PC Host GUI Manual R1.04

1 Audience 2
2 Organization of the GUI 3
2.1 Basic Structure of GUI Software 4
2.2 GUI Start Up Sequence 4
2.3 Note on the GUI data Path 5
3 Basic Operation of the GUI 5
3.1 GUI Controls 5
3.1.1 Apply Button 5
3.1.2 Refresh Button 6
3.1.3 Revert Button 6
3.1.4 Defaults Button 6
4 GUI Panel Directory 6
5 OLT Panel 8
6 OLT Network Parameters 8
6.1 OAM Rate 8
6.2 Loopback Timeout Value 8
6.3 MPCP Parameters 8
6.3.1 Period 8
6.3.2 Window 8
6.3.3 VLAN Ethertype 8
7 DBA 9
7.1 Broadcast SLA 9
7.2 Aggregate Shaper 11
7.3 Priority Range 11
7.4 Shaper Drop Down Weights 12
7.5 DBA Drop Down Weights 12
7.6 Polling Rates 13
8 Port Management 15
8.1 OLT Port Management 15
8.1.1 Configuring Port in Loop Back 16
8.1.2 Manage Flow Ctrl Parameters 16
9 OLT Traffic Management 17
9.1 Bridging Configuration 17
9.1.1 Changing the bridging mode for a particular logical link 18
9.1.2 Provisioning a link in a Dedicated VlAN 19
9.1.3 Provisioning a link in a Shared VLAN 19
9.1.4 Provisioning links in Transparent VLAN 19
9.1.5 Provisioning links in a Cross Connect 20
9.1.6 Provisioning Priority VLANs 20
9.1.6.1 VID Field 20
9.1.6.2 Upstream CoS 20
9.1.6.3 Max/Min Range 21
9.2 Provisioning Filtering Rules 21
9.2.1 Selecting the Port for Filtering 21
9.2.2 Using the Rule Grid 21
9.2.3 Constructing an OLT Filtering Rule 22
9.2.4 Adding a Filtering Rule 23
9.2.5 Deleting a Filtering Rule 23
9.3 L3 Switching 24
9.3.1 DHCP Snooping Enable 24
9.3.2 DHCP Option 82 (Relay Agent Sub-Option…) 24
9.3.3 DHCP IPv4 Address Learning 24
9.3.4 ARP Snooping (Snoop ARP Frames…) 24
9.3.5 ARP Proxy 24

9.3.6 Dyn. IP Learn Table Size ... 24
9.3.7 DHCP Relay Agent IP SA ... 25
9.3.8 DHCP Timer Interval ... 25
9.3.9 DHCP Resp. Timer Interval ... 25
9.3.10 IPv4 Dynamic Filter Table ... 25
10 Alarms ... 26
10.1 Viewing Alarms ... 26
10.2 Enabling alarm auditing ... 28
10.3 Setting Alarm Thresholds ... 29
10.4 Enabling Alarm Soaking ... 30
11 ONU Data Path Configuration ... 31
11.1 ONU Queue Configuration ... 31
11.1.1 Entity Selection Control ... 31
11.1.2 Provisioning Number of Logical Links to Register ... 32
11.1.3 Provisioning Number of User Ports ... 32
11.1.4 Provisioning Downstream FIFOs ... 33
11.1.5 Provisioning Upstream FIFOs ... 34
11.1.6 Committing the Provision to ONU Firmware ... 34
11.1.7 Saving the Configuration to the Hard Disk ... 35
11.1.8 Restoring the ONU to a Previous Configuration ... 35
11.1.9 Deleting a Saved Configuration ... 35
11.2 Selecting Lookup Fields ... 36
11.2.1 Selecting a Classification Engine ... 36
11.2.2 Field Select Table ... 36
11.2.2.1 Index ... 36
11.2.2.2 Name ... 36
11.2.2.3 RefCount ... 37
11.2.2.4 LayerSel ... 37
11.2.2.5 Dword ... 37
11.2.2.6 BitOffset ... 37
11.2.2.7 FieldWidth ... 37
11.2.3 Editing a Lookup Engine Field ... 37
11.2.4 Applying the Configuration ... 38
11.2.5 Refreshing the View ... 38
11.3 Designing the ONU Classification Scheme ... 39
11.3.1 Constructing an ONU Classification Rule ... 40
11.3.2 Using the Rule Grid ... 41
11.3.2.1 Adding a Rule to the Classification Scheme ... 41
11.3.2.2 Deleting a Rule ... 42
11.3.2.3 Understanding FIFO Labeling (Q) ... 42
11.3.2.4 Applying the Configuration ... 43
11.3.2.5 Refreshing the View ... 43
11.4 Provisioning Filtering Rules ... 44
11.4.1 Selecting the Port for Filtering ... 44
11.4.2 Using the Rule Grid ... 44
11.4.3 Constructing an ONU Filtering Rule ... 45
11.4.4 Adding a Filtering Rule ... 46
11.4.5 Deleting a Filtering Rule ... 46
11.5 GUI Authentication Function ... 49

1 Audience

This document is intended for engineers evaluating the Teknovus TK37XX family of integrated EPON solutions. The document explains how to use the TK37XX PC HOST GUI TeknovusEponSystemApp.exe, for the purpose of evaluating the functionality and usability of TK37XX Host Interface Protocol. This

manual assumes that the reader has a technical background and a base level of understanding regarding the basic operation of PON equipment, but does not assume any prior experience using the TK37XX or any other Teknovus product. The Teknovus PC Host GUI is a demonstration package, intended for evaluation purposes only.

2 Organization of the GUI

The screen real estate used by the GUI is divided — MDI style — into three sash windows. The upper left panel displays the entities that may be managed by the TK37XX Host Interface, including the OLT, ONUs and Logical Links. This sash window shall be referred to as the **Element Status Window**. Left clicking on an entity with the mouse will open a tabbed panel in the upper right sash window that may be used to manage the entity. This sash window shall be referred to as the **Entity Management Window**. The bottommost sash window is used for the purpose of logging the host interface message that are sent and received by the GUI, and shall be referred to as the **Message Log**. The Message Log displays the commands that are sent and received from the GUI as well as the raw bytes sent and received by the physical layer interface.

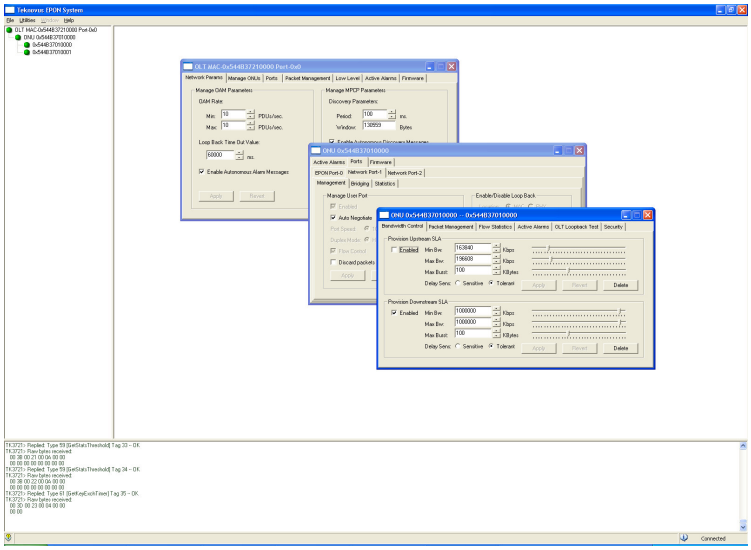


Figure 1: GUI Window

2.1 Basic Structure of GUI Software

The GUI software breaks down into 4 logical layers the first layer is the physical interface. The operating system, or driver resource, used to send and receive the raw Host Interface messages. The next layer consists of the underlying messaging system used by the GUI. This layer is responsible for parsing and queuing of Host Interface Messages as well as providing reliability. The next layer is the application layer. This layers responsibility is to display the GUI windows and provide services such as alarm auditing.

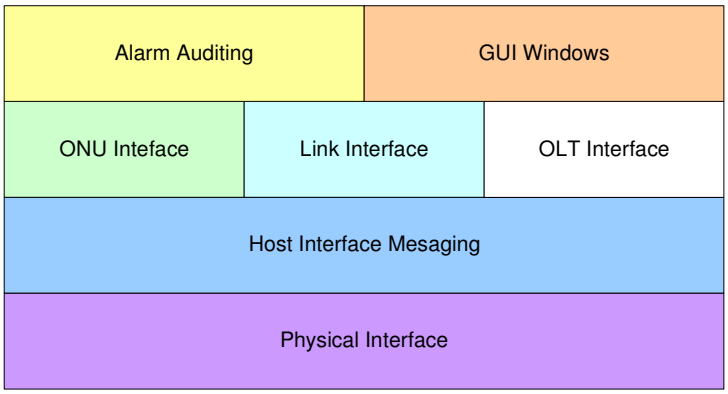


Figure 2: GUI Pancake Diagram

2.2 GUI Start Up Sequence

When the user invokes the TeknovusEponSystemApp.exe by double clicking on the T icon the GUI will perform the following functions:

Step 0: Attempt to establish a UDP connection to the TK3721. This process will continue indefinitely or until the connection is established.

Step 1: After the connection is established the GUI will test the interface by attempting to send and receive a host interface message. The natural choice (and the choice that the GUI will use) is the Get OLT Information. This message contains information about the TK3721 that the host may use to identify product version information.

Step 2: Once the interface has been established the next step the GUI shall perform is to obtain the list of discovered links. It should be noted that once the interface is detected the GUI shall initiate a process to handle autonomous events. Receiving an autonomous event will make the remaining sequence non-linear, as the autonomous events will be inserted into the GUIs message queues with other response messages, refer to the note on the GUI data path below.

Step 3: Once the GUI receives this list, it will query the links for the identity of their associated ONUs by issuing a Get ONU Info Host Interface Message for each link found in the list. Of course if an autonomous event (such as link discovery), occurs that event will also be processed simultaneously with the querying process. If the GUI is configured to authenticate its links, the link authentication will also take place. Again there is no set sequence and multiple LLIDs may be authenticated simultaneously.

Step 4: Having discovered the known managed entities the GUI will next query the TK3721 for the list of blocked links. These links will be displayed in the list of unassociated links in the managed entity status window. If the ONU is connected to the TK3721 and operating properly, then unblocking a

LLID will cause a new ONU to appear in the entity status window. The LLID will be associated with this new ONU.

Step 5: After the GUI has finished querying the OLT, it will remain in the idle state until the user performs some action. In the idle state the GUI will audit the OLT for alarm messages if configured to do so, otherwise it will not send any Host Interface Messages until the GUI operator directs it to do so, by initiating a query or provisioning action.

2.3 Note on the GUI data Path

The GUIs Data Path consists of simple non-blocking queuing mechanism that achieves very good utilization of OLT recourses. However in such a system there is no set sequence in which messages will be issued to the OLT. Thus that depending on very minor timing differences between command response times, the GUI event log trace will be different. It is important to note that all host interface messages are required to encapsulate a complete set of provisioning operations and therefore do not require that provisioning actions be performed in any set sequence.

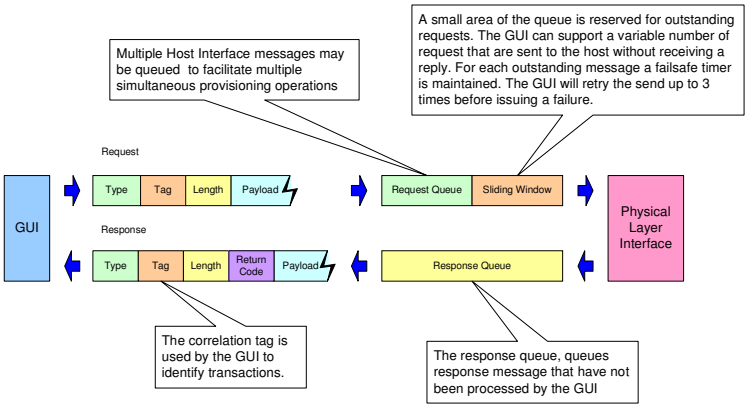


Figure 3: GUI Data Path

3 Basic Operation of the GUI

As stated earlier, left-clicking the mouse on an entity in the Status Window shall cause an associated tabbed dialog to appear in the Management Window. This dialog exposes nearly the entire set of host interface commands associated with the managed entity. The tabs are organized into roughly the same categories as the TK37XX Host Interface document. And with few exceptions all of the panels function similarly.

3.1 GUI Controls

All controls in the GUI are derived from a common set of base classes and thus operate in similar ways. Most panels include 1 or two buttons that invoke the GUI to perform various transactions with the OLT. All such controls having the same basic function will also be given the same label. For simplicity of understanding an explanation of each button type appears bellow.

3.1.1 Apply Button

Most GUI panels manage only a single TK3721 Host Interface message. Every time the panel is displayed the GUI will automatically query the OLT for the latest attributes by issuing the appropriate Host Interface Message to the TK3721 firmware. If the query operation is successful the panel will be updated with the latest values from the firmware. As a general rule, when the panel is updated from a host interface message the associated Apply button will be disabled to indicate that the values displayed are an accurate reflection

of the current state of the managed entity associated with the panel. If an error occurs the Apply button will not be disabled indicating that the displayed values are not those of the managed entity. Changing a GUI widgets value will cause the Apply button to be enabled allowing the GUI operator to apply the new provisioning to the managed entity.

3.1.2 Refresh Button

Button's labeled refresh are never disabled. The action associated with a Refresh button is always to query the state of the associated attribute. The result of a successful Refresh operation will be the same as if the panel is viewed for the first time. That is, the OLT will query the managed entity associated with the panel, and if the operation completes the Apply Button will be disabled.

3.1.3 Revert Button

The Revert Button had identical functionality to the Refresh button, but is semantically different. The idea behind the Revert Button is that you can "revert" the panel's state to the initial state of the panel prior to changing a GUI widget. Semantically, once the apply button has been pressed it is not possible to revert. The Revert Buttons are currently being phased out in favor of the Refresh Button.

3.1.4 Defaults Button

The Defaults Button is used to restore the managed entity to the default settings found in the Host Interface document. This mechanism employs a "canned" Host Interface Message that will be issued to the OLT when the button action is invoked by left clicking on the button.

For most commands a provisioning operation will also result in a subsequent query. In such cases the Apply Button will not be disabled until the query operation completes. This audit mechanism ensures that the values displayed by the panel are the same values stored in the relevant managed entity. For a few Host Interface Messages the granularity of the data is less than that of the provisioned value.

Some Apply actions result in multiple commands being issued to the OLT.

4 GUI Panel Directory

This section describes the various panels found in the GUI, their function, and the method by which they may be used to test the TK37XX Host Interface. The Panels are organized by entity and generally follow the order in which they appear in the associated tabbed dialog box. In the rare case that the GUI abstracts some detail of the host interface, a flow chart of the message exchange sequence is presented. Where the message performs a complex operation on the PON a related diagram may be present as a visual aid. Most panels are subdivided into boxes with each box controlling exactly one host interface message. In most cases the attributes are presented in the same order (as read from top to bottom) as that in which they appear in the Host Interface Message. Thus for the most part the remainder of this document is simply a rehashing of the descriptions already available in the Host Interface Document.

