# LanExpert 80 Revision History

**Version 2.26.03**

Upgraded detection on both incoming and outgoing calls for VoIP.

**Version 2.20.01**

Upgraded CDP/LLDP detection for Voice VLAN/Appliance ID tags.

**Version 2.02**

This release removes the ERASE ALL MEMORY capability which made the unit not useable.

**Version 2.01**

Internal Clean up of 2.00 version

**Version 2.00**

This version changes –

1. The maximum number of captured frames has been extended to a maximum of 8192 frames (it used to be 1024 frames).
2. The previous "LOCK" setup screen has been replaced by a SECURITY screen. This allows the user to setup user names and passwords for 4 user accounts, and also allows three different levels of SDcard secure erasure. If security is enabled (by entering a user name and/or password for the ADMIN account) then the LE80 will ask for a user name and password to be entered after showing the welcome screen at power on. See below for more information.
3. The LE80 now displays a message for about 2 seconds when a remote connection is initiated to it.
4. Added a %age figure after "SAVING" on the NETWORK ANALYSIS SAVE screen. While saving either detector or capture data, to either internal or external memory, this updates while saving.

**Security: User Accounts**

There are four user accounts (ADMIN, and USER #1 through #3).

- If both the username and password of the ADMIN account is blank then security is turned off and no logon is required.
- Any user account username and/or password can be blank.
- Any username or password can be the same as another accounts' username – the username/password pairing determines the user level. If both the username and password are the same as another user account – the lowest numbered account is logged into by that username/password.
- While logging in the password is not visible (each character is shown as an asterix character), the password is visible while editing it in the security screen.
- When successfully logging in – a temporary display is shown so that you can tell which account you just logged into.
- While logging on, or while editing the username/password the following "special" actions can be done –

- While entering the username, pressing the ENTER area ends entry of the username and starts entry of the password.
- While entering the password, pressing the ENTER area ends entry of the password and logs on or saves the edited data (as applicable).
- Pressing the EXIT (upper right corner X) both the username and password entries are terminated and the user is logged on or the username/passwords are saved as applicable.
- Pressing either of the two entry areas selects that data as being entered.
- Both the username and the password are case sensitive and can be up to 16 characters long. There are no restrictions on the characters (using the keyboard provided on the screen).
- If the user enters a username/password which does not match any enabled account, then the entry screen is restarted immediately with a blank username and password.

The ACCESS menu operates as follows (checking the respective box enables the access) and only affects USERS #1 thru 3 and can only be accessed by the ADMIN user –

- ENABLED – enables the respective user account (does not affect the stored username & password though).
- NAMES & PASSWORDS – allows the respective user to edit usernames and passwords for USERS #1 thru' 3 (a "user" can never edit the ADMIN username or password).
- SECURE ERASE – allows the respective user to perform a secure erase (a "user" can never perform a total erase).
- SELECT PROFILE - allows the respective user to change which profile is selected (if not enabled, they can still view which is selected, they just can't change it).
- SETUP PROFILE – allows the respective user to make alterations to the selected profile (i.e. all setup is disabled and the user cannot rename the profile if this is not enabled)

All of the VIEW: settings are designed to prohibit an unauthorized user from viewing potentially secure data (phone numbers, email addresses, device names etc.) –

- VIEW VoIP DATA – the user can START/STOP/CLEAR VoIP data collection, and can save the results of the collection as part of the detector database, but they cannot view it.
- VIEW EMAIL DATA – similar to VoIP DATA but affect the EMAIL screen.
- VIEW CAPTURED DATA - similar to VoIP DATA but affect the CAPTURE screen.
- VIEW 802.1X DATA - similar to VoIP DATA but affect the 802.1X screen.
- VIEW DEVICE DATA - similar to VoIP DATA but affect the DEVICES and TOP TALKERS screen.

All of the GENERATE: settings are designed to stop an unauthorized user from performing an operation which has the potential of bringing down a network or setting off a network security alarm.

- GENERATE TRAFFIC – enables/disables the respective users ability to use TRAFFIC GENERATE.
- GENERATE PINGS - enables/disables the respective users ability to use PING/TRACE.

NOTE – a “user” with an enabled account but with nothing else enabled can still use the LanExpert to collect data – this allows a lower security user to collect (and save) data from a higher security network which can later be recalled and inspected by somebody with higher clearance.

