs. The VAD function can be fine tuned for emphasis on bandwidth saving or audio quality. Too high bandwidth saving might cause audible audio artifacts as choppy speech.

The following codecs are supported by MGU:

- G.711 A- and µ-law, Appendix I (PLC) and II (VAD/CNG).

- G.729a with G.729 annex B (VAD/CNG).
- Clear Channel (bitwise exact transfer between TDM and IP, without echo canceler). Clear Channel is only intended for data or fax traffic. It shall never be used for voice, where echo canceling might be needed. Clear Channel uses dynamic payload type (PT in RTP header) as set by the MX-ONE Service Node from end-point negotiation.

Selection of codec, PLC, VAD/CNG can be made on a per call basis from the MX-ONE Service Node based on SIP/H.323 media negotiation.

MGU2 does not participate in any negotiation of media more than it reports its capabilites to the MX-ONE Service Node. It can be noted that use of VAD/CNG (“Silence Suppression”) may lower DSP load and thus increase channel density (and also lower network load). On the other hand VAD/CNG might affect voice quality, so the use is a trade-off between density and voice quality. Unless the higher density or bandwidth saving is required it is a recommendation to disable VAD/CNG for best voice quality.

The MGU2 also supports Modem & Fax Pass Through. At modem and fax tone detection on the TDM side the MGU2 automatically switch to Pass Through mode (if activated by the Service Node) using a predefined configuration which will set the RTP channel to G.711 codec and fixed jitter buffer, to be able to relay modem and fax data.

MGU2 allocates port numbers dynamically for RTP and RTCP from a port range that can be set by MX-ONE Service Node. RTCP port number is always RTP port + 1. When a new port number pair is allocated, always a pair with subsequent higher numbers is used. When highest configured port number is reached, the lowest is re-used again.

3.4.2 DTMF DETECTION AND RELAY IN RTP CHANNELS

Each RTP channel provides a DTMF detection and relay feature. In-band DTMF tones may be detected at incoming TDM side and may be relayed to packet side in one of three ways:

- Transparent, DTMF tones are passed as tone in the codec. This option is only useful when codec is G.711.
- As named telephone events (NTE) according to RFC 2833 / RFC 4733. In this mode in-band DTMF tones are removed from the TDM side and converted to events at the IP side (see also note below).
- Not relayed at all. Detected DTMF tones will be removed from the TDM side (see also note below).

The selection of detection and relay mode is made by MX-ONE Service Node based on e.g. SIP/H.323 negotiation with remote end-point/gateway or use-case. Note that DTMF detection can be enabled or disabled by MX-ONE Service Node, regardless of relay mode selected.

Note: When the RTP channel removes a DTMF tone there might be a leakage of less than 20 ms, i.e. may be audible but not detectable by any standard compliant DTMF receiver. By configuration it is possible to enable “complete removal” at the expense of longer channel latency (see section 4 Configuration on page 30). Complete removal is however only able to completely remove qualified DTMF digits.

3.4.3 SECURE RTP (SRTP)

See the SECURITY section below.

3.4.4 JITTER BUFFER

RTP packets sent over the IP network are subject to random variation in delays, out-of-sequence arrival, and a risk to be dropped. These artifacts decreases audio quality, and the jitter buffer is used to mitigate this. However, while the jitter buffer can improve audio quality it does this to the cost of increased voice delays. Long delays, especially in combination with echoes at far end (e.g. caused by 2 to 4 wire hybrids in analogue lines) makes echoes more noticeable and disturbing. Although it might be tried to minimize delays in echo situations (if not the source of the echo could be removed) it must be understood that affecting voice quality due to e.g. dropped packets might have negative impact on the echo canceler. See “Echo Canceler (EC)” on page 18..

In MGU2, the jitter buffer can be configured in adaptive or non-adaptive mode, and there are configuration parameters to adjust for actual network conditions.

Note: Configuration is per MGU2 and will affect all VoIP calls in that MGU2, including inter GW media over IP.

The configuration of the jitter buffer will be a trade off between audio quality and delays. By default, the jitter buffer in MGU2 is adaptive with settings for a fairly “normal” network, to preserve audio quality over minimizing delays. For a very delay sensitive installation, where audio quality could be negotiated and/or network is very good, re-configuration might be considered.

Although primarily the jitter buffer is for adapting to artifacts caused by network, also VoIP endpoints (phones, gateways, proxies, etc.) is part of the network and can cause these. For example, soft SIP clients with no dedicated HW (e.g. DSP) for VoIP media will have substantially more jitter in outgoing RTP packets than a HW dito. This can cause the jitter buffer to increase and thus to increase the delays even further. In those, and similar scenarios it might appear that the delay through MGU2 is longer than expected.

3.4.5 ECHO CANCELER (EC)

The Echo Canceler (EC) eliminates the possible echo of send signal from the return signal (see figure below). Echo is normally caused by reflections in transition from 2-to-4 wires, but also acoustic echo in telephones can occur. The EC is only used for calls over packet switched network (VoIP) as depicted in figure below.

There are various configurations of the EC which is described further on as well as in the See “Configuration” on page 30.

Note: Configuration is per MGU2 and will affect all VoIP calls in that MGU2, including inter-GW media over IP. Thus, the choice of EC settings might have to be a compromise.

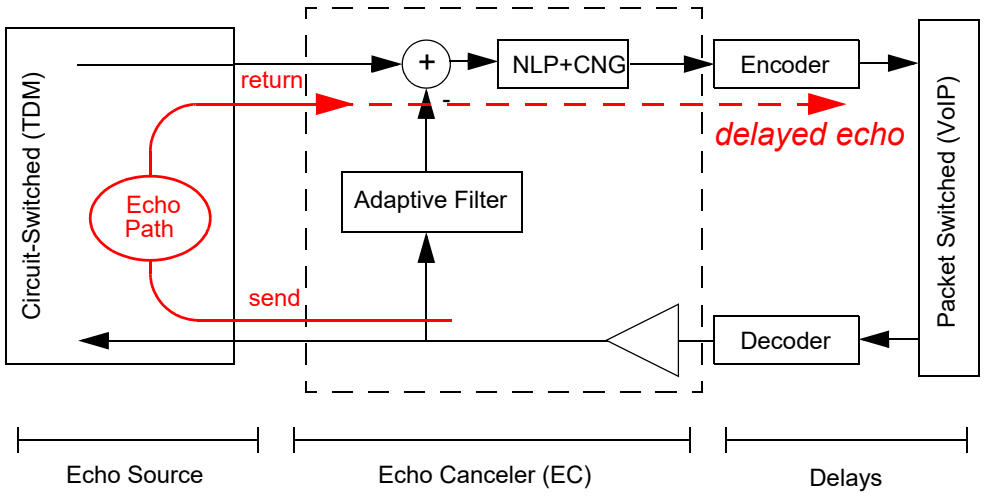


Figure 6: Schematic figure of Echo Canceler

The reason for using EC on VoIP calls is that echo in combination with (long) delays as caused by packet switched network is much more disturbing than echo when there is no or very little delay as can be expected in the circuit switched network (TDM).

The experience of how echo is perceived by the user on the packet side is a sum of echo source, echo canceler operation and packet network delays included delays in media gateways (encoding, decoding, jitter buffers), network (switches and routers) and endpoints (encoding, decoding, jitter buffers).

MGU2 supports two EC types for VoIP GW calls: Standard EC and Dual Filter EC (DFEC). EC type and settings very much impacts the MSP load.

Note: Changing EC type will cause a restart of the Media Control Application (MCA) and the MSP.

