

Auflistung der Cisco IOS XE Wireless-Funktionen pro Version

Inhalt

[Einleitung](#)

[Funktionen jeder Cisco IOS XE-Version](#)

[Dublin - 17.11.1](#)

[Dublin - 17.10.1](#)

[Cupertino - 17.9.3](#)

[Cupertino - 17.9.2](#)

[Cupertino - 17.9.1](#)

[Cupertino - 17.8.1](#)

[Cupertino - 17.7.1](#)

[Bengaluru - 17.6.3](#)

[Bengaluru - 17.6.2](#)

[Bengaluru - 17.6.1](#)

[Bengaluru - 17.5.1](#)

[Bengaluru - 17.4.1](#)

[Amsterdam - 17.3.5](#)

[Amsterdam - 17.3.2](#)

[Amsterdam - 17.3.1](#)

[Amsterdam - 17.2.1](#)

[Amsterdam - 17.1.1s](#)

[Gibraltar - 16.12.4a](#)

[Gibraltar - 16.12.3](#)

[Gibraltar - 16.12.2t](#)

[Gibraltar - 16.12.2s](#)

[Gibraltar - 16.12.1t](#)

[Gibraltar - 16.12.1](#)

[Gibraltar - 16.11.1](#)

[Gibraltar - 16.10.1](#)

Einleitung

In diesem Dokument werden die von den Catalyst Wireless LAN-Controllern der Serie 9800 unterstützten Funktionen kurz beschrieben und aufgeführt.

Funktionen jeder Cisco IOS XE-Version

Jede Funktion wird nur in der Version erwähnt, in der sie mit nachfolgenden Versionen eingeführt wurde, und listet nur Änderungen an der jeweiligen Funktion auf.

Dublin - 17.11.1

- Neue Länder mit 6 GHz-Unterstützung Siehe https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-11/config-guide/b_wl_17_eleven_cg/m_country_codes.html
- Mesh-Hintergrund-Scanning und schnelle Ahnensuche

- Webauthentifizierungsportal unterstützt mehr Zeichen
- Erweiterung des Kalenderprofils über mehrere Tage
- Client-Debug-Paket auf dem WLC
- FRA kann das redundante 2,4-GHz-Funkmodul in den Überwachungsmodus versetzen
- Verbesserte Client-Steuerung während des fortlaufenden AP-Upgrades
- Validierung der Flex OTT- und Roaming-Latenz über BGP EVPN
- Verbesserte Aktualisierungsrate der Spektrumerfassung auf 6E APs
- Jumbo Frame-Unterstützung für RADIUS-Pakete
- Standortfähiges Attribut in RADIUS-Zugriffsanforderungsnachrichten
- Sichere Datenlöschung mit AP
- Kombination aus 802.1X und lokaler Webauthentifizierung mit Mehrfachauthentifizierung
- CLI "show aaa server brief" wird eingeführt
- Effizientes AP-Image-Upgrade über HTTPS
- Ursachenverlauf erneut laden
- Abonnementsperre - Zeitraum für Telemetriedaten bei Änderungen
- Unterstützung für Aktivierung/Deaktivierung der AP-Ethernet-Port-LED
- Latenzstatistik für Wireless-Clients
- DFS auf 9136 ohne Wartezeit
- Standortprüfungsmodus, WGB- und UWGB-Unterstützung für IW9167
- RAP Ethernet-Daisy-Chain mit WSTP
- GNSS-Unterstützung auf IW 9167
- "show tech wireless ap mac <MAC>" wurde verbessert, um die Fehlerbehebung bei AP-Verbindungsproblemen zu erleichtern.
- Intelligente Datenerfassung kann nun auch drahtlose Datenerfassung (d. h. eine kanalbasierte anstatt einer clientbasierten Datenerfassung) ermöglichen.
- Verbesserte Off-Channel-Scan-Verweilzeiten für Cleanair Pro-Chips
- Unterstützung von IP-Überlappungen in zentralen Switching-Bereitstellungen.
- Verbesserte BLE-Unterstützungsbefehle am AP
- Der AP-Kernel kann jetzt Absturzdateien auslesen.
- "debug ntp state" ermöglicht das Debuggen der NTP-Synchronisierung auf APs zusammen mit "show ntp logs"

