ALBEDO Telecom
Joan d'Austria, 112 - Barcelona - SP - 08018
www.albedotelecom.com

Ethernet Traffic Generation

One of the key features of Ether.Genius / Ether.Sync / Ether.Giga tester families is the ability to generate traffic with deterministic and random bandwidth profiles. The traffic generation feature can be used to stress the network, simulate user traffic and, if a suitable payload is configured, to measure critical network performance parameters like bit errors, packet loss or latency.

The above mentioned Ethernet testers manufactured by ALBEDO, have eight independent full featured traffic generators attached to the main test port (Port A). Each traffic flow may be configured with specific encapsulation and addressing parameters thus providing great versatility in all applications requiring Ethernet and IP traffic generation.

1. Generation of Ethernet Traffic

In Ether.Genius / Ether.Sync / Ether.Giga testers, generation of custom Ethernet frames is available for Port A in *Ethernet endpoint* mode through the *Frame*, *Bandwith profile* and *Payload* settings for each of the eight available traffic flows. This is a short description of the Ethernet traffic generation menus:

Figure 1 *ALBEDO Ether.Giga is a field tester for Ethernet equipped with all the features to install and maintain Ethernet infrastructures supporting legacy features such as BER and RFC2544 while new test such as eSAM Y.1564.*

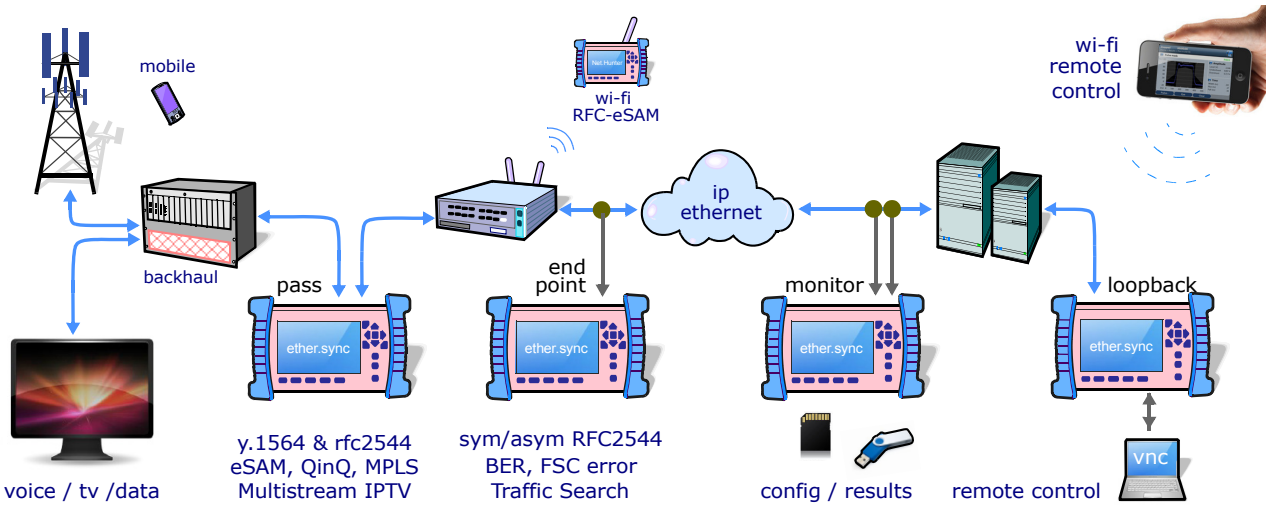


Figure 2 *ALBEDO Ether.Genius / Ether.Sync / Ether.Giga field testers in operation.*

- *Frame*: Configures the encapsulation and MAC addresses. If the Ethernet frames have any VLAN tag, this menu configures the VID and priority for these tags.
- *Bandwidth profile*: Sets the traffic generation statistics. There are four profiles to choose: *Constant*, *Periodic Burst*, *Ramp* and *Poisson*.
- *Payload*: This menu is used to set the payload to be inserted in the generated Ethernet frames. The SLA payload enables the user to measure delay, jitter and packet loss. The BERT payload (flow 1 only) is used for BER testing in framed interfaces.

  Frame generation capability is controlled by RUN button. That means that no test traffic is generated if you don't press RUN. However, the tester may generate signalling traffic or reply to certain messages like ARP or ICMP echo requests / replies even if there is not an ongoing tests. Some automatic tests like the RFC 2544 or the eSAM have their own internal traffic generation dynamics but they are controlled by the RUN button as well.

Physical Layer Settings

Before starting any frame generation test, the equipment must be connected to the network and the electrical and optical physical layer must be correctly configured. Ethernet technology has been designed to keep physical layer configuration to the minimum. But there are at least two settings you may need to check before you get a link from the DUT / SUT. These settings are the *Connector* and the *Auto-negotiation*. You will know that Port A is prepared for traffic generation and analysis when the *1000, 100* or *10* LED is displayed in green color.

Frame Settings

Most the Ethernet frame fields are available for configuration but before it is necessary to tell the tester which frame structure is going to be used for traffic generation. The *Frame type* is a port-wide setting. Once you choose an specific framing for your traffic, all streams you define for the port carry the same framing structure. The available *Frame type* settings are:

- *DIX*: Port A generates *DEC, Intel, Xerox* (DIX) frames, also known as Ethernet II frames. DIX / Ethernet II frames encode the payload type in the *Type* frame field. This is the most common framing format found in real networks: RFC 894 mandates a DIX / Ethernet II frame structure with the *Type* field set to 0x0800 for IPv4 encapsulation.
- *IEEE 802.3*: Frame format defined in IEEE 802.3 standard. It is similar to the DIX frame but it specifies a different usage for the Type field that is renamed to Type / Length value. If Type / Field is larger than 0x0600 then it has the same meaning than the DIX / Ethernet II field but otherwise it specifies the frame length in bytes. IEEE 802.3 frames leave to the IEEE 802.2 *Logical Link Control* (LLC) the specification of the payload type.