The EC also includes a Non-Linear Processor (NLP), a sub function that is capable of handling non-linear part of residual echo that the linear filter of the EC cannot cancel. By default, NLP is disabled and is only recommended to be enabled when needed.

When NLP is enabled and if engaged, it generates comfort noise (CNG) towards IP. CNG can also be changed to generate silence if CNG is not wanted.

3.4.5.1 Standard EC

The Standard EC echo tail length can be configured from 8 to 128 ms in 8ms steps, and the filter window is fixed to 24 ms. The advantage of the Sparse EC is MIPS savings which corresponds to higher channel density. The Standard EC can be improved by enabling Echo Path Change Detection (EPCD) that improves adaptation on filter window position.

Note: Setting EPCD will cause restart of Media Control Application.

3.4.5.2 Dual-Filter EC (DFEC)

The DFEC echo tail length can be configured from 8 to 128 ms in 8 ms steps. DFEC advantages:

- Avoids increased echo level caused by filter divergence during double-talk.
- Robust and fast detection of echo path changes.

The main disadvantage is that the DFE reduces DSP channel density, see further section 6 Capacity and Limitations on page 40.

3.4.5.3 Standards Compliance

- The Standard EC without Echo Path Change Detection (EPCD) enabled is compliant with G.168/2002
- The Standard EC with ECPD enabled is G.168/2004 compliant for single reflection with echo dispersion less than 24ms and echo tail span less than 128 ms.
- The DFEC is G.168/2004 compliant for echo span up to 128ms (highest complexity).

3.4.5.4 A few recommendations in case of echo problems

If disturbing echo is heard, the following actions can be recommended. (for information on parameters and settings, refer to See “Configuration” on page 30.):

1. Analyze the traffic scenario to make sure echo canceler is turned on. Of special interest is the media path where the transition IP to TDM takes place (for instance, the Media Gateway where the call is routed to/from public ISDN trunk). Check that ClearChannel (ClearMode) codec is not used in RTP which always have EC turned off.
2. Turn on the NLP (Non-Linear Processor, a sub-function of the EC). By default NLP is disabled. The NLP will be able to take care of non-linear residual echoes that the linear filter cannot.
3. Turn on the DFE (Dual-Filter EC). This is a more complex EC algorithm and significantly improves echo canceling. Note however that DFE has some impact on MGU2 capacity, as further described in section 6 Capacity and Limitations on page 40.
4. If echo canceling is improved after (re-)configuration, but comes back again, make sure the configuration that was made is persistent, i.e. parameters are marked “reload” in the MX-ONE Service Node and that proper data backup has been made.
5. Sometimes the echo delay path is longer than the echo canceler can handle (default is 64 ms, but can be changed up to 128 ms). The echo delay is the time from media (talker) is sent out on TDM and when it returns (attenuated) back to TDM. Usually, this is quite short, e.g. less than 10 ms but might be much longer in some situations. If the echo path is bigger than 64 ms but less than 128 ms the EC filter lengths may be adjusted. Note however that a longer filter length will have some impact on MGU2 capacity.

3.4.6 SSRC GENERATION, DETECTION AND COLLISION HANDLING

For the outgoing (audio) RTP stream in a VoIP call, MGU2 creates a random 32-bit SSRC (Synchronization Source) value. This value is used for all RTP packets in that stream throughout the stream is active. If a call is put on hold, or any setting of the actual RTP stream is changed (e.g. DTMF relay mode is changed) by the MX-ONE Service Node, the current stream is closed and replaced by a new. Hence, a new SSRC value is created for the new stream.

On corresponding incoming RTP stream, the MGU2 validates all received RTP packets. Packets with any SSRC value will be accepted as long as two packets with

consecutive numbers and same SSRC are received. This allow the sender to change the SSRC value for a RTP stream. However, if the SSRC value changes too often during a shorter time period (about 1 second), this is referred to as a “SSRC violation”, and will cause the used RTP port to be blocked for a while to avoid violating port to be re-used. This situation is usually caused by two or more interleaved RTP streams towards same RTP port. If this happens there is probably a RTP sender that has not properly closed its RTP stream. In situations where such violations are expected for a longer time, the “ssrc_violation_filter_time” can be increased (or disabled), see further section 4.4 System configuration files on page 36.

3.5 FAX RELAY T.38

The MGU2 supports ITU-T Recommendation T.38:

- Procedures for real-time Group 3 facsimile communication over IP Networks”,ITU –T, June, 1998.

When in fax mode, the MGU2 stops encoding and decoding samples from the line as voice. Instead it encodes and decodes fax events according to the selected fax coding scheme, and passes these event indications over the packet network.

T.38 channels are dynamic resources in MSP and the amount of available channels depends on actual load of MSP.

3.6 KEYCODE RECEIVER

Keycode Receiver (KR) provide in-band DTMF and MFC (R1 and R2) detection on TDM timeslots from the TDM switch. MGU2 supports connecting KR in serial or parallel to the PCM stream. Serial connection is usually only applicable to DTMF tones, when in-band detection is used, e.g. for mobile extension calls.

Connecting KR in serial makes it possible to remove (see note below) the DTMF tones from the PCM stream, but adds an extra latency of about 65 ms per default, which can cause echo problems in certain conditions. For DTMF tones it is possible to have alternative settings to lower latency to as low as 16 ms at the cost of DSP channel density.See section 4.2.4 Keycode Receivers & Senders on page 34.

Note: When KR removes a DTMF tone there might be a leakage of less than 20 ms, thus may be audible but not detectable by any standard compliant DTMF receiver. Currently, there is no way to enable “complete removal” for KR as it is for DTMF receiver in VoIP channels.

In parallel KR connection, virtually no additional latency is imposed by KR, but DTMF tones are passed through the PCM stream.

Selection of serial/parallel connection is controlled by MX-ONE Service Node when KR connection is ordered.

KR is a dynamic resource in the MSP and number of available resources depends on actual usage and load of the MSP.

The KR in MGU2 is normally used in Mobile Extension (ME) calls. Currently, serial connection is used to by default setup KR for ME calls, thus each ME user will have an extra delay of about 65 ms in their speaking path.

3.7 KEYCODE SENDER

The Keycode Senders (KS) provides in-band DTMF and MFC (R1 and R2) sending on TDM timeslots to the TDM switch. The duration (1-255 ms, or continuous) and attenuation (0-36dBm0) of the DTMF and MFC key codes is determined by the MX-ONE Service Node in the start of the KS resource and attenuation setting in the TDM switch.

KS is a dynamic resource in the MSP and number of available resources depends on actual usage and load of the MSP.

3.8 TONE SENDER

The Tone Senders (TS) provides in-band call progress tone generation on TDM timeslots to the TDM switch. Tone characteristics are defined in tone configuration files, one per supported market (see further section 4.3 Market files on page 36). Note however that attenuation level of a tone might be affected by the attenuation in the TDM switch connection established by MX-ONE Service Node.

TS is a dynamic resource in the MSP and number of available resources depends on actual usage and load of MSP.

There are however a few Tone senders that are permanently setup by the MX-ONE Service Node at start-up. These can be connected later at demand through sun-fan connections to several receivers.

3.9 RECORDED VOICE ANNOUNCEMENT

MGU2 provides locally stored Recorded Voice Announcements (RVA) to be played out on demand by a Media player channel in MSP on timeslots connected to TDM switch. The local storage area (i.e. the flash disk) on MGU2 allows about 60 minutes of media files, corresponding to about 30Mbyte, to be stored.

