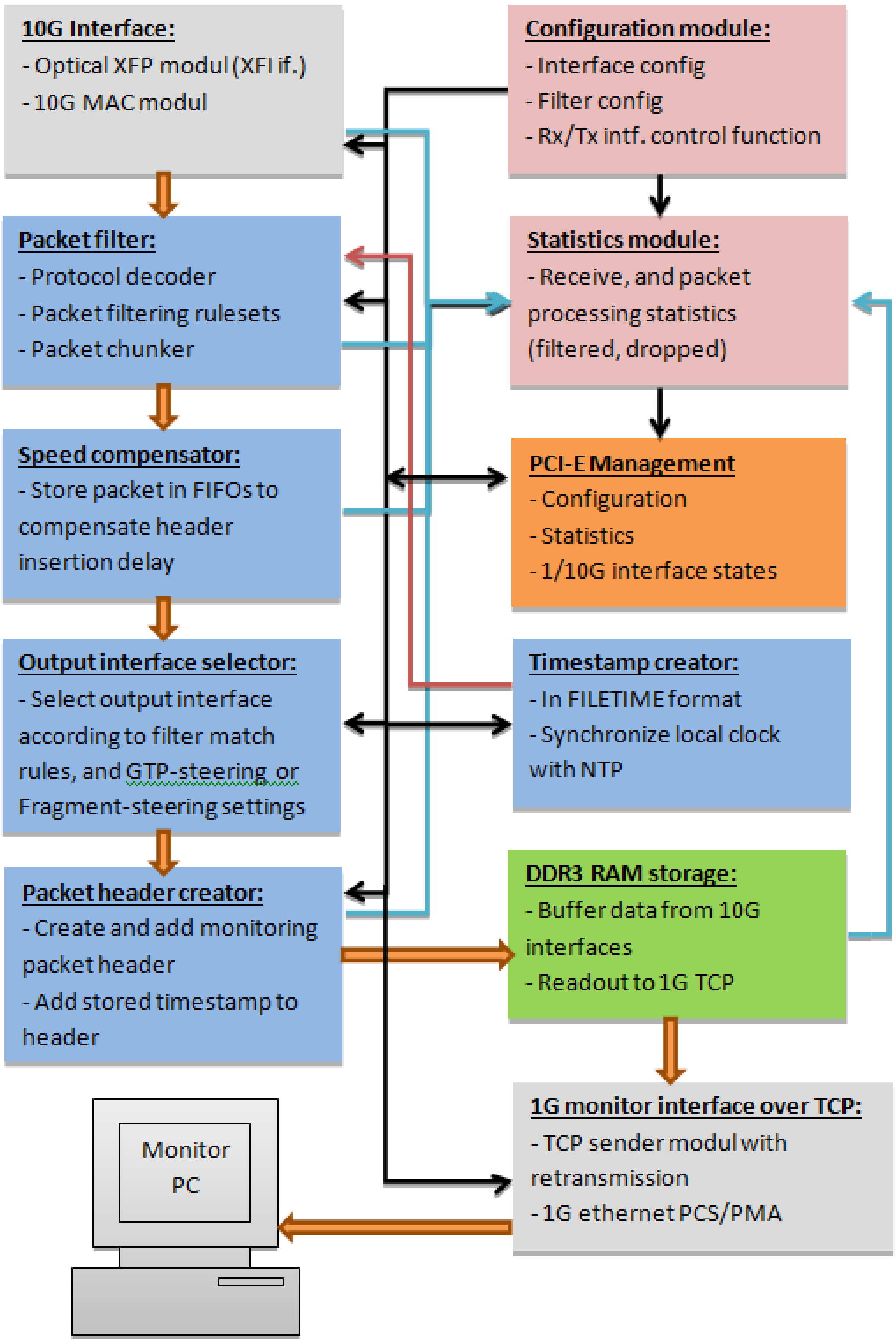
AITIA

C-GEP 20 10 Gb/s Monitoring application

1. C-GEP 20 operational block diagram

1.1. Packet processing path



10G Interface:
- Optical XFP modul (XFI if.)
- 10G MAC modul

Packet filter:
- Protocol decoder
- Packet filtering rulesets
- Packet chunker

Speed compensator:
- Store packet in FIFOs to compensate header insertion delay

Output interface selector:
- Select output interface according to filter match rules, and GTP-steering or Fragment-steering settings

Packet header creator:
- Create and add monitoring packet header
- Add stored timestamp to header

Monitor PC

Configuration module:
- Interface config
- Filter config
- Rx/Tx intf. control function

Statistics module:
- Receive, and packet processing statistics (filtered, dropped)

PCI-E Management
- Configuration
- Statistics
- 1/10G interface states

Timestamp creator:
- In FILETIME format
- Synchronize local clock with NTP

DDR3 RAM storage:
- Buffer data from 10G interfaces
- Readout to 1G TCP

1G monitor interface over TCP:
- TCP sender modul with retransmission
- 1G ethernet PCS/PMA

1.1.1. Fig – Packet processing module hierarchy

The incoming packets are processed in a pipelined architecture during packet processing. This means, that the modules are serially connected one after another, the output of the previous module is the input for the next module in the chain. This architecture results in constant packet processing delay.

Constant delay is not applicable for the following modules:

- Packet header creator module (an overhead is added to every packet)
- DDR3 RAM storage module (variable delay for DDR3 read/write access)
- TCP output module (depends on the far end receivers processing speed)

The main reason for variable delay are the FIFO-s used for temporaly storage, and shared network resources.

Figure 3.1.1 shows a simplified module hierarchy. Besides packet processor modules management, and statistics functions are shown too. Arrows show the direction of the internal data bus system.

Colored paths:

- Orange: monitored data flow
- Black: communication, control
- Blue: statistics
- Red: timestamp

The next chapters give a functional description from every module in the datapath.

1.1.2. *10G interface module*

The CGEP-20 has 2 optical XFP cages. The XFP modules have an XFI electrical host interface (2x1 wires at 10.3125 GHz, 64b/66b coding), the FPGA connects directly to this interface.

The MAC module is responsible for detecting the ethernet frames, removes the preamble, and aligns the received data on the first byte of the internal 64 bit bus. It also verifies the CRC32 checksum of the received ethernet frame.

There is no data throttling at this point, everything passes through with a constant delay, therefore frame loss can not occur here, the framesize has to be in the range specified by the 802.3 standard.

1.1.3. *Packet Filter module*

The packet filter module contains many processing submodules determined by the application type. Basic submodules are the „Protocol Decoder", „Packet Filtering" and „Packet Chunker".

Also timestamping of the processed frames is handled on this level, the high precision timestamp is ensured by the „Timestamp Creator" submodule using NTP protocol. From this point the timestamp travels parallel with the monitor data to the „Packet Header Creator".

The „Protocol Decoder" is responsible for determining the packet header structure, and reading out the protocol specific fields relevant for packet processing.

The following protocol fields are supported:

- 802.1Q VLAN
- IPv4 Addresses
- L3+ protocols:
    - MPLS (2 levels)
    - VLAN
    - UDP/TCP
    - GTP-U

The „Packet Filtering" submodule fits the filtering rules on the incoming packets, and determines the additional processing needed depending on the filtering decision. The rules are ordered in hierarchy, that means, that the one on top has the highest priority. After the first matching rule is found, subsequent rules are ignored.

Filter rule setup:

- *Traffic distribution* (From - To)
    - The C-GEP 20 monitoring firmware distributes matching packets evenly between the specified interfaces.
- *LinkID*

  - This field appears in the monitoring header as additional data.
- *Catch All* option
  - All incoming frames match the filter if enabled.
- *Filter Mode*
  - What to do with the matching packet:
    - Pass: packet is passed to the next processing module.
    - Drop: the packet is dropped.
- *Filter rule*
  - Normal mode: Source and Destination IP Address filtering
  - Swapping mode: Filter for Source and Destination IP Address match and for the transposed matches too (received Src = filter Dst, received Dst = filter Src)
- *VLAN ID* (From - To)
  - Filter for VLAN TAG value range. The packet has to contain a valid VLAN header, and the TAG value must be in the range specified by the From – To parameters.
- *Source IP* (From - To)
  - Filter for Source IP Address range. The packet has to cointain a valid IP header, and the Source/(* or Destination) Address must be in the range specified by the From – To parameters. (*filter rule swapping)
- *Destination IP* (From - To)
  - Filter for Destination IP Address range. The packet has to cointain a valid IP header, and the Destination/(* or Source) Address must be in the range specified by the From – To parameters. (*filter rule swapping)
- *IP Protocol*
  - Filter for the protocol field of the IP header. Can be specified by the byte code of the protocol, or selectable for TCP and UDP protocols.

- *Source Port*
  - Filter for the UDP/TCP source port value. The packet has to contain a valid UDP or TCP header, and the source port must equal to the one specified.
- *Destination Port*

    - Filter for the UDP/TCP destination port value. The packet has to contain a valid UDP or TCP header, and the destination port must equal to the one specified.
- *Truncate*
    - You can specify how many bytes to save from every incoming frame. This means that the maximum of this many bytes are captured, if the frame is shorter, then this setting has no effect. This option is important to conserver monitoring and processing bandwidth as only the useful information is forwarded. Packet truncate falls always on a 8 byte boundary. (If the value specified can not be divided by 8 without a remainder, then it will be rounded up).

If the packet passes the filtering rule then we pass it on to the next processing unit.

1.1.4. *Speed compensator module*

The output of the „Packet Filter" module is connected to the „Speed compensator". The filtered packets are tagged with an extension (monitoring) header. The „Speed compensator" has to ensure that data is buffered for the additional delay introduced by the „Packet Header Creator" modules header insertion function.

Warning! Packet loss may occur if the total bandwidth of the original data, and the added monitoring header exceeds 10 Gbps!

1.1.5. *Output Interface selector/steering module*

Specifies the output interface according to the matching rule, or distributes traffic evenly across the specified output interfaces.