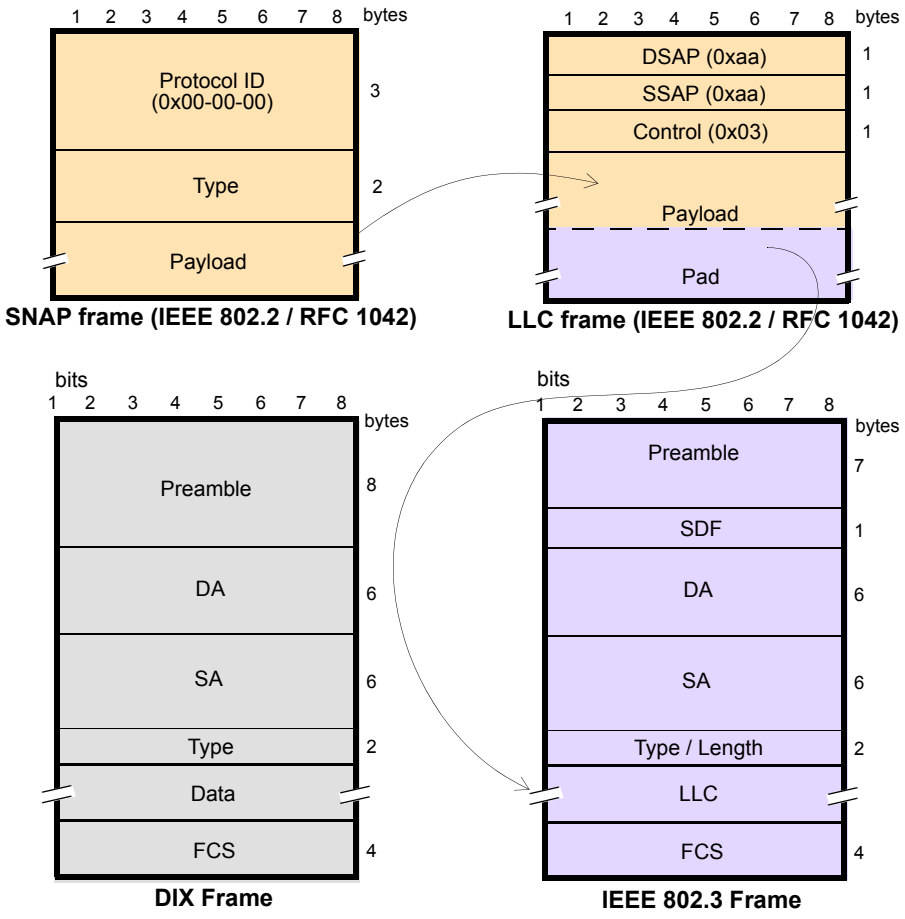


Figure 3 *MAC frame structure: IEEE 802.3 and DIX.*

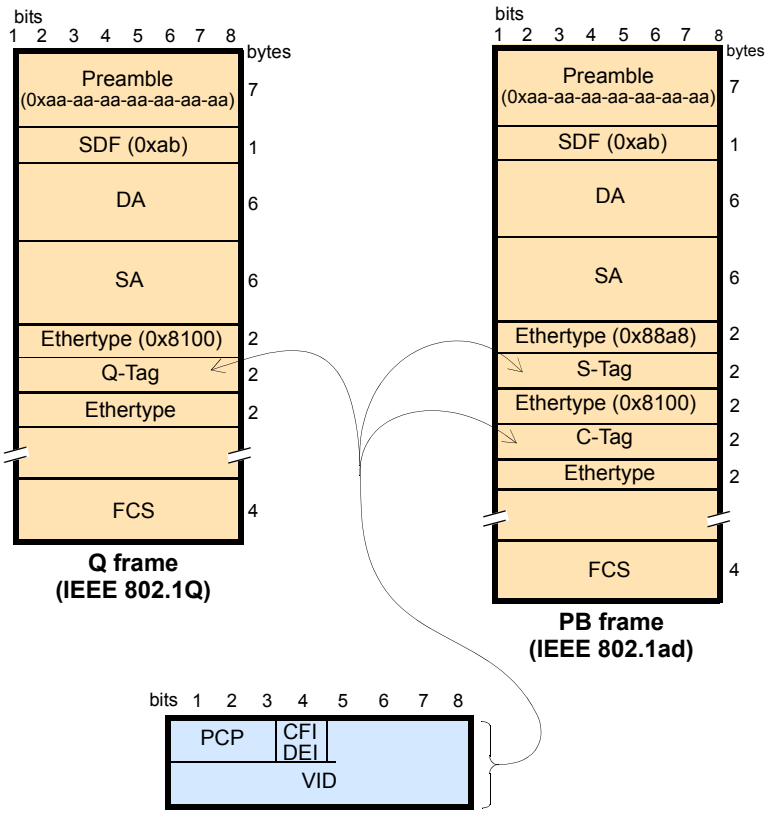


Figure 4 *IEEE 802.1Q y IEEE 820.1ad frame structures.*

The second port-wide setting to be configured is the Maximum Transmission Unit (MTU). This setting is relevant for the analyzer only and it configures the largest frame size accepted without declaring the *Oversized* defect. Standard IEEE 802.3 specifies an MTU of 1518 bytes for ordinary Ethernet frames but 1522 is admitted for VLAN frames and 1526 valid for frames carrying two VLAN tags (IEEE 802.3ad, Q-in-Q). Some switches provide support for much larger frames know as jumbo frames. These frames are more efficient because the ratio of header bytes to payload bytes is smaller for larger frames but they are currently not accepted by any international standard.

The following steps illustrate the frame configuration procedure. Both the port-wide and flow-specific configuration is included.

1. Make sure that your tester is connected to the network. The physical layer must be up and working.
2. From the *Home* panel, go to *Setup*. The test port settings panel is displayed.
3. Select either Port A or Port B to enter in the port specific configuration.
   Note: Most of the frame configuration settings are not available from Port B because traffic generation is not available from this port.
4. Enter in the *Frame* menu.
   All settings related with frame configuration are displayed.

