Cisco SWAN Release Notes 2.2.127.9

System Release 2.2

These Release Notes cover Cisco Wireless LAN Controllers, Cisco 1000 Series lightweight access points, and Cisco Wireless Control System, which comprise part of the Cisco Structured Wireless-Aware Network (Cisco SWAN). This document includes the following sections:

- *Cisco Structured Wireless-Aware Network Components*
- *Requirements for Cisco SWAN Components*
- *New Features Available in Release 2.2*
- *Issues Corrected in this Release*
- *Technical Notes*
- *Open Issues in Operating System Software*
- *Interoperability Tables*

Cisco Structured Wireless-Aware Network Components

- Operating System (Cisco Wireless LAN Controller and Cisco 1000 Series lightweight access point) Software, version 2.2.127.9.
- Cisco Wireless Control System (Cisco WCS).
- Cisco 2000 Series Wireless LAN Controllers.
- Cisco 4100 Series Wireless LAN Controllers.
- Cisco 1000 Series IEEE 802.11a/b/g lightweight access points (Cisco 1000 Series lightweight access points):
    - AIR-AP1010-A-K9, AIR-AP1010-E-K9, and AIR-AP1010-J-K9
    - AIR-AP1020-A-K9, AIR-AP1020-E-K9, and AIR-AP1020-J-K9
    - AIR-AP1030-A-K9, AIR-AP1030-E-K9, and AIR-AP1030-J-K9

Requirements for Cisco SWAN Components

- Requirements for Web User Interface – Windows XP SP1 or Windows 2000 SP4 running Internet Explorer 6.0.2800.1106.xpsp2.130422-1633 or higher. You also need to load patch KB831167 found at http://www.microsoft.com/downloads/details.aspx?FamilyID=254eb128-5053-48a7-8526-bd38215c74b2&displaylang=en. Note that there are known issues with Opera, Mozilla and Netscape; these are unsupported.
- Requirements for Web Browser when using Web Authentication – Internet Explorer 6.0 with SP1 or Netscape 7.2. There are known issues with Opera.

New Features Available in Release 2.2

- QoS Enhancements - The Cisco SWAN Quality-of-Service subsystem has been enhanced with the following capabilities:
  - Five queues in each Cisco 1000 Series IEEE 802.11a/b/g lightweight access point (Cisco 1000 Series lightweight access point)
  - Cisco 1000 Series lightweight access point Queuing enhanced to support rate shaping per queue per user (i.e. token bucket shaper)
  - Specialized support for real time applications
  - Enhanced support for wireless phones and SIP clients
  - Users can limit the total amount of bandwidth any given 'group' can have over the air
  - Bandwidth provisioning based on user identity
- IDS Enhancements - The Intrusion Detection System (IDS) capabilities of the Cisco SWAN have been enhanced to detect the following IDS events:
  - Sensing Clients probing for "ANY" SSID
  - Sensing if Cisco 1000 Series lightweight access points are being contained
  - Notification of Man-in-the-Middle (MiM) Attacks
  - Notification of Network Stumbler
  - Notification of Wellenreiter
  - Management frame detection
  - RF Jamming detection
  - Airjack detection (spoofed deauth detection)
  - Broadcast deauth detection
  - Null Probe Response Detection
  - Fake AP detection
  - AP impersonation detection
  - Honeypot AP detection
  - Valid Station Protection
  - Misconfigured AP Protection
  - Rogue AP detection
  - Ad-hoc detection and protection
  - Wireless bridge detection
  - Detecting and locating clients that launch RTS denial of service attacks
  - AusCERT Attack
  - 802.11 DOS detection – RTS attacks
  - Detection of weak WEP encryption
  - MAC spoofing detection
  - The Operating System also allows users to define their own attack signatures and update the OS in real time
- 802.11i Fast Roaming (Proactive Key Caching) - Proactive Key Caching enables enterprises to couple the security benefits of the recently ratified IEEE 802.11i specification with real-time

