



**SX-500  
Firmware Release Notes  
Version 1.44**

**2010.11.18**

**Classification:**

Firmware

**Description:**

This firmware supports the SX-500 and SX-510 Serial Servers.

**Version:**

V1.44            2011.11.18

**Part Numbers:**

75188-010H

**Purpose:**

Test Release to correct defects and add features.

**Files Released:**

tathsti144.bin

**Installation Instructions:**

Use TFTP protocol to download across the LAN.

**Limitations:**

1. Ad hoc operation may not work with some PC radios [65]
2. TTLS with forced certificate on Steel Belted Radius not supported [81]
3. WPA-TLS fails on DLink DWL-7100 AP [76]
4. Dynamic WEP does not work with Aruba AP [104].
5. Dynamic WEP does not work with EAP-FAST [102].

**Revision History:****V1.44 (2010.11.18)**

1. Renamed V1.43c to V1.44 for release.

**V1.43c (2010.11.18)**

1. Fixed PEAP ack response to return the same version number as the corresponding request. BlueSocket Radius requires this.

**V1.43b (2010.11.02)**

1. Modified EAP state machine to ignore EAPOL key message sent when no valid PMK is present, and send EAPOL-START instead [105].
2. Added SET PORT S1 RFC2217RSP100 command to support alternative RFC2217 response code as requested by OEM customer (RFC is ambiguous on the proper code to use).

V1.43a (2010.10.14)

1. Removed WFA test code.
2. Modified IP startup w/DHCP to start the stack with address 0.0.0.0 until an address is acquired, to avoid confusing routers/bridges that acquire the first IP address seen.
3. Fixed problem with EAP-FAST and Cisco ACS [94]
4. Fixed problem with EAP-FAST and Steel Belted RADIUS [80]
5. Fixed problem with Dynamic WEP on Aruba and Meru APs [79]
6. Added custom RFC2217 options for OEM customer.

**V1.42 (2010.07.30)**

1. Renamed V1.41p for release.

V1.41p (2010.07.30)

1. Fixed WFA test traffic\_send\_ping operation.

V1.41n (2010.07.23)

1. Fixed miscellaneous problems in WFA test interface.

V1.41m (2010.07.16)

1. Fixed bug in WFA test parse, input string was being truncated due to assumption about input data method/format.

V1.41k (2010.07.15)

1. Added ECable UDP configuration to web page.
2. Fixed bug in WFA test response generator which caused multiple response messages to be sent.

V1.41j (2010.07.09)

1. Fixed EAP-FAST handshake.
2. Added WFATEST command to support WFA test suite.

V1.41h (2010.05.14)

1. Restored SET NW WPASTART command removed in 1.41g.
2. Removed Tactical software authentication for an OEM customer added in V1.35a.

V1.41g (2010.03.12)

1. Added option for eCable destination address to be entered as a symbolic name, and support for a related DNS lookup.
2. Modified web server security check to require authentication hash once logged in (previously assumed the last value if not provided, which proved problematic with proxy servers).

V1.41f (2010.02.18)

1. Modified WPA-PSK handshake to inhibit the sending of an EAPOL-START message, which bothers Siemens APs. SET NW WPASTART command added to allow message to be sent if needed in some case.

V1.41e (2010.01.22)

1. Fixed memory leak during wireless disconnect/reconnect operations.
2. Modified WPA supplicant to support APs (Symbol, Proxim) that support multiple authentication/key management methods at the same time (EAP+PSK).

V1.41d (2009.12.03)

1. Fixed network flow control bug in RFC2217 data processing. If receive window went to zero, it would never be re-opened.
2. Put work-around in host certificate parsing during the EAP-TLS handshake to allow the code to ignore the certificate signature if an unsupported signature algorithm is present in the certificate chain (TLSSIGIGNORE command).
3. Fixed problem with parsing of host certificate chains longer than 2.