Force link rediscovery de-registers a Logical Link, while allowing it to re-register, as if it had been newly attached to the EPON network. This command is useful, for example, when the Network operator wants to be able to force a re-arrival as part of their debugging process to try to clear a problem, or to re-authenticate the user/ONU on that link.

The Block Link command prevents the given Logical Link (MAC address) from registering on the EPON. The OLT will simply ignore registration requests from the blocked ONU. If the given ONU is already registered, the Logical Link will be deregistered, causing the ONU to depart from the network. All further requests to register from the ONU are ignored until the Host issues an Unblock Link command.

Up to 256 ONU labels (MAC addresses) can be on the block list at one time.

Link blocking is intended to be a temporary measure used to suspend service for reasons such as late payments or a troublesome customer. When the issue has been resolved, or the ONU has been physically removed from the network and no longer requests service, it can be removed from the blocked list with the Unblock Link command. If the ONU is still connected to the network and attempting to register, the ONU will be once again allowed onto the network.

Service provisioning such as SLAs or Bridging modes are not affected by the Block Link command. Any ONU provisioning should be deleted with the appropriate other commands, if desired. A blocked link will appear with a black status icon.

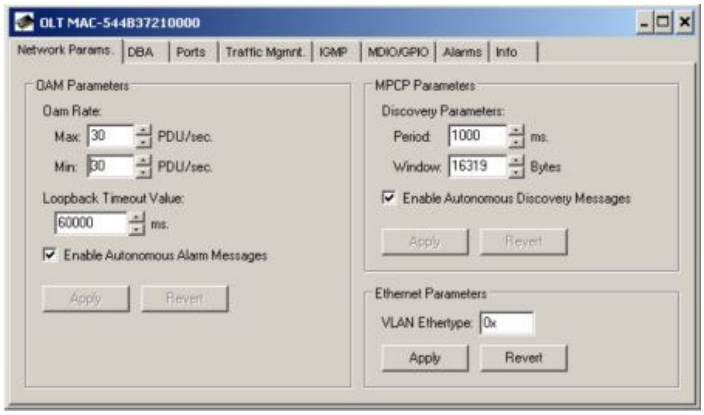
Please note the difference in the behavior with respect to the Block Link command where an Unblock Link is required to undo its effect. Link Rediscovery invites the ONU to re-register this link with the network, while Block Link prevents the ONU from returning on that link after de-registration.

5 OLT Panel

The OLT panel is used to apply settings to OLT attributes. In some cases this may also involve OAM transactions with ONUs. It should be noted that certain attributes of the OLT such as SLAs are controlled via the Link Panel.

6 OLT Network Parameters

These commands allow the host to configure the way the PON will be managed.



6.1 OAM Rate

This command is used to view the default OAM rate

6.2 Loopback Timeout Value

This sets the loopback failsafe timer. If the operator sets a port in loopback mode the loopback the OLT will initiate a count down timer for Loopback Timeout Value ms. When the timer expires the loopback will automatically be canceled.

6.3 MPCP Parameters

6.3.1 Period

The interval at which the OLT will issue a discovery gate.

6.3.2 Window

The discovery window size in bytes.

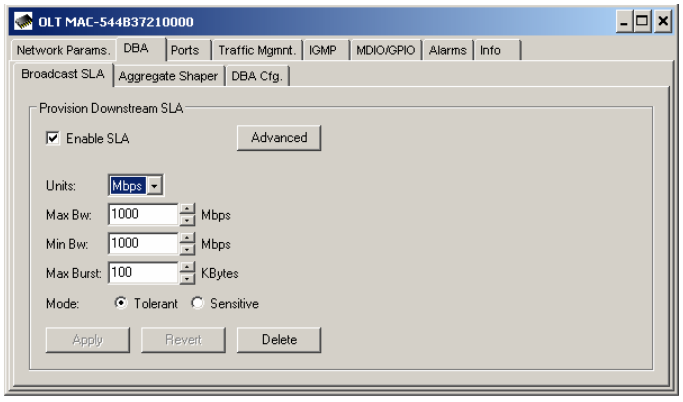
6.3.3 VLAN Ethertype

This is the Ethertype value that the OLT will use to classify VLAN traffic (default = 0x8100)

7 DBA

The DBA tab allows the user to control virtually every parameter of the TK3721's highly flexible and efficient Hierarchal Weighted Round Robin DBA algorithm. The DBA algorithm supplied with the OLT is similar to algorithms found in high performance ATM switches and is capable of issuing 4 grants every 282 micro seconds, by far the fastest cycle time of any EPON system deployed today. The TK3721's DBA can meet 1 ms. latency requirements for high priority services in a 32 ONU deployment.

7.1 Broadcast SLA



This command is identical to the functionality of the Link SLA Panel except that it is used to provision an SLA for the broadcast channel, as apposed to a unicast link. This unique feature of the OLT allows the OLT To use its large 40Meg buffer ram to serve the requirements of all ONUs, resulting in a 1:32 cost reduction (assuming 32 ONU deployment).

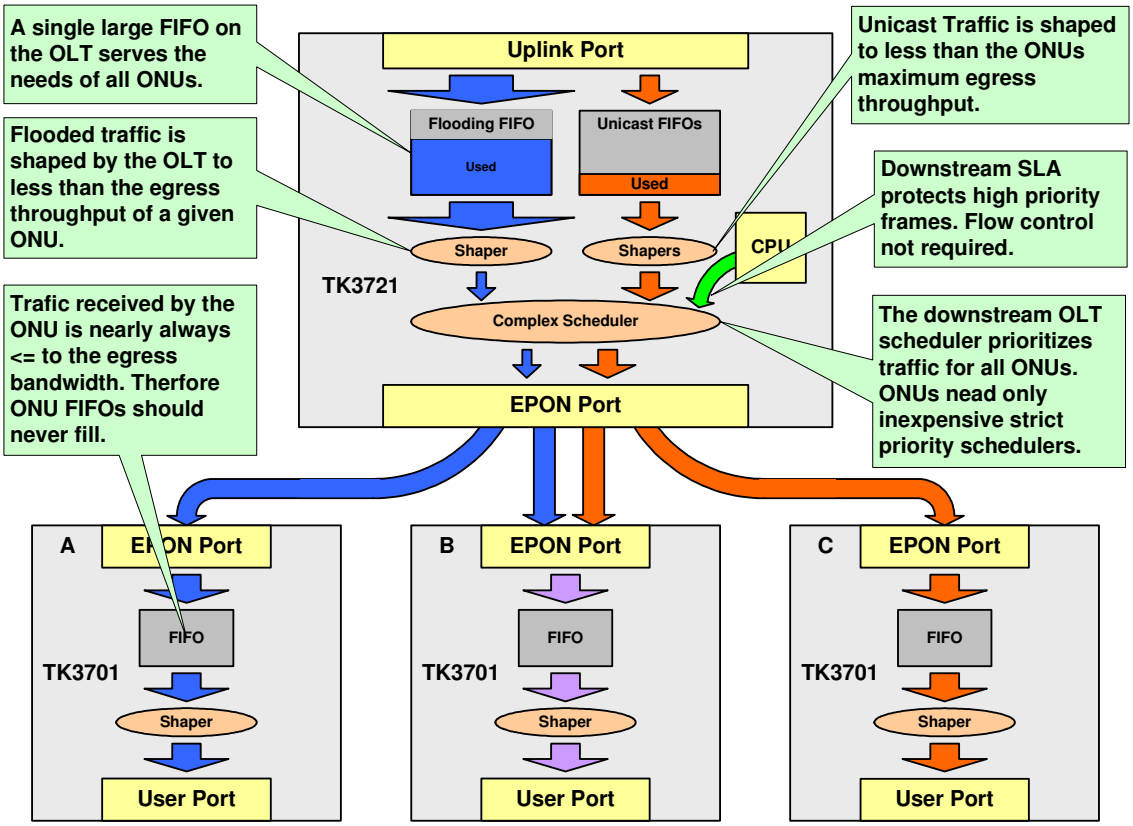
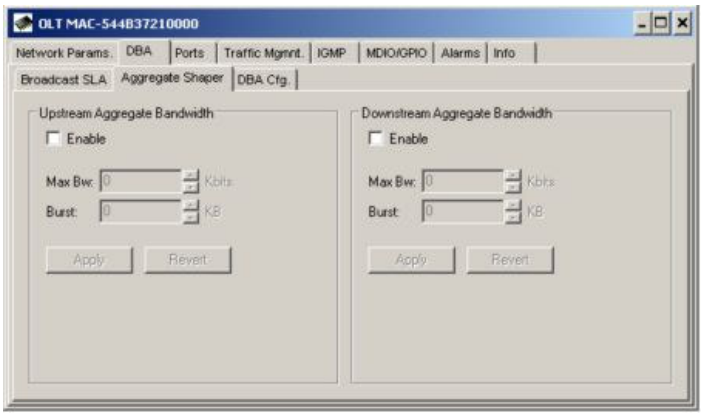


Figure 4: Use of broadcast SLA

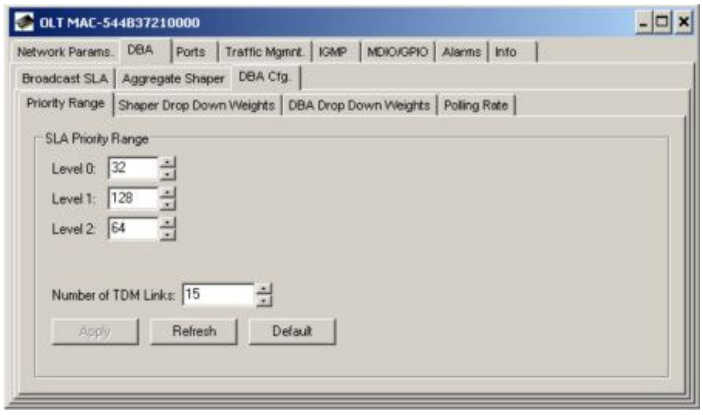
7.2 Aggregate Shaper



This command lets the Host restrict the bandwidth available to the OLT for user data traffic in each direction. This feature can be used to protect the core network from bursty upstream flows and increase the accuracy of SLA enforcement. Aggregate bandwidth control can be disabled by setting the parameters to zero; the feature is disabled by default.

For accurate Min SLA enforcement. Teknovus recommends that the upstream aggregate shaper be provisioned for 50-100Mbps less than the maximum bandwidth of the PON. Typical values are 800-850Mbps.

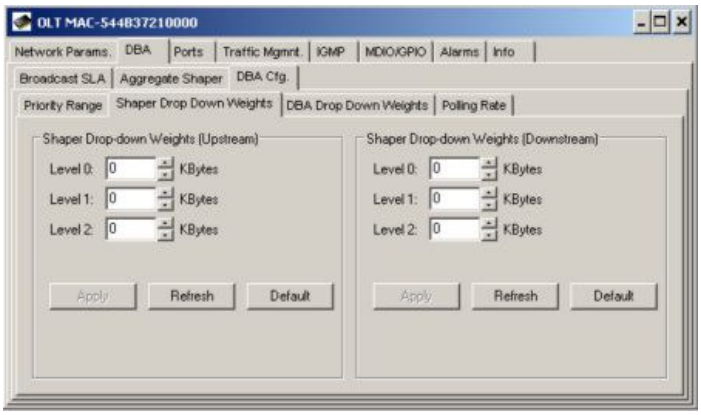
7.3 Priority Range



The priority range determines how many links may be registered in each priority level. This command should be applied immediately before registering any links, or after links are deregistered using the Disable OLT command. It is a good idea to configure the OLT in strict boot mode, allowing the host software time to apply this command and then explicitly enable the OLT to register links.

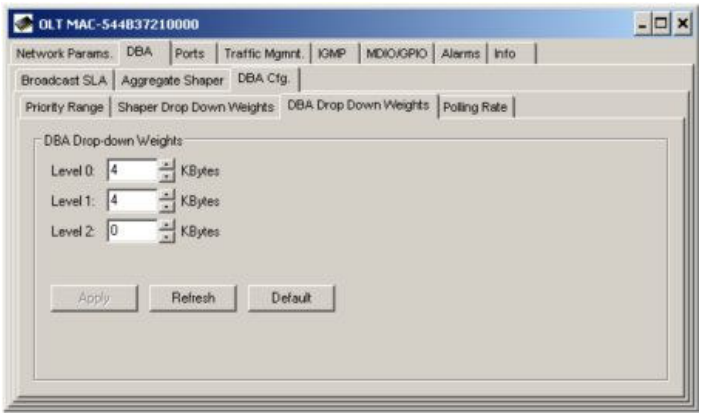
The OLT must be disabled prior to applying this command; otherwise the OLT FIFOs will become corrupt. It is recommend that this operation be performed once during the initial bring up of the PON.

7.4 Shaper Drop Down Weights



This command is not available for the TK3721, and applies to future chipsets only. The TK3721 has a strict priority FIFO scheduler.

7.5 DBA Drop Down Weights



DBA drop down weights are used by the DBA to reserve bandwidth for each priority level. This allows the OLT to fix the latency and reserve a percentage of bandwidth for links in each priority level.

The drop down weight for priority level n **MUST** be greater than or equal to the provisioned DBA Weight for all links in priority level n + 1.