The supported media file format is WAVE audio, ITU-T G.711 A-law/µ-law, mono 8000 Hz. Normally, A-law is used on a A-law market, and µ-law is used on a µ-law market, but MGU2 allows the media files to be stored in any of these, independent of market.

The RVA Management function is located in Operation & Maintenance Application (OMA) subsystem. The function is responsible for the RVA Management interface to Service Node (SN) and to download files from a Web server. The RVA Management informs (Media Control Application) MCA when new RVA files have been downloaded and activated. The maximum file size (current default value is 30Mbyte) and maximum number of files (current default value is 250) that can be downloaded to the flash disk can be changed. After downloading to flash disk, MCA take care of downloading (activating) files into MSP external SRAM. The activation order is received from OMA after download to file system.

Note: Download and activation of RVA files is done by very low prioritized tasks in order to minimize impact on run-time traffic, thus might take various time to finalize depending on actual traffic load conditions.

Run-time handling of RVA messages (Media player sessions) are then handled by MCA on demand from MX-ONE Service Node.

The Media player channels are dynamically allocated from MSP by MX-ONE Service Node orders, and the maximum achievable density depends on the actual MSP load. One Media player load is roughly about twice the load of a G.711/20ms RTP channel.

Media files can be played out on one TDM timeslot or many using the TDM switch multi-cast function (sunfan). A media file can be played once or in repeat, as controlled by MX-ONE Service Node orders. At media file upgrade all running media player sessions will be terminated, informing MX-ONE Service Node by a play ended event. Sessions that are playing in repeat, need to be re-started by MX-ONE Service Node.

3.9.1 MEDIA STREAMING WITH MGU

MGU does not provide media streaming, but can receive plain RTP stream(s) from Media Servers to provide media streaming for legacy device boards.

Media streaming is used for MOH, MOW and RVA, thus media files is not required to install on MGUs when media streaming is enabled. Refer MEDIA STREAMING section in MX-ONE Media Server description for more information.

3.10 MULTI PARTY

The Multi Party resource (MP) is used in conference and intrusion calls. Up to 16 participants are allowed to be connected into same MP resource, but is limited by MX-ONE Service Node to 8 participants. All participants, VoIP or TDM side participants, are connected to the MP resource via the TDM switch.

The MP resource also contains a tone sender, providing conference/intrusion tone characteristics according to market specification (see further section 4.3 Market files on page 36) for the MP participants.

MP is a dynamic resource in the MSP and number of available resources depends on actual usage and load of the MSP.

3.11 IP NETWORK REDUNDANCY AND SECURITY

3.11.1 GENERAL

The MGU2 is supporting IPv4 and it is also supporting IPv6 in the MX-ONE 6.0 release or later versions. The IP version configuration combination can be IPv4 only or both versions IPv4 & IPv6.

The factory default configurations do not contain any IPv6 settings except for the IPv6 Local Link (LLC) address which will be set at boot up.

Note: This means that if you want to use security (encryption) you cannot use IPv6.

The control interface and the media interface parameter for IPv6 should be configured using MX-ONE Service Node's media gateway control and media gateway interface commands.
The NV parameter names for these interfaces are
eth0_ip6 (control interface) and
eth2_ip6 (media interface).

Note: The LLC address is only visible in the linux network configuration information and not visible in the MGU's NV parameter area.

The MGU2 also support 2 types of network redundancy.

- Switched (Ethernet) redundancy (Link Fail Over).
- Subnet (IP) redundancy

Note: Subnet redundancy is not supported in MX-ONE release 6.0 or later version.

The MGU2 also supports Server redundancy by allowing a standby server to take over the MGU2 from the ordinary server.

The MGU2 supports both media security (SRTP) and IP signaling security (IPsec).

3.11.2 SWITCHED REDUNDANCY (LINK FAIL OVER)

Link Fail Over (LFO) is handled by the MGU's internal switch. The Media Stream Processor's (MSP) and the Device Processor's (DP) Ethernet traffic will be switched towards one of the LAN ports (active LAN ports). At fail over the traffic will be redirected towards the redundant LAN port and the MGU2 will stay in that state until a new failure appears. However, there is a period of about 30 seconds after a link switch before link monitoring starts again.

LFO is activated when both LAN ports are connected.

Link switch will occur when a link suddenly disappears or if no control signaling messages are received and the default gateway is not reachable.

Note: At link switch, LAN1 port will inherit the PHY configuration from LAN0 port. It is not supported to have different PHY configuration on the LAN ports when LFO is used.

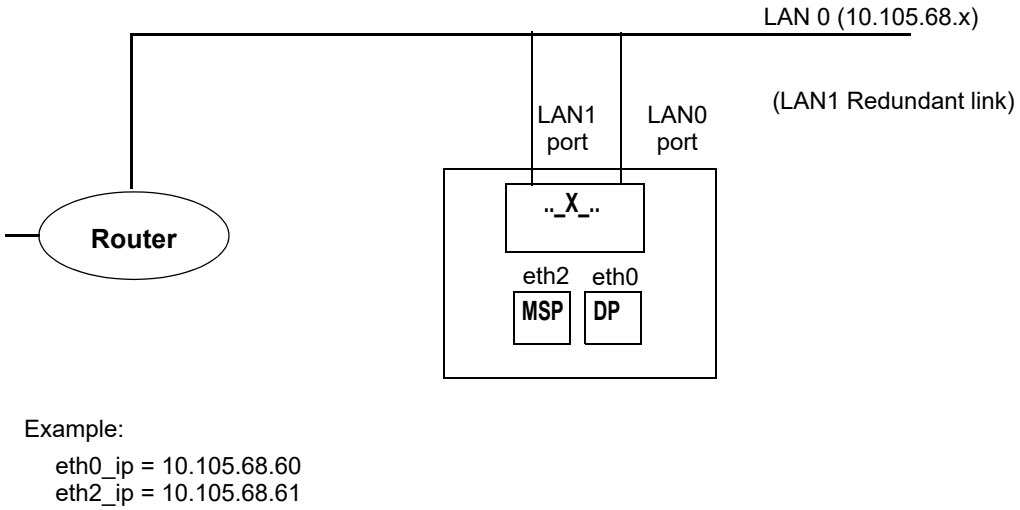
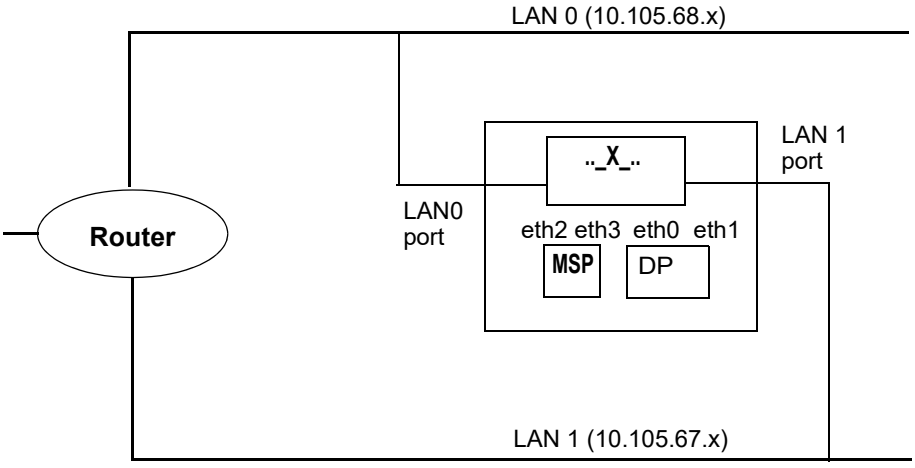


Figure 7: Switched redundancy

3.11.3 SUBNET REDUNDANCY (NETWORK REDUNDANCY)

Note: Subnet redundancy is not supported in MX-ONE release 6.0 or later version.