performance and seamless mobility. Proactive Key Caching (PKC) enables each client to have its own Pairwise Master Key that follows them as they roam across a wireless network. This extension, which is one hundred percent compliant with the 802.11i standard, was developed in conjunction with Funk Software and Atheros Communications to eliminate the need for wireless devices to repeatedly reauthenticate with a backend RADIUS server when roaming between Cisco 1000 Series lightweight access points. PKC reduces latency and increases scalability through more efficient operation, creating a completely secure Wireless LAN (WLAN) environment that is ideally suited for any business application, from voice and video to real-time data applications.

- DHCP Server - A DHCP server has been added to the OS. The following capabilities are supported:
  - Multiple DHCP scopes
  - Configurable parameters include start and end addresses, netmask, default gateway, lease time, DNS domain name, DNS servers, and NetBIOS name servers
  - Enable and disable individual scopes
- Enhanced RLDP - The Cisco SWAN Rogue Location Discovery Protocol (RLDP) has been enhanced to detect whether a Rogue AP is on the trusted network or not. This is achieved by placing a Cisco 1000 Series lightweight access point into a mode called 'Rogue Detector'. When in Rogue Detector mode, the Cisco 1000 Series lightweight access point does not provide RF service of any kind (its radios are disabled). It does, however, receive periodic rogue reports from the Cisco 4100 Series Wireless LAN Controller, and monitors all ARP packets on the wire. If it finds a match between an ARP request and a MAC address it received from the Cisco 4100 Series Wireless LAN Controller, it generates a rogue alert to the Cisco 4100 Series Wireless LAN Controller. The interface to the user is exactly the same as the current RLDP, meaning that the rogue shows up as a threat.

  Using 802.1Q trunking, the Cisco 1000 Series lightweight access point can parse all of the ARPs on all VLANs - so it is not necessary to have one per subnet.
- New Cisco 1000 Series lightweight access point Fallback behavior - The Cisco 1000 Series lightweight access point can now be configured to have primary, secondary, and tertiary Cisco Wireless LAN Controllers. This allows for more granular control for Cisco 1000 Series lightweight access point failover scenarios.
- Finer control over Client Exclusion Policies - The Cisco SWAN currently has a single client exclusion enable/disable flag. This feature has been enhanced to provide finer-grained control over which events will cause client exclusion. The following controls are provided:
  - Excessive 802.11 Association Failures
  - Excessive 802.11 Authentication Failures
  - Excessive 802.1x Authentication Failures
  - External Policy Server Failure
  - IP Theft or IP Reuse
  - Excessive Web Authentication Failures
- RFC 3576 Support.