Dublin - 17.10.1

- Unterstützung für herunterladbare ACLs (dACLs) für zentrale Switch-Bereitstellungen Keine Unterstützung für dACLs in Flexconnect-Bereitstellung oder auf EWC-AP-Plattformen
- AP Prime-Profil zur Massenkfiguration von primären, sekundären und tertiären WLC-Namen und IP-Adressen in den Access Points
- Lastfaktor, wenn Sie APs/Site-Tags über WNCds hinweg zuordnen, um einen gleichmäßigeren Lastenausgleich über WNCds hinweg zu erreichen.
- Erweiterte NetFlow-Monitore von 2 bis 4
- Neue SFP-Unterstützung: genaue Informationen finden Sie in den Versionshinweisen.
- AP-Stromsparfunktion mit Funkdatenströmen und flexiblen PoE
- Yang-Modelle auf 1.1 aktualisieren
- WGB-Modus-Unterstützung bei 9124 und 9130
- CleanAir-Unterstützung auf 6 GHz
- Überwachung der Anwendungsleistung (mit Flex- und Fabric-Modi)
- DNS-Center-Client-Ereignis und SSID-Telemetriefilter
- XML-Aktualisierungssystem für die Geräteklassifizierung
- Sicheres Zurücksetzen auf Werkseinstellungen mit Datenlöschung
- Geräteanalysedaten können über RADIUS Accounting gesendet werden

Cupertino - 17.9.3

- Unterstützung von IOS-basierten APs (x700-Serie)

Cupertino - 17.9.2

- Weitere 75 Länder werden von den Cisco Catalyst Access Points der Serie 916x und Cisco Catalyst Access Points der Serie 9136 unterstützt. Weitere Informationen zur Liste der unterstützten Länder finden Sie im Kapitel [Regulatory Compliance Domain](#).
- iPSK-Passphrase wird für die SAE H2E-Authentifizierung im lokalen Modus unterstützt
- Die Kanäle 120, 124 und 128 für den Zulassungsbereich E werden von den Serien 9124 und 9130 unterstützt.
- 9162I AP wird unterstützt
- Der WLC kann weiterhin bis zu 8 IPv6-Adressen pro Wireless-Client abrufen, ab 17.9.2 wird jedoch kein Datenverkehr mehr vom Client verworfen, wenn nach dem Abruf der 8. Adresse eine neue IP-Adresse dazukommt, sondern eine vorhandene IP-Adresse durch die neue ersetzt wird und der Datenverkehr weiter geleitet wird.
- UNII 3-Band unterstützt für UK in -ROW-Domäne auf 9136 und 916x APs.
- AP-Fallback zu Controllern Priming vom WLC.
- Die MIB CISCO-ENVMON-MIB wurde hinzugefügt

Cupertino - 17.9.1

- Einführung von Quoten und Prioritäten für die skalierte Klassifizierung nicht autorisierter APs (zur Bestimmung, welche nicht autorisierten APs entfernt werden)
- Unterstützung für FT-SAE-Sicherheit
- Unterstützt TLS 1.3 auf dem 9800-Webserver
- Der Access Point kann unabhängig von der WLC-Zeitzone im AP-Join-Profil mit einer Zeitzone konfiguriert werden.
- Unterstützung für CW9164 und CW9166 Access Points
- Erweiterter Standortprüfungsmodus für Wi-Fi6E Access Points
- RADIUS- und TACACS-Authentifizierung und Accounting-Unterstützung für aktive und Standby-WLCs in einem HA SSO-Paar
- Unterstützung für gebührenpflichtige Benutzeridentität in RADIUS-Accounting
- KI-optimierte RRM-Unterstützung für 6E
- Unterstützung für den Scan-Modus von Cleanair Pro
- Gleichzeitige Funkunterstützung für WGBs auf Catalyst APs
- Konfigurieren der standortbasierten mDNS-Filterung mithilfe der Standortgruppe
- Möglichkeit zum Aktivieren oder Deaktivieren der AP-Konsole vom WLC aus
- FRA-Unterstützung in 9166 AP
- HA SSO-Unterstützung für ACI Fabric-Bereitstellungen
- Möglichkeit zum Deaktivieren der Zwischenabrechnung im Richtlinienprofil
- LLDP-Unterstützung auf Standby-WLC
- Kontoführungsunterstützung für Konfigurationsänderungen der Webbenutzeroberfläche
- Mesh-Backhaul-RRM
- Weitere Länder zur -ROW-Domäne hinzugefügt
- Standortbasiertes Rolling AP-Upgrade in N+1-Netzwerken
- 6-GHz-Unterstützung in Kanada
- Unterstützung von RFC 5580-Standortattributen im Controller
- VLAN-Gruppe zur Unterstützung von DHCP und statischen IP-Clients
- Unterstützung für Wireless-Bandbreite für nicht autorisierte Kanäle
- Zero-Wait DFS für 9130 APs in bestimmten Domänen.
- Wireless AP Multicast Unicast-Option für mDNS-Kontrollverkehr auf dem 9800 WLC
- BLE-Funktion für gleichzeitiges Scannen und Beacon