Steering function:

- GTP-U steering:
  - Identified GTP-U traffic is distributed across the specified outputs. Packets belonging to the same flow are always forwarded to the same output interface.
  - Distribution is done by a lookup table, and calculated hash values derived from the following fields:
    - GTP-U TEID value
    - contained IPv4 Source Address
    - contained IPv4 Destination Address
    - contained IPv4 Protocol ID
- Fragment steering:
  - Identified framgmented IP traffic is distributed across the specified outputs. Packets belonging to the same flow are always forwarded to the same output interface.
  - Distribution is done by a lookup table, and calculated hash values derived from the following fields:
    - IPv4 Source Address
    - IPv4 Destination Address
    - IPv4 Fragment ID
    - IPv4 Protocol ID

1.1.6. *Packet header creator module*

The „Packet header creator” module adds a monitoring header to the packets passing the filter module. This header is inserted before the ethernet header, and contains information needed for further software analysis. Assembled packets are written into FIFOs. The queue readout depends on the 1 Gb/s output interfaces TCP throughput.

The „Packet header creator” module controls the packet assembly by communicating with the „Speed compensator” module. **If the incoming and**

filtered packet stream has a higher throughput than the 1 Gb/s output interface, then packet loss can occur in the „Speed compensator" module!

The monitoring header structure is shown in chapter 3.2.

1.1.7. *DDR3 RAM storage module*

Filtered and headered monitoring packets are written into the DDR3 memory modules connected to the FPGA. The DDR3 memory is divided to that many independent buffers as many output interfaces are present.

- **The buffer space assigned to a given output interface gets full if the 1 Gb/s TCP module has lower read throughput. In this case packet loss can occur!**
- **If no TCP connection is present, then no DDR3 write operation is made, all packets addressed to the given output interface are dropped.**

For optimal DDR3 read/write speed we have to access the module in burst mode. This means, that the controller module buffers at least 1 Kbyte data, and then writes it in one step into the DDR3 memory. If no new packet arrives in a given time (timeout value is configurable), then fill-in packets are sent to load the buffer up to 1Kbyte. This ensures, that no short packets get stuck inside the buffers (also acts as keep-alive for the TCP connection). If there is traffic to be routed to a given output interface, then no fill in packets are inserted.

1.1.8. *„1G monitor Interface over TCP" module*

The packets read out from the DDR3 temporal buffer are sent through an 1 Gb/s TCP connection to the monitoring PC listening on the receiving side. The TCP stack implemented in the FPGA supports data streaming between the C-GEP 20 and the monitoring PC. If packet loss occures during the transmission, then the lost TCP segments get retransmitted. Retransmission buffer sizes are between 8 and 32 Kbyte. Assuming an optimal case of a point-to-point TCP connection and a powerful PC without load, a simple receiver software can achieve data speeds sligtly above 900 Mb/s.

If the TCP module does not read out packets fast enough from the DDR3 module because of far-end throttling, or TCP retransmissions, then packet

loss can occur if the DDR3 memory segment for the given output interface gets full!

1.1.9. *Timestamp creator module*

The C-GEP 20 device contains an internal clock source for timestamping. The „Timestamp creator” module synchronizes the local clock by using „NTP” protocol. The NTP client inside the module synchronizes to a given NTP servers reference clock by using our own control algorithm for smooth offset equalization.
This module is responsible for generating the timestamp in FILETIME format used in monitoring header creation.

1.1.10. *Configuration module*

The „Configuration” module is responsible for initializing and controlling the network interfaces and data processing modules, and also can disable or reset some parts of the C-GEP device. Configuration commands are sent through the PCI-E user interface.

The „Configuration” module is connected to the following modules:

- 10 Gb/s interface: disable the reception of ethernet frames, can reset the MAC module, disable or enable traffic mirroring (far-end loopback function).
- Packet Filter: upload filtering rules.
- Output interface selector: assign output interfaces for the filtering rules, set up IP fragment, and GTP-U steering.
- 1 Gb/s monitor interface over TCP: set up the network parameters for the monitor-interfaces: source and destination IP Addresses, ports. Output interfaces can be disabled separately if needed.
- NTP client: set the IP address of the NTP client, the remote NTP server, and the NTP update frequency.

1.1.11. *Statistics module*

The purpose of the „Statistics” module is to collect counter values, and maintain an event log. Statistics and events are then presented on the Web-interface.

The module maintains the following counters:

- Frames received on the 10 Gb/s interface
- Frames received with CRC error on the 10 Gb/s interface
- Frames received by filtering rule match
- Frames dropped during packet processing (Speed compensator module, Header Creator module)
- Frames dropped because of data transfer queueing (DDR3 RAM storage, TCP throttling)

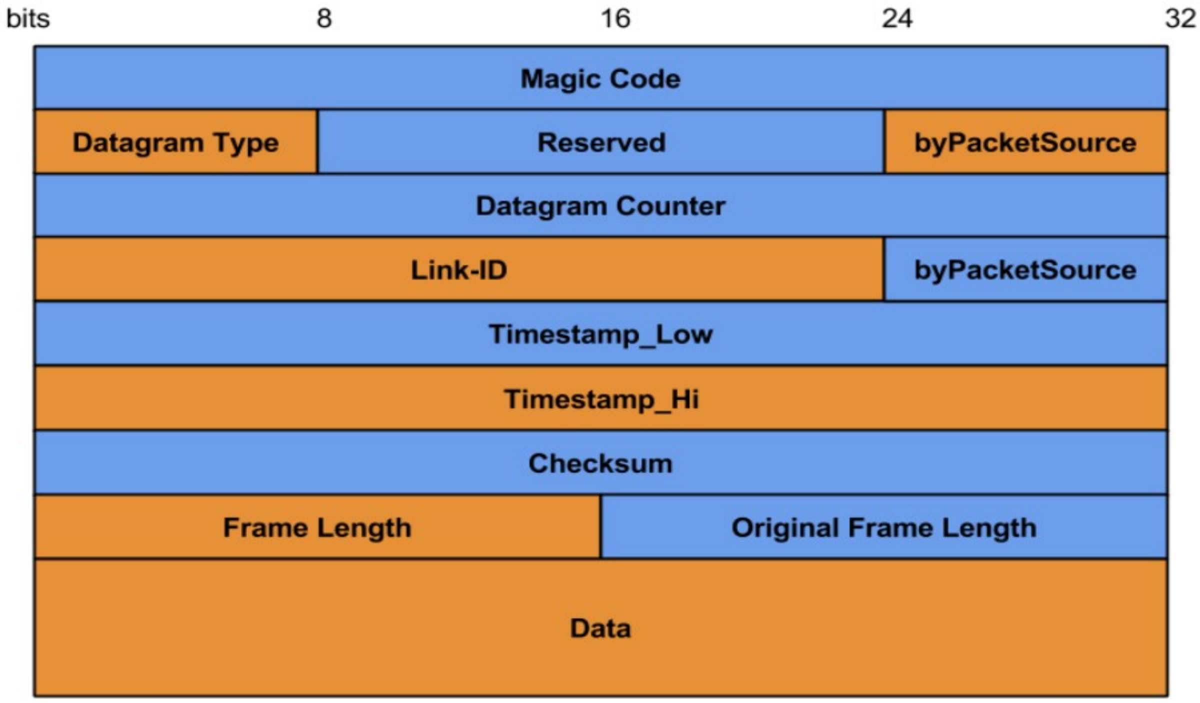
The module watches for the following event occurences:

- Frame loss
- Was there traffic in the last time interval? (default value: 5 minutes)
- Status of the NTP synchronization
- Link statuses for the 1 Gb/s and 10 Gb/s interfaces

Other internal state variables:

- FPGA temperature
- FPGA firmware release date
- Time on the FPGA, and on the management PC

1.2. Monitoring header structure



1.2.1. Figure – Structure of the monitoring header

1. Magic code: 32 bit value. The monitoring software seeks for the first header by synchronizing to the magic code value in the TCP stream. After the first valid header is found, a sync lock is achieved, and following the data another valid header must follow.

   Field value for this application: 0x07172738

2. Datagram type: 8 bit value. Type of the transferred packet.

   Value:

   0: Fill-in packet
   1: monitored data packet

3. Reserved: 16 bit, value 0.

4. byPacketSource: 8 bit value. Contains the monitored 10 Gb/s interfaces ID value.

5. Datagram counter: 32 bit value. The value of this counter increases by every data packet. Packet loss is detected by observing this counter.

6. Link-ID: 24 bit value. The ID of the monitoring output interface.
7. byPacketSource: 8 bit value. Contains the monitored 10 Gb/s interfaces ID value.
8. Timestamp_LOW: The first 32 bits of the 64 bit timestamp. The timestamp is in FILETIME format, showing the frame's time of reception on the 10 Gb/s interface.
9. Timestamp_HI: The last 32 bits of the 64 bit timestamp. The timestamp is in FILETIME format, showing the frame's time of reception on the 10 Gb/s interface.
10. Checksum: 32 bit value. Byte sum of the header fields and data bytes.
11. Frame-length: 16 bit value, contains the carried data without the size of the header. If truncate is enabled for the filter matching the packet, and the original frame length was bigger than the truncate length, then this value is equal to the truncate length.
12. Original Frame-length: 16 bit value, contains the original length of the received Ethernet frame.
13. Data: Data field, contains the Ethernet frame partially or completely depending on the truncate setting. The size of the data field is always divisible by 8, because of the internal bus-width used during packet processing. The value of the padding bytes after the data field is unspecified, and must be ignored.

1.3. C-GEP 20 services

- C-GEP 20 Web-UI:

  - This Web interface is responsible for configuring, and managing the C-GEP 20 device. The Web-UI provides access to the different statistic counters, and events that occured on the device. The Web-UI service is realized by using an Apache web-server, and uses html, php and javascript code.

  - The C-GEP Web-UI queries FPGA counters periodically over the PCI-E interface, and produces raw event codes for further processing. The query interval is 1 minute, the poller-client transfers this events to the poller-server.

- cg_poller - Poller-client program:

  - Client program responsible for processing statistics and events produced by the C-GEP 20 device, and transferring them to the 7N-poller (monitor-server) application.

  - The Poller-client periodically looks for new events (poll interval), and converts this data to a format understandable by the poller-server.

  - The Poller-client connects to the Poller-server by TCP. After that the server sends an „authentication-request” message, and the client responds with a „version” message. The C-GEP device must be registered (IP, and port) on the server-side, otherwise the poller connection won't get accepted.