Issues Corrected in this Release

- 9646 -- Channel assignment timer appeared to follow last Group Update time.
- 9903 -- Syslog errors were being generated “Couldn't find rule in ACL”.
- 11656 -- SNMP agent stopped responding to requests.
- 12283 -- Failed to add Cisco 4100 Series Wireless LAN Controller if Cisco 4100 Series Wireless LAN Controller had a dynamic interface name server.
- 13121 -- Spectralink Phones failed to join.
- 13326 -- Cisco 4100 Series Wireless LAN Controller stopped responding to IKE.
- 13460 -- Web Auth with IE did not redirect when IE settings disabled Http1.1.
- 13523 -- Interface address page allowed invalid addresses and subnets.
- 13536 -- Web wizard accepted more than 24 characters for username/password.
- 13545 -- WLAN session timeout did not deauthenticate webauth users.
- 13657 -- WPS code: Did we need the WLAN tab on the Cisco 4100 Series Wireless LAN Controller.
- 13672 -- WPS Code: Enhanced RLDP was not working.
- 13729 -- WebAuth pre-authentication ACL only worked down 11 lines of the ACL.
- 13773 -- Cisco 1000 Series lightweight access point was sending disassociation type for no apparent reason.
- 13778 -- 1250 Cisco 1000 Series lightweight access point could not associate with Cisco 2000 Series Wireless LAN Controller when the Cisco 1000 Series lightweight access point first connected.
- 13811 -- The Cisco 1000 Series lightweight access point IP address was not sychronized between Cisco 1000 Series lightweight access point and the Cisco 4100 Series Wireless LAN Controller.
- 13853 -- Radio SNMP MIB-Walk terminated if Cisco 1000 Series lightweight access point showed 0 number of slots.
- 13963 -- Cisco 1000 Series lightweight access point bitmap was not updated when WLAN removed.
- 14052 -- Cisco 4100 Series Wireless LAN Controller crash.
- 14059 -- Incorrect error message when trying to disable dhcp req for contivity wlan.
- 14082 -- Crash in sshpmMainTask.
- 14116 -- Show Inventory CLI command showed the Licensed Cisco 1000 Series lightweight access points as 12.
- 14117 -- Check box to configure SONMP via GUI was not available.
- 14126 -- Network/Netmask/Address Pool fields for DHCP Scopes was too small.
- 14127 -- DHCP Lease Time default to 120 seconds was too short.
- 14128 -- DHCP Lease Time configuration should allow minutes and/or day.
- 14141 -- AEPI - Handling of Failures/Timeout and Plumbing Rules.
- 14145 -- 2260: client disconnected and get new IP address after expiration of lease time in internal DHCP server.

- 14174 -- The bsnAclTable went to infinite loop when doing a MIB walk.
- 14189 -- Needed a Measurement Interval field in IDS signature.
- 14190 -- A NAK from a second DHCP canceled out the ACK from the first DHCP, preventing an associated client from getting authenticated.
- 14195 -- Cisco 4100 Series Wireless LAN Controller crashed in 2.2.67.1 and 2.2.95.0.
- 14198 -- Supported value for beacon period was 20-1000 msec in Web User Interface but mib shows only 100-600 msec.
- 14203 -- TFTP filepath and filename length maximum should be changed to 63 chars.
- 14206 -- Device IP addresses sent by Outpost are reversed.
- 14211 -- DHCP - Cisco 4100 Series Wireless LAN Controller Used Same IP to Proxy ARP For Multiple Clients.
- 14212 -- BT - Added timer information to the backtrace to assist in debugging crashes.
- 14213 -- Remote Cisco 1000 Series lightweight access point Debug - Did not properly handle multiple arguments.
- 14230 -- Cisco 4100 Series Wireless LAN Controller sent Reassociation Response for Association Request.
- 14231 -- IPsec/Contivity CPU usage too high which crashed the Cisco 4100 Series Wireless LAN Controller.
- 14232 -- Cisco 1000 Series lightweight access point in L2 Appliance Mode could not connect.
- 14233 -- Cisco 4100 Series Wireless LAN Controller crash “(pre=5e5---------NPU Counter Semaphore Log”.
- 14236 -- RSN PMK caching was not working.
- 14247 -- Cisco 1000 Series lightweight access points running 2.2.127.3 crashed with the msg “Assert In Software Task” with Task = “tNetTask”.
- 14258 -- Cisco 1000 Series lightweight access point could not join the Release 2.2 Cisco 4100 Series Wireless LAN Controller.
- 14272 -- Crash: kernel access of bad area for Senior and Junior Cisco 4100 Series Wireless LAN Controller.
- 14274 -- WEP IVs were incorrect when WMM was enabled with WEP encryption.
- 14283 -- Cisco 1000 Series lightweight access point Policies - AAA auth failure caused duplicate Cisco 1000 Series lightweight access points.
- 14301 -- Cisco 1000 Series lightweight access point Rebooted in routeSockLibInit.
- 14314 -- Collecting crashes in quicksec.
- 14315 -- “Back” button always returned to first page when viewing multiple Client screens.
- 14321 -- Cisco SWAN builds should read max-APs from EEPROM.
- 14326 -- Cisco 1000 Series lightweight access point - Crash in frameEndianChange for EAPOL-Key Frames.
- 14337 -- “Unable to remove AP 00:0b:85:04:de:70 from fast path” error in Message Log.
- 14339 -- s5Chassis MIBs s5ChasComType.4.5.0 returned the wrong value.
- 14340 -- s5Chassis MIBs s5ChasComRelPos.3.5.0 returned the wrong value.