V1.41c (2009.11.09)

1. Added configuration value and associated code to allow roaming hysteresis to be controlled to some extent.
2. Added configuration value to enable disabling of preauthentication support notification in the WPA2 IE (Linksys WRT54G seem to require this bit to be off).
3. Fixed problem with web interface to scan mask for DFS channels.
4. Modified the home page manufacturer web links to reflect the current Silex web page structure.
5. Fixed buffer overflow in HTTPS firmware download which caused processor trap and download failure.
6. Fixed bug in EAP state machine – after disconnect/reconnect to the AP, EAP timers were not being started which could hang the state machine.
7. Modified EAP state machine so that EAP ID request received during EAP-HELD

state transitions to EAP-CONNECTING instead of EAP-ACQUIRED. With Proxim AP, which sends ID requests very frequently even when the handshake has not been started, this prevented return to the EAP-CONNECTING state, and so no EAPOL-start was sent, and so no connection ever occurred.

8. Fixed bug in PEAP state machine – TLV phase II response was not being properly decoded, which could lead to false negatives from the PEAP handshake.
9. Fixed bug in HTTPS firmware download – host transfer of certain size packets could cause memory overwrite.

#### V1.41a (2009.06.28)

1. Fixed wireless configuration misalignment introduced in V1.38 which could cause wireless authentication mode setting to be lost after firmware upgrade.

#### **V1.40 (2009.04.28)**

1. Renamed V1.39h to V1.40 for release

#### V1.39h (2009.04.28)

1. Fixed text string errors on French wireless web config page..

#### V1.39g (2009.03.27)

1. Fixed problem with WPA2-PEAP created when exponent length problem fixed.

#### V1.39e (2009.03.24)

1. Fixed problem with WPA-TTLS failing with latest free radius server. New server does not request a certificate and does not like it if a dummy certificate is included in the response.

#### V1.39d (2009.03.12)

1. Blocked 802.11a DFS channels (50-144) in all regulatory domains, not just the US.
2. Fixed problem with WPA2-WPA mode with EAP authentication.
3. Added RFC2217 modem control line & break support
4. Fixed user channel scan mask so it works with background scans as well as foreground scans.

V1.39c (2009.02.11)

1. Fixed problem with signal quality check during GDL testing.
2. Fixed problem with local certificate loaded via web not being saved properly

V1.39b (2009.01.06)

1. Improved signal strength reporting algorithm to handle cases where the unit is not transmitting data.

V1.39a (2008.12.29)

1. Fixed problem with parsing certificates with 1 byte exponents.
2. Fixed memory leak in self signed certificate key precomputation task.

### **V1.38 (2008.11.17)**

1. Renamed V1.37b to V1.38 for release

V1.37b (2008.11.17)

1. Fixed length of console mode string web entry field to be 31 characters max to match maximum variable string length.
2. Fixed problem with parsing of host certificates with 512 bit keys.
3. Fixed problem with parsing of host certificates that do not define an Authority Key ID field.
4. Modified data port console mode so it can be entered even if there is an active remote connection.
5. Added console trace buffer dump command (SH PORT S1 CONDUMP).
6. Fixed problem with EAP-FAST and some Cisco APs
7. Added support for differential serial operation for SX-510 models
8. Added individual wireless channel scan control.
9. Added wireless transmit power control.
10. Added custom default console mode string for an OEM.

### **V1.36 (2008.08.14)**

1. Renamed V1.35g to 1.36 for release to OEM customer.

V1.35g (2008.08.14)

1. Changed IP method to static for an OEM customer.

V1.35f (2008.08.13)

1. Implemented missing RFC 2217 support for setting of parameters other than baud rate (parity, character size, flow control).

V1.35c (2008.07.28)

1. Modified product number for an OEM customer.

V1.35b (2008.07.17)

1. Modified model name for an OEM customer.

V1.35a (2008.07.15)

1. Added Tactical software authentication for an OEM customer.

V1.32 (2008.06.06)

1. V1.31g renamed for Japan production release. Not used because STI had already shipped 1.31g to customers.

V1.31g (2008.06.06)

1. Removed extraneous data in AT filter console command responses.
2. Fixed problem with console set of WEP key which required the unit to be booted up (rather than configured for) WEP before a key could be entered.
3. Added device ID option 60 to DHCP request.
4. Added ARP validation of offered IP address in DHCP.