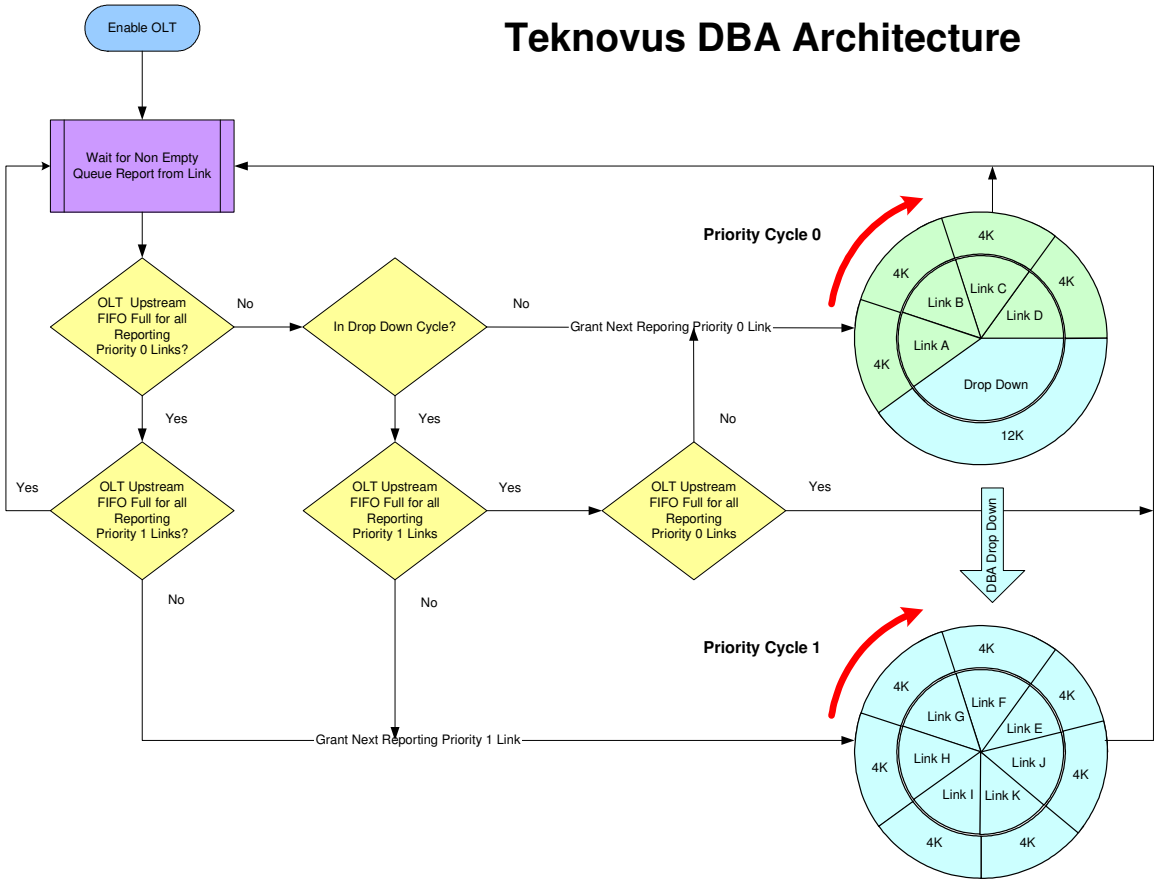
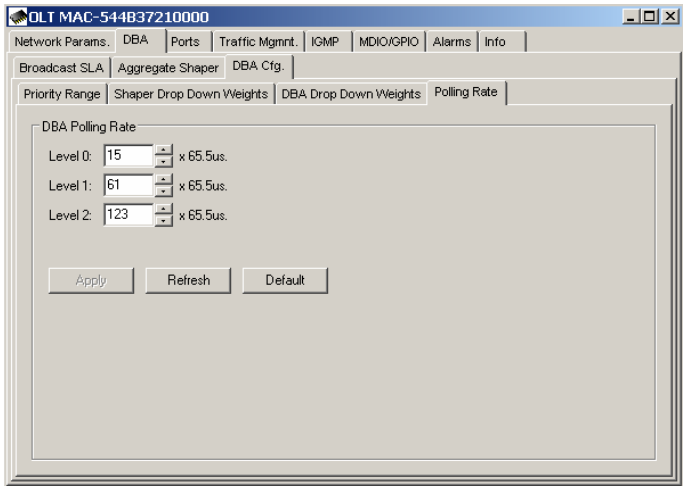


Figure 5: Basic DBA Architecture

7.6 Polling Rates

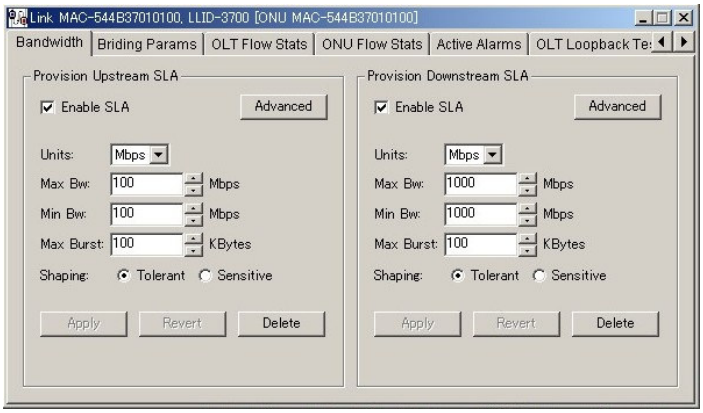


The polling rates panel allows the operator to configure the rate at which each link will be solicited to determine if it has any data to transmit. Smaller values result in lower latency and increased overhead. For priority 0, the scheduling latency is approximately equal to the larger of the polling rate and the cycle length.

7.7 Service Level Agreements

Every element scheduled by the OLT has an associated SLA record which can be configured by the Teknovus GUI or other host systems.

7.8 Unicast SLA



Every Logical Link registered by the TK3721 has an associated SLA maintained by the TK3721, and stored internally in its NVS database (if enabled to do so). In the upstream direction, the TK3721 uses a reporting mechanism specified by 802.3ah to monitor the status of each registered link. When a particular Link's FIFO(s) has data to send this information will be conveyed to the OLT in the form of a report message. The OLT will use this information and the SLA associated with the link to schedule a time slot in which the link may transmit its data. Because the OLT schedules the links, rather than relying on mechanisms in the ONU, service contracts are enforced in the central office, and excess bandwidth may be allocated efficiently. SLA enforcement is accurate to within 2% of the provisioned value.

7.8.1 Enable SLA

If checked, the OLT will allow the element to transmit user data.

7.8.2 Max Bw

Configures the maximum sustained rate at which a link may transmit data.

7.8.3 Min Bw

Configures the sustained rate at which the user may transmit without loss of data, this value should always be less than or equal to Max Bw.

7.8.4 Mode

Determines the scheduler level

From the perspective of the GUI or other external devise managing the TK3721 "Delete" semantically equivalent to restore factory default and "Create" is equivalent to change the SLA from default value.

7.8.5 Enable SLA

This attribute allows the host to disable SLA's

- It is important to note that though the logical link panel appears grouped under the ONU, logical link attributes are NOT necessarily attributes of the ONU itself. Logical links ALWAYS make two associations one with the ONU and one with the OLT. Unless explicitly specified, logical link parameters may be parameters of the OLT, ONU or both. It is best to assume that ALL operations performed on a logical link involve OAM transactions with the ONU.

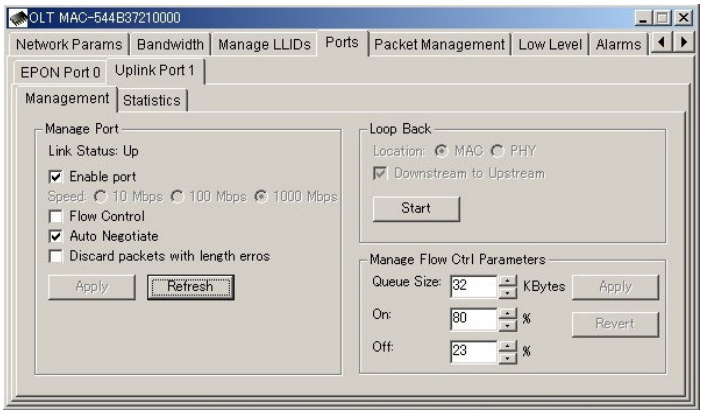
- Though the TK3721 has a Min/Max FIFO scheduler in the upstream direction, the DBA is not directly influenced by the Min scheduler. Instead it responds to signals generated by queue depth. To ensure that the Min's are scheduled accurately it is necessary to restrict the total upstream bandwidth of the PON by 50 to 100Mbps. This can be accomplished by provisioning an aggregate SLA.

- As per IEEE 802.3ah, any ONU admitted to the network will be granted a small amount of bandwidth sufficient for minimal OAM operation, even if the SLA is disabled. A disabled SLA can use up to 256K. As per specification the ONU is not aware of SLA's, and thus will continue to transmit user data which will be dropped by the OLT. To prevent the ONU from transmitting this unwanted data it is recommended that the ONU be configured in strict boot mode. In this mode the ONU will ONLY transmit user data after the host software has explicitly enabled it to do so.

- In strict (or host driven) boot mode the SLA will be configured in the disabled state every time the link is registered. In auto-boot mode the state of the SLA is enabled by default and stored in the OLT NVS if NVS is enabled.

8 Port Management

8.1 OLT Port Management



Allows the user a simple interface to control port parameters such as line speed and flow control. If Auto Negotiation is enabled, the speed and duplex settings used will be based on the result of negotiating with the link partner. Default values depend on the personality settings. The table below describes the Set command. In the current firmware release, flow control is not auto negotiated. If flow control is enabled the firmware will configure the Phy to advertise flow control. Note however that pause frames will be transmitted regardless of the capabilities reported by the link partner.

8.1.1 Configuring Port in Loop Back

Allows the user to set a loopback, currently the loopback position must be set to MAC.

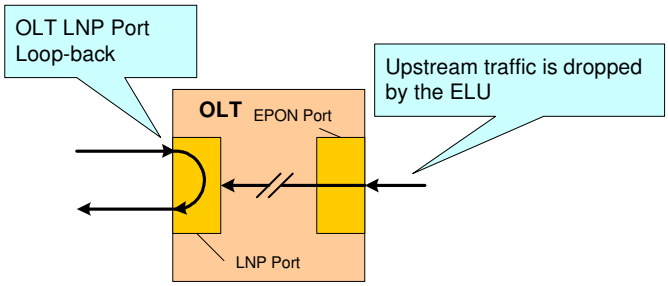


Figure 6: Uplink Port Loopback

8.1.2 Manage Flow Ctrl Parameters

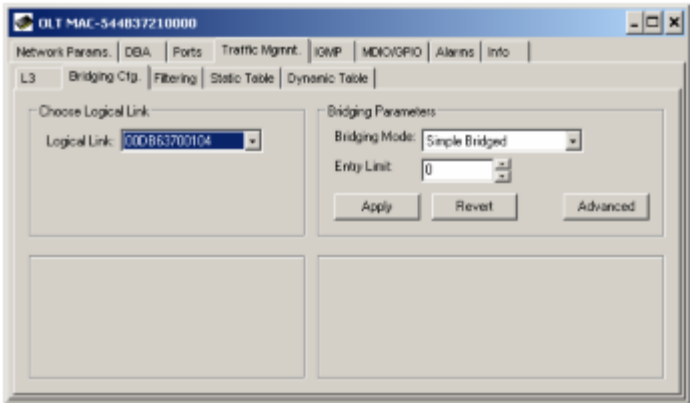
Sets the flow control on/off threshold values.

For the Flow Ctrl thresholds: the precision of the values is less than the displayed percentages. So small changes between the provisioned and actual value may exist

9 OLT Traffic Management

The traffic management panel allows the user to change bridging modes, apply complex filters, and expose many of the OLTs advanced hardware and software features related to traffic management.

9.1 Bridging Configuration

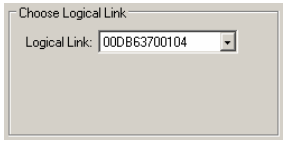


This panel facilitates provisioning of the bridging mode for each link, as well as the size of the dynamic forwarding table on a per link basis. If the bridging mode supports VLAN, the VLAN tag or tags may be specified using this panel. For certain VLAN modes such as priority shared VLAN multiple links may be provisioned in the same VLAN. These modes will make forwarding decisions based on multiple fields such as MAC address and VID.

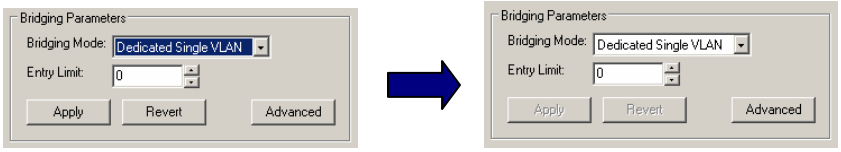
A link may be provisioned in only one bridging mode. However, multiple links, each provisioned in a different mode, may be associated with a given egress ONU port.

9.1.1 Changing the bridging mode for a particular logical link

Step 1. Choose the logical link

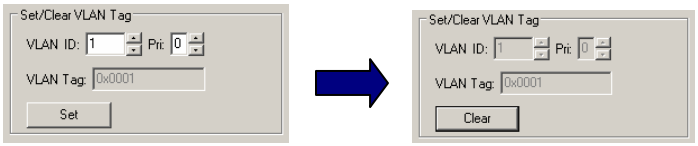


Step 2. Apply the new bridging mode.



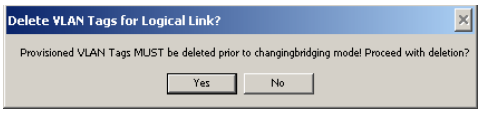
Notice that after the bridging mode has been applied the Apply button will change to a grey color.

Step 3. Apply the VLAN provisioning.



Notice that after the VLAN has been provisioned the panel will change to a grey color. The user must delete the VLAN provisioning before applying a new tag value.

Once a VLAN has been provisioned, the OLT will not permit the bridging mode to be changed without first deleting the VLAN provisioning. If an attempt is made to change the bridging mode, the GUI will display a dialog box allowing the user an opportunity to automatically delete the VLAN provisioning.

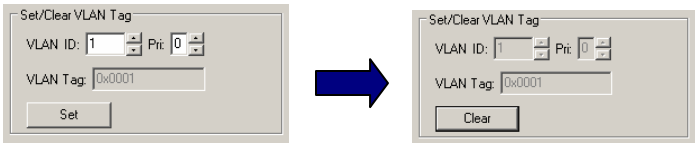


Clicking “Yes” will delete the VLAN tag and change the bridging mode. Clicking “No” will abort the operation.

The exact panel used to apply VLAN provisioning will change based on the provisioned VLAN mode.

9.1.2 Provisioning a link in a Dedicated VlAN

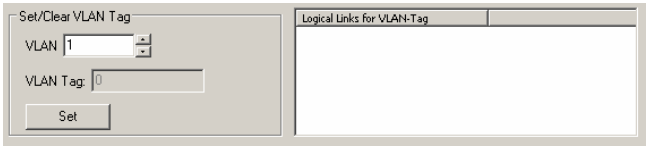
Dedicated VLAN modes associate a single VLAN tag with a particular Logical Link. The provisioned priority field (CoS) will be added to upstream frames. However, only VID is used to make a downstream bridging decision. VLANs are terminated by the TK3721.



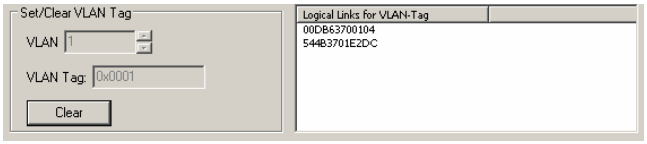
Once a value has been entered for VLAN ID and Pri (CoS), the "Set" button may be used to apply the provisioning. The "Clear" button is used to delete the provisioned tag.

9.1.3 Provisioning a link in a Shared VLAN

Shared VLAN modes associate multiple links with a single VLAN. The upstream CoS inserted by the TK3721 is always 0.



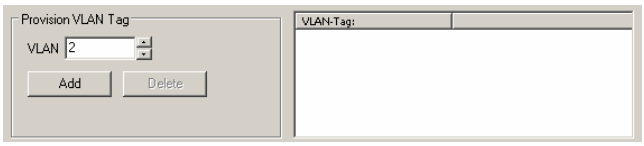
Notice that the panel features a "Set" button similar to the panel used to provision the dedicated VLAN. This button has identical functionality.