Network redundancy is handled by a supervision process on the MGU2. When the default gateway is not reachable on the present LAN the MGU2 will switch subnet and reconfigure the Media Stream Processor (MSP) with a new IP-address (ex: eth3-IP) specified by the configured MGU2 network parameters and the switch will stream the media packet towards redundant LAN (ex LAN1).



Example:

eth0_ip = 10.105.68.60
eth2_ip = 10.105.68.61
eth1_ip = 10.105.67.60
eth3_ip = 10.105.67.61

Figure 8: Subnet Redundancy.

3.11.4 SERVER REDUNDANCY

There is no specific built in support for server redundancy other than the MGU2 allows another (standby) server to take over the MGU2 when the connection to currently connected (ordinary) server is lost.

Only one server can control the MGU2 at the time, so the standby server will take over all MGU2 native resources as well as device boards in the MGU2 magazine. However, there is no support to synchronize between server and MGU2, thus when a standby server takes over, all MGU2 activities will have to be restarted by the server to take MGU2 and server to a common state (i.e. closing RTP sessions, reset TDM switch connections, and restart virtual ISDN boards and device boards).

During server downtime all media established before server fall out is kept to allow for call continuity during downtime, although, this will not guarantee that calls are not disconnected by a remote side. Note also that ALL calls will be disconnected when standby server comes up.

Note: MGU2 actually cannot distinguish between server failure and normal disconnection. Thus, MGU2 behavior is the same regardless of how disconnection from MGU2 is made.

3.11.5 PORT AUTHENTICATION USING 802.1X

IEEE 802.1X is an IEEE Standard for Port-based Network Access Control (PNAC).

It is part of the IEEE 802.1 group of networking protocols. It provides an authentication mechanism to devices wishing to attach to a LAN or WLAN.

802.1X authentication involves three parties: a supplicant, an authenticator, and an authentication server.

The supplicant, a client that provides credentials to the authenticator, is a client device that wishes to attach to the LAN/WAN. The authenticator is a network device, such as an Ethernet switch or wireless access point; and the authentication server is typically

a host running software supporting the RADIUS and EAP (Extensible Authentication Protocol) protocols. 802.1X uses EAP for message exchange during the authentication process. With EAP, an arbitrary authentication method, such as certificates, smart cards, or credentials, is used.

The most common EAP methods are EAP-TLS, EAP-TTLS and EAP-PEAP authentication.

- **EAP-TLS** is an IETF open standard, and is well-supported among wireless vendors. It offers a good deal of security. It uses PKI to secure communication to the RADIUS authentication server which provides very good security.
- **EAP-TTLS** It is widely supported across platforms, and offers good security, using PKI certificates only on the authentication server, with tunneled EAP or PAP/CHAP/ MSCHAP/ MSCHAPV2 authentication.
- **EAP-PEAP** is similar in design to EAP-TTLS, requiring only a server-side PKI certificate to create a secure TLS tunnel to protect user authentication, with tunneled EAP authentication.

With 802.1X port-based authentication, the supplicant provides credentials, such as user name/password or digital certificate, to the authenticator, and the authenticator forwards the credentials to the authentication server for verification. If the authentication server determines the credentials are valid, the supplicant (client device) is allowed to access resources located on the protected side of the network.

The Media Gateway supports 802.1x over wired LAN with EAP-TLS as the supported authentication method. The switch port to which the Media Gateway Unit is connected must be configured for 802.1X authentication of multiple hosts. That is, you must be able to connect multiple hosts to this single port for 802.1X authentication. When one client (MGU eth0 - signaling) is authenticated, all the other clients (MGU eth1 - media) are also authenticated for access to the LAN.

The picture below shows port access when the port is unauthorized (dashed line) and when the port is authorized.

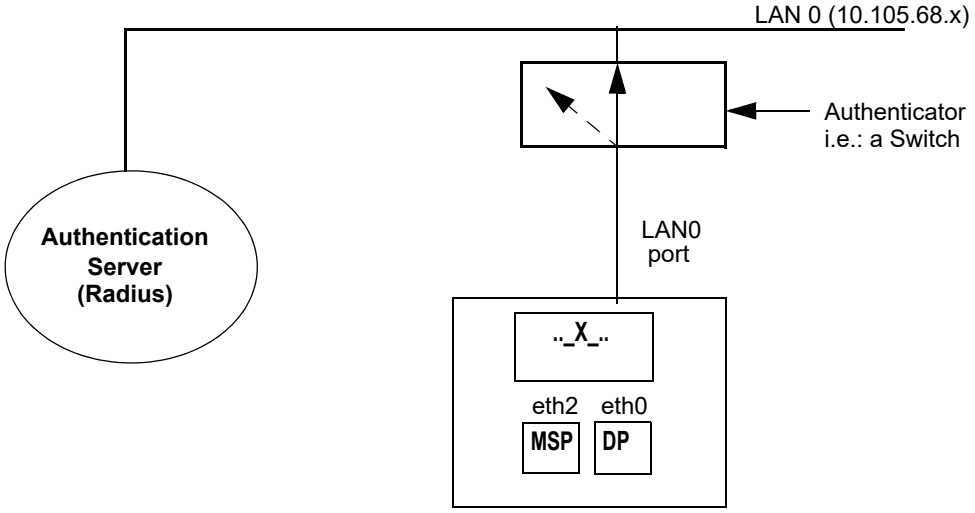


Figure 9: Port Authentication 802.1X

3.11.6 SECURITY

3.11.6.1 Media security - Secure RTP (SRTP)

MGU2 provides VoIP security according to the SRTP protocol (RFC 3711 and RFC 6188), using data flow encryption with AES in Counter Mode (CM) and authentication with HMAC-SHA1.

Data Flow Encryption

For encryption and decryption of the data flow, SRTP standardizes utilization of only a single cipher, Advanced Encryption Standard (AES), which can be used in two cipher mode: Integer Counter Mode (CM) or F8 Mode. Only CM is supported in MGU2.

Authentication

AES algorithm does not secure message integrity itself, to authenticate the message and protect its integrity, the keyed-Hash Message Authentication with Secure Hash Standard (HMAC-SHA1) algorithm is used

Key Derivation

In SRTP, the different keys used in a crypto context (SRTP encryption and salt keys, and SRTP authentication key) is derived from one single Master Key (per media direction). That is, from the master keys all the necessary session keys are generated by applying the key derivation function. MGU2 derives the Master key for the transmitted SRTP stream from a high entropy random source. The Master key for received SRTP stream (derived by remote end-point or gateway) is received from the MX-ONE Service Node. The master keys are derived only once before the call set up. Re-keying is thus not supported.

3.11.6.2 IP signaling security (IPsec)

MGU2 supports Internet Protocol Security (IPsec) that can be used to secure IP communication between MGU2 and a remote IPsec peer (a remote Service Node or Gateway/ Firewall). For example, IPsec may be used in a branch node scenario where Service Nodes are located in a head office and MGU2s in branch offices while signalling over the Internet. IPsec is supported for MGU2 signaling over IPv4 networks.