- 14348 -- Broadcast key update was not working for WPA wlan.
- 14362 -- WPA/TKIP - Rekey failed because of an M5/M6 exchange failure.
- 14365 -- URL was duplicated in the Web User Interface for Web Authentication.
- 14374 -- Gig Port - Tx Link Failure Not Detected.
- 14379 -- Cisco 1000 Series lightweight access points crashed if fragmentation changed from default.
- 14383 -- Cisco 4100 Series Wireless LAN Controller crashed during show run-config.
- 14386 -- Rogue AP not cleared from the Rogue AP table even when Rogue AP was powered down.
- 14387 -- In Web Wizard AP-Mgr parameter was required even when in Layer 2 LWAPP mode.
- 14394 -- IPSec stopped responding to user connections; could only recover with reboot.
- 14398 -- SNMP was skipping entries on some tables and thus Cisco WCS could cause loss of config on Cisco 4100 Series Wireless LAN Controller.
- 14399 -- SNMP did not return a value for LWAPP transport mode, so the Cisco 4100 Series Wireless LAN Controller addition to Cisco WCS sometimes failed.
- 14403 -- RF-network name not updated with mobility domain name change.
- 14411 -- Cisco 1000 Series lightweight access point in Hung state after Cisco 4100 Series Wireless LAN Controller Upgrade.
- 14422 -- Cisco 4100 Series Wireless LAN Controller crashed while accessing a Rogue AP under Rogue AP menu.
- 14423 -- AAA - Needed to log when a RADIUS server failed.
- 14432 -- Cisco 4100 Series Wireless LAN Controller crashed after Download Config command executed.
- 14460 -- Error Message - Invalid MSCB State.
- 14464 -- ACLs did not take effect for non-ICMP traffic.
- 14467 -- AAA - Improper memory management in sync AAA calls.
- 14469 -- Console message: found a corrupted timer on a bucket from module.
- 14486 -- Cisco 4100 Series Wireless LAN Controller Crash after two days running IPSec Stress.
- 14491 -- Appliance was not sending RADIUS trap.
- 14521 -- Made Reaper more Robust.
- 14524 -- Client was reconnected every five minutes (idle timeout) when receiving multicast traffic from a Cisco 1030 remote edge lightweight access point.
- 14544 -- The mscb became corrupted when static wep was configured.
- 14547 -- Crash on Reaper Reset: Task “SNMPTask” missed software watchdog.
- 14559 -- Cisco 4100 Series Wireless LAN Controller did not see clients whereas Cisco 1000 Series lightweight access points associated had client entries.
- 14575 -- If Internet Protocol address was entered using the DHCP Server Override setting and SAVE was done, the Internet Protocol address display became abnormal.

- 14581 -- Cisco 1000 Series lightweight access point IP Fallback - Cisco 1000 Series lightweight access point was unable to join Cisco 4100 Series Wireless LAN Controller in same broadcast domain.
- 14587 -- Reassociation on foreign Cisco 4100 Series Wireless LAN Controller stopped client data traffic.
- 14602 -- Cisco 1000 Series lightweight access point kept printing the assert condition messages on the console.
- 14651 -- Data only Cisco 4100 Series Wireless LAN Controller could not be added to Cisco WCS (signature check parameter did not return value).
- 14703 -- PEM 802.1X Timer was Too Small.
- 14713 -- Direct-connected Cisco 1000 Series lightweight access point unable to attach to the Cisco 4100 Series Wireless LAN Controller in L3 Mode - AP-Manager VLAN is different from the Management VLAN.
- 14722 -- Port Autonegotiation failed for a Cisco 2000 Series Wireless LAN Controller.
- 14732 -- Cisco 4100 Series Wireless LAN Controller crashed on Em web.