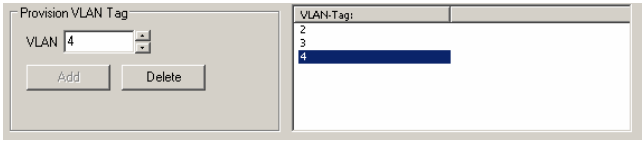
In addition to the VLAN provisioning box, a second box appears to the right that is used to display a list of all logical links in the provisioned VLAN. No links will be displayed in this box until the VLAN provisioning is applied. Clicking on a logical link in this list allows the user to quickly change the context of the panel to the other logical link. This is useful when changing links to a different VLAN.

9.1.4 Provisioning links in Transparent VLAN

Transparent VLAN uses the VLAN tag for downstream bridging decisions but does not modify the tag. A single link may be provisioned with multiple VIDs. It should be noted that the CoS field is not used for bridging decisions. Upstream frames shall be bridged regardless of the Tag value.



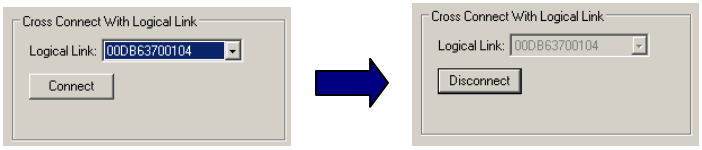
The "Add" button is used to add a VID and the "Delete" button is used to remove a VID.



A box to the right of the provisioning window is used to display all of the VIDs associated with a particular logical link provisioned in Transparent VLAN. Selecting a VID in the box moves it into the provisioning window, allowing it to be quickly deleted. Once a VID is deleted the VLAN field in the provisioning window will take on one of the other provisioned values, allowing all VLANs to be quickly deleted with repetitive mouse clicks.

9.1.5 Provisioning links in a Cross Connect

Cross Connects are used to create a private link between two ONUs on the same PON. For instance, a link Cross Connect might be used to facilitate data communication between two offices within the same organization. Both links must be provisioned in the Link Cross Connect mode before a Link Cross Connect can be established. Once both links have been provisioned in Cross Connect mode, use the Connect button to bridge the links.



Once cross-connected the control will gray out indicating that the action was completed successfully.

Only a single Cross-Connect may be established with any given link.

9.1.6 Provisioning Priority VLANs

Priority VLANs use the ToS or CoS field to make bridging decisions. The decision of which field should be used is based on a per link attribute, however, in the TK3721 this is a global setting. Once one link has been provisioned in a priority VLAN, all links MUST provision the ToS/CoS select the same way. It should be noted that if L3 switching is used only ToS may be used for the priority field.

9.1.6.1 VID Field

This field allows the user to select the VID. The VID will be inserted into upstream frames arriving on links provisioned in the VLAN. Downstream the VID will be used for classification.

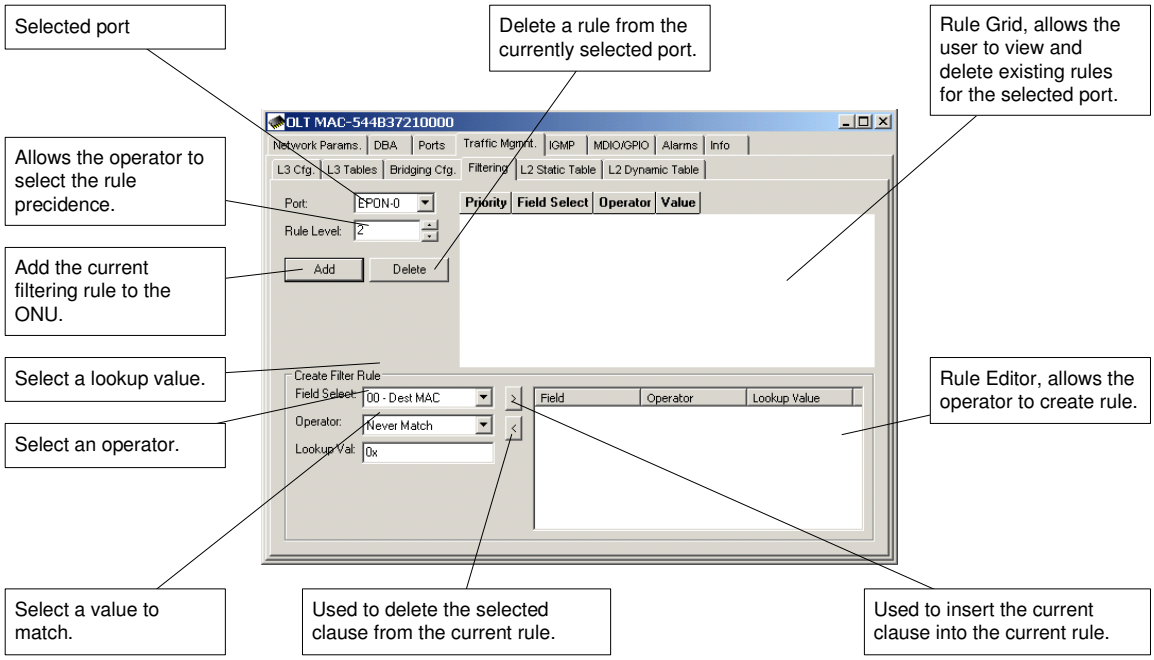
9.1.6.2 Upstream CoS

The upstream CoS is the CoS value that will be inserted into upstream frames, forwarded on the VLAN. It is VERY important to notice that a unique upstream CoS and VID combination defines a unique VLAN. For every link provisioned in a unique VLAN, EVERY attribute in the VLAN record other than the link label, MUST be identical. Identical, means that for link A and link B provisioned in VLAN C a bitwise comparison of the two records used for provisioning would show equality. If this is not the case the TK3721 will not function correctly, and NVS erase followed by system reset may be required to restore proper functionality.

9.1.6.3 Max/Min Range

Allows the user to provision an INCLUSIVE range of priority values used for downstream classification. Packets with matching VID and a CoS/ToS value in the range specified will be classified onto the VLAN. It is VERY important that for every VID, there exists VLANs $\{V_0, V_1, \ldots, V_n\}$ such that together they specify a complete range [0 7] with no holes. Also note that for any two unique VLANs with VID=A, it is illegal that the two VLANs Max/Min contain ANY overlapping regions (e.g. [0, 4] and [4, 7] would be illegal).

9.2 Provisioning Filtering Rules



This panel allows the operator to create rules to filter (drop received frames), based on many different criteria (Rules).

9.2.1 Selecting the Port for Filtering

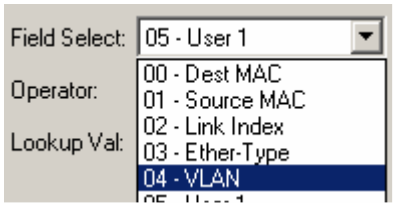
The Port to Filter is selected using the Port drop down box.

9.2.2 Using the Rule Grid

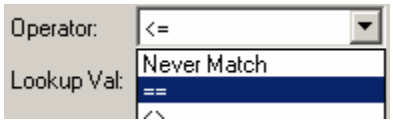
The Filtering Panel Rule Grid is almost identical to the Classification Panel Rule Grid, except that the Q column is absent, as it is not required.

9.2.3 Constructing an OLT Filtering Rule

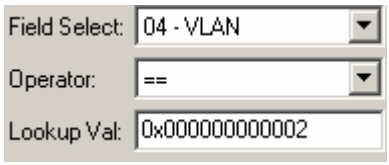
Step 1. Choose the Field Select. Field Selects defined by the OLT are given a descriptive label.



Step 2. Choose an appropriate Operator. The operator tests the portion of the frame specified by the field select.

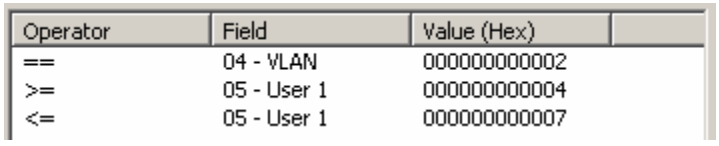


Step 3. Choose an appropriate Lookup Value. This is the value that will be used by the operator in the comparison. This step is only applicable to binary operators. If the operator selected is unary (such as Field Exists) the Value field will be disabled.



Step 4. Add the clause to the Rule Editor using the left arrow button. Note that the right arrow button can be used to remove a selected clause from the Rule Editor.

Step 5. Repeat steps 1-4 until the desired rule has been created. The TK3711 supports a maximum of 2 clauses / rule. The TK3701 supports a maximum of 8 clauses / rule.

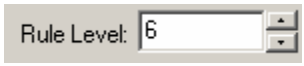


Operator	Field	Value (Hex)
==	04 - VLAN	000000000002
>=	05 - User 1	000000000004
<=	05 - User 1	000000000007

9.2.4 Adding a Filtering Rule

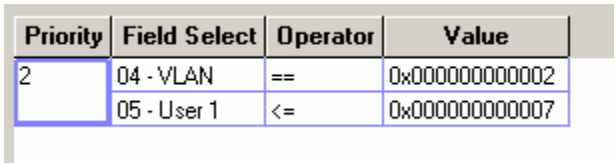
Step 1. Select the Port to Filter.

Step 2. Set the rule precedence level. The Rule Level may be configured for 1 of 8 different precedence levels, 0 being the highest priority and 7 being the lowest. Currently the precedence level of user provisioned filtering rules is of little importance.



Step 3. Add the filtering rule to the OLT by clicking the Add button.

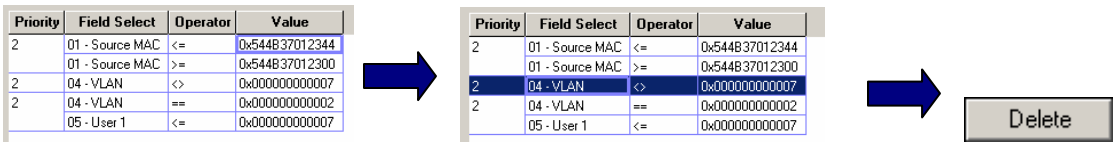
Adding a filtering rule will cause the OLT to be updated without an additional apply action.



Priority	Field Select	Operator	Value
2	04 - VLAN	==	0x000000000002
	05 - User 1	<=	0x000000000007

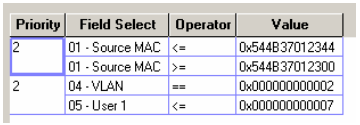
9.2.5 Deleting a Filtering Rule

Once a filtering rules has been added the rule may be deleted by selecting it from the Rule Grid and clicking the Delete button.



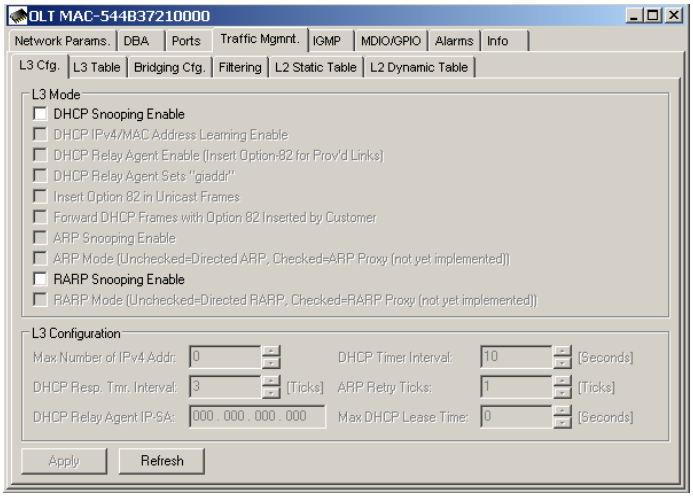
Priority	Field Select	Operator	Value
2	01 - Source MAC	<=	0x544B37012344
	01 - Source MAC	>=	0x544B37012300
2	04 - VLAN	<>	0x000000000007
2	04 - VLAN	==	0x000000000002
	05 - User 1	<=	0x000000000007

Once the rule has been successfully deleted it will be removed from the Rule Grid.



Priority	Field Select	Operator	Value
2	01 - Source MAC	<=	0x544B37012344
	01 - Source MAC	>=	0x544B37012300
2	04 - VLAN	==	0x000000000002
	05 - User 1	<=	0x000000000007

9.3 L3 Switching



The OLT may be configured as an L3 bridge, enabling the OLT to learn IPv4 destination addresses. The L3 panel allows the user to configure the OLT for L3 switching. This operation should generally be performed prior to applying any VLAN provisioning. Bridging configurations that make use of the CoS field are incompatible with L3 switching. The primary advantage of L3 switching is security. L3 switching enables the OLT to direct ARP and RRARP frames based on the learned IP address, making the network less susceptible to MAC spoofing attacks.

9.3.1 DHCP Snooping Enable

This parameter enables the OLT to learn IP frames based on snooping DHCP offer messages.

9.3.2 DHCP Option 82 (Relay Agent Sub-Option…)

If L3 switching is enabled the OLT may be configured as a DHCP relay agent (RFC 3046.) This will enable the OLT to insert the Relay Agent Sub-Option into snooped frames.

9.3.3 DHCP IPv4 Address Learning

Enables IPv4 address learning via DHCP snooping. Frames shall not be forwarded until L3 address is learned. ARP frames shall be unicast to appropriate link.

9.3.4 ARP Snooping (Snoop ARP Frames…)

Enables the OLT to classify ARP frames into its processor FIFO. This allows the OLT to redirect the frames based on learned IPv4 destination address.

9.3.5 ARP Proxy

This is future functionality and will be described upon completion.

9.3.6 Dyn. IP Learn Table Size

Specifies the number of IP addresses that may be learned.

9.3.7 DHCP Relay Agent IP SA

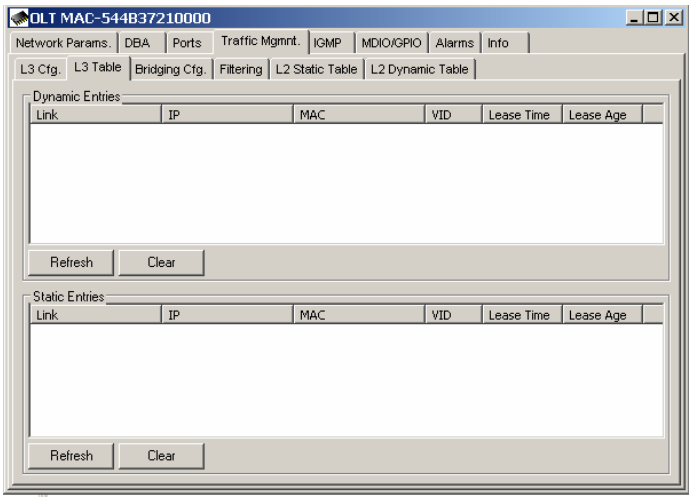
Specifies the IP source address to be used for the relay agent. This is the address to be used for grAddr , inserted into DHCP frames modified by the OLT.