V1.31f (2008.05.20)

1. Fixed problem with SNMP interface to IP method value introduced in V1.31d.

#### V1.31e (2008.04.28)

1. Fixed problem with SNMP interface to IP address values introduced in V1.31d.
2. Updated SNMP unsigned32 definition to match RFC1902. Fixes problem with SNMP trap not being recognized by some handlers that do not support the obsoleted item type encoding.

#### V1.31d (2008.04.11)

1. Added code to update the default MAC address if the current MAC address for the unit is at the factory default or one of the product test setting.
2. Disabled the automatic redirect of HTTP to HTTPS if HTTPS enabled and HTTP is disabled, so that HTTP port is closed.
3. Added SET NW TRACE command to enable radio driver trace when needed.

#### V1.31c (2008.02.14)

1. Added China support information for ExtendView.
2. Fixed problem with WEP encryption if the transmit index on the SX-500 did not match the transmit index on the AP.

#### V1.31b (2008.02.13)

1. Added user interface check code to require open authentication to be used if encryption is disabled, since authentication is only supported in combination with encryption.
2. Removed RTS option from wireless web page, the current driver does not support changing it.
3. Removed International roaming (802.11d) configuration setting, current driver does not support setting it.
4. Removed wireless speed setting, current driver does not support setting it. Added display of current transmit speed in its place.
5. Added Japan support phone number to information returned to Extendview.

#### V1.31a (2008.02.01)

1. Added support for OEM to set MAC address.

#### V1.30 (2008.01.18)

1. Per customer request, modified the serial driver to discard the NULL byte received when a break is detected.
2. Modified signal quality display to scale from 0-100 for the V5 radio driver (RSSI range is different than for the previous MadWifi driver). This corrects a problem seen during production testing.
3. Modified eap key setting to properly handle unicast keys with a key index other than zero. This fixes a problem seen with LEAP and Cisco 1200 APs with 12.3 (8) JEA (3) firmware.
4. Modified IP address acquisition so that it waits until a packet is received after the link is up and authenticated before beginning. This is to improve performance with switches or APs which perform the spanning tree algorithm, and drop packets (such as DHCP requests) while doing so.

#### **V1.28 (2007.12.03)**

1. Renamed V1.27H to V1.28 for release.

#### V1.27H (2007.12.03)

1. Fixed problem with receipt of dynamic WEP key messages. If the timing was just right (wrong), the unicast key message could be lost while the broadcast key was being loaded.

#### V1.27G (2007.11.27)

1. Fixed problem with regulatory domain setting which could cause invalid channels to be displayed as available.

#### V1.27E (2007.11.12)

1. Fixed problem with parsing of server certificates created by some IAS implementations.
2. Added timer to WPA handshake to recover from situation where the AP does not receive our responses.
3. Added watchdog timer as a countermeasure for connection problem seen with Symbol APs.

#### V1.27D (2007.10.26)

1. Fixed packet leak in the radio driver.
2. Added code to prevent buffer overruns in radio driver.
3. Fixed LWAPP WPA2 problem with V5 driver.

#### V1.27C (2007.10.24)

1. Fixed problem with setting the proper MAC address for field upgrades – with the V5 driver, the wrong address was used if the unit came up in wireless mode.

#### V1.27B (2007.10.19)

1. Updated with Atheros V5 reference driver to address intermittent roaming issues.

#### V1.27A (2007.10.17)

1. Added internal configuration switch to handle MAC addresses properly on field upgrades.

#### V1.26 (2007.10.05)

1. Modified the alert/trap web page to make it easier to use.
2. Changed the default trap and alert port mask to 1 for each entry, so the first port is enabled by default.
3. Fixed bug in web server when remote client TCP window went to zero, introduced while refactoring code in V1.25A..

#### V1.25F (2007.08.09)

1. Improved Ad-hoc performance with PC clients.
2. Added FTP access to store files in the flash file system for OEM use.
3. Modified the web server to allow files from the FFS to be used to modify the web page appearance for OEM use.

#### V1.25E (2007.07.27)

1. Updated Chinese web text.

#### V1.25D (2007.07.26)

1. Improved ad-hoc performance further.
2. Fixed problem with ad-hoc channel selection

### 3. Updated Chinese web text

#### V1.25C (2007.07.25)

1. Improved ad-hoc performance, though some issues remain.
2. Added support for blank SSID handling in no encryption and WEP modes.
3. Added serial port status information to status web page per customer request.
4. Added Chinese language to web pages.
5. Added no-cache meta tags to web pages.