- ALL PROFILES – secure erases all user settings and returns them to factory defaults, except security itself, selects profile #1 (factory defaults). This takes a few seconds.
- ALL SAVED DATA – secure erases all user internally stored results (detectors, captured frames and stress test results). This takes about an hour.
- ALL MEMORY – secure erases all used areas of the SDcard and turns off the unit, which is then unusable. This takes a few hours. This will result in the customer sending the LanExpert back to the factory and a service fee will be applied.

*NOTE* – ALL MEMORY is only available if a) security has been enabled (i.e. the ADMIN account has a valid username and/or password) and the ADMIN user is logged in. All three of these require the user to confirm the operation.

**Security: Secure Erase**

When the START button is pressed for the selected erase area the LE80/85B displays a message for about 2 seconds, telling them that this cannot be undone and they need to confirm the requested secure erasure. When it returns to the security screen the respective START button is now CONFIRM and must be pressed again to actually perform the erasure. For the ALL MEMORY selection, the message is different (warning that this renders the unit inoperable), and the unit automatically powers down after completion, but is otherwise similar. While erasing, the percentage completion is displayed to the right of the respective START/CONFIRM button.

*NOTE* – changes made in the security screen to user names and/or passwords do not take effect until the next power cycle.

*NOTE* – to log off (and back on again) the user must cycle power to the LE80/85B.
A few notes regarding user names and passwords –

- All save and recall activities now have a percentage completion shown if possible
- If available, the VCT (cable length) data is now included with the saved detectors and displayed when recalled.
- The detected LLDP, CDP and FDP frames are now included with the saved detector data and can be displayed from the recall screen.
- The detected 802.1X frames are now included with the saved detector data and can be displayed from the recall screen.

**802.1X Data**

The last 50 802.1X packets received (from either port in INDEP mode, the active port in SINGLE mode, port 1 in INDEP mode). Each packet will have a date/timestamp, and the pertinent details stored enabling us to display the following for each packet –

- The source MAC address of the packet

- The destination MAC address of the packet.
- The 802.1X version # (they are presently at v3, v4 to be released shortly)
- The 802.1X packet type (EAP, Start, Logoff, EAPOL-key, EAPOL-ASF Start, MKA, Announcement-Generic, Announcement-Specific, Announcement-Request, or just the byte numeric if not known).
- The length of the EAPOL body (i.e. everything else).
- If it's a EAP 802.1X packet type then –
    - EAP code (Request, Response, Success, Failure or just the byte numeric if not known).
    - EAP ID #
    - EAP Body length (adjusted to remove the code, ID and length)
    - If it's a Request or Response EAP code then –
        - § The EAP request/response type (Identity, Notification, Nak, MD5 challenge, OTP challenge, Generic Token Challenge, TLS, and perhaps others, or just the byte numeric if not known).

Note – this is very similar to what we do for LLDP/CDP/FDP.

The LanExpert must be positioned between the Supplicant (AKA client – i.e. the PC) and the Authenticator (i.e. the switch/router) and to really tell what's going on there should only be the one set of 802.1X traffic occurring.

## Version 1.75

This version changes –

- Previously, if the user configured a port for AUTO-DETECT MDI/X (in the ports configuration) and it failed to link either as a LAN or a NIC then it was not reported as a "PROBLEM". This has been corrected.
- The LINK screen has been altered to have a single page while linking. The operation once linked is as before. On the single page, while linking, the screen shows the status of both ports 1 and 2.
- The screen shows one of the following for each port –
    - When initially linking (for up to about 4 seconds) – LINKING
    - If it fails to link then it shows one line per pair, each showing one of –
        - OK – indicating that the pair is properly terminated.
        - OPEN followed by two numbers. The first shows the reflected amplitude (16 = none, <16 = short, > 16 = open) in the range 0 through 31. The second shows the length in feet and meters up to 178 Meters or 583 feet.
        - SHORT followed by two numbers is displayed the same as described for OPEN.
        - UNKNOWN. The LE could not determine what was wrong because of external signal presence.
    - The linked speed (this only shows if configured for INLINE or INDEP mode and the other port is not linked).