9.3.8 DHCP Timer Interval

Placeholder

9.3.9 DHCP Resp. Timer Interval

9.3.10 IPv4 Dynamic Filter Table



The learned IPv4 address table is exposed by the L3 Table tab on the GUI

If any of the checkboxes in the Mode box are checked the L3 switching shall be enabled. Otherwise L3 switching is disabled.

If desired, Relay Agent IP SA may be provisioned with the same value as the IGMP Proxy.

All L3 parameters must be selected in-order for the OLT to insert DHCP Option 82 into upstream DHCP frames.

Currently the OLT appends DHCP Option 82 to all L3 frames.

The Relay Agent IP must be an IP on the same subnet as the DHCP server.

If the L3 switching function is enable the Dyn. IP Learn. Table Size field should be provisioned with a non-zero value.

10 Alarms

The OLT alarms manger works in concert with the ONUs to provide enhanced management capabilities and complementary set of OLT specific alarms. Features include:

- A common management interface for ONU and OLT alarms
- Soak of alarms on a per alarm ID basis
- Auditing of all alarms known to the OLT
- Setting of alarm thresholds for ONU and OLT alarms
- Autonomous alarm reporting

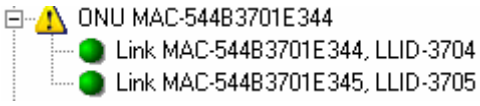
10.1 Viewing Alarms

Unlike the ONU CLI the OLT CLI does not offer any ability to control the alarms manger. Fortunately the Teknovus Evaluation Kit GUI exposes all of the underlying functionality.
Observing Alarm Events
Alarm may be observed remotely via the Teknovus Evaluation Kit GUI, in 4 ways:

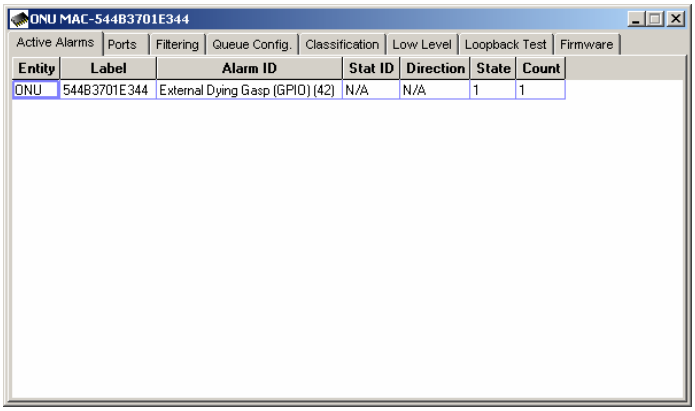
The GUI Log Window will display all autonomous alarm messages received from the OLT's 10/100 craft port. If alarm auditing is enabled the GUI may also be configured to display messages received based on the audit.

```
TK3721> Replied: Type 32769 [AutoAlarmReport] Tag 107 -- OK
TK3721> Raw bytes received:
   80 01 00 6B 00 0A 01 54
   4B 37 01 E3 44 42 01 01
```

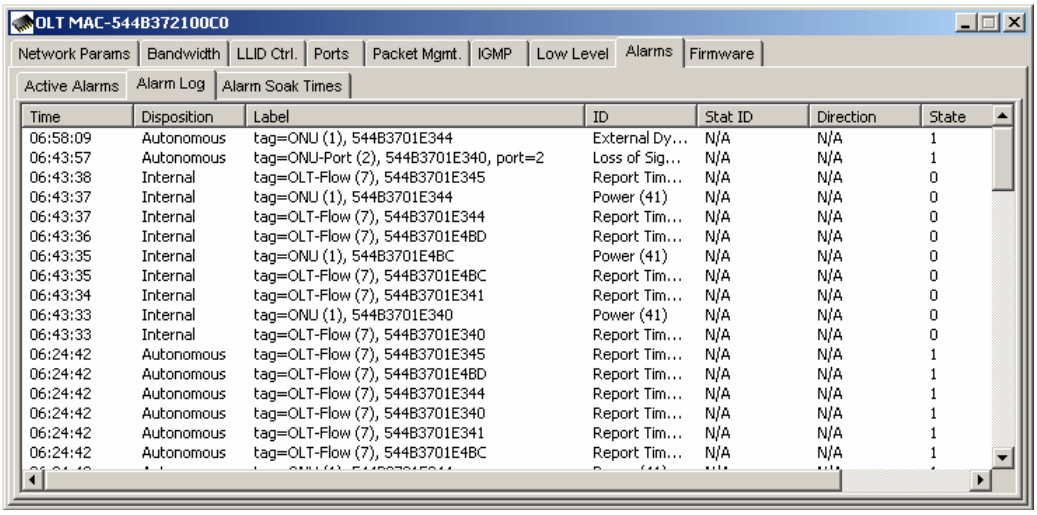
The appropriate Status Icon will change to a yellow triangle indicating that an alarm is raised.



The Active Alarms panel associated with the alarmed entity will indicate the exact alarm that has been received from the host interface. This record will be maintained until an event causes the alarm to clear. Alarms will be cleared when the GUI receives a clear alarm message or another network event signifying that the alarm condition is no longer present.



The GUI Alarm Log will display a new entry, retained until the GUI is terminated. The GUI Alarm Log will indicate the way in which a particular alarm was detected, or the reason why it was cleared in the column labeled Disposition. The GUI has 3 different alarm "dispositions": autonomous, audit, and internal.



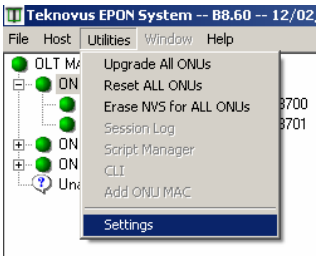
Time	Disposition	Label	ID	Stat ID	Direction	State
06:58:09	Autonomous	tag=ONU (1), 544B3701E344	External Dy...	N/A	N/A	1
06:43:57	Autonomous	tag=ONU-Port (2), 544B3701E340, port=2	Loss of Sig...	N/A	N/A	1
06:43:38	Internal	tag=OLT-Flow (7), 544B3701E345	Report Tim...	N/A	N/A	0
06:43:37	Internal	tag=ONU (1), 544B3701E344	Power (41)	N/A	N/A	0
06:43:37	Internal	tag=OLT-Flow (7), 544B3701E344	Report Tim...	N/A	N/A	0
06:43:36	Internal	tag=OLT-Flow (7), 544B3701E4BD	Report Tim...	N/A	N/A	0
06:43:35	Internal	tag=ONU (1), 544B3701E4BC	Power (41)	N/A	N/A	0
06:43:35	Internal	tag=OLT-Flow (7), 544B3701E4BC	Report Tim...	N/A	N/A	0
06:43:34	Internal	tag=OLT-Flow (7), 544B3701E341	Report Tim...	N/A	N/A	0
06:43:33	Internal	tag=ONU (1), 544B3701E340	Power (41)	N/A	N/A	0
06:43:33	Internal	tag=OLT-Flow (7), 544B3701E340	Report Tim...	N/A	N/A	0
06:24:42	Autonomous	tag=OLT-Flow (7), 544B3701E345	Report Tim...	N/A	N/A	1
06:24:42	Autonomous	tag=OLT-Flow (7), 544B3701E4BD	Report Tim...	N/A	N/A	1
06:24:42	Autonomous	tag=OLT-Flow (7), 544B3701E344	Report Tim...	N/A	N/A	1
06:24:42	Autonomous	tag=OLT-Flow (7), 544B3701E340	Report Tim...	N/A	N/A	1
06:24:42	Autonomous	tag=OLT-Flow (7), 544B3701E341	Report Tim...	N/A	N/A	1
06:24:42	Autonomous	tag=OLT-Flow (7), 544B3701E4BC	Report Tim...	N/A	N/A	1

Explanation of GUI Alarm Dispositions		
Disposition	Applies to:	Description
Audit	All Alarms	The specified alarm event was discovered based on an audit of the ONU or OLT alarm manager.
Autonomous	All Alarms	The specified alarm event was discovered based on an autonomous alarm report, generated by the OLT or ONU.
Internal	Std. Dying Gasp, Power, Temperature, Keep Alive Timeout, Report Timeout, Gate Timeout, External Dying Gasp,	The alarm event was discovered based on an indirect observation of the system state, such as an autonomous discovery message. Alarm events of this type will always be clear events for alarms that signify link deregistration.

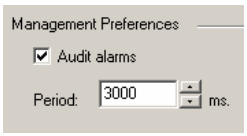
10.2 Enabling alarm auditing

The GUI can be configured to perform a periodic audit of the ONU and OLT alarms. By default this feature is disabled. To enable Alarm auditing follow the steps below.

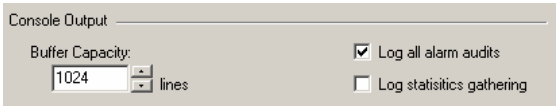
Step 1. Open the Settings dialog box as illustrated below:



Step 2. Click on the Audit alarms, check box. The Period field is used to determine the rate at which a single ONU/OLT is audited. The GUI ensures that the time between audits remain exactly the same for all entities.



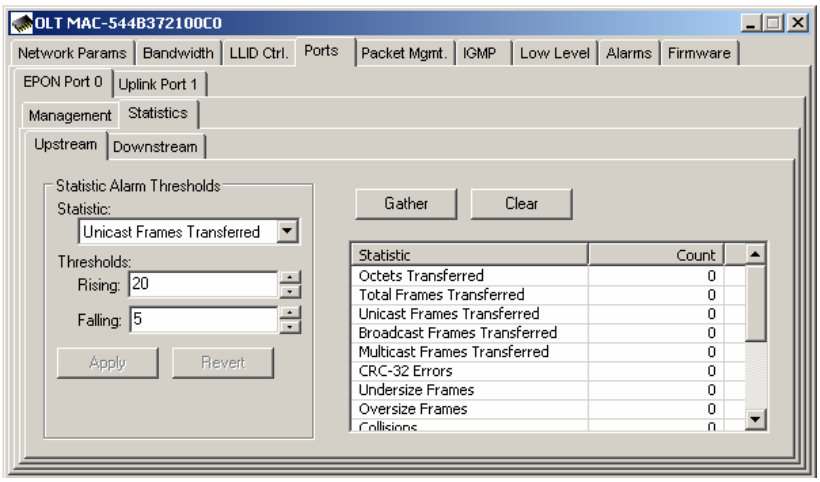
Step 3. By default the GUI does not display the reports generated by alarm audits. To enable the GUI to display alarm audits in the GUI Log Window, check the box labeled "Log all alarm audits."



Note that once changed, the GUI will write the new settings to a file named "default.conf" that is located in the installation directory with the GUI. The next time the GUI is executed, the new settings will be used by default. In some cases it is mandatory that the GUI be reset in order for the new settings to take effect. If the GUI is run from a read only volume such as a CDROM, it will not be able to write the "default.conf" file and will fall back to default settings. If the "default.conf" file becomes corrupt, or is deleted a new file will be generated the next time the GUI is run.

10.3 Setting Alarm Thresholds

Alarm thresholds may be set via the Teknovus Evaluation Kit GUI. This process is the same for ONU and OLT statistics thresholds. The units for all thresholds are in events/second. To set a threshold, enter an appropriate value for the rising and falling thresholds, and then click the apply button. When the transaction completes successfully the Apply and Revert buttons will turn grey indicating that the OLT and GUI values are synchronized. Note that not all statistics are present for every entity. Refer to the host interface document for supported statistics.



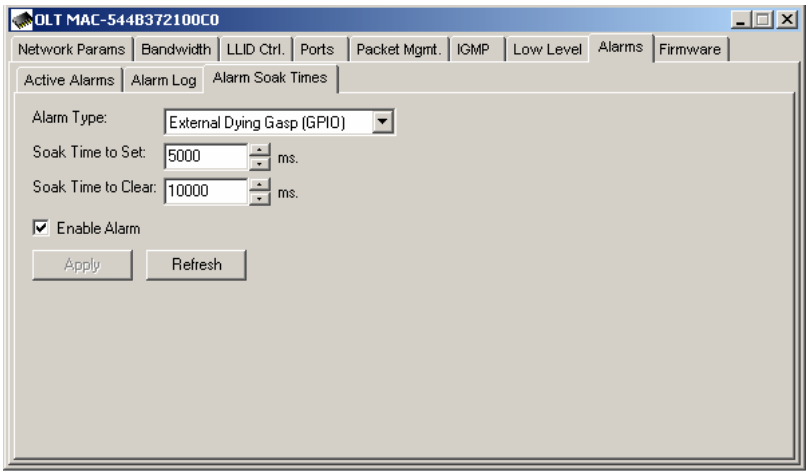
When the rate meets or exceeds the rising threshold the alarm will be issued. When the rate meets or falls below the falling threshold the alarm will be cleared.

Locating Statistics Threshold Panels	
Associated Entity:	GUI Panel:
OLT EPON Port Statistics	OLT/Ports/EPON Port 0/Statistics
OLT Uplink Port Statistics	OLT/Ports/Uplink/Statistics
OLT Link Statistics	Link/OLT Flow Stats
ONU EPON Port Statistics	ONU/Ports/EPON Port 0/Statistics
ONU UNI Port 0 Statistics	ONU/Ports/User Port 1/Statistics
ONU UNI Port 1 Statistics	ONU/Ports/User Port 2/Statistics
ONU Link Statistics	Link/ONU Flow Stats

10.4 Enabling Alarm Soaking

Alarm soaking is controlled by selecting an alarm type to soak and entering the desired set and clear times. Un-checking enable alarm will suppress all alarm events for the alarm type specified. When the panel is first loaded or a new alarm type is selected, the GUI will query the OLT for the current values. When the values have been retrieved they will be displayed in the panel and the apply button will grey, indicating that the OLT and GUI are synchronized. After the parameters have been entered, use the Apply button to transfer them to the OLT. As before, once the GUI has successfully completed the transaction with the OLT the apply button will grey.