Technical Notes

- Web User Interface OS upgrade from 2.0 MR5 to 2.2 *appears* to fail at end of upgrade - There is a software defect in 2.0 MR5 (2.0.142.0) where an upgrade using the Web User Interface completes the upgrade, but fails to redirect to the normal reboot page and appears to not complete in normal fashion. Actually, the upgrade does complete, and a reset of the Cisco 4100 Series Wireless LAN Controller after all activity ceases results in the Cisco 4100 Series Wireless LAN Controller powering up with the correct 2.2 image running.
- Voice WLAN Configuration - Cisco SWAN recommends that Load Balancing ALWAYS be turned off in any WLAN that is supporting voice, regardless of vendor. When Load Balancing is turned on, voice clients can hear an audible artifact when roaming and the handset is refused at its first reassociation attempt.
- The Upgrade Process – When a Cisco Wireless LAN Controller is upgraded, the code on the associated Cisco 1000 Series lightweight access points is also upgraded. When a Cisco 1000 Series lightweight access point is loading code, each of its lights blink in succession. Do not power down a Cisco Wireless LAN Controller or a Cisco 1000 Series lightweight access point during this process! Upgrading a Cisco Wireless LAN Controller with a large number of Cisco 1000 Series lightweight access points can take as long as 30 minutes. The Cisco 1000 Series lightweight access points must remain powered and the Cisco Wireless LAN Controller must not be reset during this time.

  Cisco recommends the following sequence when performing an upgrade:

  A. Upload your Cisco Wireless LAN Controller configuration files to a Cisco WCS Server to back them up.

  B. Turn off the Cisco Wireless LAN Controller 802.11a and 802.11b networks.

  C. Upgrade your Cisco Wireless LAN Controller.

  D. Re-enable your 802.11a and 802.11b networks.

- Exclusion List (Blacklist) Client Feature – If a client is not able to connect, and the security policy for the WLAN and/or client is correct, the client has probably been disabled. From the Web User Interface, Monitor page under client summary, you can see the client’s status. If they are disabled you can just do a “Remove” operation and the disable is cleared for that client. The client automatically comes back and, if necessary, reattempts authentication. Automatic disabling happens as a result of too many failed authentications. Note that clients disabled due to failed authorization do not show up on the permanent disable display. This display is only for those MACs that are set as permanently disabled by the administrator.
- IPSec Clients Supported in this Release – This release has been tested with the following IPSec clients:

  - NetScreen v8.0.0
  - Cisco Unity v3.6.2
  - SSH Sentinel v1.3.2(1)
  - Movian v3.0

  Please note that the Netscreen client does not handle fragmented ICMP packets, doesn't respond to large ping packets, and does not work with certificates. Other IP fragmented traffic should work correctly.

  Cisco SWAN supports the Cisco Unity client. However, please determine if the existing licensing agreement allows termination on a non-Cisco platform. Please review the terms and conditions of your licensing agreement before using the Cisco Unity client.