- cgep_tool: this program is responsible for the low level I/O communication between the C-GEP device, and the operating system. The Web-UI uses this tool to communicate with the FPGA too.

```
Usage: cgep_tool <Command> <arg(s)>
Commands:
        g <reg_address> = Get register value
        s <reg_address> <reg_value> = Set register value
        k <reg_address> <nr_of_DWORDS> = sinK data from register to file
        f <reg_address> <file_name> = Flood file to address
        x <command_file> = eXecute commands in file
        t <reg_address> = Set Timestamp (filetime)
```

The program can be called from command line too, but this usage is for debug purposes only!

1.3.1. *Raw event codes defined for the C-GEP 20:*

Interface events

CODE	DATA	Meaning	Interface
0x10	-	Signal OK	XFP 0
0x11	-	Signal Lost	XFP 0
0x20	-	Signal OK	XFP 1
0x21	-	Signal Lost	XFP 1
0x30	-	TCP connected	SFP 0
0x31	-	TCP connection lost	SFP 0
0x32	-	TCP connected	SFP 1
0x33	-	TCP connection lost	SFP 1
0x34	-	TCP connected	SFP 2
0x35	-	TCP connection lost	SFP 2
0x36	-	TCP connected	SFP 3
0x37	-	TCP connection lost	SFP 3
0x38	-	TCP connected	SFP 4
0x39	-	TCP connection lost	SFP 4
0x3A	-	TCP connected	SFP 5
0x3B	-	TCP connection lost	SFP 5
0x3C	-	TCP connected	SFP 6
0x3D	-	TCP connection lost	SFP 6
0x3E	-	TCP connected	SFP 7
0x3F	-	TCP connection lost	SFP 7
0x40	-	TCP connected	SFP 8
0x41	-	TCP connection lost	SFP 8
0x42	-	TCP connected	SFP 9
0x43	-	TCP connection lost	SFP 9
0x44	-	TCP connected	SFP 10
0x45	-	TCP connection lost	SFP 10
0x46	-	TCP connected	SFP 11
0x47	-	TCP connection lost	SFP 11
0x48	-	TCP connected	SFP 12
0x49	-	TCP connection lost	SFP 12
0x4A	-	TCP connected	SFP 13
0x4B	-	TCP connection lost	SFP 13
0x4C	-	TCP connected	SFP 14
0x4D	-	TCP connection lost	SFP 14
0x4E	-	TCP connected	SFP 15
0x4F	-	TCP connection lost	SFP 15
0x50	-	TCP connected	SFP 16
0x51	-	TCP connection lost	SFP 16
0x52	-	TCP connected	SFP 17
0x53	-	TCP connection lost	SFP 17
0x54	-	TCP connected	SFP 18
0x55	-	TCP connection lost	SFP 18
0x56	-	TCP connected	SFP 19
0x57	-	TCP connection lost	SFP 19
0x60	-	NTP: Eth. link down	SFP 20
0x61	-	NTP: ARP timeout	SFP 20
0x62	-	NTP: NTP timeout	SFP 20
0x63	-	NTP: Delay fail	SFP 20
0x64	-	NTP: Config. error	SFP 20
0x65	-	NTP: usrt error	SFP 20
0x66	-	NTP: Sync. skipped	SFP 20
0x67	offset in usec	NTP: Sync. OK	SFP 20

Management events

CODE	Meaning
0xA0	Filter settings has been changed
0xA1	NTP settings has been changed
0xA2	GTP-U/Fragment steering settings has been changed
0xA3	Interface settings has been changed
0xA4	Filter configuration has been set / uploaded
0xA5	Interface configuration has been set / uploaded
0xA6	NTP configuration has been set / uploaded
0xA7	Poller settings has been changed and poller has been restarted
0xA8	Board has been reseted
0xA9	Board Configuration has been uploaded
0xAA	Board IP address has been modified
0xAB	Board shutdown
0xAC	Board reboot in progress
0xAD	Board firmware upload in progress

Counters and internal sensors

CODE	DATA	Meaning
0xF0	counter	Badframes counter on XFP 0
0xF1	counter	Badframes counter on XFP 1
0xF2	counter	Received frames counter on XFP 0
0xF3	counter	Received frames counter on XFP 1
0xF4	counter	Lost frames (summ)
0xFA	temp in C	Temperature FPGA

Event codes defined by the Poller-server

CODE	Type	Meaning
0019	ERROR	NTP ERROR (NTP Server Timeout)
0020	ERROR	Monitor: Network ERROR (Interface down, ARP error, etc.)
0021	ERROR	Monitor: Too high clock adjustment
2000	MESSAGE	C-GEP20: Monitor connected
2001	ERROR	C-GEP20: Monitor disconnected
2002	MESSAGE	C-GEP20: 10 Gbit/s intf. signal OK
2003	ERROR	C-GEP20: 10 Gbit/s intf. signal lost
2004	ERROR	C-GEP20: Bad frames (XFP)
2005	ERROR	C-GEP20: Lost frames (XFP)
2006	MESSAGE	C-GEP20: Filter config. changed/set
2007	MESSAGE	C-GEP20: Intf. config. changed/set
2008	ERROR	C-GEP20 reseted
2009	ERROR	C-GEP20: Temperature is too high.
2010	ERROR	C-GEP20: No traffic int he last 1 min.

Counters

CODE	Meaning
9000	C-GEP20: Number of received frames (XFP)
9001	C-GEP20: Number of bad frames (XFP)
9002	C-GEP20: Number of lost frames

2. NTP (Network Time Protocol) based time synchronization

2.1. Configuration

The NTP configuration settings are accesible from the Web-UI:

- IP Address of the NTP server
- IP Address of the NTP client
- Maximum interval between timing synchronizations

2.2. Startup

After receiving and validating the settings, the NTP cliens tries to set the initial clock value. If it fails, then retries are sent in every second. Synchronization to the server begins after setting the initial time.

2.3. Length of the synchronization period

During normal operation the NTP client module synchronizes to the reference clock with an increasing period. The length of the first interval is 16 seconds, and gradually increases to the maximal value of 512 seconds.

The actual synchronization period doubles when the offset value between the clocks of the NTP client and NTP server are less than the predefined threshold value (tstepUP_threshold = 100us), or the interval reached the maximum value (max. 512 s). Whenever the offset value between the clock of the NTP client and server exceeds a predefined threshold (tstepDOWN_threshold = 50 us), the synchronization period will be reset to the minimum value (16 s). After that the previously mentioned interval doubling method is used.

The tstepUP_threshold= 100us and tstepDOWN_threshold = 50 us are constant values defined in firmware code.

2.4. Synchronization burst

The NTP client uses the „burst” mode, meaning that the message with the least round-trip-delay (RTT) of 8 consecutive messages is used to calculate the offset for the controller.

2.5. Synhronizing the internal clock

The C-GEP 20's internal clock depends on the offset indicated by the NTP server, the length of the synchronization period, and the internal variables of the control loop. The control algorithm sets the incrementum of an internal counter during the synchronization periods. (this counter is the internal clock)

There are no abrupt clock changes, the speed of the internal clock gets continously corrected according the time difference between the C-GEP device and the NTP server. The offset between the NTP client and server is smoothed by a control algorithm.

The offset value mainly depends on network response time changes. Network devices between the C-GEP 20 and the NTP server (router, switch) increase the response time spread, resulting a highly variable offset. The offset changes are continuously smoothed by the control algorithm according to RFC-5905.

Suggestion: The C-GEP 20 and NTP server must be „close enough” to prevent high offset spread, meaning, that as less as possible network components are allowed between them. If thats not possible, then the NTP server and C-GEP 20 must be assigned to the same high priority VLAN segment.

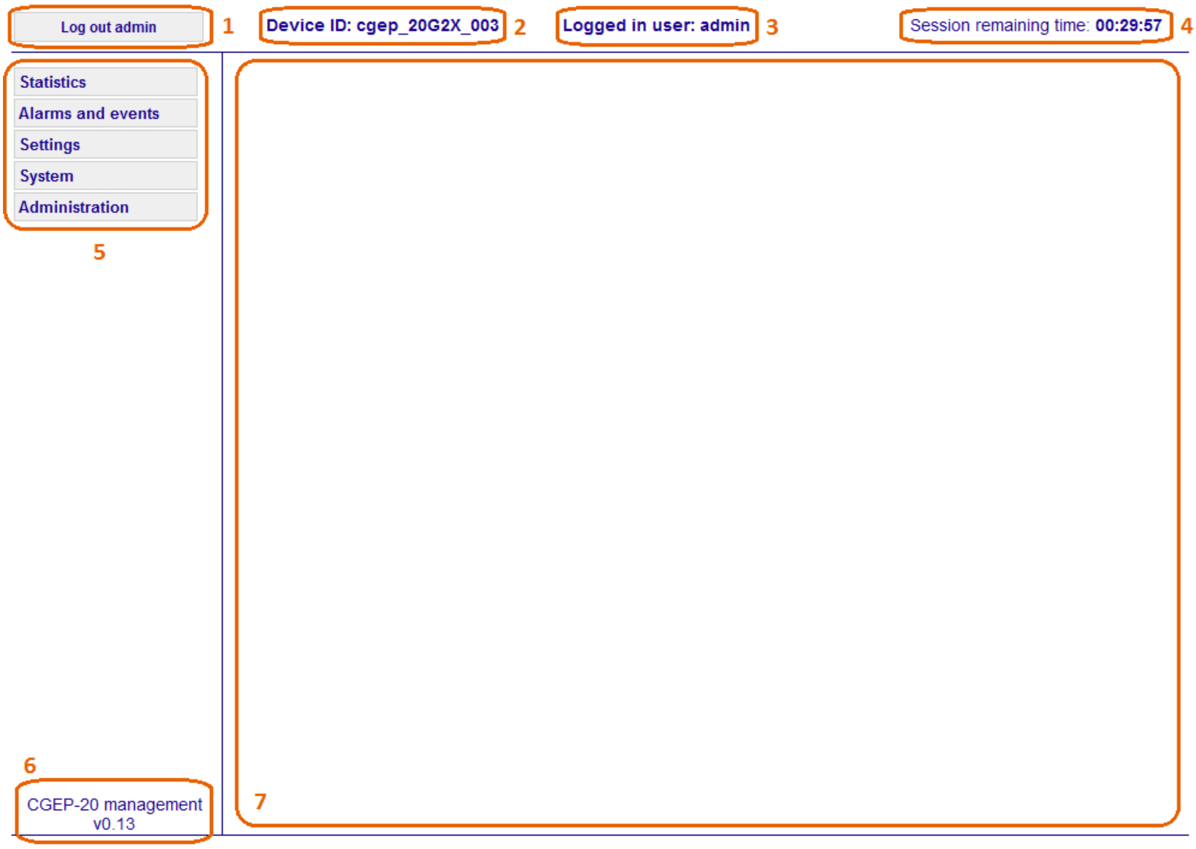
2.6. What is the clock change resolution?