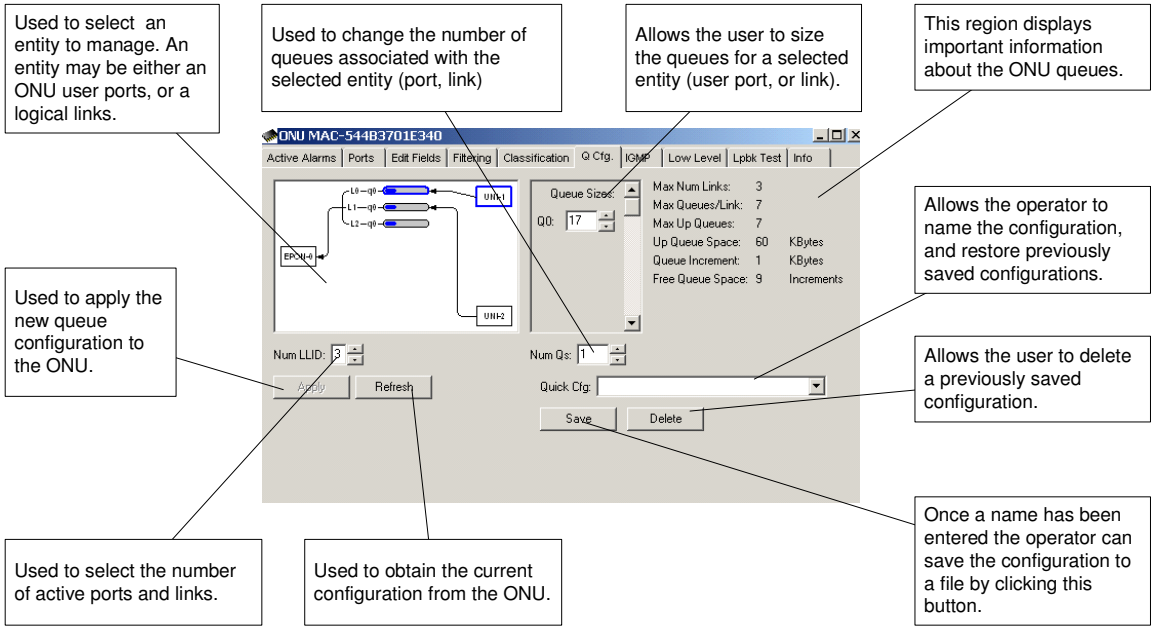
In the example below the OLT will only notify the Element Management Layer of an external dying gasp if the alarm condition persists for at least 5 seconds. After the alarm is cleared an additional 10 seconds must pass (without receiving any dying gasp alarms) before the OLT will notify the Element Management Layer that the dying gasp has been cleared.



11 ONU Data Path Configuration

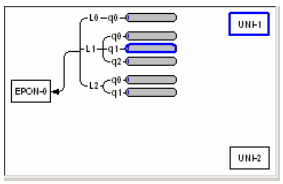
The GUI may be used to configure various aspects of the ONU data path. Such as the ONU queue configuration, classification of user data traffic and filtering of user data traffic. Because these operations are very complex the user interface is divided between several panels.

11.1 ONU Queue Configuration

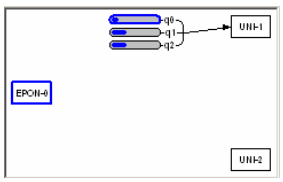


The ONU Queue configuration panel allows the operator to change queue sizes and save configurations.

11.1.1 Entity Selection Control

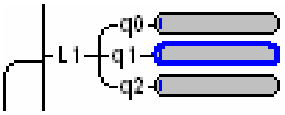


Upstream Configuration

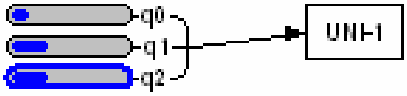


Downstream Configuration

The Entity Selection Control is a graphic representation of the ONU data path. This control allows the operator to select an entity to manage by clicking on a graphical representation. An entity many be either an ONU User Port ONU Logical Link, or ONU FIFO. The EPON port is depicted as a box labeled EPON. The two User Ports are represented by boxes labeled UNI-1 and UNI-2 respectively. Depending on whether the EPON Port or a User Port is currently selected the FIFOs shown will correspond to either the upstream or downstream data path. The convention is “from port to FIFO.” Thus selecting a port “from” which a frame is received displays the FIFOs to which the frame may be classified. Classification will be discussed in the next section. Selecting any FIFO terminating at a particular port or logical link has the effect of also selecting the related entity. In the example above link 1 has been selected.



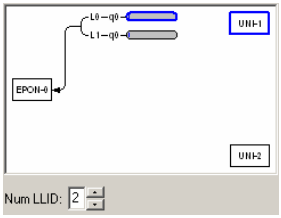
Notice that downstream FIFOs are labeled relative to their associated link. For downstream FIFOs the GUI uses the naming convention Link.FIFO. Therefore the “full name” of the selected FIFO is 1.1.



Upstream the GUI will use the convention Port.FIFO. In the example above the full FIFO name is 1.2, indicating that the FIFO is #2 of User Port 1.

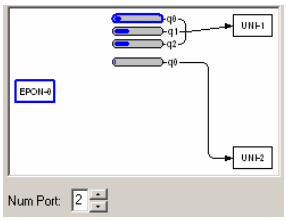
11.1.2 Provisioning Number of Logical Links to Register

Up to 3 Links may be registered per ONU (6 on a TK3711). The number of Logical Links is determined by the Num LLID control. This control is only visible when one of the User Ports is selected.



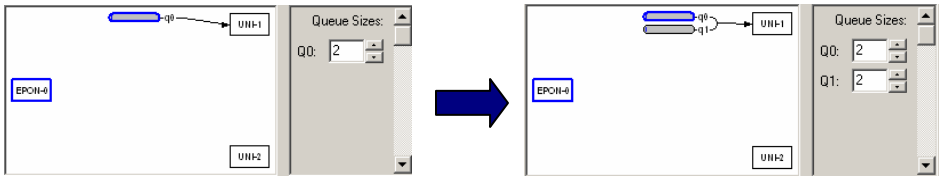
11.1.3 Provisioning Number of User Ports

In practice either ONU user port may be used exclusively. However, for the purposes of the GUI only User Port 1 may be used exclusively. To select whether both User Port 1 and 2 should be used, or only user port 1, set the number of ports to 2 (both ports) or 1 (only port 1). The number of ports will not be changed if all of the FIFOs have already been allocated to user port 1, or there is insufficient FIFO space available. The Num Port field is only visible if the EPON port is selected.

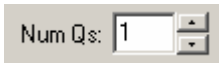


11.1.4 Provisioning Downstream FIFOs

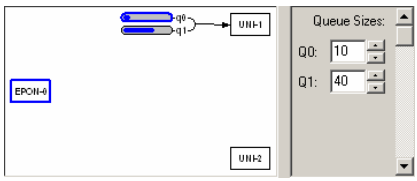
Step 1. Downstream FIFOs are associated with ONU user ports. The Entity Selection Control displays queues using a "From-To" convention. To add a queue to an ONU User Port, first click on the ONU EPON port ("From") and then select any one of the ONU User Port's FIFOs ("To").



Step 2. Use the Num Qs control to add a second FIFO, by changing the value from 1 to 2. Notice that a second FIFO will appear in the diagram as depicted in the figure above.

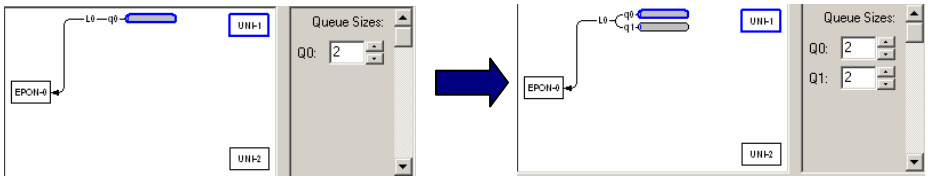


Step 3. Size the FIFOs using the Queue Size Control. Notice that as the size of a given FIFO changes the picture will be updated to graphically illustrate the relative space allocated to each FIFO. To calculate the FIFO size in KBytes, multiply the provisioned size by the FIFO increment displayed on the panel. The remaining space is displayed on the panel as the Flooding Q Size. This value is automatically updated when a change is made to a User FIFO. Space that is left unallocated by the operator will automatically be assigned to the Flooding FIFO by the GUI. It is important to note that not all configurations make use of the Flooding FIFO, however all FIFOs including the Flooding FIFO must be allocated a minimum queue space of 2KBytes, to ensure that there is enough free space to hold a 1536 byte packet. The exact purpose of the Flooding FIFO is beyond the scope of this document.

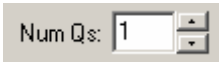


11.1.5 Provisioning Upstream FIFOs

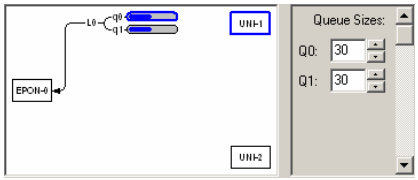
Step 1. Adding a FIFO to an ONU Logical Link is a similar procedure. First click on either of the ONU's User Ports and then click on any of the existing FIFOs associated with the logical link to which a new FIFO is to be added.



Step 2. Use the Num Qs control to add a second FIFO, by changing the value from 1 to 2. Notice that a second FIFO will appear in the diagram as depicted in the figure above.



Step 3. Size the FIFOs using the Queue Size Control. Notice that as the size of a given FIFO changes the picture will be updated to graphically illustrate the relative space allocated to each FIFO. To calculate the FIFO size in KBytes, multiply the provisioned size by the FIFO increment displayed on the panel. There is no upstream equivalent to the Flooding FIFO, therefore all the queue space can be allocated to the User FIFOs.

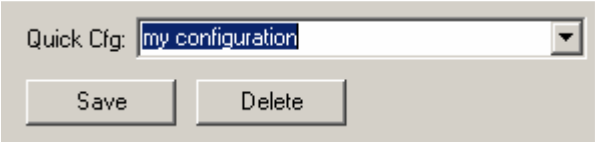


11.1.6 Committing the Provision to ONU Firmware

Once a FIFO configuration has been created clicking the Apply button will commit the changes to the ONU. The ONU **MUST** be reset to complete the configuration process (this can be performed with the GUI). It should be noted that the GUI applies the new Classification scheme with the FIFO configuration; this is INCORRECT behavior that will be fixed in a future version of the GUI. Well behaved host software should apply the classification rules only after the ONU has been reset. The refresh button performs the converse function of Apply, causing the GUI state to be updated to reflect the state of the ONU.

11.1.7 Saving the Configuration to the Hard Disk

Once a queue configuration has been created, it can be saved to the hard disk by entering a descriptive name for the configuration into the Quck Cfg drop down box and clicking the Save button. The GUI will save both the Queue Configuration and the Classification Scheme (Filtering Rules will not be saved). These attributes are stored in a binary file located in the distribution directory. This file is called "OnuQueueCfgRepository.dat". If desired the file may moved to a newer distribution to recover the saved configurations.



11.1.8 Restoring the ONU to a Previous Configuration

To restore an ONU to a previous configuration, select the configuration from the Quick Cfg drop down box and press the Apply button to transfer the stored configuration to the ONU.

11.1.9 Deleting a Saved Configuration

Once a configuration has been saved, it can be deleted by selecting it from the Quick Cfg drop down box or typing its name and clicking the Delete button.

Notice that the GUI prevents the user from adding more FIFOs than the ONU supports. It will also prevent the user from adding a second FIFO if there is no free space available.

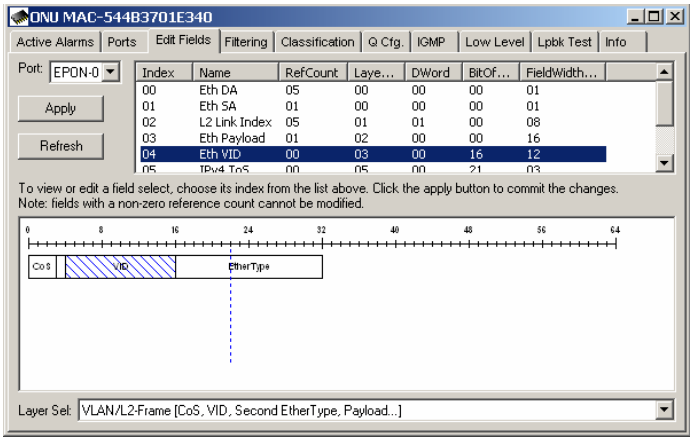
The fee space available is clearly displayed so that it is easy to determine when there is no longer sufficient resources.

It is important to note that not all configurations make use of the Flooding FIFO, however all FIFOs including the Flooding FIFO must be allocated a minimum queue space of 2KBytes, to ensure that there is enough free space to hold a 1536 byte packet. The GUI enforces this restriction.

Picking the right FIFO size is easy. In a typical configuration the ONU is Burst Tolerant to the provisioned FIFO Size. A typical PC running Windows XP has a default TCP Window size of 17K. Therefore the FIFO should be at least 17K if it is to carry PC data. Typically 4-10K is enough for voice traffic depending on the type of service. Generally speaking 32K of Burst Tolerance is more than adequate for high throughput applications such as FTP.

The ONU **MUST** be reset to complete the configuration process (this can be performed with the GUI). It should be noted that the GUI applies the new Classification scheme with the FIFO configuration; this is INCORRECT behavior that will be fixed in a future version of the GUI. Well behaved host software should apply the classification rules only after the ONU has been reset.

11.2 Selecting Lookup Fields



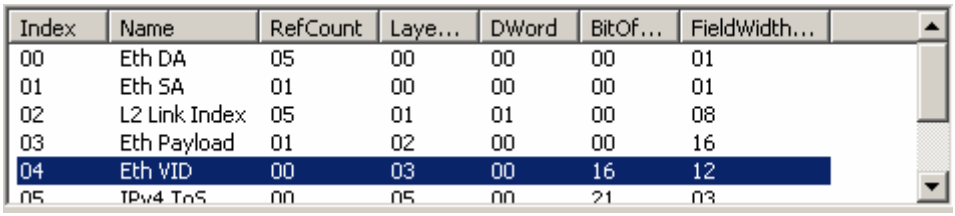
The TK3701/TK3711 and future Teknovus ONUs support highly configurable line rate classification engines. Depending on the model, the ONU lookup engine is capable of simultaneously examining anywhere from 8-12 fields in the frame! The position and size of each field is programmed into the lookup engine prior to use in filtering and classification rules.

Depending on the device the ONU reserves a certain number of fields that cannot be changed by the user. These fields may be used to construct user provisioned classification and filtering rules, however their definitions may not be changed. All of the currently provisioned fields including those reserved by the ONU may be viewed by clicking on the Edit Fields tab.

11.2.1 Selecting a Classification Engine

Most ONU classification engines are configured on a per port basis. However, the TK3701 supports only upstream and downstream classification. The Port field allows the operator to choose the set of field selects to modify. Depending on the port that is chosen the provisioning may be different. For ONUs supporting only upstream and downstream classification, the EPON port designates downstream, and selecting either User Port selects upstream.

11.2.2 Field Select Table



The Field Select Table displays the Field Selects associated with the currently selected port, and allows field selects to be selected for modification.

11.2.2.1 Index

A number used to identify the field select.

11.2.2.2 Name

An ASCII description of the field select.

11.2.2.3 RefCount

The number of rules currently using the filed select. A non-zero value means that the field select may not be modified.

11.2.2.4 LayerSel

This is the Host Interface layer select value provided for reference.

11.2.2.5 Dword

This is the Host Interface Dword value, provided for reference.

11.2.2.6 BitOffset

This is the Host Interface Bit Offset, provided for reference.

11.2.2.7 FieldWidth

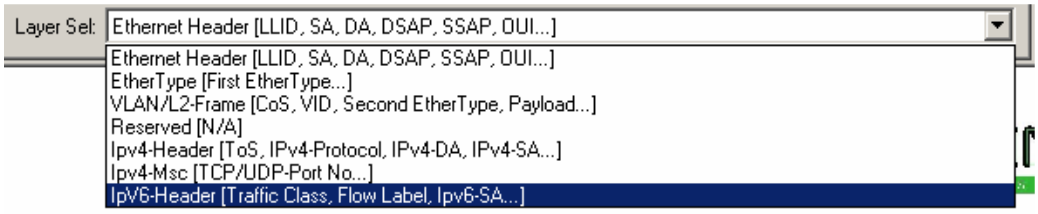
This is the Host Interface Field Width, provided for reference.

11.2.3 Editing a Lookup Engine Field

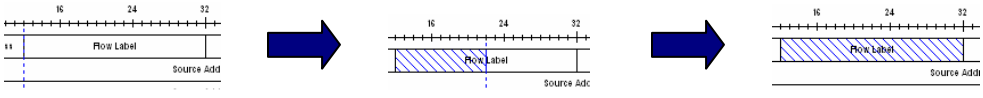
Lookup Engine Fields may only be modified if they are not currently being used in any rule. The ONU keeps track of the fields currently being used by maintaining a reference count. This reference count is displayed in the Field Select Table. To edit a field with zero reference count follow the procedure below.

Step 1. Click on the Field Select index to be edited.

Step 2. Using the Layer Sel drop down list, select an appropriate frame format. The ONU will use the frame format to qualify the field select value.



Step 3. Using the Edit Tool, drag a box over the field select by depressing the mouse button at the start of the field dragging it to the end of the field and then releasing the mouse button.



Notice that after the field has been selected, the Name will change to reflect the selected value.

11.2.4 Applying the Configuration

The field select values may be applied to the ONU by clicking on the Apply button.

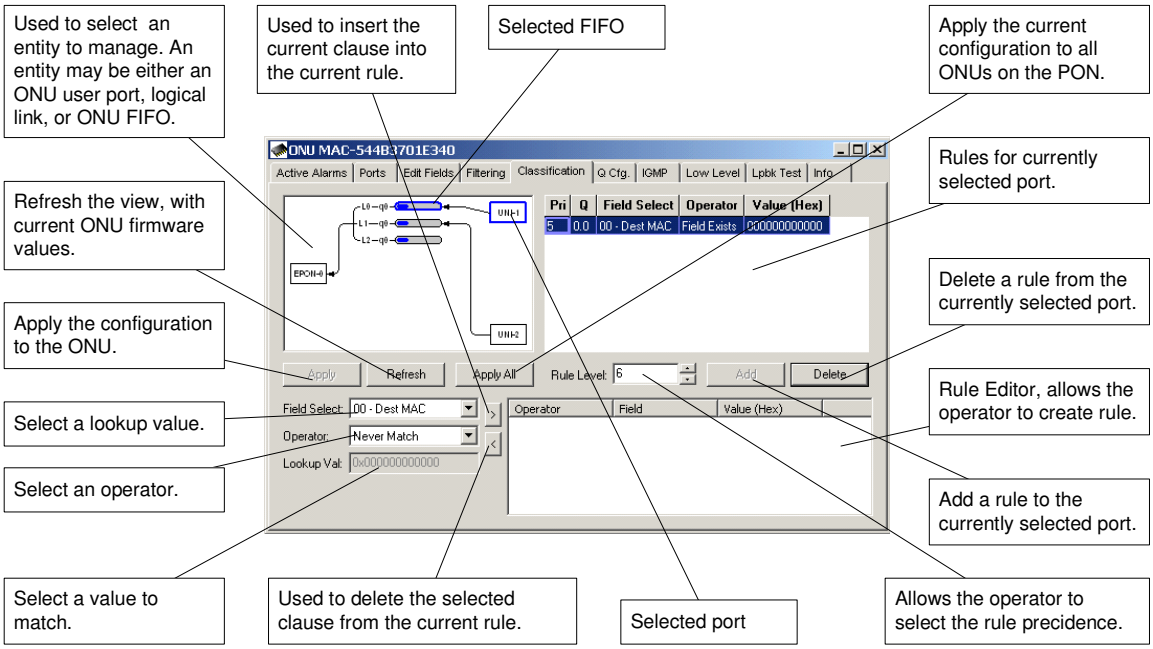
11.2.5 Refreshing the View

To refresh the currently displayed field select values to match the ONU click the apply button.

Lookup Engine Fields may **NOT** be modified if they are in use. The ONU keeps track of the fields currently being used by maintaining a reference count

Most ONU classification engines are configured on a per port basis. However, the TK3701 supports only upstream and downstream classification. The Port field allows the operator to choose the set of field selects to modify. Depending on the port that is chosen the provisioning may be different. For ONUs supporting only upstream and downstream classification, the EPON port designates downstream, and selecting either User Port selects upstream.

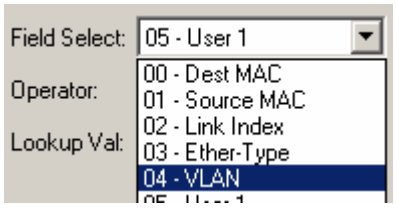
11.3 Designing the ONU Classification Scheme



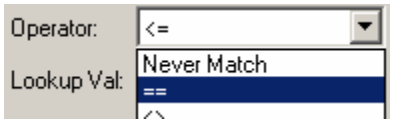
An ONU classification scheme allows the operator to define a custom function to determine which packets will be forwarded to each of the ONUs configured priority FIFOs. The classification function for a given FIFO is composed of multiple independent rules. A rule consists of multiple ANDed expressions known as clauses. Each rule is used to classify traffic into a single FIFO, 1 or more rules may be used to classify traffic into the same FIFO.

11.3.1 Constructing an ONU Classification Rule

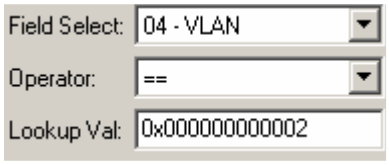
Step 1. Choose the Field Select. Field Selects defined by the ONU are given a descriptive label. User Defined field selects are labeled User 1, User 2.., User N. All field select labels begin with an index value. The index value correlates with the index value on the Edit Field panel.



Step 2. Choose an appropriate Operator. The operator tests the portion of the frame specified by the field select.

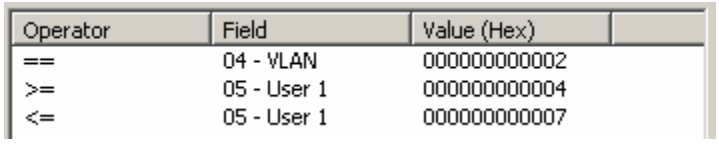


Step 3. Choose an appropriate Lookup Value. This is the value that will be used by the operator in the comparison. This step is only applicable to binary operators. If the operator selected is unary (such as Field Exists) the Value field will be disabled.



Step 4. Add the clause to the Rule Editor using the left arrow button. Note that the right arrow button can be used to remove a selected clause from the Rule Editor.

Step 5. Repeat steps 1-4 until the desired rule has been created. The TK3711 supports a maximum of 2 clauses / rule. The TK3701 supports a maximum of 8 clauses / rule.

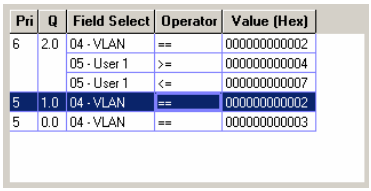


Operator	Field	Value (Hex)
==	04 - VLAN	000000000002
>=	05 - User 1	000000000004
<=	05 - User 1	000000000007

The right arrow button is useful for correcting mistakes. Using this button we can remove a selected clause that is incorrect.

11.3.2 Using the Rule Grid

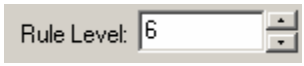
The Rule Grid is used to view the classification scheme and delete unwanted Classification Rules. The Rule Grid displays the rules for the port that is currently selected. Selecting a different port will reveal the rules associated with that port.



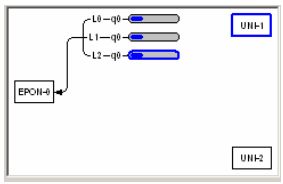
Pri	Q	Field Select	Operator	Value (Hex)
6	2.0	04 - VLAN	==	000000000002
		05 - User 1	>=	000000000004
		05 - User 1	<=	000000000007
5	1.0	04 - VLAN	==	000000000002
5	0.0	04 - VLAN	==	000000000003

11.3.2.1 Adding a Rule to the Classification Scheme

Step 1. Set the rule precedence level. The Rule Level may be configured for 1 of 8 different precedence levels, 0 being the highest priority and 7 being the lowest. The ONU firmware installs system rules at precedence levels 0..3 and 7. It is recommended that user provisioned classification rules be provisioned in the range that the ONU does not use. If two rules (classifying traffic into different FIFOs) match the same frame, the provisioned Rule Level will determine where the frame is classified. A classification rule with higher precedence than a filtering rule can be used to override a filtering function.



Step 2. Select the FIFO for classification. First select the ingress port (the port the classified frame arrives at), next select the egress FIFO (the FIFO that the frame will be classified into). Notice that selecting an ingress port automatically selects the set of available egress FIFOs. Black lines drawn from the FIFO to the ONU port indicate which port the forwarded frames will be sent to. Arrowhead serve to indicate the direction the data will be transported (in the figure below the direction is upstream).



ALL downstream classification rules **MUST** include a clause to indicate the link on which the forwarded frames arrive. The consequences of not inserting this clause are unknown, but random device failure is a possibility! The **ONLY** supported operator for this rule is: "==." The Link Index is the same as N, where Base MAC + N = Link MAC.

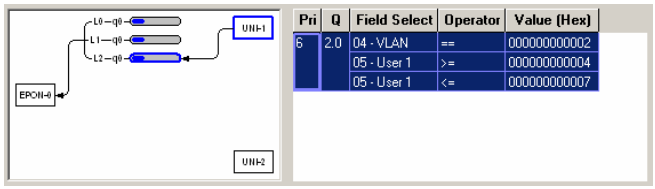
Operator	Field	Value (Hex)
==	02 - Link Index	000000000000

Selecting an ingress port automatically selects the set of available egress FIFOs. Black lines drawn from the FIFO to the ONU port indicate which port the forwarded frames will be sent to. Arrowhead serve to indicate the direction the data will be transported.

If two Classification Rules or a Classification Rule and a Filtering Rule (next section) match the same frame, the action associated with the **HIGHEST** priority rule will be carried out (0 is highest priority). If the precedence levels **MATCH** the action is **UNDEFINED**!

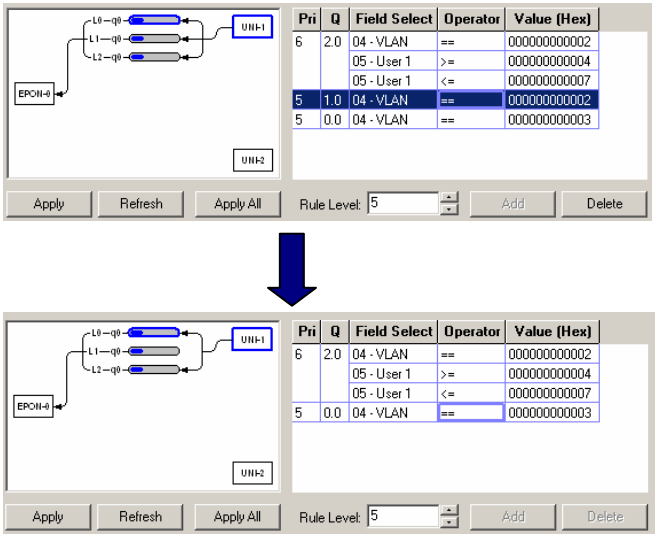
Step 3. Adding the classification rule to the ONU. Once we have selected the FIFO for classification adding the rule is as simple as clicking the Add button. The GUI software will not allow the addition of identical rules.

Adding the rule will cause the Entity Selection Control to draw a connection from the selected port to the selected FIFO for classification. The Rule Grid will also be updated to display the new rule.



11.3.2.2 Deleting a Rule

To delete a rule from the Classification Scheme, simply click any where in the rule to select it, and then click the delete button.



11.3.2.3 Understanding FIFO Labeling (Q)

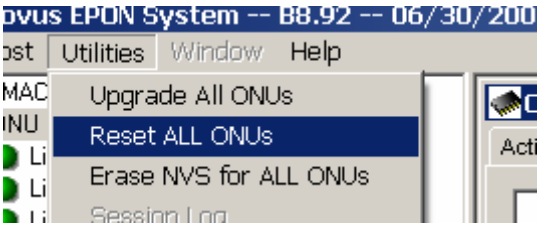
The GUI Uses the convention <Entity ID>.<FIFO Number> to denote a particular FIFO. The Entity ID corresponds to link index upstream, and the ONU User Port upstream. If you forgot to add the Link Index clause to your downstream classification rules your ONU might disappear into an alternate universe (you have been warned). For instance the label 2.0 indicates the 0^{th} FIFO associated with link 2.

11.3.2.4 Applying the Configuration

Once the configuration has been completed it may be easily applied to the ONU by clicking the Apply button.

The Apply All button is used to apply the configuration to all ONUs on the PON.

Once the configuration has been applied the ONU MUST be reset. This is because the GUI also applies both the Classification Scheme and the FIFO Configuration together. This is an issue in the GUI that will be fixed in a future software release. Properly designed hosts MUST NEVER apply a new Classification Scheme after changing the FIFO Configuration until after the ONU has been reset. The Reset ALL ONUs is convenient when multiple ONUs must be reset.



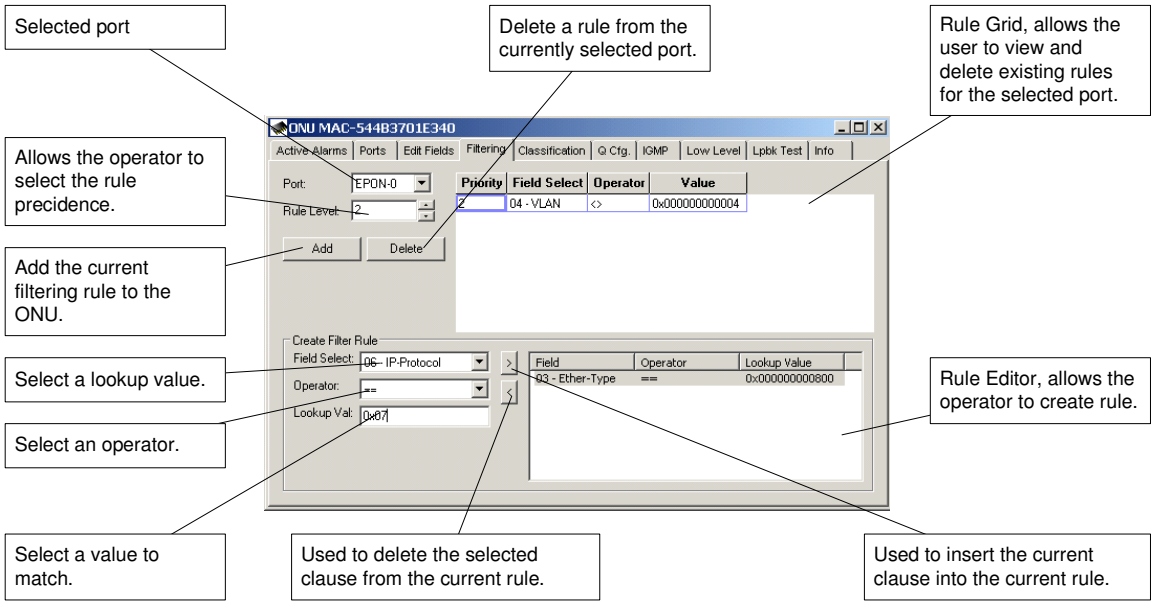
11.3.2.5 Refreshing the View

The Refresh button is used to refresh the Classification Scheme with the values currently stored in the ONU.