- XAuth Configuration with NetScreen – Do not enable XAuth on the NetScreen client. Configure XAuth on the Cisco 4100 Series Wireless LAN Controller. The Cisco 4100 Series Wireless LAN Controller initiates the XAuth session and the NetScreen client responds and begins inter-operating. Configure the NetScreen client with pre-shared keys only. You also need to set up a separate connection in the clear to your DHCP server.
- Rekeys are not supported with Cisco VPN client – If a rekey occurs clients must re-authenticate. To mitigate this problem, log into the Cisco 4100 Series Wireless LAN Controller, navigate to the WLANs page, select Edit to display the WLANs > Edit page, choose Advanced Configuration, and change Lifetime (seconds) to a large value, such as 28800 seconds (this is the default), depending upon your security requirements.
- RADIUS Servers – This product has been tested with the following RADIUS servers:
  - Odyssey Server and Odyssey Client v1.1 and 2.0 from Funk Software.
  - Steel-Belted RADIUS from Funk Software version 4.40.337 Enterprise Edition.
  - Microsoft Internet Authentication Service (IAS) Version 5 on Windows 2000 Server/ SP4; Microsoft Internet Authentication Service (IAS) Version 5.2.3790.0 on Windows 2003 server.
  - CiscoSecure ACS, v3.2.
  - FreeRADIUS version 0.9.3, with OpenSSL 0.9.7B.
- Management usernames and Local netuser usernames must be unique, because they are stored in the same database. That is, you cannot assign the same name to a Management User and a Local Netuser.
- 802.1x and MicroSoft Windows Zero-Config supplicant – Clients using Windows Zero-Config and 802.1x MUST use WLANs configured for 40 or 104-bit Key Length. Configuring for 128-bit Key Length results in clients that can associate, but not authenticate.
- When Cisco 4100 Series Wireless LAN Controller reboots, dropped Cisco 1030 remote edge lightweight access points attempt to associate with any available Cisco 4100 Series Wireless LAN Controller. If the Cisco 1030 remote edge lightweight access points cannot contact a Cisco 4100 Series Wireless LAN Controller, they continue to offer 802.11a/b/g service on WLAN 1 only.
- WEP Keys – This release supports four separate WEP index keys. These keys cannot be duplicated between WLANs. At most four WEP WLANs can be configured on a Cisco 4100 Series Wireless LAN Controller. Each of these WLANs must use a different key index.
- DCA and Transmit Power Algorithms are designed to work with four or more Cisco 1000 Series lightweight access points – If there is a need to enable these algorithms for a smaller number of Cisco 1000 Series lightweight access points, please contact Cisco Technical Assistance Center (TAC).
- Using the Backup Image – The Cisco 4100 Series Wireless LAN Controller Bootloader (ppcboot) stores a copy of the active primary and the backup image. If the primary image should become corrupted, you can use the Bootloader to boot with the backup image.

  After you have booted with the backup image, be sure to use Option 4: Change Active Boot Image on reboot to set the backup image as the active boot image. If you do not, then when the Cisco 4100 Series Wireless LAN Controller resets it again boots off the corrupted primary image.
- Home page retains Web Auth login with IE 5.x – This is a caching issue in the operator's Internet Explorer version 5.x browser. Clearing history corrects it, or upgrade your operator workstation to Internet Explorer version 6.x.

- RLDP Enable/Disable – RLDP Enable/Disable refers to the RLDP protocol which detects rogues on your wired network. Autocontainment enable/disable indicates whether you want the Cisco 4100 Series Wireless LAN Controller to automatically contain new Rogues that it finds on the wire. Disabling RLDP or autocontainment does not disable containment for Rogues that are being contained. When Rogues are being contained, you must manually disable containment for each Rogue individually.
- Ad-hoc Rogue Containment – Client card implementations may mitigate the effectiveness of ad hoc containment.
- Apple iBook – Note that some Apple OSs require shared key authentication for WEP. Other versions of the OS actually do not work with shared key WEP set unless the client saves the key in their key ring. How you should configure your Cisco 4100 Series Wireless LAN Controller is based on the client mix you expect to use. Cisco SWAN recommends testing these configurations before deployment.
- Features Not Supported on the Cisco 2000 Series Wireless LAN Controller:
  - Hardware Features:

    - Power over Ethernet.

    - Service port (separate out-of-band management 10/100 Mbps Ethernet interface).
  - Software Features:

    - VPN Termination (for example, IPSec and L2TP).

    - Layer 2 LWAPP.

    - Spanning tree.

    - Port mirroring.

    - Cranite.