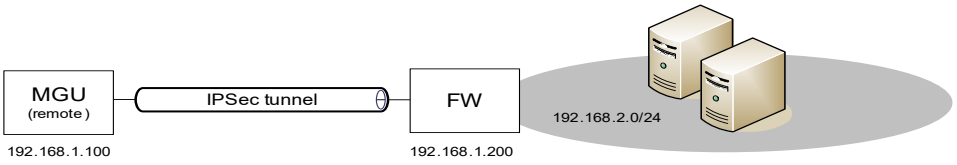


Figure 10:

The IPsec protocol suite is an open standard described in RFC 2401. IPsec is based on the following protocols:

- Authentication Header (AH) to provide connectionless integrity, data origin authentication, and an optional anti-replay service.
- Encapsulating Security Payload (ESP) to provide confidentiality (encryption), and limited traffic flow confidentiality. It also may provide connectionless integrity, data origin authentication, and an anti-replay service.

- Internet Key Exchange protocol (IKE) to provide automatic establishing of Security Associations (SA) and peer authentication. MGU2 supports IKE version 1 (IKEv1). IKE is only used in automatic key management procedures.

AH and ESP may be used in combination, but usually only one of them is used. When only ESP is used it is usually in combination with authentication. By default MGU2 enables ESP with authentication. Most importantly, ESP will protect the confidentiality of the SRTP keys exchanged between Service Node and MGU2 for secure RTP. For some installations it might make sense to only use AH.

IPsec may be used in tunnel (a.k.a VPN tunnel) or transport mode. In tunnel mode, the entire IP packet is protected by IPsec. This means IPsec wraps the original packet, encrypts it, adds a new IP header and sends it to the IPsec peer. In transport mode, only the IP payload is protected by IPsec. Tunnel mode is usually used between networks or host-to-networks, and transport mode is usually used end-to-end between two hosts. MGU2 creates a transport if a destination address is specified or a tunnel if destination network is specified.

MGU2 allows automatic IPsec SA establishment and peer authentication through IKE/ISAKMP using either pre-shared keys or RSA signed digital certificates. It is also possible to use manually configured SAs, but is usually not recommended.

It is possible to setup multiple IPsec tunnels/transports between MGU2 and remote peers.

For more information about how to setup IPsec, see Operational Directions *MGU SECURITY CONFIGURATION*.

3.12 VISUAL INDICATIONS

There are a few LEDs on the MGU2 front showing operational status of the board and interfaces. There is the main Status LED and additional LEDs on each Ethernet and E1/T1 port.

3.12.1 STATUS LED

The Status LED on MGU2 shows general operating status as follows:

- **Flashing red** - The board is in boot loader mode or an alarm is raised.
- **Steady red** - The board is not active.
- **Steady green** - The board is activated (connection with MX-ONE Service Node established on all three communication ports).
- **Flashing green** - The board is activated, and signaling packets (SCTP) are transmitted between MX-ONE Service Node and MGU2.

3.12.2 ETHERNET LEDS

- **Left LED** - Shows flashing green when ethernet packets are sent or received.
- **Right LED** - Shows steady green when in 1000Mbit mode
  and yellow when in 100 Mbit mode.
  The LED shows flashing green and yellow when the reset button is pressed.
  The green LED light will be set to fixed, when the reset button has been pressed for more than 5 seconds.

3.12.3 E1/T1 LEDS

- **Green LED** - Shows steady green when layer 1 is activated and there is incoming frame synch. Flashes when there is layer 2 activity, i.e. HDLC data frames are sent or received.
- **Yellow LED** - Shows steady yellow if the link is PCM syncronization source.

3.13 ALARM HANDLING

Each alarm type has a unique number and an alarm text which is sent in a status message to MX-ONE Service Node. Alarms are also logged in the MGU's syslog at ./var/log/syslog in MGU's file system

The alarm table below enumerates all alarms that can be generated from the MGU2 board, with their alarm number and severity. These alarms belongs to the Media GW alarm domain (5) in MX-ONE Service Node. When an alarm occurs, the front LED will change state red flashing.
If the alarm condition is cleared, the LED will go back to its previous (normal) state.

Table 2 Alarms. The Media Gateway alarms and Alarm encodings. All Media Gateway alarms belongs to "alarm domain" 5 in Telephony System.

Encoding *)		Alarm description	Severity
Code	Id		
9	9	Power Problem: -5V failure in backplane	Critical
9	10	Power Problem: +5V failure in backplane	Critical
9	11	Power Problem: -12V failure in backplane	Critical
9	12	Power Problem: +12V failure in backplane	Critical
13	13	Temperature Problem: MGU	Alert
18	18	Equipment Malfunction: External alarm A raised **)	Indetermined
19	19	Equipment Malfunction: External alarm B raised ***)	Indetermined
20	20	LAN Error Lost connection to LAN 0	Warning
20	21	LAN Error Lost connection to LAN 1	Warning
22	22	LAN Error: LAN0 Gateway unreachable	Warning
22	23	LAN Error: LAN1 Gateway unreachable	Warning
24	24	VLAN Error: VLANs with same GW MAC ADDR	Warning

*) In Telephony System's alarm log, only the alarm code (and domain) is logged (e.g. 5 and 22 for LAN Error). In MGU's syslog, only the alarm Id is logged, as for example: "AlarmSupervisor-raiseAlarm for id = 23 MO = MGW" indicating LAN1 Gateway unreachable.

**) The alarm definition (alarm code and alarm text) is configurable from MX-ONE Service Node to describe actual alarm source.

***) The alarm definition (alarm code and alarm text) is configurable from MX-ONE Service Node to describe actual alarm source.

4 CONFIGURATION

Most configuration of MGU2 is made through MX-ONE Service Node and/or MX-ONE Manager and sent to MGU2 via its communication interface.

For normal operation there is no need to change any of the settings described here. Changing these settings should only be made if advised by Mitel Service Technician.

Exception to this is the IP address for LAN0 which is required to setup at installation time.

Note: MGU2 generally don't validate configuration parameters, thus it is important to check that reasonable values are used

4.1 BOOT PARAMETERS

The boot parameters are mainly to boot the operating system and are stored in non-volatile memory on the board. Although these parameters can be changed both in boot loader mode and linux mode (i.e. the mode that will be entered after board has restarted), it shall never require to modify them from boot loader.

In linux mode the boot parameters can be changed through the Maintenance port (USB) using a serial (V.24) dongle at 9600 baud, no parity, 1 stop bit. Only serial dongles using the PL2303 device are supported. It can be noted that the USB port is not active in boot loader mode.

It is also possible to change parameters through SSH login (but obviously, the IP address need to be known then).

Note: The only settings required by end-user is the IP address and default router for LAN0, i.e. parameters def_route and eth0_ip (IPv4), and def_route6 and eth0_ip6 (IPv6). Other parameters are set indirectly through MX-ONE Service Node commands. Faulty settings or removing parameters might cause malfunction of the MGU2.

Note: There is no check that boot parameters are spelled correctly (a misspelled parameter will create a new parameter, not recognized by applications), thus check spelling if change doesn't take effect.

4.2 MARKET/SITE PARAMETERS (ATTRIBUTES)

The MGU's management application (OMA) maintains a set of configurable parameters in an internal (non-persistent) data base in the application. This data base is initially loaded with default and market specific values from MGU's file system (see also "4.3 Market files on page 36" below). The valid market is selected by MX-ONE Service Node command **mxone_maintenance**.

Each parameter can also be viewed and set with the **media_gateway_info** command from the MX-ONE Service Node to override the default or market settings.

Any time the data base is changed, OMA will push out changes to other MGU2 applications. In addition, if an application is restarted it will request settings from OMA. A restart of OMA (or MGU) will reload data base from files and cause MX-ONE Service Node to send all changed parameters again.

Below is a brief description of all parameters (grouped functional wise).

Note: Be aware of that some parameters will cause restart of MGU2 applications in order to take immediate effect. Thus, it is only recommended to change these during maintenance hours.