Time resolution inside the NTP module:

- The lower 32 bits of the NTP timestamp represents the fractional part of seconds. This means, that one value quantum is 2^{-32} seconds. (233 ps)
- The FPGA's timestamp module uses a clock source of 125 MHz, so the highest achievable resolution is 8 ns.
- The timestamp in the monitoring header is in FILETIME format, this results in a 100 ns resolution.

3. Graphical User Interface – Web Interface

The C-GEP 20 has a graphical user interface accessible from any web browser for configuring and maintaining the device. The user must log into the device by supplying a user name and password on the login screen. After succesful authentication the main window appears as shown on the fig. 5.1 below.



5.1. Fig. – C-GEP 20 WebUI

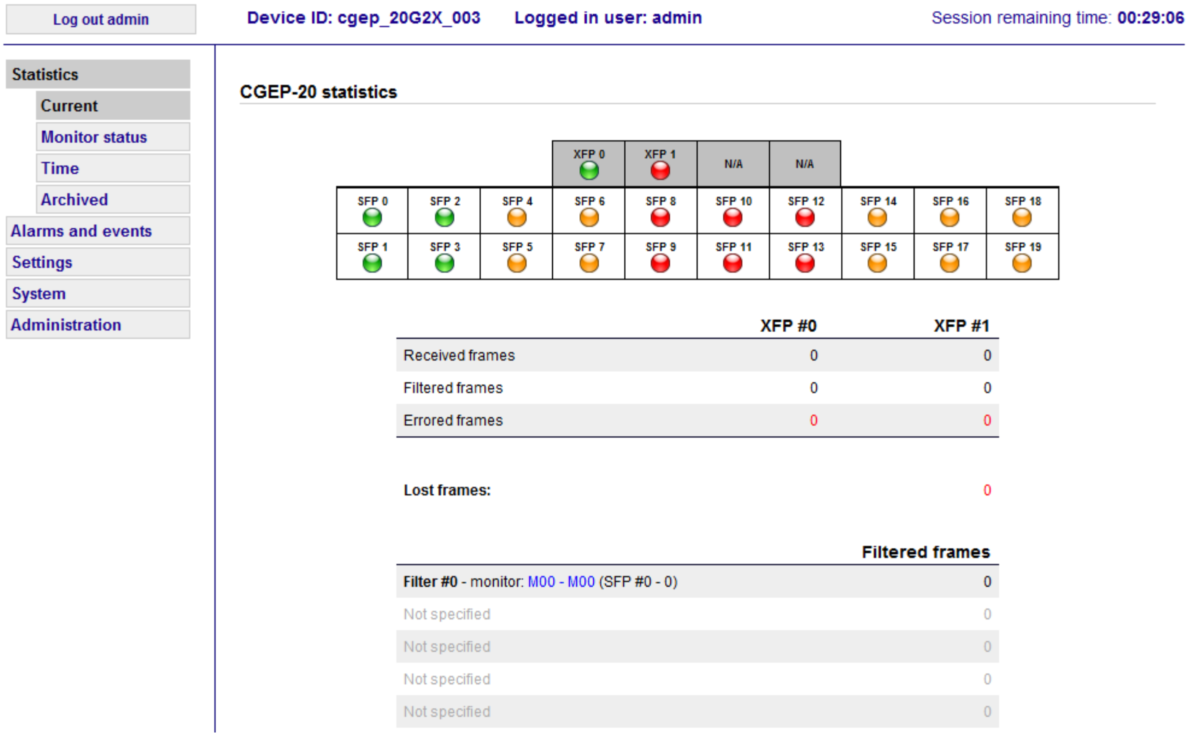
1. Logout for active user.
2. The device ID of the C-GEP 20.
3. User name of the currently logged in users.
4. Time remaining from the current session. The user is logged out if the timer runs out, every user activity resets the timer.
5. Menu items.
6. Web-UI version number.
7. Content for the currently selected menu item.

3.1. „Statistics” menu

Statistics menu item structure:

- Statistics
  - Current
  - Monitor status
  - Time
  - Archived

„*Current*” submenu:



Device ID: cgep_20G2X_003 Logged in user: admin Session remaining time: 00:29:06

CGEP-20 statistics

			XFP 0 🟢	XFP 1 🔴	N/A	N/A			
SFP 0 🟢	SFP 2 🟢	SFP 4 🟠	SFP 6 🟠	SFP 8 🔴	SFP 10 🔴	SFP 12 🔴	SFP 14 🟠	SFP 16 🟠	SFP 18 🟠
SFP 1 🟢	SFP 3 🟢	SFP 5 🟠	SFP 7 🟠	SFP 9 🔴	SFP 11 🔴	SFP 13 🔴	SFP 15 🟠	SFP 17 🟠	SFP 19 🟠

	XFP #0	XFP #1
Received frames	0	0
Filtered frames	0	0
Errored frames	0	0

Lost frames: 0

	Filtered frames
Filter #0 - monitor: M00 - M00 (SFP #0 - 0)	0
Not specified	0
Not specified	0
Not specified	0
Not specified	0

3.1.1. Fig. – „Current” menu

The statistics collected by C-GEP 20 are shown under the „Statistics/Current” menu.

The pictograms above show the status of the SFP/XFP modules:

SFP/XFP link states:

- Red: module not plugged
- Orange: module present, no link
- Green: link ok

XFP interface statistics:

- Received frames: Number of received frames on the 10 Gb/s interface.
- Filtered frames: Number of frames matching at least one filter-rule.
- Errored frames: Number of frames received with CRC checksum error.

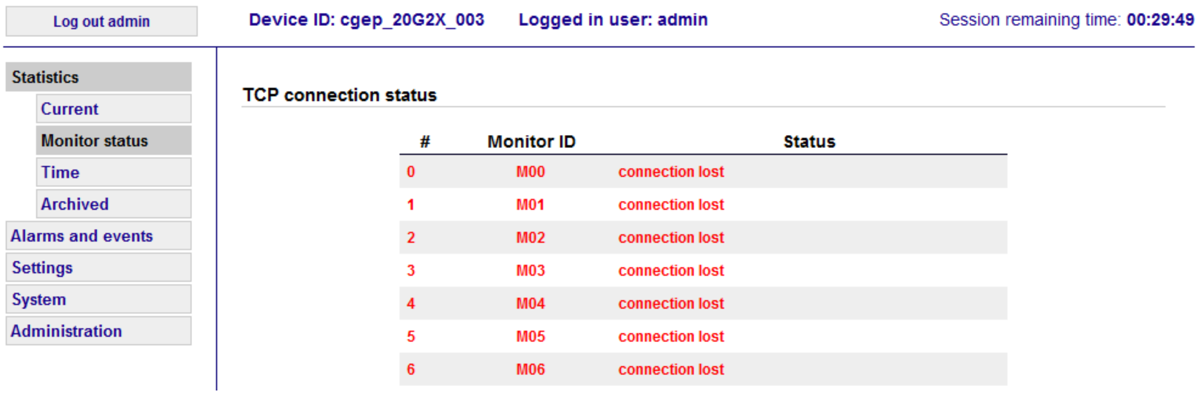
XFP and SFP interface statistics:

- Lost frames: Frames dropped on the input and output side of the processing chain.

SFP interface statistics:

- Filtered frames: Number of frames that matches the given filter, and is used to forward the packet to a monitor.

„*Monitor status*" submenu:



Device ID: cgep_20G2X_003 Logged in user: admin Session remaining time: 00:29:49

TCP connection status

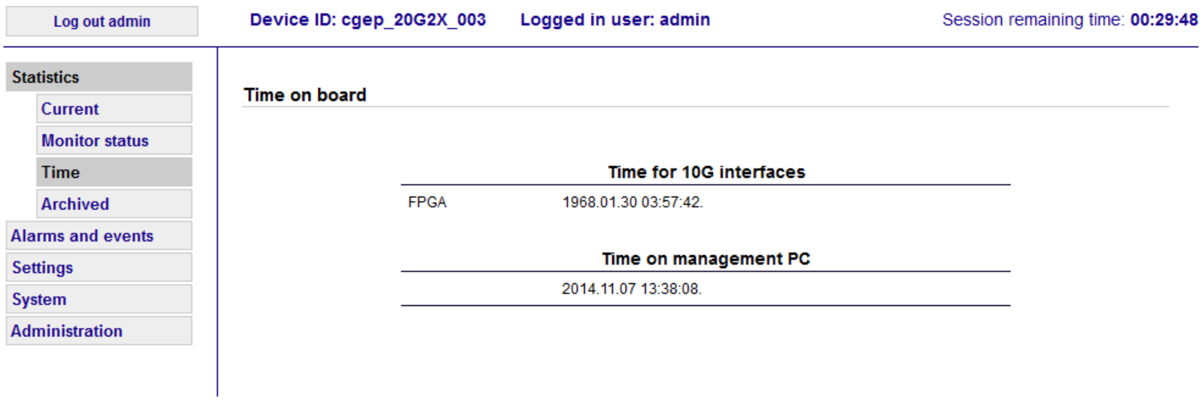
#	Monitor ID	Status
0	M00	connection lost
1	M01	connection lost
2	M02	connection lost
3	M03	connection lost
4	M04	connection lost
5	M05	connection lost
6	M06	connection lost

3.1.2. Fig. – „Monitor status" menu

Shows the C-GEP 20 monitoring TCP connection status:

- Green: Connected. Active error free state
- Red: Connection lost. Error in connection, not connected.

„*Time*" submenu:



Device ID: cgep_20G2X_003 Logged in user: admin Session remaining time: 00:29:48

Time on board

Time for 10G interfaces	
FPGA	1968.01.30 03:57:42.