#### V1.25B (2007.06.15)

1. Modified radio driver to support setting the MAC address to simplify manufacturing final test and configuration.

#### V1.25A (2007.06.13)

1. Added remote connected device and serial port statistics to the status page.
2. Fixed occasional processor trap which occurred when connected to a Linksys AP but with no data transferred for an hour or more.

#### V1.24 (2007.05.10)

1. Renamed V1.23B for release.

#### V1.23B (2007.05.10)

1. Corrected packet handling problem in EAP-PEAP state machine and Cisco LWAP access point. A duplicate packet received shortly after a disconnection/reconnection could cause an internal queue error.

#### V1.23A (2007.04.30)

1. Corrected problem with WPA2 authentication on Cisco LWAP access points. Newer units require exact key size to be specified and a null length for the supported rate field.

#### V1.21H (2007.04.17)

1. Improved Ad-hoc performance.
2. Eliminated processor trap in rate computation code in Ad-hoc mode.

V1.21D (2007.04.02)

1. Fixed problem with Ecable application in Ad-hoc mode of application – protocols were not started until a packet was received, but if both units are using the same algorithm nothing ever gets sent, and no protocols are started.
2. Modified disconnect reset timer to only work in infrastructure mode.

V1.21B (2007.03.30)

1. Fixed problem with WPA reconnection after AP reconfiguration found in regression testing.
2. Fixed problem in TCP stack with retransmissions caused by earlier change to reduce window update acknowledgments.

V1.21A (2007.03.22)

1. Fixed problem with WPA2 IE construction found in regression testing.
2. Added low latency serial port reception option (SET PORT Sn LOLAT).
3. Fixed problem with certificate chain where not all keys are the same size (e.g., 2048 bit key in one certificate signing 1024 bit key in next certificate).
4. Added UDP mode option to E-cable mode.
5. Added multi-host option along with UDP option (data can be sent to multiple hosts).

V1.19Z (2007.03.15)

1. Fixed problem with unit connecting to Buffalo WLA-L11G AP (STI #302).
2. Fixed problem with connection on channel 14 (STI #303).

V1.19Y (2007.03.13)

1. Modified to increase radio transmit power.

V1.19W (2007.03.08)

1. Modified serial port trap processing so that up to 30 events can be queued and signalled in order.
2. Improved association time in Ad-hoc mode (STI #287)
3. Fixed problem with Extendview discovery in Ad-hoc mode (STI #291).

V1.19V (2007.03.06)

1. Fixed processor trap in WEP mode introduced when attempting to debug another issue in V1.19U.

V1.19U (2007.03.05)

1. Fixed problem with WPA-PSK computation with odd length passphrases (STI #258).
2. Fixed problem with disconnect when another unit connects to the AP (STI #278).
3. Fixed problem with connection to Buffalo access point (STI #302).

V1.19T (2007.02.28)

1. Fixed problems with Ecable mode reception of serial data when TCP connection is in the SYN-SENT state or the network connection is down for an extended period. Under certain conditions, buffers were lost in a wait queue, leading to a resource lock.
2. Fixed problem with Ecable mode reception of serial data when network link is down. Under certain conditions, buffers were lost in a wait queue, leading to a resource lock.
3. Reduced SNMP community fields on web page to 31 characters, to match the effective Extendview maximum size (STI #295).
4. Modified SNMP entry for user ID to return option realm (@xxx) if so configured (STI #261)
5. Fixed problem where unit could take a long time to reconnect to an AP after it is power cycled (depends on AP) (STI #272).
6. Fixed problem with reboot in Ad-hoc mode when Ethernet cable is attached and then detached (STI #288).
7. Fixed problem with DTR polarity, it was inverted from standard operation.

V1.19S (2007.02.14)

1. Fixed problem with Extendview reset of wireless parameters clearing SSID and regulatory domain (STI #245)
2. Fix for problem with unit not reconnecting to AP after AP power cycled (STI #270).
3. Fixed problem with unit not receiving broadcast packets from AP after AP is power cycled (STI #275).
4. Fixed problem with dynamic WEP key set up for non-LEAP authentication methods.