    - Fortress.

    - AppleTalk.
- Some clients can only see 64 AP MAC addresses (BSSIDs) at a time - In a crowded RF environment, clients may not be able to detect the desired SSID because of internal table limitations. Sometimes disabling and then enabling the client interface forces a rescan. Your RF environment needs to be controlled. Cisco SWAN Rogue AP detection and containment can help you enforce RF policies in your buildings and campuses.
- Pinging from any network device to a dynamic interface IP address is not supported - Clients on the WLAN associated with the interface pass traffic normally.

Open Issues in Operating System Software

- 9121 - Session timer passed from RADIUS server may not be correct.
- 10339 - <Back> link on Web User Interface Rogue Detail Page does not work correctly.
- 10719 - RADIUS alarms should carry the IP address of the problem server.
- 12703 - Downgrade from 2.2 to 2.1 results in the loss of RADIUS configurations.
- 13192 - Bytes get swapped in IP address in Cisco 2000 Series Wireless LAN Controller SNMP Trap Logs.
- 13257 - Internal DHCP server data entry does not ensure valid Network Address.
- 13258 - Internal DHCP server data entry does not ensure valid Router Gateway Address.
- 13291 - Client “ipconfig/renew” does not working on foreign client when using DHCP server.
- 13330 - Cisco 2000 Series Wireless LAN Controller Config Wizard returns an error when RADIUS is enabled. Disabling RADIUS allows configuration to be saved.
- 13341 - Cisco 2000 Series Wireless LAN Controller Config Wizard returns an error when L2 mode is configured. Contact Cisco Technical Assistance Center (TAC) to acquire a workaround.
- 13494 - Where Management-Interface and AP-Manager are reconfigured to reside on the same network, the Cisco 4100 Series Wireless LAN Controller must be rebooted in order to prevent mobility issues.
- 13495 - WPA-PSK security does not work when Cisco 1030 remote edge lightweight access point disconnects and moves to Standalone mode.
- 13532 - Under certain circumstances, duplicate IP addresses will not be detected or correctly noted in the logs.
- 13599 - 802.11a channel management does not adjust channels reliably. 802.11b/g channel management functions correctly.
- 13614 - Rogue AP detail page incorrectly shows Preamble = “Long” for 802.11a. This is not valid for that radio type.
- 13987 - Displays show external antenna option for 802.11a on Cisco 1000 Series lightweight access points containing no external antennas.
- 13992 - Multicast Packets Received in port statistics do not increment correctly.
- 14077 - 802.1p tag Policy Granularity not passed from Foreign to Anchor during mobility events.
- 14218 - The Cisco 2000 Series Wireless LAN Controller Web Authentication Session Timeout expiration does not correctly invoke a reauthentication of credentials.
- 14219 - Session timer is not passed correctly during mobility event.

Interoperability Tables

The following table shows which WLAN cards have been tested and tracked for the Release 2.2 Operating System.

WLAN Card	Driver Version	Radio	Status
Belkin F5D7010	3.30.15.0	802.11g	tested
Centrino	7.1.2.10	802.11b	tested
Cisco 350	8.1.7.31	802.11b	tested
Cisco – Air-CB20A	5.01.02	802.11a	tested
Dlink DWL-650	3.0.0.43 (Atheros Driver)	802.11b	tested
Linksys WPC11	5.158.1001.2003	802.11b	tested
Linksys WPC55AG	2.3.0.97	802.11a/b/g	tested
Netgear MA401	2.0.2.0	802.11b	tested
Netgear Prism 2.5 – MA401	2.0.2.0	802.11b	tested
Netgear WAB501	2.0.1.2541	802.11a/b	tested
Netgear WAG511	3.1.1.48 (Atheros Driver)	802.11a/b/g	tested
Nortel LAN2201	3.0.0.43 (Atheros Driver)	802.11a/b	tested
Orinoco 8460	2.4.2.17	802.11a/b	tested
Orinoco Gold	2.0.306.0	802.11a/b	tested
NEC WL54AG	1.1.3.0	802.11a/b/g	tested
I-O DATA WN-AG/CB2	3.0.0.45	802.11a/b/g	tested
PLANEX GW-NS54AG	3.0.0.43	802.11a/b/g	tested
I-O DATA WN-G54	1.0.20.83	802.11b	tested
COREGA CG-WLUSB2GT	1.0.5.1000	802.11g	tested

The following table lists the 802.1X RADIUS Server - Supplicant support matrix.