## Version 1.74

Internal Release Only

## Version 1.73

This version shifted the External Calibrated Rx Optical power reported for a Fiber SFP downwards by 10dBm. Internally calibrated Rx power and both types of Tx power are unaffected. (FOR LE85 ONLY)

**Version 1.72**

This version adds CDP TLV decode as follows–

- ☐ CDP Type 1 TLVs –
  - o Displays “Type 1 – Device ID”
  - o Displays “LENGTH: “ followed by the actual string length in the TLV(up to 25 characters)
- ☐ CDP Type 2 TLVs –
  - o Displays “Type 2 – n Addresses” (where n is the actual number of addresses contained in the TLV – note this displays “1 address” if the number of addresses is 1)
  - o Displays one line per address in the TLV as follows (n is 1 upwards indicating the position in the TLV) –
    - ☐ Either : “n: IPv4 xxx.xxx.xxx.xxx” where xxx.xxx.xxx.xxx is the IPv4 address in this part of the TLV
    - ☐ Or : “n: IPv6”
    - ☐ Or : “n: IP UNKNOWN” if the length of the address field was not 4 or 16
    - ☐ Or : “n: NLPID UNKNOWN” if defined using NLPID but the protocol was not the IP type (0xCC)
    - ☐ Or : “n: 802.2 UNKNOWN” if defined using 802.2 but the protocol was not 8 bytes, or was not 0xAAAA030000000800
    - ☐ Or : “n: PROTOCOL UNKNOWN” if not defined suing either NLPID or 802.2
- ☐ CDP Type 3 TLVs –
  - o Displays “Type 3 – Port ID”
  - o Displays “LENGTH: “ followed by the actual string length in the TLV(up to 25 characters)
- ☐ CDP Type 4 TLVs –
  - o Displays “Type 4 – Capabilities”
  - o Displays “VALUE: “ followed by the capabilities value in the TLV (in hexadecimal format, e.g. 0x00000000)
- ☐ CDP Type 5 TLVs –
  - o Displays “Type 5 – Version”
  - o Displays “LENGTH: “ followed by the actual string length in the TLV(up to 25 characters)
- ☐ CDP Type 6 TLVs –
  - o Displays “Type 6 – Platform”
  - o Displays “LENGTH: “ followed by the actual string length in the TLV(up to 25 characters)
- ☐ CDP Type 7 TLVs –
  - o Displays “Type 7 – n IP Prefixes” (where n is the actual number of prefixes contained in the TLV – note this displays “1 Prefix” if the number of prefixes is 1)
  - o Displays one line per prefix in the TLV as follows (n is 1 upwards indicating the position in the TLV) –
    - ☐ “n: xxx.xxx.xxx.xxx:yy” where xxx.xxx.xxx.xxx is the IP prefix in this part of the TLV and yy is the subnet mask number
- ☐ CDP Type 9 TLVs –
  - o Displays “Type 9 – VTP Domain”

- Displays “LENGTH: “ followed by the actual string length in the TLV(up to 25 characters)

☐ CDP Type 10 TLVs –
- Displays “Type 10 – Native VLAN”
- Displays “VALUE: “ followed by the VLAN tag value from the TLV

☐ CDP Type 11 TLVs –
- Displays “Type 11 – Duplex”
- Displays “VALUE: “ followed by the duplex value from the TLV

☐ CDP Type 14 TLVs –
- Displays “Type 14 – Appliance ID”
- Displays “VALUE: “ followed by the VLAN tag value from the TLV

☐ CDP Type 16 TLVs –
- Displays “Type 16 – Power”
- Displays “VALUE: “ followed by the power consumption from the TLV

☐ Any other type of CDP TLV –
- Displays “TYPE 0xyyyy” where yyyy is the hexadecimal type # of the TLV

☐ Added detection of FDP in addition to CDP and LLDP.

☐ Added FDP to the PROTOCOLS screen similarly to CDP and LLDP protocols.

☐ Added FDP to the capture screen just like CDP and LLDP. NOTE – previously the user could select to filter the frame capture for LLDP frames, this actually included both LLDP and CDP frames, now it includes LLDP, CDP and FDP frames.

**Version 1.71**

1. Increased the resolution of the /1s, /10s and /1min VITALS data from 300ms to 40ms to improve data accuracy.

2. The traffic generate system has been modified as follows:

a. Previously traffic generate set for a length of time would transmit a pre-determined number of frames. When the user configured a fixed period of time, the number of frames calculated assumed there were no pause frames. This could cause traffic generate to continue well over the configured time when there were pause frames. This has been changed to use the configured time instead of a pre-determined frame count (unless configured for number of frames).

b. Previously, if the user configured for random frame sizes, switching between frame sizes was controlled within the “screen”. If the user navigated away from the traffic generate screen for that specific port, then random changes would no longer occur. Now the user can navigate among the screens without affecting the traffic generate.