4.2.1 VOIP

Table 3 RTP parameters (RTP MO)

Name	Value range	Description
ComfortNoiseGeneration		Parameter is not used
JB_adaptionPeriod	1000..65535 ms	Controls the speed at which the jitter buffer can adapt downwards when current network conditions allow. Default is 10 s, which can be set lower for good networks.
JB_delayInit	0..200 ms	Initial delay of jitter buffer. Default is 0 ms.
JB_delayMax	0..200 ms	Controls maximum size of jitter buffer. Default is 200 ms. If “Hardmode” is selected this is the maximum size jitter buffer can grow. If “Softmode” then deletion occurs at “JB_deletionThreshold”.
JB_delayMin	0..200 ms	Controls minimum size of jitter buffer. Default is 0 ms.
JB_deletionMode	0..1 (boolean)	0=Softmode (audio quality focus, default) 1=Hardmode (delay focus)
JB.deletionThreshold	delayMax..500 ms	Packets exceeding deletionThreshold are deleted. Default is 500 ms.
PacketLossThreshold		Parameter is not used
VADTune	0..4	Controls VAD threshold to improve bandwidth (low value) or improve voice quality (high value). Too low value might give undesirable impact on voice quality. It is recommended to set at least 1 (default)
VLANTagValue	0..4095	VLAN ID for RTP packets (0 disables VLAN tagging)

Note: Setting delayMin = delayMax = delayInit makes jitter buffer non-adaptive

Table 4 VoIP channel DTMF detection parameters (TDM MO).

Name	Value range	Description
DTMF_CompleteRemoval	0..1 (boolean)	0 = Detected DTMF tones (valid DTMF digits) are removed, but can be audible 1 = Detected DTMF tones are removed totally (adds channel delay)
DTMF_MinToneOnTime	0..8191 ms	Min tone length to qualify as DTMF digit

Name	Value range	Description
DTMF_MinToneOffTime	0..8191 ms	Separation between digits
DTMF_MaxDropoutTime	0..8191 ms	Max tone dropout to qualify as one digit

Note: There are further DTMF parameters that can be set with AUXKR MO (see table 9, note 2).

Note: To meet the most industry standards, default settings minToneOn=30ms, minToneOff=35 and minDropoutTime should be used.

Table 5 VoIP channel Echo Canceller parameters (TDM MO).

Name	Value range	Description	EC type
EC_ECType	0..1	Selects Echo Canceller type: 0 = Standard Echo Canceller (STD) 1 = Dual-Filter Echo Canceller (DFE)	STD/DFE
EC_DFECFilterSize	8..128 ms (in steps of 8 ms)	Filter length for DFEC	DFE
EC_DFECMinErl		DFEC Minimum ERL setting (do not change)	DFE
EC_DFECAttenuation		DFEC Rx output digital gain (do not change)	DFE
EC_ECCrossCorrelationCalculation		Not used	-
EC_EchoPathChange	0..1 (boolean)	0 = Disable EPCD 1 = Enable EPCD	STD
EC_ErlChangeDetection		Not used	-
EC_FastConvergenceControl	0..1 (boolean)	Accelerates filter convergence for long filters	STD
EC_ECWindowSize	24 ms	EC window size for Standard EC	STD
EC_NLPControl	0..1 (boolean)	0 = Disble NLP 1 = Enable NLP	STD/DFE
EC_NLPTune	0..2	Not used.	STD
EC_ECTailLength	8..128ms (in steps of 8 ms)	Filter length for STD EC	STD
EC_EchoCancellerEnable		No used	.
EC_CNGEnable	0..1 (boolean)		STD/DFE
SilenceToPCMInterface	0..1 (boolean)	Not used (parameter is controlled indirectly by CNG settings)	-

Note: The column “EC type” tells for which EC type the parameter is valid.

Note: Changing EC parameters from default values might lower VoIP channel and other DSP resource densities

4.2.2 DIGITAL TRUNKS

Table 6 ISDN parameters, common to all trunks (ISDN MO) (Activation of TX Slipbuffer can be done on each indivdual trunk).

Name	Value range	Description
Freebits	0..127	Default = 127
CRC_Threshold		Not used
N2x4		Not used
K	0..127	
N200	1..10	Default = 3
N201	260	Do not change
T200	1000..2000 ms	Default 1000 ms
T203	5000..20000 ms	Default 10000 ms
TX_Slipbuffer	0-15	Activation of TX elastic buffer. Default 0 = Off for all PRI:s. The parameter is bit oriented, see table 7 below.

Table 7 Tx_Slipbuffer

Binary value	Decimal value	PRI to enable Tx elastic buffer
0001	1	PRI 0
0010	2	PRI 1
0100	4	PRI 2
1000	8	PRI 3
1010	10	PRI 1 & PRI 3
1111	15	PRI 0 to 3 (all)

Note: There are also configuration parameters per PRI/trunk that are set in run-time from MX-ONE Service Node.
Physical interface = E1 or T1.
User Network = User or network side.

Note: Changing the value for the Tx_Slipbuffer parameter requires the corresponding “virtual board” (PRI interface) to be restarted in order to take effect.

Note: Activation of Tx_Slipbuffer on PRI shall not be used when the PRI provides synchronization to a remote system.

4.2.3 TONE SENDERS

Table 8 Tone Sender parameters (AUXTS MO)

Name	Value range	Description
N/A	N/A	N/A

4.2.4 KEYCODE RECEIVERS & SENDERS

Table 9 Keycode Receiver parameters (AUXKR MO).

Name	Value range	Description
AntiTapDetection		Do not change
DetectionDelay (see note 2)	18/30/40 ms	Specifies the minimum on time of DTMF signals to be detected as valid digits.
DtmfRemovalLevel	0..2	Not Used
EarlyDetection		Not Used
FrequencyDeviation (see note 2)	15..25 (1.5-2.5%)	Frequency deviation of DTMF tone pair
MaxAntiTapToneDropoutTime		Do not change
MaxDropoutTime	0..8191 ms	Max tone dropout to qualify as one digit
MaxToneDropoutTime		Do not change
MinAntiTapToneOffTime		Do not change
MinAntiTapToneOnTime		Do not change
MinLevelThreshold (see note 2)	140-480 (-14 to -48dBmo)	Min threshold level for DTMF frequency components
MinToneOffTime	0..8191 ms	Min tone off length to qualify as digit
MinToneOnTime	0..8191 ms	Min tone length to qualify as DTMF digit
NegativeTwist (see note)	10..160 (1-16dB)	Negative Twist
PacketSize	5,10,20,30,40,50,60 ms	Changes channel latency for DTMF receiver at the expense of channel density (30 ms is default).
PositiveTwist (see note 2)	10..160 (1-16dB)	Positive Twist
SnrThreshold (see note 2)	-30..60 (-3 to 6dB)	Signal to Noise ratio. 16 bit value. Negative values are specified as sign bit + value, e.g. 32768 + 30 = -3.0 dB.
ZeroInterDigitDetection		Do not change

Note: 1) To meet the most industry standards, default settings should be used.
2) These parameters are also applicable to DTMF receivers in VoIP channels

Table 10 Tone Sender parameters (AUXTS MO)

Name	Value range	Description
N/A	N/A	N/A

4.2.5 MULTI PARTY (CONFERENCE BRIDGE)

Table 11 Multi Party (Conference) parameters (AUXMP MO).