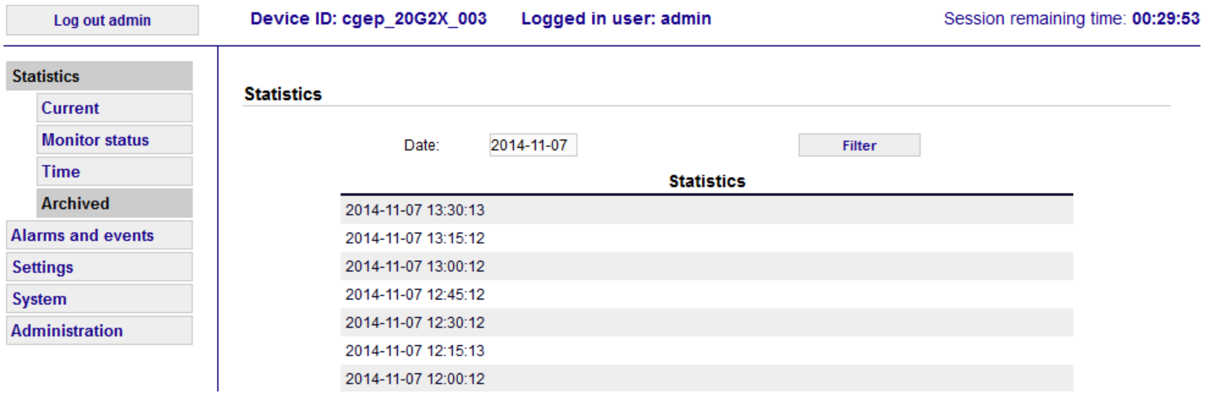
Time on management PC
2014.11.07 13:38:08.

3.1.3. Fig. – „Time” menu

Shows the internal clocks of the C-GEP 20 device:

- current internal clock value of the NTP client used for timestaming (Time for 10G interfaces)
- current internal clock value of the mini-PC

„*Archived*” submenu:



Device ID: cgep_20G2X_003 Logged in user: admin Session remaining time: 00:29:53

Statistics

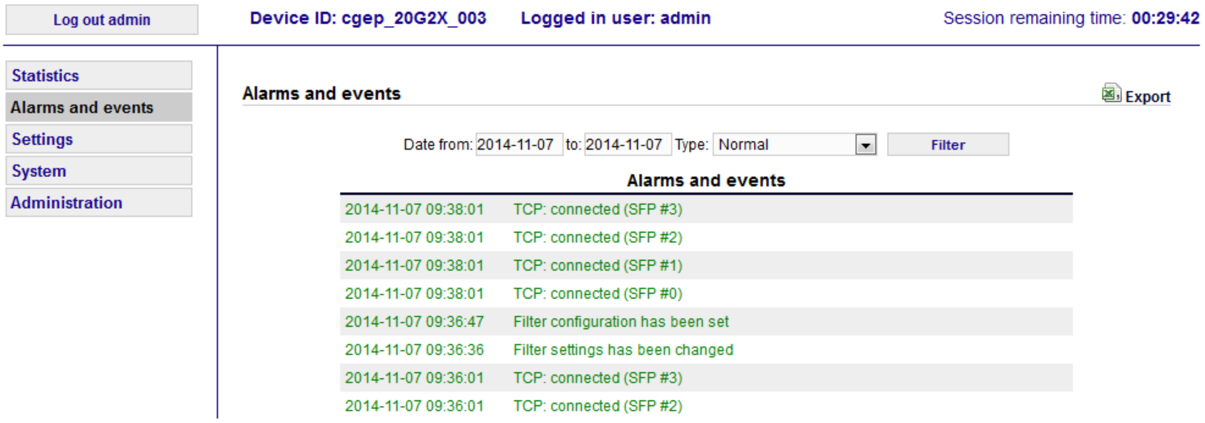
Date: 2014-11-07

Statistics
2014-11-07 13:30:13
2014-11-07 13:15:12
2014-11-07 13:00:12
2014-11-07 12:45:12
2014-11-07 12:30:12
2014-11-07 12:15:13
2014-11-07 12:00:12

3.1.4. Fig. – „Archived” menu

The C-GEP 20 saves the statistic counter values into a database every 15 minutes. The statistic counter values are reset at the same time. The „Archived” submenu allows us to view previously saved statistics. You can select a specific date from the date picker, and hit the „Filter” button. The statistic period can be selected from the list below. The timestamp of the entry shows the exact moment the counters were saved, and then reset. Clicking on one of the entries the actual statistics are show in a window popup (without showing the status LED-s) like on the current statistics page.

3.2. „Alarms and events” menu



Device ID: cgep_20G2X_003   Logged in user: admin   Session remaining time: 00:29:42

Alarms and events

Date from: 2014-11-07 to: 2014-11-07 Type: Normal

Alarms and events

2014-11-07 09:38:01	TCP: connected (SFP #3)
2014-11-07 09:38:01	TCP: connected (SFP #2)
2014-11-07 09:38:01	TCP: connected (SFP #1)
2014-11-07 09:38:01	TCP: connected (SFP #0)
2014-11-07 09:36:47	Filter configuration has been set
2014-11-07 09:36:36	Filter settings has been changed
2014-11-07 09:36:01	TCP: connected (SFP #3)
2014-11-07 09:36:01	TCP: connected (SFP #2)

3.2.1. Fig. – „Alarms and events” menu

This menu is for viewing the occured events during the operation of the C-GEP 20 device. The start and end date of the query can be selected, and the event type too.
The event type can be selected from the drop down menu, and then the „Filter” button must be pressed.

Event types:

- Normal: Events occuring during normal operation including NTP synchronization events.
- Warning: Non critical error event, user intervention is needed. Fe.: packet loss.
- Error: Functional or physical error. Fe.: FPGA error, or link loss
- Info: Other informations. Fe.: NTP time offset value
- All (without info): Display all events except the *Info*.

Remark: Depending on the selected time interval it can take several minutes until the events are displayed!

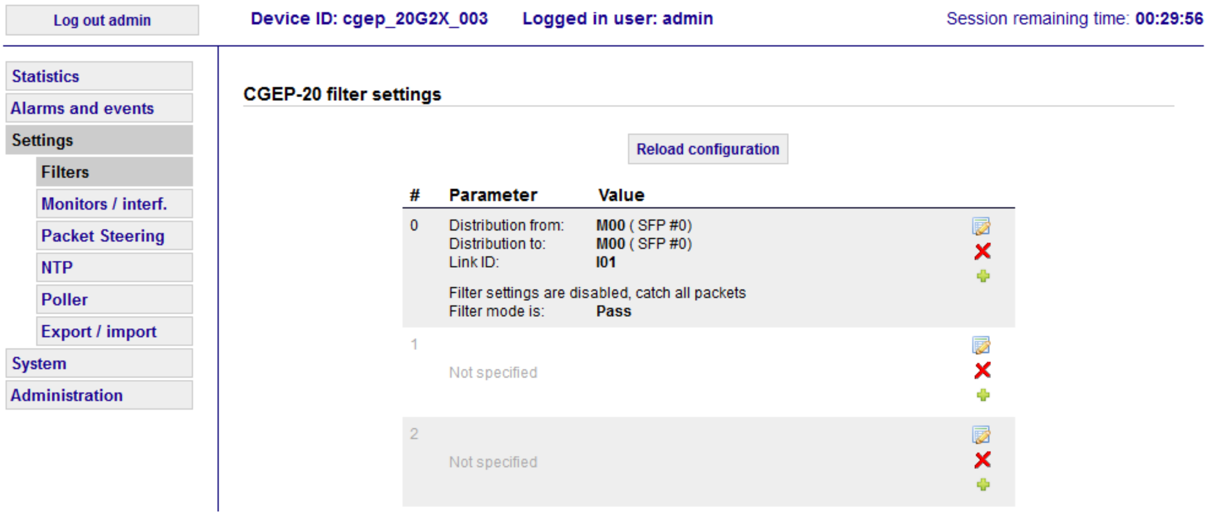
3.3. Settings menu

„*Settings*” menu structure:

- Settings
  - Filters
  - Monitors / interf.
  - Packet Steering
  - NTP
  - Poller
  - Export / import

„***Filters***” submenu

After clicking on the „Settings” menu, the most used „Filters” submenu appears. The „Filters” submenu contains the 32 C-GEP 20 filter rules (0 – 31). The first rule (0.) has the highest priority in the filtering decision, and the last (31.) has the lowest priority.



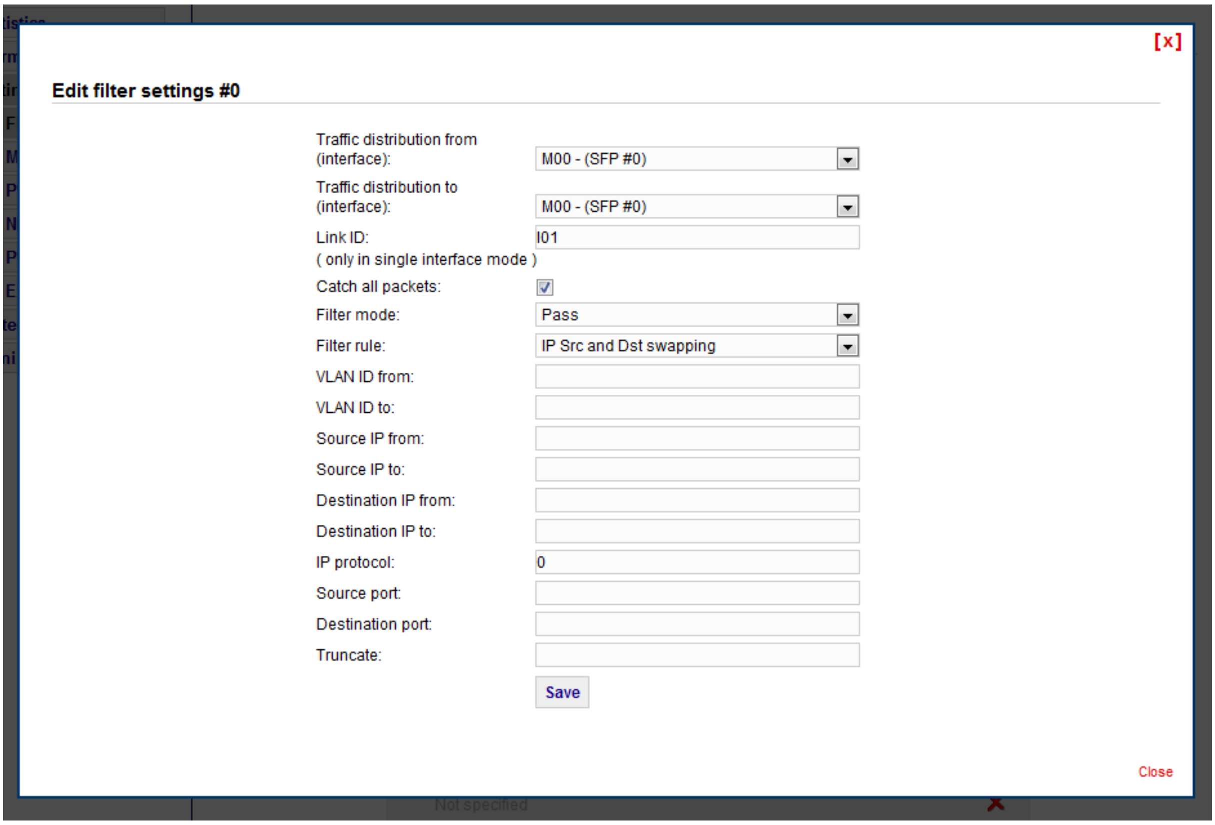
#	Parameter	Value
0	Distribution from: Distribution to: Link ID:	M00 (SFP #0) M00 (SFP #0) I01
	Filter settings are disabled, catch all packets Filter mode is:	Pass
1	Not specified	
2	Not specified	