c. There was an issue with using random frame sizes when performing a REMOTE->LOCAL generate. This has been corrected.

d. There was an issue with simultaneously performing a traffic generate from port 1 to port 2 and vice versa when configured for INDEP mode. This has been corrected.

e. There was a potential issue if the user pressed the PAUSE button just a few frames before the traffic generate would have normally finished. Since it takes short period of time for the pause to stop the actual generator (particularly in the REMOTE->LOCAL direction), the user was able to press PAUSE because the test wasn’t finished, but by the time the pause made it through the system the traffic generate had stopped anyway. If the user now presses continue (available since it was apparently paused), the traffic generate will be restarted, but it will never stop since the “end” had already occurred. This has been corrected.

f. Previously the control of pausing and continuing traffic generate was performed within the "screen". This occasionally created timing mistakes, particularly when performing a REMOTE->LOCAL traffic generate. This has been changed, the pause and continue capability is now performed as part of the Ethernet system with exact timing. NOTE – when continuing a paused random frame size traffic generate, the frame size will always change when continued. As previously, the frame size will change nominally every 10sec if not paused.

g. Previously, if the user configured for a specific % utilization frame rate, it was uncertain what the rate would be if using INLINE mode with different speed ports, or when performing a REMOTE->LOCAL generate. This has been changed, the actual rate will now always be the configured %age of the link on port 1 (in INLINE mode), and/or of the local LE80 or LE85 (for REMOTE->LOCAL).

NOTE: If the user configures for a fixed time of traffic generate, then it must be noted that this is the total time of traffic generation and not "real time". For fixed frame sizes there is little difference, but when using random frame sizes there are short gaps in the traffic when making frame size changes – this makes "real time" a few % longer (typically 2%-5%) than the configured time. The total time of actual traffic generation is accurate.

3. Previously, if the user aborted a stress test, the results stopped updating (as expected), but the actual stress test generated traffic would continue until it expired normally (this could be for several minutes or longer). Although this didn't create any measurement issues, the traffic should have stopped when the user aborted the test. This has been corrected.

## Version 1.70

Added protocol detection for PROFINET as follows:

| | | |
|---|---|---|
| profinet-rt | 34962/tcp PROFInet RT Unicast | Displayed as 34962PRU |
| profinet-rt | 34962/udp PROFInet RT Unicast | Displayed as 34962PRU |
| profinet-rtm | 34963/tcp PROFInet RT Multicast | Displayed as 34963PRM |
| profinet-rtm | 34963/udp PROFInet RT Multicast | Displayed as 34963PRM |
| profinet-cm | 34964/tcp PROFInet Context Manager | Displayed as 34964PCM |
| profinet-cm | 34964/udp PROFInet Context Manager | Displayed as 34964PCM |

## Version 1.66

Version 1.66 update provides significant improvements to the Traffic Generate feature and adds the Loopback feature.

In this release, the **Loopback** feature is introduced. The Loopback sends traffic to its own IP address through a remote device. This remote device must be configured in an external loopback mode to send the packets back to the LanExpert. In a reflector mode, the remote swaps the source and destination addresses. In loopback, the packets are not handled by the remote MAC they are just passed from the receive portion of the phy to the transmit portion and the source and destination addresses are unchanged. The two LanExpert ports can both be independent source devices but do not provide the external loopback function.

In this release, **Traffic Generate** can only be configured from the traffic generate screen, has separate port 1 and 2 configurations, PAUSE capability, full traffic generate Tx and Rx counts, and the ability to generate VLAN tags in the generated frames.

Previously if traffic generate was configured for BROADCAST then traffic was generated to the requested IP but with a broadcast MAC address (i.e. the traffic would generated throughout the network).

Starting with this version, if configured to BROADCAST then an ARP is generated for the requested IP. If there is a response to the ARP then traffic is generated to the requested IP with the responding MAC address but it is assumed not to be a LE80 type interface so only the generated frame count etc. is displayed. If there is no response to the ARP then the traffic generated is as before. NOTE – if a non-local IP is requested then the traffic is now generated with the gateway MAC and the requested IP. On the traffic generate screen the target IP address is now shown in several colors –

- RED – if the user did not set for BROADCAST and the target did not respond correctly.
- ORANGE – if the user did not set for BROADCAST and the target has not yet been properly accessed, AND/OR the user set for BROADCAST but the requested IP did not respond to an ARP.
- WHITE – otherwise

On the traffic generate screen there is a line below the target IP as follows –

- If the user did not set for BROADCAST and the target did not respond correctly then text IP NOT REACHED is displayed in RED
- If the user set for BROADCAST but the requested IP did not respond to an ARP then text NETWORK BROADCAST is displayed in ORANGE.