Supplicant	Steel Belted 4.0				Odyssey 2.0				Microsoft IAS Win XP / 2003		Cisco ACS 3.2				FreeRADIUS 0.9.3			
	TLS	TTLS	PEAP	LEAP	TLS	TTLS	PEAP	LEAP	TLS	PEAP	TLS	PEAP	EAP-FAST	LEAP	TLS	TTLS	PEAP	LEAP
Odyssey Client	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	pass	NS	pass	pass	NS	NS	pass
XP Native	pass	NS	pass	NS	pass	NS	pass	NS	pass	pass	pass	pass	NS	NS	pass	NS	NS	NS
win2k Native	pass	NS	pass	NS	pass	NS	pass	pass	NS	NS	pass	pass	NS	NS	NS	NS	NS	NS
Cisco ACU	pass	NS	pass	pass	pass	NS	pass	pass	NS	NS	pass	pass	pass	pass	NS	NS	NS	NS

Note 1: NS = Not Supported.

Note 2: EAP-FAST has been tested and works with Cisco ACS 3.2.3 and Aironet Client Driver version 6.3.

The following table lists the WPA RADIUS Server - Supplicant support matrix.

Supplicant	Steel Belted				PSK		Odyssey				Microsoft IAS		Cisco ACS 3.2				FreeRADIUS 0.9.3		
	TLS	TTLS	PEAP	LEAP	TLS	TTLS	TLS	TTLS	PEAP	LEAP	TLS	PEAP	TLS	PEAP	FAST	LEAP	TLS	TTLS	PEAP
Odyssey Client	pass	pass	pass	pass	pass	NS	NS	pass	pass	pass	pass	pass	pass	pass	NS	NS	pass	NS	NS
XP Native	pass	NS	pass	pass	pass	NS	NS	NS	pass	pass	pass	pass	pass	pass	NS	NS	pass	NS	NS
Cisco ACU 6.1+	pass	NS	pass	pass	pass	NS	pass	NS	pass	pass	pass	pass	pass	pass	pass	pass	NS	NS	NS

Note 1: NS = Not Supported.

Note 2: EAP-FAST has been tested and works with Cisco ACS 3.2.3 and Aironet Client Driver version 6.3.

The following table lists the RSN/WPA2 - Supplicant support matrix.

Supplicant	Steel Belted				PSK		Odyssey				Microsoft IAS Win XP/ 2003		Cisco ACS 3.2			FreeRADIUS 0.9.3			
	TLS	TTLS	PEAP	LEAP	TLS	TTLS	TLS	TTLS	PEAP	LEAP	TLS	PEAP	TLS	PEAP	LEAP	TLS	TTLS	PEAP	LEAP
Odyssey Client	pass	pass	pass	pass	pass	NS	NS	pass	pass	pass	pass	pass	pass	pass	NS	pass	NS	NS	pass
XP Native	pass	NS	pass	NS	pass	NS	NS	NS	pass	NS	pass	pass	pass	pass	NS	pass	NS	NS	NS
Cisco ACU	pass	NS	pass	pass	pass	NS	pass	NS	pass	pass	pass	pass	pass	pass	pass	NS	NS	NS	NS

Note 1: NS = Not Supported.

Note 2: EAP-FAST has been tested and works with Cisco ACS 3.2.3 and Aironet Client Driver version 6.3.

Notes: