Firmware for TAP-213 Series Release Notes

Version: v1.8	Build: 21090318
Release Date: Nov 24, 2021	

Applicable Products

TAP-213 series

Supported Operating Systems

N/A

New Features

• The system log now records Wi-Fi DFS channel change events.
• Added support for fixed CCA settings.
• Added support for the remote diagnostics feature on the Troubleshooting page.
• Added a Clear Log option to the Maintenance page.
• Added support for Moxa Wireless Protect.
• Added Login/Authentication Failure Message settings in System Information.
• Added IP Aliasing, Management IP Address, and Management subnet mask settings to Network Settings.
• Added the Management Frame Encryption Password setting in Basic WLAN Setup.
• Added additional Multicast rate options for Advanced Wireless Settings.
• Added the option to enable or disable CCA.
• Added the option to enable or disable proxyArp for Client-router Mode in Advanced Wireless Settings.
• Added an SNR option for Roaming and AP candidate thresholds to Advanced Wireless Settings.
• Added a client-to-AP retry count (1-4) option to Advanced Wireless Settings.
• Added support for a bidirectional Keep Alive mechanism for controller-based roaming.
• Added a bi-directional Keep Alive Check option.
• Added Alive Check interval and count settings.
• Added a LAN (Management) section to VLAN Settings.
• Added Port Forwarding Settings to NAT/Port Forwarding.
• Added support for user account authentication in SNMP Agent.
• Added support for Multicast IP settings.
• Added an option to enable or disable Link Fault Pass-Through for Client mode in Link Fault Pass-through.
• Added Turbo roaming events to System Log Event Types and Syslog Event Types.
• Added Coordinator Status events to Notification Event Types and Trap Event Types.
• Added Coordinator Status events to Relay Event Types
• Added the SMTP Port and SMTP Security Mode options to E-mail Server Settings.
• Added the Outgoing Packets and Incoming Packet status to Wireless LAN Status.
• Added an Export Log button to the DHCP Client List page.
• Added a page range to System Logs.
• Added the System, Account, ARP, Bridge, and LLDP Status to Status.

Enhancements

• AeroLink now blocks traffic in the IDLE state to prevent short looping.
• Added a dB value to the AeroLink threshold.
• Added B-Mode in Sniffer mode.
• The AeroLink LAN link-interval has been increased to 5 seconds before real traffic is processed to avoid loops.

• Added a null SSID check.
• Added auto/manual refresh on the RSTP status page.
• Adjusted the accuracy of the transmission (tx) rate to the second decimal.
• Increased the number of Port Forwarding rule entries from 16 to 32.
• Increased the number of MAC Filter, IP Protocol Filter, and TCP/UDP Port Filter entries from 8 to 32.
• Cybersecurity enhancements.
• Enhanced the group check logic for WLAN, 50 ms roaming, security mode, and WAC settings.
• Network information (including IP, subnet mask, and gateway) has been added to the “Reboot” and “Save Configuration and Restart” pages to show the expected network settings after performing these tasks.
• Added support for individual policies for MAC Filter, IP protocol Filter, and TCP/UDP Port Filter rule entries.
• Added an ARP filter option for IP Protocol Filter entries.

Bugs Fixed

• Wireless clients are sometimes unable to connect to the AP during startup.
• Wireless clients time out during authentication if using WEP encryption,
• Setting a null configuration triggers a false configuration change.
• The power saving status of wireless clients is not handled correctly by the AP during roaming.
• Changing IP address settings does not trigger the system to restart.
• Some tx power values for N mode are inaccurate.
• AeroLink sometimes reinitializes unexpectedly.
• Failed SSH login does not trigger an event log.
• No response when using the Wireless Search Utility to configure IP settings.
• RSSI report handoff messages are in an incorrect format.
• Web browsers will redirect users to a wrong address If changes to IP settings are not saved.
• The DHCP maximum numbers of users setting is not applied correctly.
• The order of txpower settings is incorrect.
• The DHCP status would appear incorrect in the Wireless Search utility.
• The rate tables for A/G are incorrect.
• SNMP does not return a “N/A” response if certain wireless status parameters values are blank.
• Wireless clients are unable to reauthorize after being disconnected in enterprise mode during controller-based roaming.
• The device may reboot automatically while upgrading the firmware.
• Wireless clients do not leave an AP after receiving a DEAUTH message.
• The system log cannot be exported when using the Firefox browser.
• The name of the wlanSignal SNMP node is incorrect.
• Language errors on the Turbo Chain status page.
• ARP Request messages in Client-mode are in an incorrect format.

Changes

• Changed the default device name to “Model name_xx:yy:zz”, where xx:yy:zz are the last 3 bytes of the device’s MAC address.
• Changed the RF type default value from “B/G/N Mixed” to “2.4G N”.
• Changed the Wireless default state on the Operation Mode page from “enabled” to “disabled”.
• Changed the default value of the Client lease time for the DHCP server from 5 days to 14400 min.
• Changed the default state of HTTP and Telnet on the Console Settings page from “enabled” to “disabled“.
• Renamed “Multicast rate” to “Multicast and broadcast rate” in the web interface.
• Removed the ability to press Enter to trigger the ping function.

Notes

N/A

Version: v1.2	Build: Build 17103018
Release Date: Dec 01, 2017	

Applicable Products

TAP-213-EU-CT-T, TAP-213-JP-CT-T, TAP-213-US-CT-T

Supported Operating Systems

N/A

New Features

N/A

Enhancements

N/A

Bugs Fixed

• KRACK (Key Reinstallation Attack) WPA2, [CVE-2017-13077]: Issue Descriptions: Wi-Fi Protected Access (WPA and WPA2) allows reinstallation of the Pairwise Transient Key (PTK) and Temporal Key (TK) during the four-way handshake, allowing an attacker within radio range to replay, decrypt, or spoof frames.
• KRACK (Key Reinstallation Attack) WPA2, [CVE-2017-13078]: Issue Descriptions: Wi-Fi Protected Access (WPA and WPA2) allows reinstallation of the Group Temporal Key (GTK) during the four-way handshake, allowing an attacker within radio range to replay frames from access points to clients.
• KRACK (Key Reinstallation Attack) WPA2, [CVE-2017-13080]: Issue Descriptions: Wi-Fi Protected Access (WPA and WPA2) allows reinstallation of the Group Temporal Key (GTK) during the group key handshake, allowing an attacker within radio range to replay frames from access points to clients.

Changes

N/A

Notes

N/A

Version: v1.1	Build: Build 17072815
Release Date: N/A	

Applicable Products

TAP-213-EU-CT-T, TAP-213-JP-CT-T, TAP-213-US-CT-T

Supported Operating Systems

N/A

New Features

• First release.

Enhancements

N/A

Bugs Fixed

N/A

Changes

N/A

Notes

N/A