V1.19R (2007.02.08)

1. Fixed problem with Ad-hoc mode performance (STI #181)
2. Added disconnect timer to reset the unit if wireless connection is not made within the configured period.

V1.19Q (2007.02.05)

1. Fixed problem with data link rate computation and idle link handling which caused periodic disconnects (STI #226)

V1.19P (2007.02.02)

1. Fixed problem with self signed certificate not being saved to non-volatile memory when generated via web page (STI #267)

V1.19N (2007.01.31)

1. Fixed Japanese translation errors (STI #268, 269)

V1.19M (2007.01.30)

1. Forced current SSID, signal strength, and related values to blank or zero if wifi link is not established (STI #244)
2. Modified service TCP port upper limit to be 65534, since 65535 is reserved (STE #266).

V1.19L (2007.01.29)

1. Disabled shared key authentication as it does not seem to work (STI #265)
2. Fixed STE email support contact for Extendview (STE #241).
3. Adjusted maximum field length for network security user id field (STI #237).
4. Disabled AP density display in console SHOW NW command if AP density is not supported (STI #236).
5. Removed help for SET/SHOW LOAD from console, since XModem download does not work with TeraTerm emulator (STI #177)

V1.19K (2007.01.19)

1. Fixed miscellaneous console formatting issues
2. Added email support contacts for Extendview.
3. Fixed connection to Japanese APs on channels 12-14 (STI #182).

V1.19J (2007.01.16)

1. Removed mark and space options for serial port parity, since their operation is problematic on PCs (STI #185)

V1.19H (2007.01.15)

1. Fixed problem with file downloads (certificates, firmware) being allowed without providing the update password (STI #188)
2. Fixed miscellaneous console formatting issues.

V1.19G (2007.01.12)

1. Fixed problem with MIB error with numeric value in get community name. (STI #190).
2. Updated miscellaneous Japanese translations.

V1.19F (2007.01.11)

1. Fixed problem with setting IP address via ARP/PING introduced in V1.19E. (STI #186)
2. Made formatting/translation changes requested by STI (#187, 189, 191, 193, 194).
3. Added error message for invalid IP address in access list setup (STI #195)
4. Added upper bounds check on TCP window and Service TCP port (STI #198).

V1.19E (2007.01.05)

1. Fixed problem with FTP PWD command generating command not recognized message. Remote command sent may be XPWD, which was added to the command table (STI #164)
2. Replaced 'troy' string in FTP DIR output with 'silex' (STI #163).
3. Fixed problem with FTP help command not formatted correctly, causing the connection to hang and then close (STI #165).
4. Fixed problem with FTP get – help file could not be fetched, all others could (the opposite of proper behavior) (STI #173)
5. Restored FTP certificate load links deleted when build converted to NSS in V1.19A.
6. Updated Japanese translation of public key/private key strings (STI #130).
7. Fixed problem with using WEP keys other than #1 (STI #184)
8. Fixed problem with server using IP address after DHCP lease expires (STI #169).
9. Fixed problem with getting an IP address via a DHCP relay agent (STI #170).

#### V1.19D (2006.12.20)

1. Fixed SNMP urls which were still pointing to troygroup.com, redirected them to silex.jp. (STI #176)
2. Added code to network startup to wait not only for the network link to be up, but for a number of packets to be received before starting up the protocol stacks (STI #172)

#### V1.19C (2006.12.19)

1. Fixed problem with WPA association with newer Cisco AP firmware introduced in V1.19A.
2. Fixed problem with Ad-Hoc mode Open System introduced in V1.19A.
3. Fixed problem with SET POWERON nn causing a watchdog reset if nn >= 10 (STI #175).
4. Fixed data alignment issue in IP reassembly code which caused large Ping packets to fail (STI #168 & 171).

#### V1.19B (2006.12.12)

1. Fixed problem with WPA association with older versions of Linksys WRT54G routers introduced in V1.19A.
2. Fixed problem with foreign language web page posts when translated strings are in select items.
3. Fixed hardware and firmware error trap handlers so that the watchdog properly resets the unit to recover.