3.3.1. Fig. – Filters submenu

The listing view contains the main parameters and its values defined by the actual rule. You can insert a new rule with the ✚ button. The new rule gets inserted on the place of the actual rule, the actual rule, and the rules below get shifted down by one. If there are already 32 rules defined, then the last rule is dropped. You can delete the actual rule by pressing the ✗ button. The selected rule gets deleted, and the rules below get shifted up by one.

You can edit a given rule by clicking on the ✎ button. The filter settings appear in a popup window as shown on figure 5.3.2.

After editing the new filter configuration changes must be uploaded to the FPGA by pressing the „Reload Configuration” button. The „Reload Configuration” calls the „cgep_tool” which updates the filter rules by register write calls on the PCI-E interface.



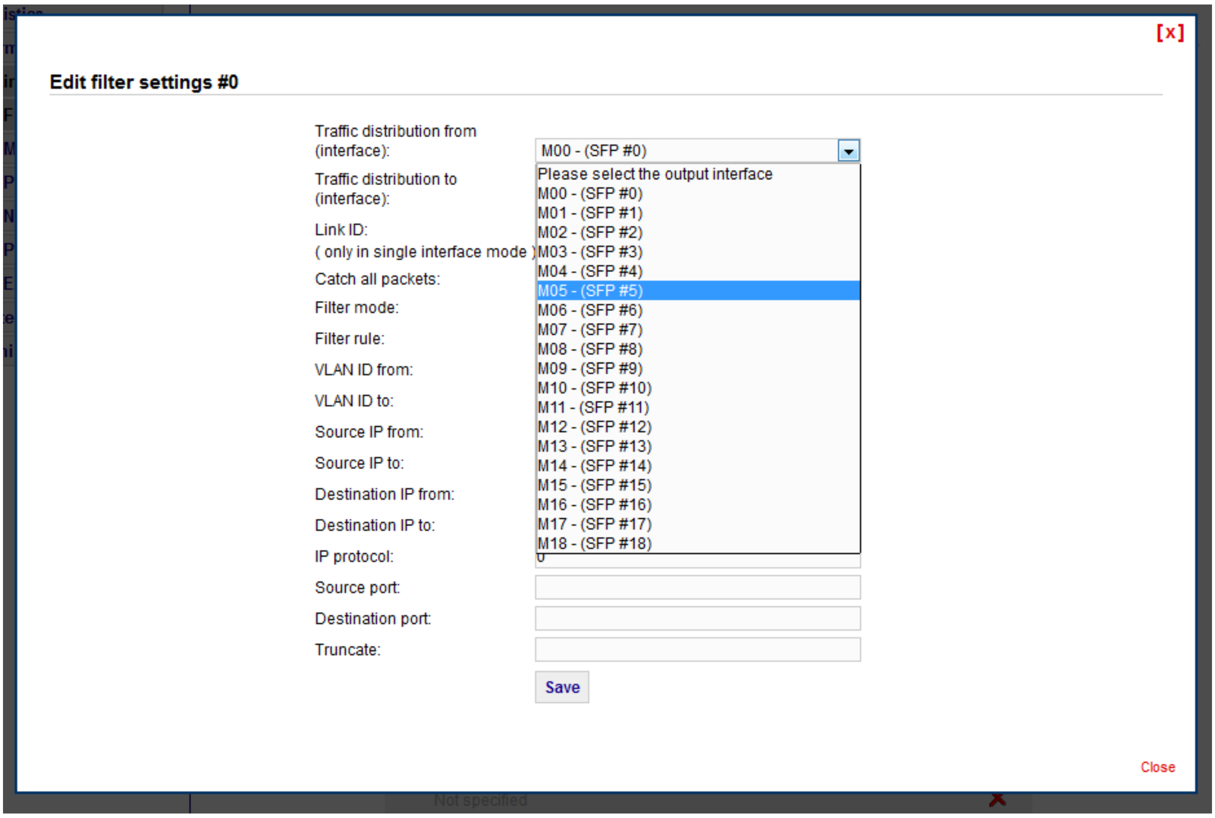
Edit filter settings #0

Traffic distribution from (interface):	M00 - (SFP #0)
Traffic distribution to (interface):	M00 - (SFP #0)
Link ID: (only in single interface mode)	I01
Catch all packets:	☑
Filter mode:	Pass
Filter rule:	IP Src and Dst swapping
VLAN ID from:	
VLAN ID to:	
Source IP from:	
Source IP to:	
Destination IP from:	
Destination IP to:	
IP protocol:	0
Source port:	
Destination port:	
Truncate:	

3.3.2. Fig. – „Edit filter settings” window

You can see the actually edited filters number after the # in the left upper corner.

The meaning of the filter setting fields are described in chapter 3.1.2: Packet filter module.



Edit filter settings #0

Traffic distribution from (interface): M00 - (SFP #0)

Traffic distribution to (interface):

Link ID:
(only in single interface mode)

Catch all packets:

Filter mode:

Filter rule:

VLAN ID from:

VLAN ID to:

Source IP from:

Source IP to:

Destination IP from:

Destination IP to:

IP protocol: 0

Source port:

Destination port:

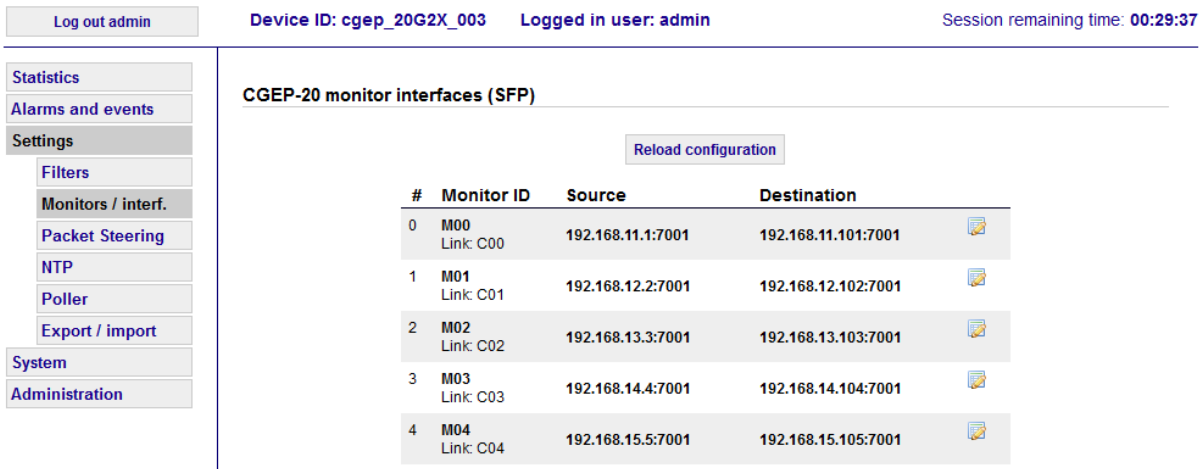
Truncate:

5.3.3. Fig. – Output interface selection

Out of the 20 output interfaces only 19 are selectable because one 1 Gb/s interface is reserved for NTP synchronization. Using other synchronization methods (like the custom SGA-ClockCard interface) all 20 1 Gb/s interfaces can be used as monitoring outputs.

„**Monitors / interfaces**” submenu

The „Monitors/interfaces” submenu contains network settings for the 1 Gb/s output interfaces. The list contains the 19 accessible interfaces. You can configure the selected interface by clicking on the ✎ icon.