Once the configuration has been applied the ONU **MUST** be reset. This is because the GUI also applies both the Classification Scheme and the FIFO Configuration together. This is an issue in the GUI that will be fixed in a future software release. Properly designed hosts **MUST NEVER** apply a new Classification Scheme after changing the FIFO Configuration until **AFTER** the ONU has been reset.

The Reset ALL ONUs is convenient when multiple ONUs must be reset.

11.4 Provisioning Filtering Rules



Filtering Rules and Classification Rules work in apposing directions to achieve the same ultimate goal: control the user's access to the PON. In the previous section we learned that Classification Rules are used to allow certain classes of traffic into the ONU data path. As you might imagine, Filtering Rules serve the opposite purpose, blocking certain classes of traffic from entering an ONU Port. Filtering rules use the same hardware resources, Field Selects, Operators, and Precedence values as Classification Rules and are constructed in a similar fashion. A Classification Rule can override a Filtering Rule by setting its precedence higher.

11.4.1 Selecting the Port for Filtering

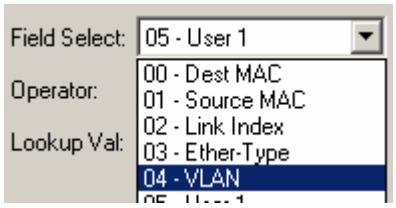
The Port to Filter is selected using the Port drop down box.

11.4.2 Using the Rule Grid

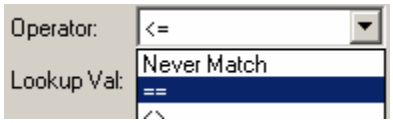
The Filtering Panel Rule Grid is almost identical to the Classification Panel Rule Grid, except that the Q column is absent, as it is not required.

11.4.3 Constructing an ONU Filtering Rule

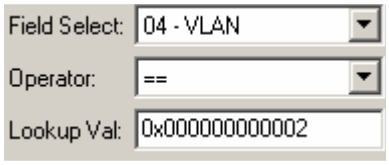
Step 1. Choose the Field Select. Field Selects defined by the ONU are given a descriptive label. User Defined field selects are labeled User 1, User 2.., User N. All field select labels begin with an index value. The index value correlates with the index value on the Edit Field panel.



Step 2. Choose an appropriate Operator. The operator tests the portion of the frame specified by the field select.

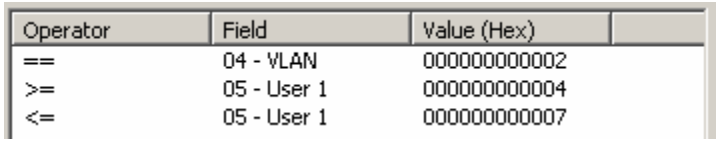


Step 3. Choose an appropriate Lookup Value. This is the value that will be used by the operator in the comparison. This step is only applicable to binary operators. If the operator selected is unary (such as Field Exists) the Value field will be disabled.



Step 4. Add the clause to the Rule Editor using the left arrow button. Note that the right arrow button can be used to remove a selected clause from the Rule Editor.

Step 5. Repeat steps 1-4 until the desired rule has been created. The TK3711 supports a maximum of 2 clauses / rule. The TK3701 supports a maximum of 8 clauses / rule.

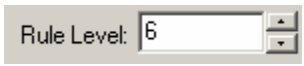


Operator	Field	Value (Hex)
==	04 - VLAN	000000000002
>=	05 - User 1	000000000004
<=	05 - User 1	000000000007

11.4.4 Adding a Filtering Rule

Step 1. Select the Port to Filter.

Step 2. Set the rule precedence level. The Rule Level may be configured for 1 of 8 different precedence levels, 0 being the highest priority and 7 being the lowest. The ONU firmware installs system rules at precedence levels 0..3 and 7. It is recommended that user provisioned classification rules be provisioned in the range that the ONU does not use. If two rules (classifying traffic into different FIFOs) match the same frame, the provisioned Rule Level will determine where the frame is classified. A classification rule with higher precedence than a filtering rule can be used to override a filtering function.



Step 3. Add the filtering rule to the ONU by clicking the Add button.

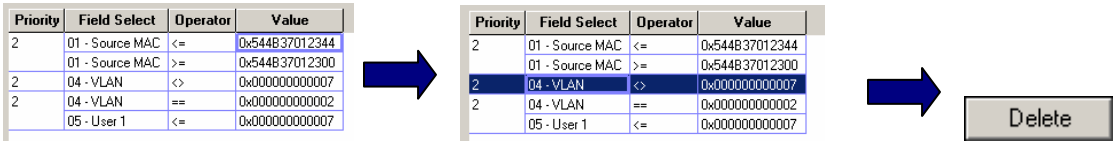
Unlike the Classification panel, adding a filtering rule will cause the ONU to be updated without an additional apply action.

Priority	Field Select	Operator	Value
2	04 - VLAN	==	0x000000000002
	05 - User 1	<=	0x000000000007

The TK3701 and TK3713 support 8 clauses per rule, however the TK3711 only supports 2. It is important to consider the capabilities and limitations of each chipset when designing filtering schemes.

11.4.5 Deleting a Filtering Rule

Once a filtering rules has been added the rule may be deleted by selecting it from the Rule Grid and clicking the Delete button.



Once the rule has been successfully deleted it will be removed from the Rule Grid.

Priority	Field Select	Operator	Value
2	01 - Source MAC	<=	0x544B37012344
	01 - Source MAC	>=	0x544B37012300
2	04 - VLAN	==	0x000000000002
	05 - User 1	<=	0x000000000007

12 IGMP

Teknovus EPON chipsets include an RFC 2236 compliant IGMP solution that leverages the power of the underlying hardware classifiers, shapers and priority FIFOs to deliver high quality IP multicast content over EPON. From a functional perspective the feature set may be roughly divided into 4 broad classes of functionality:

1. Control over IP multicast data traffic at the network and customer edge.
2. Burst protection for customer premise equipment (CPE.)
3. Scheduling of IP multicast data traffic.
4. Aggregation of reports sent by CPE, greatly limit the burdon placed on RFC 2236 queriers such as a video server residing in the CO.

These 4 primary functions are distributed between the OLT and the several ONUs, based on the design principle that functionality should be implemented, as much as possible, at the network's edges. Thus preserving the bandwidth of the PON and taking maximum advantage of the combined resources of the several ONUs.

12.1 Brief Overview of Proxy Concepts

On the customer edge the OLT acts as an RFC 2236 querier. Hosts connected to one of the ONUs UNI ports perceive the queries sent by the OLT as originating from a media server behind the OLT. On the network edge the OLT behaves as an RFC 2236 "non-querier," aggregating the reports sent by the several connected hosts, and making the system appear to an attached video server or other device connected to the OLT's NNI as if there existed only a single STB behind the OLT.

12.1.1 Behavior of ONU

By default the ONU shall block all IGMP multicast data traffic preserving the bandwidth of the user network. When an STB or other host attached to one of the ONU's UNI ports requests to join a multicast group, the query is snooped by the ONU's CPU before being forwarded to the EPON port without modification.

12.1.1.1 Report Received from UNI

If no host is joined to the group on the attached interface, the ONU will install a new rule to forward the group to the provisioned IGMP multicast data FIFO.

12.1.1.2 Leave Received from UNI

If the LMQC variable is set to 0 ("fast leave") and at least one host is joined to the group on the attached interface, the ONU will remove the forwarding rule for the associated group.

12.1.1.3 General Query Received from EPON

If any groups are present on either of the ONUs UNI ports, the ONU will start a count down timer that is equal to: [provisioned robustness count] * [Max Response Time specified in query]. If a report is not received within this interval, for any group joined on either of the ONU's UNI ports, the group will be removed from the ONU's multicast forwarding table.

12.1.1.4 Group Specific Query Received from EPON

If any groups are present on either of the ONUs UNI ports, the ONU will start a count down timer that is equal to: [provisioned GSQC] * [Max Response Time specified in query]. If a report is not received within this interval, for the specified group joined on either of the ONU's UNI ports, the group will be removed from the ONU's multicast forwarding table.

12.1.2 Behavior of OLT

By default the OLT shall block all IGMP multicast data traffic preserving the bandwidth of the PON and user network. When an STB or other host attached to one of the several ONU's UNI ports requests to join a multicast group, the query is snooped by the OLT's CPU, and conditionally forwarded upstream.

12.1.2.1 Report Received from Logical Link

If no host is joined to the group on the attached interface, the OLT will install a new rule to forward the group to one of the several IGMP multicast data FIFOs. The OLT will pick the FIFO with least groups joined.

Group Insertion Process:

```
if (not FindGroup (group))
    {
    q = fifos[0]
    for (n in fifos)
        {
        if (n.numGroup < q.numGroup)
            {
            q = n
            }
        }
    q.numGroup = q.numGroup + 1
    InsertGroup (group, q)
    SendJoin (group, UpstreamUplinkQ)
    }
```

12.1.2.2 Leave Received from Logical Link

The OLT will issue LMQC GSQs, spaced by LMQI until one of the following two events occurs (whichever occurs first).

1. 1 or more reports are received upstream for the group specified in the leave message.
2. No report is received after LMQI units from the time that the final LMQ was issued.

In case (1), the load balancing algorithm will be applied as described above. In case (2) the group will be removed from the forwarding table, and the OLT will transmit a leave message, with the provisioned source IPv4 Address, from the OLT's NNI.

Group Removal Process:

```
q = FindGroup (group)
if (q)
    {
    q.numGroup = q.numGroup - 1
    RemoveGroup (group, q)
    SendLeave (group, UpstreamUplinkQ)
    }
```

12.1.2.3 General Query Issued

The OLT will periodically issue General Queries every Query Interval units. The use of the General Query in IGMPv2 is very different from the way it was used in IGMPv1. In IGMPv2 the General Query is used for failure detection only. In IGMPv1 the General Query was the only mechanism used to detect a leave. Because failures are extremely rare in modern networks the Query Interval may be provisioned to a very large value. Query Response Timeout units after the OLT issues the General Query the OLT will decrement the robustness variable for each group joined for which the OLT has not received a report. When the robustness for a particular group is 0, the OLT will assume that an implicit leave has occurred and start the same process as described above. Since IGMPv2 has a different mechanism than IGMPv1 to guarantee robustness - the Group Specific Query Count - it is probably not necessary to provision the Robustness Count to a large value. The value recommend by the standard for backwards compatibility with IGMPv1 is 2, however, if the target system will only have IGMPv2 capable clients, a robustness count of 1, is probably a better choice.

Group Table Audit Process:

```
while (ProxyRunning())
    {
    Wait (QueryInterval)
    for (group in groups)
        {
        group.dirty = True
        }
    SendGeneralQuery (DownstreamEponPortQ)
    starttime = now()
    runtime = 0
    while (QueryResponseTimeout < runtime)
        {
        report = WaitReport (QueryResponseTimeout - runtime)
        if (report)
            {
            group = FindGroup (report.grId)
            if (group)
                {
                group.dirty = False
                }
            }
        runtime = starttime - now()
        }
    for (group in groups)
        {
        if (group.dirty)
            {
            group.robustness = group.robustness - 1
            if (group.robustness == 0)
                {
                HandleLeave (group)
                }
            }
        }
    }
```

The protocol description assumes that IGMP snooping and proxy are enabled. If these functions are disabled, IGMP multicast data packets will be forwarded based on the Host provisioned classification scheme and bridging mode(s).

If faster leave operation is desired, the GSQC may be set to 1, and the Last Member Query Max Response Time provisioned to a smaller value than the default.

The ONU Snooping and OLT Proxy functions **MUST** be configured identically. Otherwise multicast traffic will **NOT** be forwarded as expected.

The number of IGMP multicast data FIFOs used **MUST NOT** be changed when the OLT PON Plant is enabled.

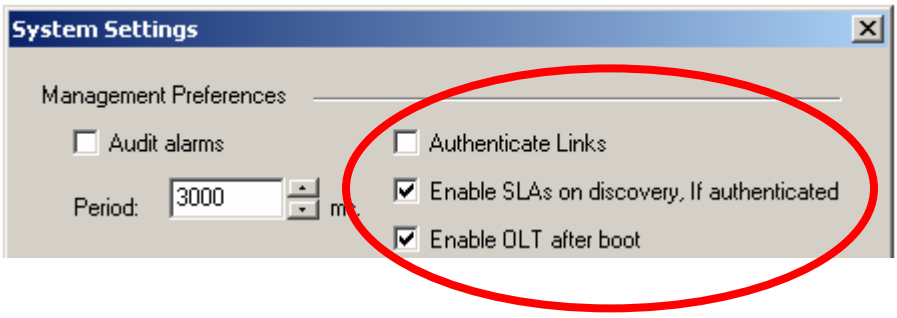
12.2 GUI Authentication Function

The authentication function in the GUI requires the creation of an external database of authentication secrets. The external database is to be a plain ASCII text file named “Prov.db”. The first line in the database contains the number of authentication records.
Each record consists of an LLID MAC Address, end-line, authentication secret, and end-line.

Example File:

```
2
544B37010000
thisIsASecret
544B37010001
thisIsAnotherSecret
```

Three Boolean attributes found in the Utilities/System Settings panel control the authentication behavior:



- Authenticate Links:
  If checked the GUI will use its database of authentication secretes to authenticate each link when the GUI is opened or on autonomous link discovery. Discovered links that are not authenticated will appear with a grey icon. Links that do not exist in the authentication database will be treated as unauthenticated links.
- Enable SLAs on discovery, if authenticated:
  If checked and Authenticate Links is also checked the SLAs will be enabled only if the authentication succeeds. Otherwise, if checked, SLAs will be enabled unconditionally. This is useful for strict boot mode.
- Enable OLT after boot:
  If checked this attribute will cause the OLT to be enabled after boot up in order to facilitate the strict boot mode.

If the Prov.db file is not present, an authentication database with no records is assumed.