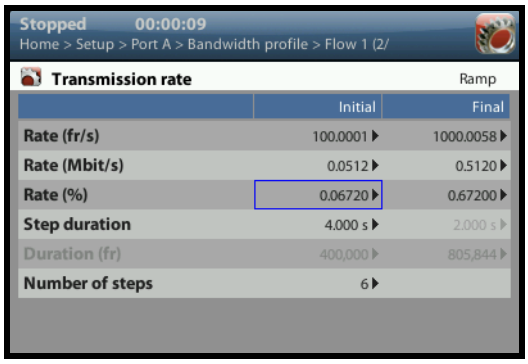


Figure 5 *ALBEDO Ether.Genius / Ether.Sync / Ether.Giga bandwidth profile configuration panel.*

5. Configure the correct MTU with the help of the *MTU* menu. You may want to set the MTU to 1518 bytes for traffic analysis in line with IEEE 802.3 or to other value to allow jumbo frames. The maximum allowed MTU is 10,000 bytes.
6. Select one of the traffic flows between *Flow #1* and *Flow #8* to enter in the flow specific configuration.
7. Configure the encapsulation you are going to use in the generated frames. Basically, the *Encapsulation* menu sets the number of VLAN tags to be included in the generated frames.
8. Enter the source MAC address with the help of the *Source MAC address from* and *Source MAC address* controls. You can configure the factory MAC address as the source address for the generated frames or enter a custom address.
9. Enter the destination MAC address or addresses by using the *Destination MAC address from*, *Destination MAC address* and *Address range size*. If you choose to generate a destination address range you will be requested to enter the number of addresses that made up the range.
10. Configure the *Ethertype* value.
    Note: Some frame structures require an specific value of the Ethertype. This field cannot be configured in this case.
11. If you are using frames carrying one (IEEE 802.1Q) or two (IEEE 802.1ad, Q-in-Q) VLAN tags, enter the *C-VID* and *C-VLAN priority*.
12. If you are using frames carrying two VLAN tags (IEEE 802.1ad, Q-in-Q), enter the *S-VID*, *S-VLAN priority* and *Drop-ligible Indicator*.
13. If you are generating not-standard Q-in-Q frames, set the *S-VLAN TPID* to one of the allowed values.
14. Configure the frame length to the correct value with the help of *Frame size*.
15. If necessary, repeat the specific flow configuration for one or more traffic flows (*Flow #1* to *Flow #8*) from the *Frame* menu.

Table 1
Ethernet Frame Settings.

Setting	*Description*
Encapsulation	This field configures the way the data is encapsulated in Ethernet frames for transmission in the current stream. The allowed encapsulations are the following ones: • *None*: A DIX or IEEE 802.3 frame carries the test data, depending on the current value of the *Frame type* setting. • *VLAN*: Transmitted frames are labelled with an IEEE 802.1Q frame tag. Settings related with configuration of the VLAN tag are enabled when this option is selected. • *Q-in-Q*: Transmitted frames carry two VLAN tags, one service provider tag (S-VLAN) and a customer tag (C-VLAN). The C-VLAN is identified by the normal IEEE 802.1Q Ethertype and the S-VLAN carries one of the not-standard Ethertypes. • *IEEE 802.1ad*: Transmitted frames carry two VLAN tags. It is similar to the Q-in-Q encapsulation but this option follows strictly the standard IEEE 802.1ad encapsulation for Provider Bridges (PB). Specifically, the IEEE 802.1ad carries the special 0x88a8 Ethertype within the S-VLAN.
Source MAC address from	Establishes the origin of the source MAC address for the current stream. There are two possible settings: • *Local*: The source address is set to the factory MAC address assigned to the port. Use this setting if there is no other requirement. • *Manual*: The source address is set to the value configured in *Source MAC address*. Use manual MAC addresses if you want to simulate traffic generated by an equipment different to the tester or, in multi-stream operation, to simulate traffic transmitted from different stations. Most of the times you will want to avoid duplicated addresses in your network. For this reason, make sure that no other equipment is using the manually configured MAC address.
Source MAC address	Source MAC address carried by the frames generated in the current stream if *Source MAC address type* is set to *Manual*. Anything from 00-00-00-00-00-00 to ff-ff-ff-ff-ff-ff is allowed.
Destination MAC address from	Establishes the origin of the destination MAC address for the current stream. There are three different settings available for configuration: • *ARP*: Uses the Address Resolution Protocol (IETF RFC 826) to configure the destination MAC address without user intervention. The ARP requires the IPv4 destination address to be previously configured to work. For this reason, ARP is available only in *IP endpoint* mode. • *Manual*: The destination address is set to the value configured in *Destination MAC address*. • *Range*: Test data in the current stream is transmitted to a group of MAC addresses configured with *Destination MAC address* and *Address number within range*. Use this option if you want to deliver the test data sequentially to many different destinations.
Destination MAC address	Destination MAC address carried by the frames generated in the current stream if *Des. MAC address type* is set to *Manual*. If *Des. MAC address type* is set to *Range*, this field contains the first destination MAC address within the range. Anything from 00-00-00-00-00-00 to ff-ff-ff-ff-ff-ff is allowed for this field.
Address range size	Configures the number of MAC addresses within an address range. This control is valid only if *Des. MAC address type* is set to *Range*. In this case, the ethernet frames transmitted in the current stream will contain as many destination addresses as previously configured in this field. The destination MAC address is increased by one unit for each transmitted frame starting with the value configured in *Destination MAC address*. If there are no more addresses left in the range, transmission returns to the initial address and starts the process from the beginning.
Ethertype	Ethertype value carried by the frames generated in the current stream. This value is found within the Ethernet *Type* header field in DIX / Ethernet II frames or within the LLC / SNAP header in IEEE 802.3 frames. Depending on the configuration, the *Ethertype* value is fixed and cannot be set by the user. If the operation mode is *IP endpoint*, the Ethertype is automatically configured to 0x0800 (Internet Protocol, version 4). If the payload type is configured to *SLA* in *Ethernet endpoint* mode, the Ethertype is set to 0x8902 (IEEE 802.1ag / ITU-T Y.1731 OAM) to account for the special structure of the Ethernet SLA measurement payload.

Table 1
Ethernet Frame Settings.