Starting with this version, A **bps column** has been added to the RFC throughput screen. This column shows the bits per second achieved during throughput testing. This is valid while performing the test, after performing the test, and when viewing recalled stress test data.

## Version 1.53

Version 1.53 update provides significant improvements to the RFC 2544 Stress Test and the Traffic Generate feature.

In this release, the Stress Test and Traffic Generate can be run from the Local to the Remote Unit (upstream) or from the Remote to the Local unit (downstream).

When a stress test is initiated by the user pressing the START button, the LanExpert now always performs a small throughput test using a set of 100 frames being generated at 100frames/sec with 64 bytes/frame. If this test fails to create any packets, then the stress test is aborted and a “REMOTE DEVICE NOT FOUND” error display (2 seconds) is shown. Following this the REMOTE IP text and the configured remote IP shown near the top of the Stress Test screen is shown in RED. NOTE – this takes 1 to 5 seconds to timeout. During this pre-test the results buttons are not shown on the main Stress Test screen.

In previous releases, both the local and remote LanExpert had to be in the same LAN or both had to have routable IP addresses in the Public or Wide Area Network (WAN) to exchange Traffic Generate or Stress

Test data packages. If either LanExpert was behind a device (typically a router) that used Network Address Translation (NAT), the test would fail because the router modified the transmitted packet which was then rejected by the receiving unit as a corrupted packet. In this release, the receiver uses data from the packets received in the initial communications to establish the data match between the local and remote units so there is no reliance on the route taken by the Stress Test or Traffic Generate packets. The only restriction on the network between the generator and the receiver is that the remote end MUST be routable from the local end (i.e. the remote end must be either in the same subnet or be at a publically routable IP address). The local end can be at any convenient IP address, including a non-routable one typically assigned on a LAN.

In this release, communications between the local and remote end have been improved. If the initial communication between the generator and the receiver fails, then the test is immediately aborted and the throughput/loss rate immediately set accordingly. If the loss of communications occurs during a test (i.e. the initial communications were confirmed but the receiver became unreachable later) then this situation is resolved similarly to previous releases for that individual test attempt – but the next attempt will immediately fail so the overall test speed is significantly improved.

In prior releases, if the remote end of a STRESS TEST was inaccessible and a test was performed, the results would slowly decrease and finally stop at zero. Loss of communication with the remote unit is now quickly detected and "----" is displayed instead.

The minimum frame rate supported by the LanExpert has been changed from 20 frames per second to 10 frames per second to allow testing of low speed data rates used in satellite and other communications links.

## Version 1.46

Version 1.46 update provides significant improvements to the Wiremap screen and added CDP/LLDP Port Info feature.

In this release, the wiremap screen has changed dramatically.

Added a "568A" button which toggles between 568A and 568B – selecting the colors displayed for each cable pin.

The left side of the screen are the pin #'s (and Sh if a shield is detected) at the LanExpert side of the cable, the right side is the other end of the cable.

If the cable is wired correctly, colored bars extend from the left number to the right number, which are the same number and both are displayed in white.

If the respective is open, then only the left side has a colored bar and is followed by the word OPEN, if all wires are open, then the text NO TERMINATOR FOUND is also displayed.

If the respective wire is detected as being crossed, then only the left side has the correct colored bar, the word CROSSED is displayed in the center, the right side has a colored bar in the color of the detected wire #, and the right side has the detected wire number shown in red.

If the respective wire cannot be detected properly, then only the left side has a colored bar and is followed by the word UNKNOWN.

Added TCP and UDP Port 104 as DICOM protocol.

VLAN tag entry increased from 0 to 255 to 0 to 4095.

## Version 1.36

Version 1.36 update introduces CSV formatting for the RFC 2544 Stress Test and MAC OUI.

In this release, RFC 2544 has been updated and now is able to save the data internally or externally in .CSV format which can be displayed in excel. The MAC OUI has been implemented and can be viewed in the Top Talkers, Devices and VoIP Screens. The first three octets of a MAC address identify the organization that issued the identifier and are known as the Organizationally Unique Identifier (OUI).