Name	Value range	Description
AGCEnablePCMtoMixer	0 = Disable AGC 1 = Enable AGC	Automatic Gain Control. Not Supported.
AGCPCMtoMixerMaxGain		Not Used.
AGCPCMtoMixerMinGain		Not Used.
AGCPCMtoMixerRate		Not Used
AGCPCMtoMixerTargetLevel		Not Used.
HighAttenuation	0 .. 14 dB	Attenuation applied to participants when number of participants in a conference is above “ParticipantThreshold” (default 6dB).
LowAttenuation	0 .. 14 dB	Attenuation applied to participants when number of participants in a conference is below or equal to “ParticipantThreshold” (default 3dB)
ParticipantThreshold	3 .. 15	Determines the number of participants in a conference when low or high attenuation shall be applied (default 4)

4.2.6 RECORDED VOICE ANNOUNCEMENTS

Table 12 Voice Sender parameters (AUXVS MO)

Name	Value range	Description
N/A	N/A	N/A

4.2.7 QUALITY OF SERVICE (QOS)

Table 13 Quality Of Service parameters (QOS MO)

Name	Value range	Description
TypeOfServiceForMedia	bit mapped (decimal value)	The ToS field in the IP header for RTP packets. Default value is 184 (decimal). Refer also to RFC 2474.

Name	Value range	Description
TypeOfServiceForControl	bit mapped (decimal value)	The ToS field in the IP header for control signaling between MX-ONE Service Node and MGU2 services. Default value is 152 (decimal). Refer also to RFC 2474. NOTE: Changing this parameter causes restart of MGU2 services.

4.3 MARKET FILES

The /etc/mgw/markets directory on MGU2 contains files with default configuration settings and call progress tone characteristics for all supported markets. There is one common file with default settings for all markets and one file per unique market where differences compared to the default settings is stored. At MGU2 startup, the default file is read into an internal data base, and when MX-ONE Service Node orders MGU2 to select market, the corresponding market file and tone characteristics file is loaded, updating the data base.

Note: Some parameters in the market files might require or cause restart of MGU2 applications if different from default file, but normally market is not changed in run-time.

Note: Market settings changed by the MX-ONE Service Node command “media_gateway_info” only updates the internal data base rather than writing changes to the market files.

4.4 SYSTEM CONFIGURATION FILES

In the /etc/mgw/system directory are stored some MGU2 system configuration files, *.conf. These contains settings for the MGU2 SW applications, which are read and used when the applications starts or re-starts. Thus, if any setting is changed, then the applications need to be restarted for the new setting to take effect.

Note: Some settings are overwritten by the applications in run-time. Installing a new RPM will also overwrite the previous file.

For more information about these settings, see comments in respectively file.

5 MGU2 SOFTWARE

This chapter describes the MGU2 software to get a brief understanding of the main applications and where different functions are handled in the SW.

5.1 GENERAL

The software consists of the following parts:

- Boot loader.
- Linux operating system and root file system stored on-board in local (NAND) flash file system.
- Media Gateway applications. There are three server applications on MGU2, each using SCTP protocol and a well-known port that an external MX-ONE Service Node may connect to and communicate with application through. These applications are named “Device Board Server” (eridbs), “Media Control Application” (erimca) and “Operation & Maintenance Application” (erioma) using SCTP ports 2816, 2818 and 2817, respectively.
- Media Gateway commands. Not for normal usage. There are commands mainly for manufacturing and development purposes, but also a few possible to use for fault isolation. These are further documented in the mgw man-page (e.g. enter “man mgw” when logged in on MGU).

5.2 INSTALLATION AND UPGRADE

MGU2 utilises RPM package manager for SW and FW installation/upgrade. There is only one RPM for the whole MGU2 installation which contains all previously mentioned SW and also MSP and FPGA FW (FirmWare) images.

The MGU2 RPM is named **mgw-X.Y.Z-1.ppc.rpm**, where stepping X means “a new generation SW”, Y means “functional extension” and Z means “fault correction”.

MGU2 provides support for downloading the RPM from a SW server using HTTP protocol. Installation is normally ordered by MX-ONE Service Node through O&M signaling port, but can be done with MGU2 upgrade or linux rpm commands as well.

Installation of the RPM might involve reboot of MGU2, e.g. if boot loader or linux has been changed.

5.3 BOOT LOADER

The boot loader is the bootstrapping process that starts operating systems (Linux) on the MGU2.
It handles:

- Basic initialization of the MGU2 board.
- Chip Select setup.
- SDRAM configuration.
- Linux boot.

The boot loader have also a Programmable Built-In Self-Test (PBIST) support.

The bootloader also share configuration data with the OS (Linux) which resides on a NOR-flash memory.

The flash contains:

- Boot configuration parameters.
- Manufacturer data (MAC addresses, serial number etc).
- Product information (ROF, index numbers and revision information).
- Configuration data (IP-network and linux configuration data)

Printout sample from nor flash:

```
DISP *ROF_num = ROF 137 6304/1

DISP *ROF_rev = R1A
DISP *ROF_ser = T01D896676
DISP *eth0_mac = 00:13:5E:F0:AD:C3
DISP *eth1_mac = 00:13:5E:F0:AD:C2
DISP *eth2_mac = 00:13:5E:F0:AD:F4
DISP *eth3_mac = 00:13:5E:F0:AD:F5
DISP  nfsroot = /mgu_root
DISP  lilo_arg = root=/dev/mtdblock1 rw rootfstype=yaffs noatime
DISP  autoupdate = no
DISP  eth0_ip = 10.105.68.57/24
DISP  autoboot = yes
DISP  nfsboot = no
DISP  phy0_mode = AUTO
DISP  lan_active = LAN0
DISP  lan_primary = LAN0
DISP  eth2_ip = 10.105.68.58/24
DISP  phy1_mode = AUTO
DISP  eth1_ip = 10.10.1.2/24
DISP  def_route = 10.105.68.1
DISP  def_route1 = 10.10.1.1
DISP  eth3_ip = 10.10.1.3/24
```

5.4 OPERATING SYSTEM AND ROOT FILE SYSTEM

The operating system and root file system is based on Wind River® Linux version 1.4.

5.5 DEVICE BOARD SERVER

The device board server (DBS) subsystem in MGU2 hosts the ISDN signaling and Device Board interface functions.

The message passing on Service Node (SN) interface is carried out using Stream Control Transmission Protocol (SCTP) on port 2816.

SCTP has many features but mainly message integrity and safe data delivery is currently in use.

The messages from the SN use configured multiple number identities (in the message header) to address the functions.

The ISDN and Device Board functions are described in other parts of this document.

5.6 MEDIA CONTROL APPLICATION

The Media Control Application (MCA) is a service on the MGU which main function is to provide control of media related functions for MX-ONE Service Node on SCTP port 2818.
In short, these functions include:

- Creating and managing VoIP (Voice media) and FoIP (T38).
- Creating and managing secure VoIP streams, using SRTP/SRTCP.
- Controlling auxiliary functions like DTMF signal detection and playing recorded voice announcements.
- Quality of Service (RTCP/RTCP-XR, VLAN and Diffserv).

5.7 OPERATION & MAINTENANCE APPLICATION

The Operation and Maintenance Application (OMA) is a service on MGU2 that provides an interface for MX-ONE Service Node on SCTP port 2817 for the following functions:

- Selection of market and time zone.
- Setting and retrieving run-time parameters.
- Alarm configuration and reporting.
- Inventory information (SW, FW and HW revisions).
- Network configuration.
- Installation & Upgrade of SW and FW.
- Installation of Recorded Voice Announcements.
- Selection of TDM synchronization source.
- Common restart functions, such as MGU2 restart, reboot and shutdown.