Setting	*Description*
C-VID	VLAN identifier assigned to tagged frames (IEEE 802.1Q) or C-VLAN identifier for double tagged frames (IEEE 802.1ad, Q-in-Q). In frames with two VLAN tags, the C-VID usually accounts for the VLAN structure corresponding to the customer network. Any value within 0 to 4096 is allowed for this field.
C-VLAN priority	3-bit class of service (CoS) field defined to set frame groups with different priorities or to provide specific treatments to special frames within a network or an administrative domain. This field is carried by the Q-tag of Ethernet frames with a single tag or by the C-tag of Ethernet frames with two tags. Any value from 0 to 7 is allowed for this field. Specific actions to be carried out on frames with different CoS labels depend on the network and the service provider.
S-VLAN TPID	Ethertype to be associated to the S-VLAN tag in Q-in-Q frames. Four different values are possible: 0x8100, 0x9100, 0x9200 and 0x9300. It the encapsulation is set to IEEE 802.1ad, the S-VLAN Ethertype is automatically set to 0x88a8 and this field is not available for configuration.
S-VID	VLAN identifier assigned to the S-tag in double tagged frames (IEEE 802.1ad, Q-in-Q). In frames with two VLAN tags, the S-VID usually accounts for the VLAN structure corresponding to the service provider network. Any value within 0 to 4096 is allowed for this field.
S-VLAN priority	3-bit class of service (CoS) field defined to set frame groups with different priorities or to provide specific treatments to special frames within a network or an administrative domain. This field is carried by the S-tag (service provider tag) of Ethernet frames with two tags. Any value from 0 to 7 is allowed for this field. Specific actions to be carried out on frames with different CoS labels depend on the network and the service provider.
Drop-eligible indicator	This is a single bit field that is used to mark drop eligible frames. These frames are usually dropped first when congestion is detected in a network node. The Drop eligible operator is carried within the S-tag of IEEE 802.1ad frames.
Frame size	Ethernet MAC frame size including the destination MAC address, source MAC address, type / length field, payload, FCS and any VLAN tag carried by the frame. Anything between 64 B and 10000 B is allowed but frames longer than 1518 B (without VLAN tags and MPLS labels) are out of the IEEE 802.3 standard. It is possible to generate frames longer than the port Maximum Transmission Unit (MTU) but these frames are considered oversized frames when they are analyzed by the tester. To avoid an *OverS* anomaly in this case, increase the value of the port MTU.

Configuring the Bandwith Profile

In the same way that the *Frame* menu configures the frame format for each of the available traffic flows, the Bandwidth profile sets how many frames are transmitted and how transmission events are distributed in time. The simplest is to generate frames with a constant bit rate specified in frames per second, bits per second or as a percentage of the total transmission channel capacity. However, Ether.Genius / Ether.Sync / Ether.Giga provide other alternatives to the constant transmission like the periodic burst and ramp transmission or random transmission with Poisson statistics.

The bandwidth profile settings are available only in port Port A because the traffic generator is not available in Port B. The procedure to configure the bandwidth profile in a traffic flow is as follows:

1. Make sure that your tester is connected to the network. The physical layer must be up and working.
2. From the *Home* panel, go to *Setup*,
   The test port settings panel is displayed.
3. Select Port A to enter in the port specific configuration.
   Note: There is no bandwidth profile configuration for Port B because Port B is unable to generate synthetic traffic.
4. Enter in the *Bandwidth profile* menu.
5. Select one of the traffic flows between *Flow #1* and *Flow #8* to enter in the flow specific configuration.
   All configuration items related with the bandwidth profile are displayed.
6. Configure the transmission mode to one of the available profiles with the help of the *Mode* control.
7. Configure the transmission rate parameters with *Transmission Rate*.
   Note: Depending on the current transmission mode you will be requested to

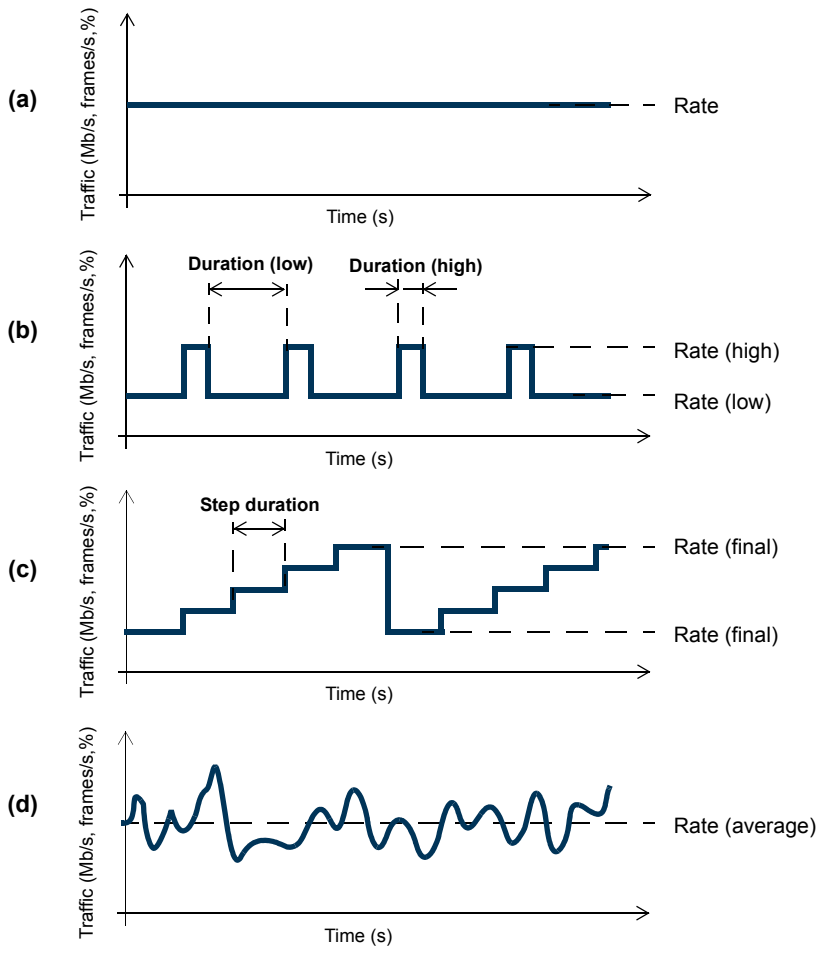


Figure 6 *Bandwidth profiles for ALBEDO Ether.Giga / Ether.Genius / Ether.Sync testers: (a) Continuous traffic generation, (b) Periodic burst generation, (c) Ramp generation, (d) Random traffic generation with Poisson probability distribution.*

enter different traffic parameters in the *Transmission Rate* panel.
Note: Changing some transmission parameter may affect the value of other parameters previously configured in the same panel. For example, setting the transmission rate in frames per second modifies the rate in bits per second and the percentage value of the transmission rate.
Note: If the channel capacity varies, the transmission rates configured as percentages of the overall channel capacity are kept to se same value but the bits per second and frames per second are recomputed for the new channel capacity.

