Release Notes – Firmware v2.2.0.1919

1. Overview

This document summarizes the major updates for the AP firmware from v2.1.0.1312 to v2.2.0.1919.

The firmware update is applicable to the below products.

AP Product Series:	H/W version
C1n/C1xn/C1ni	>= 1.3
C1an/C1xan/C1ani	>= 1.2
C2	All
A2c	All
A2	>= 2.0
A3	All
A8n/A8n(ac)	All

2. What's New in v2.2.0.1919

2.1. New Features

1. 802.11v: BSS transition management support, enabling network-assisted roaming of a client device.

2. 802.11k: Radio resource management support, including neighbor AP reports, beacon reports, QBSS (QoS Enhanced Basic Service Set) load IE; all these can facilitate clients speeding up the discovery and selection process of the next target AP for roaming.

3. 802.11w: Protected management frame support, protecting some management frames with encryption keys to prevent attackers from sending spoof de-authentication/disassociation frames to disrupt or tear down a valid connection between AP and clients.

4. Dynamic VLAN support, enabling user-role based VLAN assignment for client traffic.

5. Passpoint R2 support.

6. Hardware NAT support on A3c/A3w/C2s, used to offload CPU loading and speed up wired traffic between LAN and WAN ports while doing NAT.

7. 802.11r: Fast BSS transition (FT roaming) support on station/repeater modes.

8. Firewall support based on domain and IP/TCP for WLAN packet filtering.

9. Support client OS and hostname detection.

10. Support WiFi syslog configuration on a per-WLAN basis. When enabled, all those event logs related to client association/disassociation of the WLAN will be written to syslog file instead of wifi file for easier troubleshooting.

11. SNMP v3 support.

12. Support guest login control, i.e. enabled/disabled, and guest password modification.

13. Reverse SSH tunneling support, allowing the AP can be SSH'ed even though it is sitting behind a firewall.

14. Support promiscuous mode for Tcpdump, allowing raw 802.11wireless packet capture.

15. MAT (MAC address translation) support on STA/Repeater modes, used to work with third party APs which do not support WDS, or those which support WDS but do not work compatibly.

16. Support Ethernet ingress packet rate-limit on unknown unicast to avoid loading up the AP's CPU and hence the unresponsive Web or SSH or ping due to unicast flood.

17. Support wifi log severity configuration and relocate wifi log to /etc/log/wifi.

18. Support awrt-uci command set under "admin" login.

19. GRE (Generic Routing Encapsulation) tunnel support; used for layer 2 tunneling so that the user data traffic on a particular SSID can be carried from an AP to a remote termination point over a Layer 3 network.

20. EoIP (Ethernet over IP) tunnel support; used for layer 2 tunneling so that the user data traffic on a particular SSID can be carried from an AP to a remote termination point over a Layer 3 network.

21. Support 802.3ad LACP (Link Aggregation Control Protocol) packet passthrough over WDS link.

22. Profinet support for A8n/A8n(ac)/A2/A2c/C1n/C1an; used for data communication in PLC network.

2.2. Enhancements

1. WPA/WPA2 configuration review. The authentication mode is simplified and provides 4 modes: (1) WPA2-Enterprise; (2) WPA2-Personal; (3) WPA/WPA2-Enterprise; and (4) WPA/WPA2-Personal.

2. Fine adjustment to the maximum power limit for A3c/A3w products.

3. Re-organize WebUI structure: Tools > Ping Watchdog.

4. Include configuration file in the log package.

5. Hide "Band Steering Mode" parameter when either 2.4G or 5G is set to station/bridge mode.

6. Provide a "ACL" file sample for user's reference for blacklist/whitelist preparation.

7. Modify the default log file name so as to contain AP information and timestamp for easier troubleshooting.

8. Support "Prefix Length" field for static IPv6 configuration.

9. Rename the parameter "Country Code" as "Country (Region) Code".

10. Reduce log message amount due to excessive RADIUS retry attempts.

11. Tidy up the association list of AP/repeater modes, and the connection info table of station/repeater modes.

12. Remove the time synchronization requirement for AP to enable 802.11r FT roaming feature; i.e. the APs under the same FT domain do not need to synchronize time with a NTP server.

13. Modify WLAN configuration table for quick WPA2-Personal or WPA/WPA2-Personal configuration.

14. Limit concurrent WebUI session to one regardless of the permission levels, admin or guest, so as to reduce unnecessary CPU loading.

15. Rename the name "RADIUS Retry Timeout" to "Retry Primary RADIUS Interval", after which the RADIUS client, i.e. AP, will retry to use the primary RADIUS server even though the currently used secondary server is still working.

16. Reduce log message amount due to excessive tunnel process restart.

17. Remove the parameter "Debug Level" from Remote Management to keep configuration simple.

18. Clean up unnecessary debug wifi logs for station mode.

19. Enhance min client SNR feature to handle sticky clients.

20. Enhance preferred AP list feature; enabling the station always to stay connected to the top preferred AP whenever available.

21. Add a warning message to avoid enabling PPPoE connection when two or more interfaces are assigned to WAN.

22. Disable/Hide "DHCP Server" and "Port Forwarding" configuration UI when switch mode is enabled.

23. Bridge throughput enhancement.

24. Allow multiple BSSID selection, up to 3 of the same SSID, from the scan result for the station to connect with the target SSID.

25. Disable/Hide "MAC clone" option under gateway mode.

26. The "Preferred AP" and "Roaming" features are mutually exclusive, so one will be greyed out while another is enabled.

27. Disable/Hide "MAC Clone List" page when repeater mode is on as the feature does not apply to repeater mode.

28. Set C1an 5G default channel from Auto to Ch36.

29. Support "Short GI" configuration when A8 is running on HT20 of wireless mode.

30. Relax maximum length of SNMP Read/Write Strings to 128 characters long.

31. Limit the length of admin/guest passwords to 40 characters long.

32. Provide hints of correct MAC format for ACL input.

33. Provide portal ACL update time and file download link once the file is successfully uploaded.

34. Radio WMM parameter support under bridge mode.

35. Remove restrictions of "Packet Count" and "Capture File Size" for tcpdump tool.

36. Remove "Authentication Mode" from bridge configuration because it supports just one mode "Open" only.

37. Shorten WDS entry aging timeout.

38. Remove the text "Auto" from the channel field on the status page when the device is running on station mode.

2.3. Bug Fixes

1. WLAN off in the time window when switching from main access controller to backup one under VRRP configuration.

2. Station statistics info, i.e. 2.4G/5G radio, channel and RSSI, was found incorrect on access controller.

3. Window pop-up issue when leaving blank in IP entry.

4. Client IP addresses sometimes displayed as 0.0.0.0 unexpectedly when there is a large number of clients connecting to an AP.

5. Client not able to resolve local domain name with a local DNS server when connecting with an AP running on gateway mode.

6. CPE, with mac clone and WEP enabled, becomes unreachable from the AP side upon CPE power-cycle.

7. Remove the parameter "Protection Mode" from 5G radio advanced configuration page, as the item is no longer valid.

8. Re-size the table of static mac clone entries to fix the issue of station unreachable to a backend network.

9. Connection failure to AltaiCare and access controller when trust IP is enabled.

10. Unable to change AP login password of "admin" and "guest" via access controller.

11. Failed to configure the parameter "syslog server IP" via access controller.

12. C1n firmware update failure on special occasions.

13. Incorrect 5G max Tx power of A3 series when using RoW of country code.

14. Fix the issue that the "Nearby AP List" feature is able to sniff non-operating channels when the AP is running on auto-channel mode.

15. Intermittent connection drop for static MAC bridge mode.

16. Incorrect client Rx traffic statistics found in the association list.

17. STP malfunctions over a WDS link when multicast traffic is disabled.

18. Occasional panic reboot upon wireless configuration change via AltaiCare/access controller.

19. EoIP tunnel fails when AP's IP configuration and tunnel configuration are saved and applied together.

20. CPE unable to get access to the backend network when connecting with EoIP-enabled SSID.

21. IPv4 DNS Server displayed as 1.1.1.1 when PPPoE connection fails.

22. WebUI sometimes inaccessible after AP joining AltaiCare.

23. RADIUS authentication occasionally fails when the RADIUS client, e.g. AP, uses DHCP for IP connection.

24. AltaiCare Portal-related settings remain active in the AP after switching the AP connection from AltaiCare to access controller.

25. Ethernet compatibility issue for A3/A2/A2c/C2s when connecting with old Cisco switch models.

26. C2s Ethernet LED lights green when running on 1000M of speed.

27. Panic reboot upon wireless reload.

28. Log file sometimes found incomplete via WebUI download.

29. The values of WLAN uplink/downlink control swapped upon save/apply when running on station mode.

30. AP does not run on an auto-channel as expected when the previously-configured static channel is changed to the auto one.

31. WebUI returning no response sometimes when trust IP is enabled.

32. Device running on station/repeater modes fails to connect with target remote SSID which is selected from the scan result.

33. CPE unreachable from its Ethernet end when VLAN and MAC clone is enabled together.

34. Panic reboot due to WDS table overflow.

35. Unusual A8n panic reboot when remote management is enabled.

36. C2s Ethernet unreachable after abnormal reboot.

37. AP inaccessible via safe mode when VLAN is enabled.

38. Incorrect Eth1 traffic statistics for A3 and C2s.

39. Abnormal reboot caused by ACS fatal error.

40. A3/C2s AMSDU-related panic reboot caused by RTSP.

41. A3/C2s 5G connection failure due to AMSDU.

42. C2s 5G radio configuration missing issue in special cases.

43. A8 reboot when using PPPoE connection.

44. AP unable to process RADIUS authentication with “Secondary RADIUS server”.

45. Re-apply and save ACS channel list when making changes of other radio settings.

46. Re-apply and save DCS setting when making changes of other radio settings.

47. Data rate shows “0” for station association with A2c.

48. Eth0/Eth1 cannot be assigned to different WAN/LAN interfaces for A3/C2s products.

49. A3, with 2.4G running on station mode, suffers panic reboot when it remains in a non-associated state.

50. ACS crash on A2c when periodic mode is set 1min.

51. Client can get IP address via DHCP from another client (DHCP server) of other WLAN (DHCP-trust enabled), even though inter-WLAN user isolation is enabled.

52. Clients not able to access to WAN under gateway mode when trust IP is enabled.

53. When “Access Traffic Right” is set to “AP Management Only” and “User Isolation” is disabled, two clients of the same WLAN can still reach each other, meaning that “User Isolation” is put in a higher priority than “Access Traffic Right” when processing client traffic.

54. Secondary IP access issue for WAN and LAN connections when PPPoE is disconnected.

55. Ping AP lost while applying wireless configuration, due to multi-address MAC clone enabled.

56. Abnormally high throughput value found when Eth0 interface is disconnected, followed by network reload.

57. Unable to perform scan on station mode when it is in a disconnected state from a target WPA-enabled SSID.

58. 5G Data rate cannot go up to 300Mbps when A8n is running on a station mode with short GI enabled.

59. Multicast to unicast conversion not in effect for uplink traffic from A2c running on station/bridge modes.

60. Inappropriate error message pops up when adding illegal format of MAC entries to rogue station list for A2c.

61. Multiple entries of a MAC entry can be created and saved on A2c.

62. WPA-Enterprise authentication fails for A3 when the primary RADIUS server is unreachable but the secondary RADIUS server is.

63. Static bridge ARP fails, resulting in WDS aging and connection issue.

64. Minor change found on the SSID name of the last row of scan table for CPE connection.

65. The 5G operating Tx power of A2c is found with a slight difference from the configured one.

66. AP reboots while connecting with an UBNT WDS-enabled CPE.

67. WAN interface field can be left empty under gateway mode when switching from repeater mode to AP mode.

68. Station, making an abrupt offline, remains in the AP association list even after inactivity timeout, when the FT roaming is enabled in the AP end.

69. 5G ACL not working when AP is running on thin AP mode connecting with AltaiCare.

70. AP reboots when running throughput test and tcpdump for packet capture at the same time.

71. Unusually high latency and packet loss while CPE is roaming.

72. DBDC performance degraded due to unexpected WMM values.

73. New Tx power configuration not in effect after switching between static channel mode and auto mode.

74. With the "User Isolation in different WLAN (SSID)" enabled, stations from one SSID are still able to acquire IP address from another SSID, of which "DHCP Trust Port" is enabled.

75. Local accounts still work for AP login when the Authentication Type is selected as "RADIUS Authentication" only.

76. High retransmission rate and packet lost for 5G 802.11ac radio when there is a large number of client association, i.e. > 60.

77. Error message pops up in WebUI while the nearby AP list is showing incorrect SSIDs.

78. No timestamps associated to log messages in C2s.

79. WebUI error message when SSID is configured to contain some special characters, e.g. "&".

80. MAC entries update issue when switching configuration between "Preferred AP MAC" and "Lock AP MAC".

81. HTTP port and HTTPS port can be configured the same, which should not be allowed.

82. Non-management VLAN IP address does not take effect after save and apply.

83. Bridge remote IP varying in the connection info table when the bridge is set up in a VLAN-enabled environment.

84. Uptime at the upper right corner not updated occasionally.

85. Panic reboot due to thin AP module restart, i.e. remote management configuration change.

86. A8/A2 wireless data rate capped at 270Mbps and cannot go further up to 300Mbps for 2.4G radio when running on 802.11n HT40 of wireless mode.

87. WLAN0's ACL remains in effect and is not removed for safe mode access.

88. Http daemon unable to load up when the system running out of storage.

89. Occasional page rendering error in Web UI.