#### **V1.19A (2006.12.06)**

1. Fixed problem with WPA association with TP-Link router.
2. Internal note: changed build to use NSS.
3. Added support for Shared Key authentication.

#### **V1.18 (2006.11.15)**

1. Renamed V1.17Q to V1.18 for production release.

#### **V1.17Q (2006.11.15)**

1. Fixed problem with wireless driver buffer initialization which could cause data to be written beyond the end of the buffer allocated, causing memory corruption.
2. Improved disassociation fix from 1.17K to work properly in all disassociation cases.

3. Improved re-association performance after disassociation.

#### **V1.117K (2006.11.14)**

1. Fixed problem with dangling pointer during disassociation process which could cause memory corruption.

#### **V1.117G (2006.11.09)**

1. Changed title of page to be server description, which matches the server model name by default (STI #147).
2. Modified wireless web page post processing to ignore errors in the channel input in Infrastructure mode. (STI #148)
3. Disabled Shared Key as an authentication option (STI #145).

#### **V1.117F (2006.11.09)**

1. Changed default keepalive setting to 1 minute from disabled, to avoid routing problems with some APs when the unit is idle (STI #140).
2. Fixed display of signal strength to not exceed 100% (STI #144)

#### **V1.17E (2006.11.08)**

1. Fixed problem with WEP broadcast key handling (STI #141).

#### **V1.17C (2006.11.07)**

1. Fixed problem in serial driver where the UART was not signaling a reception idle timeout, causing receive processing to hang.

#### **V1.16 (2006.11.03)**

1. Fixed input flow control issue – flow control was not being asserted early enough to avoid overruns in some situations.

#### **V1.14 (2006.10.25)**

1. Fixed typo in email alert web page which caused it not to display properly.
2. Fixed reporting of current SSID
3. Fixed problems with handling of WPA control messages caused by rate change fix in V1.12.

## **V1.12 (2006.10.25)**

1. Fixed radio firmware version display to show the HAL version.
2. Fixed radio data rate control so link speeds adjust with link condition.
3. Fixed radio speed setting – 54 Mbps support removed in previous version due to a confusion with Extendview speed setting.

## **V1.11 (2006.10.13)**

1. Changed 'Print Server Status' on configuration page printout to 'Server Status' (STI issue #124).
2. Corrected STE support telephone number (STI issue #97)
3. Adjusted web page entry field lengths for system description, location and contact to match the maximum valid length of the corresponding string (STI issue #134).
4. Fixed local certificate/key handling of CR-LF separated records. Added DES-CBC as a supported decryption algorithm.
5. Fixed 10baseT LED indication & report to Extendview (STI issue #96)
6. Fixed SNMP regulatory domain handling – if non null-terminated country string passed via SNMP, memory could be corrupted. (STI issue #95)
7. Fixed handling of IPP requests – connection cleanup on close was not being properly handled when IPP is not supported. (STI issue #139).
8. Fixed IP capability reporting for Extendview to not report WINS if NetBEUI is disabled. (STI issue #24).
9. Fixed radio state structure initialization to fix garbage current SSID reported when not connected (STI issue #126).
10. Fixed Extendview initialize packet filtering to use mac address instead of serial number, so IP configuration of uninitialized unit works (STI issue #128).
11. Fixed console/Extendview baud rate setting to allow 921600 rate (STI issue #30).

## **V1.10 (2006.09.26)**

1. Fixed problem with 802.11 state machine caused in previous version.

## **V1.09 (2006.09.21)**

1. Fixed problem with connecting to Centrino hosts in Ad-hoc mode.

**V1.08 (2006.09.19)**

1. Fixed typo in supported radio speed mask that erroneously indicated 108 Mbps support..

**V1.07 (2006.09.18)**

1. Modified web link to reference international site, silex.jp.

**V1.06 (2006.09.15)**

1. Modified so both network interfaces use the radio MAC address to avoid ARP cache delays & DHCP lease issues when switching interfaces.
2. Fixed problem with driver reset in Ad-hoc mode.

**V1.05 (2006.09.12)**

1. Fixed problem with AP disconnect in infrastructure mode.

**V1.04 (2006.09.05)**

1. Initial test release.with Japanese translations.

**\*\* END OF RELEASE NOTES \*\***