Table 2
Ethernet Payload Settings.

Setting	*Description*
Mode	• Configures the traffic shape to be used by the traffic generator in the current stream. There are five possible generation modes for this for the bandwidth profile • *Off*: No frames are transmitted in the current stream. Use this setting if you want to disable traffic generation in the current stream but you don't want to globally disable generation in the test port. • *Continuous*: Frames is transmitted at a constant speed to match a value configured in bits per second, frames per second or a percentage of the line capacity. • *Periodic burst*: Traffic generation is distributed in periodic bursts of fixed length. Between traffic bursts the user may choose to generate background traffic or disable traffic generation. • *Ramp*: Generates traffic that increases its bit rate with time in steps. The number of steps and step duration are configured by the user. Minimum and maximum traffic generated in the ramp are user configurable as well. Ramp generation is periodic. Traffic generator is restarted when it finishes with the last step of an specific ramp. • *Poisson*: The number of frames generated per time unit is a Poisson random variable. This is equivalent to say that the distance between two consecutively generated frames is an exponential random variable. Use the Poisson generation profile to generate traffic that resembles network traffic as much as possible.
Transmission rate	This control displays an editable table that enables the user to enter the parameters associated with the traffic to be generated by the current stream. Parameters to be configured depend on the current bandwith profile generation mode: • *Continuous* traffic: The relevant bandwidth parameter is the transmission *Rate* configured in *fr/s*, *Mb/s* or*%*. • *Periodic burst*: Values to be entered are the high and low transmission rates (in *fr/s*, *Mb/s* or*%*) and the high and low durations expressed in seconds or frames. • *Ramp*: Relevant configuration parameters are the initial and final transmission rates (in *fr/s*, *Mb/s* or*%*), the *Step duration* configured in seconds and the *Number of steps*. • *Poisson*: The bandwidth parameter to be configured is the average transmission rate in *fr/s*, *Mb/s* or*%*.

8. If necessary, repeat the bandwidth profile configuration process for one or more traffic flows (*Flow #1* to *Flow #8*) available from the *Bandwidth profile* menu.

   Test traffic generation does not start immediately after setting the bandwidth profile parameters. Traffic generation requires a test to be started with the RUN button.

Choosing the Test Payload for Ethernet

Traffic generated by Ether.Genius / Ether.Sync / Ether.Giga is synthetic. It does not contain any real user data. In fact, the user payload of the internally generated frames is replaced by a test payload. Many times, test payloads are much more than dummy bit sequences designed to replace the user traffic. Test payloads may contain time stamps or sequence numbers that determine which test metrics are available from the result panels or which tests will be run. For this reason, configuration of the right test payload is important to get the required results.

Selection of the test pattern is relevant both for the generator and the analyzer. When you generate a test payload or pattern in Port A, the same port is automatically configured so that it is waiting for frames carrying the same pattern in the receiver. Settings related with test payload / pattern selection are available both in Port A and Port B. The procedure to select the test payload in the tester is as follows:

1. Make sure that your tester is connected to the network. The physical layer must be up and working.
2. From the *Home* panel, go to *Setup*. The test port settings panel is displayed.
3. Select either *Port A* or *Port B* to enter in the port specific configuration.
4. Enter in the *Payload* menu.
5. Select one of the traffic flows between *Flow 1* and *Flow 8* to enter in the flow specific configuration.
   All settings related with payload configuration in the current flow are displayed.

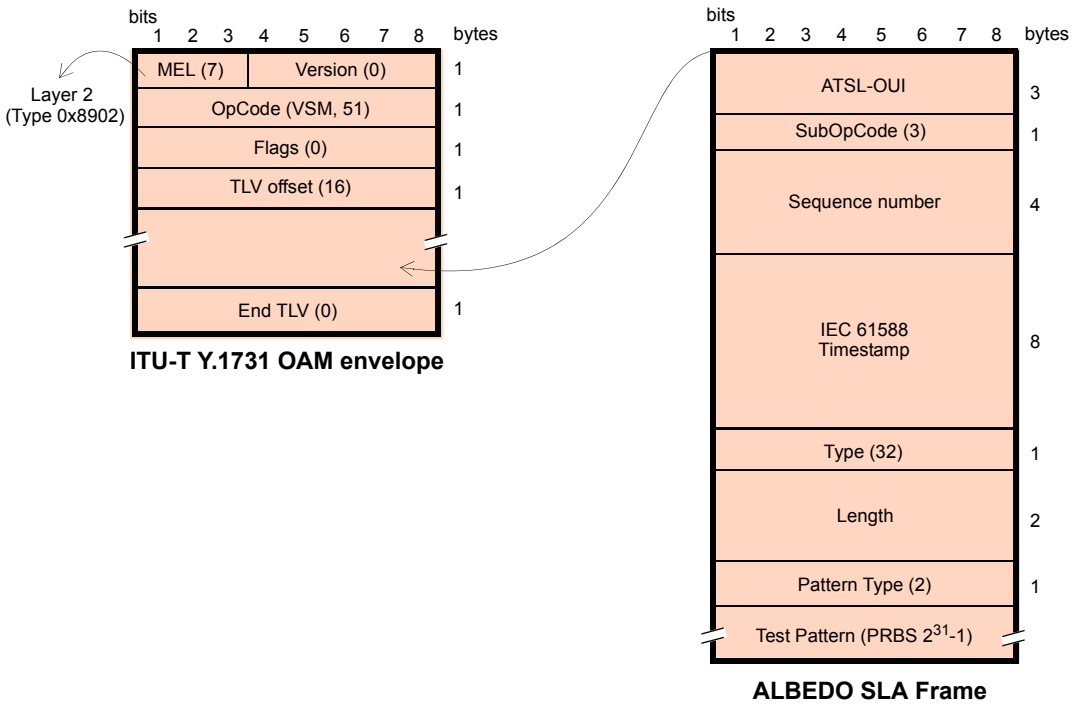


Figure 7 *ALBEDO payload for SLA tests (Ethernet Endpoint mode).*

6. Choose one of *BERT*, *SLA* or *All zeroes* in *Payload type*.
   Note: BER is available only for flow 1.
7. If you have configured *Payload type* to BER, choose the bit pattern you are going to use for generation (Port A) and analysis (Port A and Port B) with the help of the *BERT patterns* control.
8. If you have configured *BERT patterns* to *User*, enter a 32-bit test pattern in *User payload* in hexadecimal format.
9. If necessary, repeat the payload configuration process for one or more traffic flows (*Flow #1* to *Flow #8*) available from the *Payload* menu.

Table 3
Ethernet Frame Settings

Setting	*Description*
Payload Type	• BERT: The payload content is set to a bit pattern suitable for measuring the Bit Error Ratio (BER). The tester includes support for two different kinds of BERT pattern: Pseudo-Random Bit Sequences (PRBSs) or 32-bit user configurable patterns. BERT generation and analysis over framed interfaces is supported by flow 1 only. • SLA: This is the payload to be used to measure latency, packet loss and all the SLA metrics derived from them. If the current operation mode is set to Ethernet endpoint, the SLA payload constitutes a proprietary extension of the Operation, Administration and Maintenance (OAM) protocol for Ethernet defined in ITU-T Y.1531. The SLA payload in IP Endpoint mode is a proprietary ALBEDO Telecom format. • *All zeroes*: Sets the transmitted pattern to all zeroes.
BERT Patterns	Sets the transmitted and expected test pattern (port A) or the expected test pattern (port B). Supported patterns are: • *PRBS 2^{11}-1 /2^{11}-1 inverted*: This is a pseudo-random bit pattern specified in ITU-T O.153 for error performance measurements below the primary rate (2048 kb/s). The 2^{11}-1 inverted is a 2^{11}-1 bit wise inverted pattern. • *PRBS 2^{15}-1 /2^{15}-1 inverted*: This is a pseudo-random bit pattern specified in ITU-T O.151 for measurements at the primary rate or above. The 2^{15}-1 inverted is a 2^{15}-1 bit wise inverted pattern. • *PRBS 2^{20}-1 /2^{20}-1 inverted*: This is a pseudo-random bit pattern specified in ITU-T O.151 for error performance measurements at the primary bit rate or above. The 2^{20}-1 inverted is a 2^{20}-1 bit wise inverted pattern. • *PRBS 2^{23}-1 /2^{23}-1 inverted*: This is a pseudo-random bit pattern specified in ITU-T O.151 for error performance measurements at the primary bit rate or above. The 2^{23}-1 inverted is a 2^{23}-1 bit wise inverted pattern. • *User*: Sets a 32-bit, user configurable word as the transmitted pattern.
User payload	Here it is configured the value of the user payload that is used as the transmitted pattern when *BERT Pattern* is set to *User.*

Some test payloads are byte patterns (*BERT* pattern, a*ll-Zeroes* pattern) but some others have a more complex structure like the *SLA* test payload. Specifically, the SLA test payload used by Ether.Genius / Ether.Sync / Ether.Giga is a proprietary extension of the Operations, Administration and Maintenance (OAM) payload defined by standard ITU-T Y.1731.

2. GENERATION OF IPV4 TRAFFIC

Without a Network layer, all the Ethernet traffic generated by the testers would be unable lo leave the local network and reach remote networks. The Network Layer, or Layer 3, provides end-to-end connectivity between stations that can use heterogeneous underlying technologies and they are not necessarily attached to the same network. Routers do manage layer 3 protocols and data forwarding based on routing tables.

The *Internet Protocol* (IP) is the most popular Layer 3 protocol. It was conceived by the U.S. *Department of Defence* (DoD) during the cold war to facilitate communication between dissimilar computer systems and is a reliable technology. IP interconnects public or private autonomous systems providing a connectionless service.

There are two IP protocol versions (IPv4 and IPv6). IPv4 addresses are defined as a subset of the IPv6 addressing space but IPv4 and IPv6 can be regarded as different and incompatible network protocols in any other sense. Currently, Ether.Genius / Ether.Sync / Ether.Giga are compatible with version four of the IP protocol (IPv4).

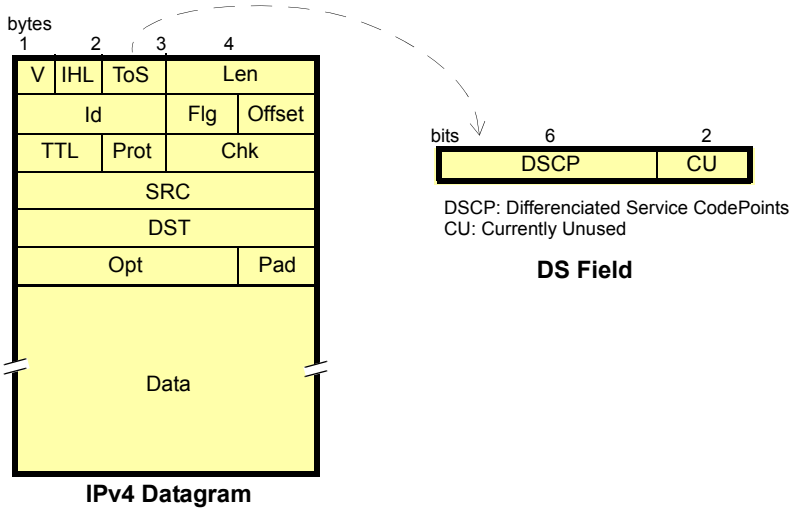


Figure 8 *IPv4 datagram structure.*

The correct operation mode for IPv4 packet generation is the *IP Endpoint* mode. Basically, the traffic generator in *IP Endpoint* mode is configured in the same way than in *Ethernet Endpoint* mode. However, there are some differences to be taken into account:

- In *IP Endpoint* mode, the test equipment becomes a host in an IP network and it has similar properties than any other network equipment. For this reason it is necessary to assign a valid IP profile to the tester either automatically (DHCP) or by hand.
- The test equipment is now ready to use some helper protocols to make the configuration process easier. Specifically, the Address Resolution Protocol (ARP), configures destination MAC address without user intervention. The

Domain Name Service (DNS) replaces the configuration of the destination IP addresses by the much simpler domain name configuration.

- Ethernet frames carry IPv4 packets with an specific structure and content. It is necessary to configure the IPv4 packet before it is prepared to generate IP datagrams.

Configuring the Physical and MAC Layers

Physical (layer 1) and MAC (layer 2) configuration is similar in *IP Endpoint* and *Ethernet Endpoint* modes (see User Guide). The only difference is that users now have at their disposal the ARP mechanism to configure the destination MAC address automatically. ARP gets the destination MAC address from the network using the destination IPv4 address by means a broadcast protocol.

To use ARP to set the destination MAC address without user intervention, you have to configure the *Destination MAC address from* to ARP. Once ARP has been configured the test units generates one or several broadcast ARP requests to compute the destination MAC address. Generation of ARP control traffic is automatic and it is not controlled with the RUN button like it happens with the test traffic.

Configuring the Port Local Network Profile

The test equipment requires a local IP profile when it is operating in *IP Endpoint* mode. Even if the traffic generator has been configured to work with a custom IP address (different to the local IP address), the equipment still requires an internal address for some tests like the IP Ping or the Traceroute. Furthermore, some control and signalling protocols may work with the information stored in the local IP profile.

Configuration of the local IP profile is available form the port specific settings within the Setup menu (see User Guide).

Configuring the IPv4 Datagram

The IPv4 packet content is set much in the same way that the MAC frame content. However, in this case, MAC addresses are replaced by IPv4 addresses. Of course, IPv4 datagrams have their own structure and they contain some fields not present in Ethernet frames.

All the IPv4 datagram configuration lays within the *Network* menu. The network menu is not enabled unless the port is configured in TX / RX mode. For this reason, there is no Network configuration menu in Port B (Port B does not support TX / RX mode).The procedure to follow to configure the IP datagram is described below:

1. Make sure that your tester is connected to the network. The physical layer must be up and working. Check that your tester is operating in *IP Endpoint* mode (See User Guide) and that the port is in *TX / RX*.

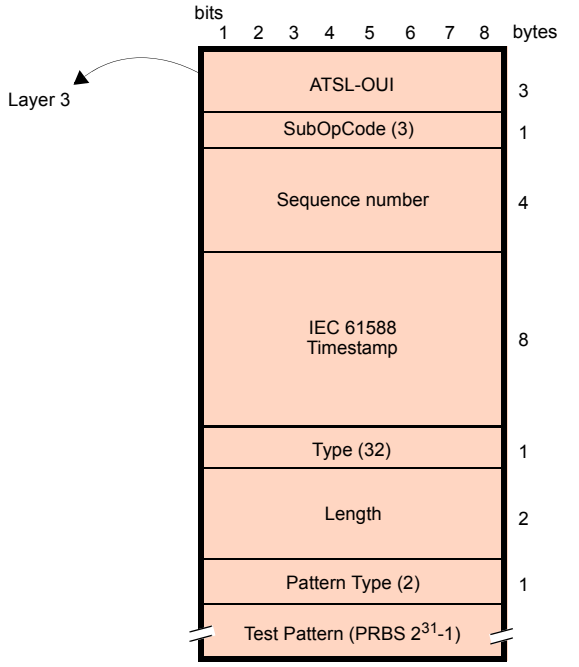
Table 4
IPv4 Packet Settings.

Setting	*Description*
Source IPv4 address from	Establishes the origin of the source IPv4 address for the current stream. There are two possible settings: • *Local*: The source address is set to the IPv4 address configured in the port local profile. The local address may be either configured by means the DHCP protocol or in may be static. • *Manual*: The source address is set to the value configured in *Source IPv4 address*. Use manual IPv4 addresses if you want to simulate traffic generated by an equipment different to the tester or, in multi-stream operation, to simulate traffic transmitted from different hosts. Probably, you will want to avoid duplicated IP addresses in your network. For this reason, make sure that no other equipment is using the manually configured IPv4 address.
Source IPv4 address	Source IPv4 address carried by the packets generated in the current stream if *Source IPv4 address from* is set to *Manual*. The address is entered in decimal, four-dotted format. Any address between 0.0.0.0 and 255.255.255.255 is admitted as a source IPv4 address.
Destination IPv4 address from	Establishes the origin of the destination IPv4 address for the current stream. There are three different settings available for configuration: • *Manual*: The destination address is set to the value configured in *Destination IPv4 address*. • *Range*: Test data in the current stream is transmitted to a group of IPv4 addresses configured with *Destination IPv4 address* and *Address range size*. Use this option if you want to deliver the test data sequentially to many different destinations. • *Host name*: Uses the Domain Name Service (DNS) to set the destination IP address by using descriptive alphanumeric strings. The DNS mechanism requires intervention of at least one DNS server. The DNS server IP address has to be configured in the local port profile either statically or by means DHCP.
Destination IPv4 address	Destination IPv4 address carried by the packets generated in the current stream if *Destination IPv4 address from* is set to *Manual*. The address is entered in decimal, four-dotted format. Any address between 0.0.0.0 and 255.255.255.255 is admitted as a destination IPv4 address.
Destination IPv4 address (DNS)	Destination IPv4 address carried by the packets generated in the current stream if *Destination IPv4 address from* is set to *Host name*. This is a read only field that it cannot be edited directly. It displays the result of the DNS name resolution carried out with the host name configured in *Destination host name.*
Address range size	Configures the number of IPv4 addresses within an address range. This control is valid only if *Destination type* is set to *Range*. In this case, the IP datagrams transmitted in the current stream will contain as many destination addresses as previously configured in this field. The destination IP address is increased by one unit for each transmitted frame starting with the value configured in *Destination IPv4 address*. If there are no more addresses left in the range, transmission returns to the initial address and starts the process from the beginning.
	Transmission of destination IPv4 address ranges is compatible with transmission of destination MAC address ranges but the address number of the MAC address range is always fixed to the same number that the IP range. It is not possible to transmit a destination MAC address range with a single IPv4 address.
Destination host name	Domain name to be used as a destination if *Destination type* is set to *Domain name*. Unlike IP addresses, domain names are easy-to-remember alphanumeric strings but they have to be translated to IP addresses before any packet can be sent to the destination. The translation process requires the intervention of at least one DNS server. The DNS server IP address has to be configured in the local port profile either statically or by means DHCP.
DSCP	Differentiated Services Code Point. It is 6-bit class of service (CoS) field defined to set packet groups with different priorities or to provide specific treatments to special packets within a network or an administrative domain. Any value from 0 to 63 is allowed for this field. Specific actions to be carried out on frames with different DSCPs depend on the network and the service provider.

Table 4
IPv4 Packet Settings.

Setting	*Description*
TTL	Initial Time To Live value configured in the packets transmitted in the current stream. The TTL is decreased by one unit each time it lefts a network node. If the value reaches zero, then the packet is discarded. The TTL is then a measure of the number of nodes the packet is allowed to transverse before reaching its destination.
UDP	Enables or disables transmission of the User Datagram Protocol (UDP) in the current stream. The UDP is defined in RFC 768 and it is a lightweight transport protocol for unreliable data transmission. RFC 768 defines an eight-byte fixed length header for UDP that is generated when UDP generation is enabled in the stream. If UDP generation is on, the *Transport protocol* field is set to 17. This value cannot be edited by the user.
Transport protocol	This setting contains an 8-bit word that constitutes the protocol identifier to be transmitted by the traffic generator. TCP uses 6 as the protocol number, UDP uses 17 for the same purpose and ICMP uses number 1. However, the payload structure does not match the structure corresponding to these protocols even if the correct protocol number is configured. To enable UDP header and payload generation, enable UDP in the current stream.
Source port	Source transport layer port transmitted in the UDP header in the current stream. Ports are service identifiers used to multiplex data from different applications generated by IP hosts. The tester supports source port generation for UDP streams only.
Destination port	Destination transport layer port transmitted in the UDP header in the current stream. Ports are service identifiers used to multiplex data from different applications generated by IP hosts. The tester supports destination port generation for UDP streams only.

2. From the *Home* panel, go to *Setup*. The test port settings panel is displayed.
3. Select Port A to enter in the port specific configuration.
   Note: There is no network configuration for Port B.
4. Enter in the *Network layer* menu.
5. Select one of the traffic flows between *Flow 1* and *Flow 8* to enter in the flow specific configuration. All settings related with network configuration in the current flow are displayed.
6. Enter the source IP address with the help of the *Source IPv4 address from* and *Source IPv4 address* controls. You can configure the IP address from the local IP profile as the source address or enter a custom address.
7. Enter the destination IPv4 address or addresses by using the *Destination IPv4 address from*, *Destination IPv4 address*, *Address range size* and *Destination host name*. If you choose to generate a destination address range you will be requested to enter the number of addresses that made up the range. If you choose to enter the destination as a host name rather than an IPv4 address, you will be requested to enter a valid domain name.
8. Configure the DSCP and TTL if necessary.
9. Enable or disable UDP generation and analysis with the help of the *UDP* control.
10. If you have enabled UDP, enter the *Source Port* and *Destination Port* to be used in the generated UDP packets.



ALBEDO Telecom Ethernet SLA Frame

Figure 9 *ALBEDO payload for SLA tests (IP Endpoint mode).*

11. If you have not enabled UDP, configure the *Transport Protocol* code.
12. If necessary, repeat the IPv4 configuration process for one or more traffic flows (*Flow #1* to *Flow #8*) available from the *Network layer* menu.

Setting the Bandwidth Profile

Setting the bandwith profile in IP Endpoint mode is the same that in Ethernet Endpoint mode.

Choosing the Test Payload for IPv4

Ether.Genius / Ether.Sync / Ether.Giga, include special packet payloads and patterns required for all usual applications, including BER tests and SLA tests. Payloads and patterns available in *IP Endpoint* mode are similar than in *Ethernet Endpoint* mode. However, there is a difference concerning the SLA payload. While in Ethernet Endpoint the SLA payload is defined as an extension of the ITU-T Y.1731 structure, in *IP Endpoint*, this payload is ALBEDO Telecom proprietary. In practical terms, the new structure of the SLA payload should not make any difference.

ALBEDO Telecom

ALBEDO Telecom designs, manufactures, and delivers solutions that enable Telecom organizations of all sizes to test, measure, troubleshoot, monitor, and migrate mission critical networks and multiplay applications.

On local segments and across distributed networks, ALBEDO enable Organizations, Installers, Operators, Service Providers and Suppliers to quickly check the health of Network Architectures, Service Agreements (SLA), IP Quality (QoS), or fix any issue.

Your Business Partner

Results. ALBEDO Telecom helps the industry to make the most of the investment on infrastructure.

Expertise. ALBEDO Telecom engineers and consultants provide industry leading knowledge in hand-held TAPs and WAN emulators, IPTV, VoIP, Carrier-Ethernet, Synchronization, Jitter, Wander, SyncE, PTP, E1, and Datacom to address customers unique needs.

Integration. ALBEDO Telecom integrates disparate telecom technologies and applications, facilitating new business efficiencies.

Agility. ALBEDO Telecom increases the ability of customers to respond quickly to new market opportunities and requirements.

Coverage. ALBEDO Telecom offers solutions that facilitates the migration and the roll-out to new architectures.

aims

+ UNDERSTAND causes of telecom interoperability issues
+ EXPERIENCE the best quality in unified networking
+ ASSESS different hardware, firmware, and software solutions
+ LEARN from experts by means of professional services and consultancy