6 CAPACITY AND LIMITATIONS

6.1 DEVICE BOARD INTERFACE

Table 14 Capacity and limitations in Device Board Interface

Signaling Protocols	2 Mbit HDLC (long signal format, i.e. up to 300 bytes payload) 128 Kbit UART short format 128 Kbit UART long format UART protocol with slow signaling is not supported

6.2 DIGITAL TRUNK INTERFACE

Table 15 Capacity and limitations in Digital Trunk Interface

Number of PRIs	4 ISDN PRI:s. Each 30B+D or 23B+D

6.3 FAX RELAY T.38

Table 16 Fax support and settings. Note that settings are fixed and are not configurable.

Max T.38 sessions	128 simultaneous sessions if only running T.38 sessions in MSP.
Supported fax signals.	V.21, V.25 and V.8 (Preamble/flags, CED, Ans and ANSam)

Table 17 T.38 Fax Configuration data used in MGU2.

TCF Procedure:	Remote TCF, the TCF data is passed across the IP network in the same way as any other page data.
Redundancy:	Allow ECM faxes in T.38.
No maximal speed limit negotiated:	No speed limit.
Redundancy count for T30 messages:	Total 7 counts.
Redundancy Count Page Data	Total 7 counts.
ECM faxes in T38:	ECM Allow.
T.38 Packet loss concealment:	No T.38 Packet loss concealment
Small ECM packet handling:	Enable small T4 ECM packet instead of waiting for complete HDLC ECM frame.

6.4 KEYCODE RECEIVER

Table 18 KR resources

KR latency	In serial connection KR adds a delay of about 65 ms per default, but can be tuned down to about 18 ms at the cost of performance (see below). In parallel connection KR adds no delay.
Max KR resources	160 simultaneous KR if DetectionDelay = 40 ms, and only running KR resources in MSP 114 simultaneous KR if DetectionDelay = 18 ms, and only running KR resources in MSP
Start KR session	Less than 15 ms
Stop KR session	Less than 10 ms

6.5 KEYCODE SENDER

Table 19 KS resources

Max KS resources	160 simultaneous KS
DTMF/MFC duration	1-255 ms, or continuous (=0)
DTMF/MFC level	0 to -36dBm0

6.6 TONE SENDER

Table 20 TS resources

Max TS resources	160 simultaneous TS.

6.7 RECORDED VOICE ANNOUNCEMENT

Table 21 Recorded Voice Announcement

RVA download time (unloaded MGU)	This time is dependent not only on MGU2 load, but also on network and web-server conditions.
RVA activation time (unloaded MGU)	To activate media files takes about 12s/Mbyte before they are active and can be used. For a maximum file size installation, installation time is about 6-7 minutes. During activation, RVA feature is disabled (RVA sessions will be rejected by MGU).
Max RVA sessions	160 simultaneous sessions if only running RVA in MSP
Supported file formats	- RIFF (little-endian) data, WAV audio, ITU-T G.711 A-law, mono 8000 Hz - RIFF (little-endian) data, WAV audio, ITU-T G.711 µ-law, mono 8000 Hz
Max number of RVA files	250
Max file size	60 minutes (approximately 30Mbyte)

Start RVA session	To allocate and start a media player (RVA) session takes less than 50 ms
Stop RVA session	To stop a media player session takes less than 50 ms

6.8 MULTI PARTY

Table 22 MP resources

Max MP resources	64 simultaneous MP resources
Max participants per MP resource	16 (Note: The MX-ONE Service Node limits the number of participants to 8)

6.9 VOICE OVER IP

Note: Only symmetric Voice traffic are supported. Receiving and sending channel must use the same type of codec and packetization interval.

Table 23 Supported codecs and packetization intervals

Codec	Packetization intervals
G.711 a-law/μ-law	5, 10, 20, 30, 40, 50 and 60 [ms]
G.729a	10, 20, 30, 40, 50, 60, 70 and 80 [ms]
G.729ab	10, 20, 30, 40, 50, 60, 70 and 80 [ms]
Clear channel	5, 10, 20, 30, 40, 50 and 60 [ms]

RTP/RTCP port range	Configurable from MX-ONE Service Node. Default range if not set is 50000..57768
Crypto Suites (SRTP)	The following encryption / authentication combos are supported: 1) AES-128 / HMAC-SHA1-80 2) AES-128 / HMAC-SHA1-32 3) AES-128 4) AES-192 / HMAC-SHA1-80 5) AES-192 / HMAC-SHA1-32 6) AES-256 / HMAC-SHA1-80 7) AES-256 / HMAC-SHA1-32
Fax PassThrough	Switching on detection of CNG, CED ,V.21 flags, ANSam ANS/, COT V8bis, V22 and Bell 103 tones.
Max RTP sessions	Up to 142 sessions if only RTP is running in MSP, but depends heavily on settings and speech characteristics. **Note:** With “clear channel” max RTP sessions could be up to 160, but lower with other codecs. See table 24 below for a few examples.
Time to establish new RTP session	To allocate and start a new RTP session takes less than 30 ms
Time to close RTP session	To stop and free RTP session takes less than 20 ms

Table 24 Max RTP sessions for various settings
STD = Standard EC with default settings, DFE = Dual Filter EC with default settings (EC type and settings is configurable through TDM MO).

Codec	Echo Canceller	Crypto suite (see table 23)	Packetization Interval		
			10 ms	20 ms	30 ms
G.711	STD	-	100	126	142
G.711	DFE	-	78	98	111
G.711	STD	6	62	94	110
G.711	DFE	6	58	74	82
G.729ab	STD	-	44	60	64
G.729ab	DFE	-	43	48	50
G.729ab	STD	6	48	56	60
G.729ab	DFE	6	40	46	48

Note: In density figures above it has not been included the effect of using “Silence Suppression”, which when enabled might lower DSP load and thus increasing channel density.

In table below, the latency on VoIP channels is stated for different codecs and packetization intervals. Latency includes the path from TDM to VoIP encoding to packet network to decoding to TDM, i.e. GW to GW VoIP delay. Latency has been measured with fixed jitter buffer of same size as packetization interval. These are minimum latencies to be expected in GW to GW calls, and external packet network and endpoints might increase latency. Also use of encryption increases latency slightly.

Table 25 End to End VoIP delays with fixed jitter buffer equals packetization interval

Codec	Packetization Interval			
	5 ms	10 ms	20 ms	30 ms
G.711	25	35	45	Not measured
G.729ab	N/A	58	58	Not measured

6.10 IPSEC STANDARDS

Table 26 IPsec

Protocols	IKEv1, AH, ESP, IP Compression
CBC ciphers	AES-128 (default), AES-256, DES, 3DES, Blowfish, Twofish, Serpent
Digests	SHA1 (default), SHA2 (SHA-256, SHA-384, SHA-512), MD5
Diffie Hellman groups	1, 2 (default), 5
IP Compression	Deflate

6.11 NETWORK REDUNDANCY

Table 27 Network Redundancy fail over-time

Fail over time (Subnet Redundancy)	Fail over time will be approximately 8 seconds
Fail over time (Switched redundancy)	Fail over time is about 1 second when the active link fails. Fail over occurs also if the subnet's gateway is not reachable and no control traffic packets are received on the LAN port. The fail over time in these case will be approximately 8 seconds.

6.12 FACTORY DEFAULT PARAMETERS

Table 28 Factory default parameters

Parameter	Value
eth0_ip	192.168.1.2/24
eth1_ip	192.168.2.2/24
eth2_ip	192.168.1.3/24
eth3_ip	192.168.2.3/24
default_route	192.168.1.1
default_route1	192.168.2.1