Device ID: cgep_20G2X_003 Logged in user: admin Session remaining time: 00:29:37

CGEP-20 monitor interfaces (SFP)

#	Monitor ID	Source	Destination	
0	M00 Link: C00	192.168.11.1:7001	192.168.11.101:7001	✎
1	M01 Link: C01	192.168.12.2:7001	192.168.12.102:7001	✎
2	M02 Link: C02	192.168.13.3:7001	192.168.13.103:7001	✎
3	M03 Link: C03	192.168.14.4:7001	192.168.14.104:7001	✎
4	M04 Link: C04	192.168.15.5:7001	192.168.15.105:7001	✎

5.3.4 Fig. – „Monitors/interfaces” submenu

The configuration window contains the following parameter settings:

- Monitor ID: This identifies the monitoring interface if no specific link ID is specified (fe. steering)
- Link ID: specifies the filter the packet fits on, see the corresponding monitoring header field
- Source IP: The C-GEP 20 output interface IP address
- Destination IP: The IP address of the monitoring PC connected to the given C-GEP 20 output interface
- TCP source Port: The C-GEP 20 output interface TCP service port
- TCP destination Port: The TCP port assigned to the monitor PC
- Gateway IP: IP address of the gateway if present
- Subnet mask: Subnet mask for network segment

„***Packet Steering***” submenu

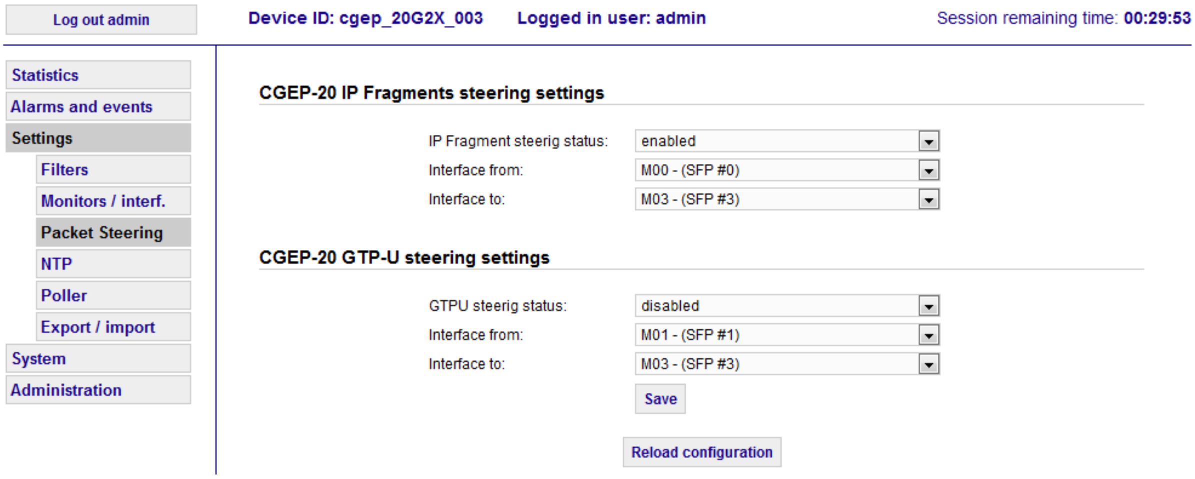
The C-GEP 20 device allows the flow based distribution of GTP-U packets and fragmented IPv4 packets between the output interfaces. Packets with the same governing parameters belong to a flow. Steering guarantees, that packets of a given flow are always routed to the same output interface.

Steering by protocol parameters:

- GTP-U (TEID and carried IP addresses)

- Fragmented IPv4 packet (IP addresses and fragment ID)

Steering settings are shown on figure 5.3.5.



Device ID: cgep_20G2X_003 Logged in user: admin Session remaining time: 00:29:53

CGEP-20 IP Fragments steering settings

IP Fragment steerig status: enabled
Interface from: M00 - (SFP #0)
Interface to: M03 - (SFP #3)

CGEP-20 GTP-U steering settings

GTPU steerig status: disabled
Interface from: M01 - (SFP #1)
Interface to: M03 - (SFP #3)

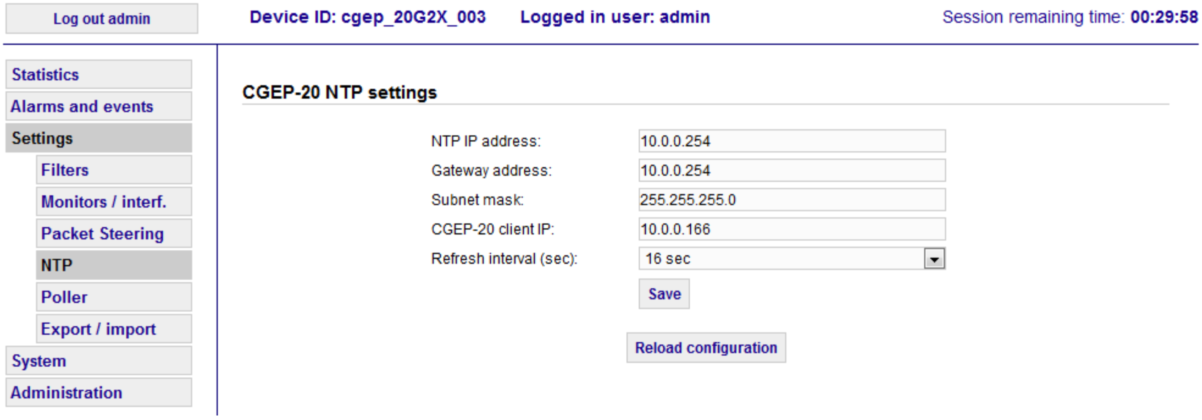
5.3.5. Fig. – „Packet Steering” submenu

After setting up the steering functions, the „Reload configuration” button must be pressed to validate the new values.

Note: Output interface selection defined by steering has higher priority than filtering rules output interface setting. This means, that after the packet is passing the filters the steering can overwrite the output interface assigned by the filters.

„*NTP*” submenu

The C-GEP 20's NTP client-settings can be defined under the „NTP” submenu.



Device ID: cgep_20G2X_003 Logged in user: admin Session remaining time: 00:29:58

CGEP-20 NTP settings

NTP IP address: 10.0.0.254
Gateway address: 10.0.0.254
Subnet mask: 255.255.255.0
CGEP-20 client IP: 10.0.0.166
Refresh interval (sec): 16 sec

5.3.6. Fig. – „NTP” submenu

After specifying the NTP server and client addresses the „Reload configuration” button must be pressed to upload the new settings.

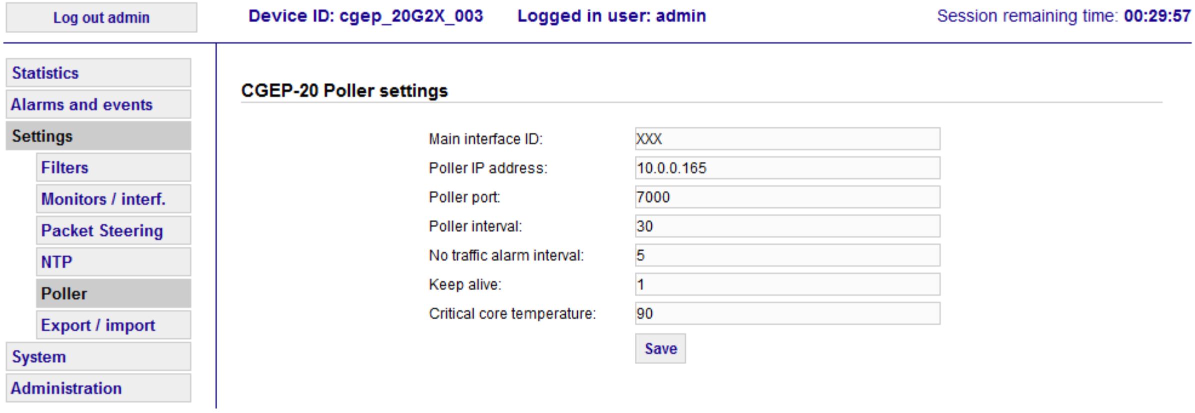
„*Poller*” submenu

This submenu is responsible for configuring the parameters of the C-GEP 20 and 7N-poller connection.

Settings:

- Main Interface ID: C-GEP 20 device ID for 7N-poller.
- Poller IP Address: IP address of the Poller server.
- Poller Port: TCP port number of the Poller server.

- Poller interval: The poller client pulls statistics from the C-GEP 20 after the specified number of seconds passed. The device polls new values in every minute, for now this setting has no effect.
- No traffic alarm interval: If no traffic is detected on the input interfaces in the given time interval, then a „no traffic” event is generated.
- Keep alive: Poller client sends keepAlive messages to the Poller server if set. (poller message, not TCP keepalive)
- Critical core temperature: If FPGA temperature rises higher than the specified value, then an alarm event is generated (may shut down board automatically as well).



Device ID: cgep_20G2X_003 Logged in user: admin Session remaining time: 00:29:57

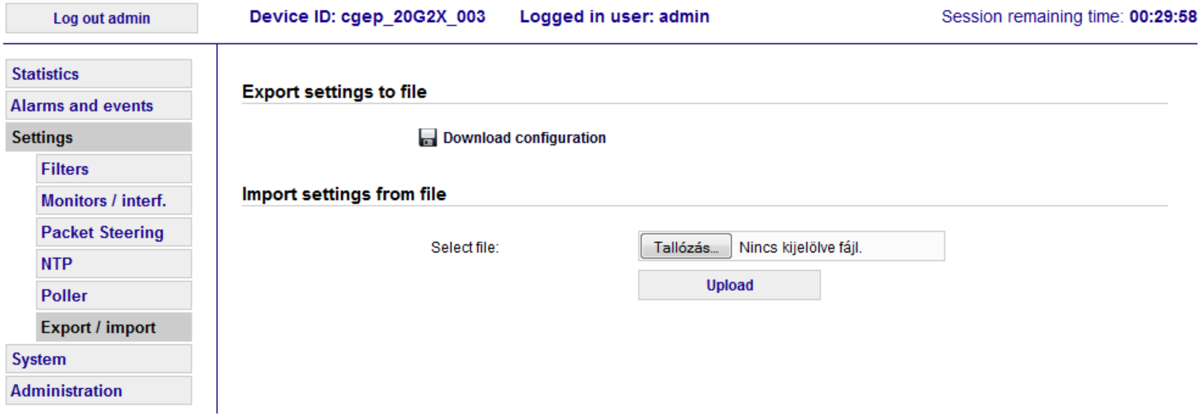
CGEP-20 Poller settings

Main interface ID:	XXX
Poller IP address:	10.0.0.165
Poller port:	7000
Poller interval:	30
No traffic alarm interval:	5
Keep alive:	1
Critical core temperature:	90

5.3.7. Fig. – „Poller” submenu

„*Export / Import*” submenu

This entry is for saving all the settings and values of the device into an xml file, or load it from a file.



Device ID: cgep_20G2X_003 Logged in user: admin Session remaining time: 00:29:58

Export settings to file

Import settings from file

Select file: Nincs kijelölve fájl.

5.3.8. Fig – „Export / Import” submenu

3.4. „System” menu

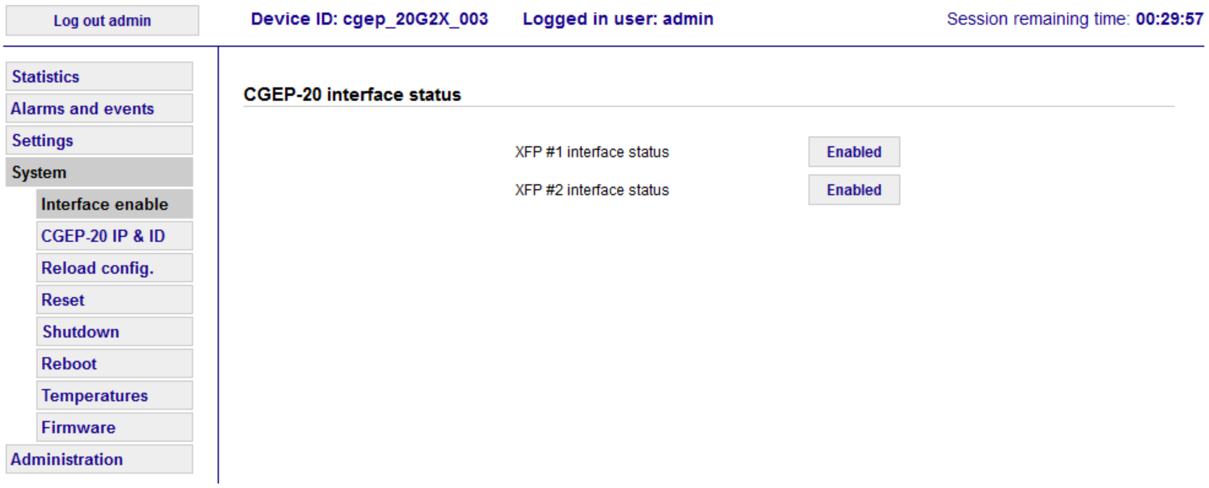
Structure of the „*System*” menu:

- System
  - Interface enable
  - CGEP-20 IP & ID
  - Reload config.
  - Reset
  - Shutdown
  - Reboot
  - Temperatures
  - Firmware

After clicking on the „System” menu, the most used „Reload Config” submenu appears.

„*Interface enable*” submenu

This entry contains the 10 Gb/s input interface controls. You can enable or disable the selected interface by pressing the button. The setting is instant, no restart or configuration reload is needed.


Device ID: cgep_20G2X_003 Logged in user: admin Session remaining time: 00:29:57

CGEP-20 interface status

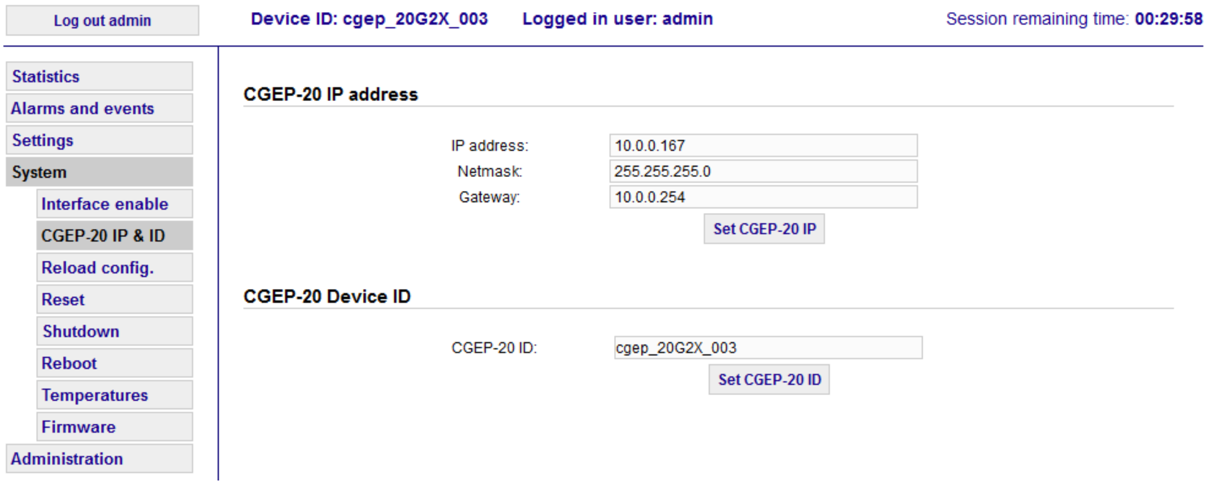
XFP #1 interface status: Enabled

XFP #2 interface status: Enabled

3.4.1. Fig. – „Interface enable” submenu

„*C-GEP20 IP & ID*” submenu

The „C-GEP 20 IP & ID” submenu is used to assign a unique identification tag (device ID) to the device. Also the C-GEP 20 management interface address can be changed here too. The device must be rebooted for the new IP address to take effect.



Device ID: cgep_20G2X_003 Logged in user: admin Session remaining time: 00:29:58

CGEP-20 IP address

IP address: 10.0.0.167
Netmask: 255.255.255.0
Gateway: 10.0.0.254

CGEP-20 Device ID

CGEP-20 ID: cgep_20G2X_003

3.4.2. Fig. – „C-GEP20 IP & ID” submenu

„*Reload config.*” submenu

This entry is used to reload all configuration settings. By pressing the „Reload configuration” button all C-GEP 20 interface controllers, XFP and SFP interface modules, and statistic modules get reseted. All filter rules, NTP settings, monitor interface settings are uploaded and updated. An event is also generated and sent to the poller-server.

„*Reset*” submenu

This entry has the same effect as the „Reload config.” but all FPGA firmware state variables are reseted additionally. This is only needed after firmware update.

„*Shutdown*” submenu

This entry is for powering down the C-GEP 20 device.

„***Reboot***” submenu

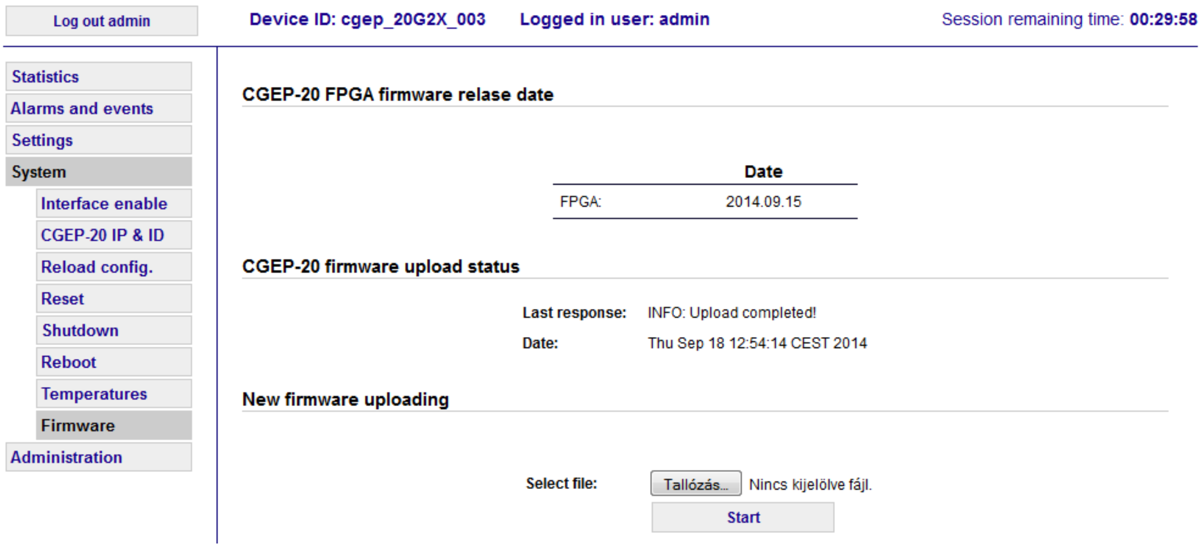
This entry is for rebooting the management PC located on the C-GEP 20 device. Only needed if the management IP Address is changed.

„***Temperatures***” submenu

This entry shows the FPGA core temperature. Suggested range is between 0 – 70 grade celsius.

„***Firmware***” submenu

The „Firmware” submenu is used to refresh the FPGA firmware. After pressing the „Tallózás” (Browse) button in the „New firmware uploading” section the new bit file must be selected. Pressing the „Start” button initiates the firmware update process. After the update is done the „CGEP-20 firmware upload status” shows the end result of the process. The current firmware release date can be seen here too.



Device ID: cgep_20G2X_003 **Logged in user: admin** Session remaining time: **00:29:58**

CGEP-20 FPGA firmware relase date

	Date
FPGA:	2014.09.15

CGEP-20 firmware upload status

Last response: INFO: Upload completed!

Date: Thu Sep 18 12:54:14 CEST 2014

New firmware uploading

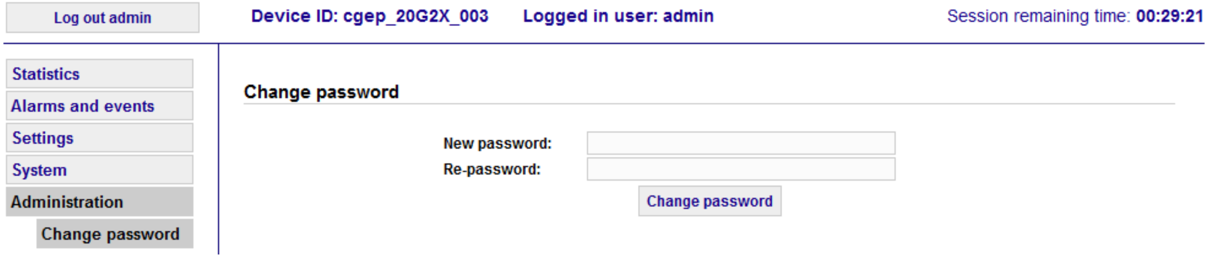
Select file: Tallózás... Nincs kijelölve fájl.

Start

3.4.3. Fig. – „Firmware” submenu

3.5. „Administration” menu

The „Administration” submenu is for changing the password for the currently logged in user.



Log out admin

Device ID: cgep_20G2X_003 Logged in user: admin Session remaining time: 00:29:21

Change password

New password:

Re-password:

5.5.1 Fig. – „Administration” menu