Cupertino - 17.8.1

- Funktionen von Access Point und WiFi6:
 - AP-Stromsparfunktion: Der Controller kann jetzt einige AP-Funktionen deaktivieren, um Strom zu sparen.
 - Der Workgroup Bridge (WGB)-Modus wird jetzt für 9105, 9115 und 9120 Access Points unterstützt.
 - BLE-Verwaltung wird auf 9136 unterstützt
 - Ab dieser Version wird die Client-Beschränkung pro AP, pro Funkmodul und pro AP-Funkmodul pro WLAN unterstützt.
 - APs mit einer flexiblen Funkeinheit (2800/3800/9120/9130) unterstützen jetzt XOR Sniffer, wobei eine einzelne Funkeinheit im Sniffer-Modus agieren kann, während die andere Funkeinheit noch Clients bedient.
 - Umgebungssensorunterstützung am 9136 AP
 - 9136 CleanAir Pro-Funkeinheit kann für Scanning verwendet werden
 - Vereinfachtes WGB-Konfigurationsmanagement mit den "**copy configuration**"-Befehlen
 - Die RLAN-Ports der OEAP-APs unterstützen den Fallback von Punkt1x zu MAB auf den kabelgebundenen Ports.
 - Die AP-Client-Trace-Funktion kann jetzt verworfene Pakete pro Protokolltyp mit dem Befehl **config ap client-trace drop-count** verfolgen.
- Möglichkeit zur Deaktivierung der IP-MAC-Bindung und zur Aktivierung/Deaktivierung von ARP-Broadcast pro VLAN, um die Geräteverfolgung von NAC-Geräten zu beenden oder Drittanbieter-WGBs zu unterstützen.
- Berichte über Geräteanalysen (einschließlich Intel Analytics) werden jetzt an das Cisco DNA Center gesendet
- Flexconnect-Site-Tags können jetzt bis zu 300 APs anstelle der bisher maximal 100 APs haben.
- OEAP Split Tunnel ACLs unterstützen jetzt IPv6- und URL-Filter
- Unterstützung des nächstgelegenen kabelgebundenen mDNS-Service-Providers und der VLAN- und MAC-basierten Filterung im zentralen Switching-Modus, benutzerdefinierte Service-Richtlinien im Flexconnect-Modus
- neue SFPs werden unterstützt
- Unterstützung für Trustsec-Inline-Tagging an Port-Channel-Schnittstellen

Cupertino - 17.7.1

- Funktionen von Access Point und WiFi6:
 - URL-basierte ACLs unterstützen Split Tunneling auf OEAP
 - SD-AVC-Unterstützung für alle AP-Modi (einschließlich Fabric und Flex)
 - Schnellerer Mesh-Netzwerkausfall, wenn der RAP einen Uplink-Fehler erkennt
 - Serielles Backhaul für 9124 APs
 - FIPS-Modus auf Mesh-APs
 - RLAN-Unterstützung auf 9124 APs
 - RLAN-Unterstützung auf Fabric-APs
 - Koexistenz von Icap- und IoT-Telemetrietunneln am AP
 - Unterstützung von 9136 APs
- Catalyst 9800 - Wireless-Innovationen:
 - Support für SUDI99-Zertifikate: Neue Cisco Root-CAs für WLC und APs mit längerer Gültigkeitsdauer
 - Bessere Erkennung von nicht autorisierten Access Points, die einen falschen Kanal melden
 - WPA3 H2E-Unterstützung für SAE-Authentifizierung
 - Unterstützung für WPA3 im Übergangsmodus deaktiviert
 - KI-Enhanced RRM-Unterstützung: Verlagerung des RRM-Algorithmus auf das DNA Center

- und die Cloud
- 9800-CL-Unterstützung in Microsoft Azure Cloud
- Steuern der Verschlüsselungssuite für die lokale EAP-Authentifizierung
- Aktivieren und Konfigurieren von AP BLE-Funkmodulen direkt über den Controller
- Durchsetzung von 9800-CL-Lizenzen
- Wartungsfreundlichkeit
 - Anpassbare Zeichenfolge als NAS-ID konfigurieren
 - Möglichkeit zum Zurücksetzen eines Access Points in Abhängigkeit vom Schwellenwert für AP-Echtzeitstatistiken
 - Unterstützung von 802.11k/802.11v über Site-Tags und WNCd-Instanzen hinweg
 - Die Webbenutzeroberfläche verfügt jetzt über eine Alarmeingangseite für kritische Ereignisse.

Bengaluru - 17.6.3

- Neues SFP unterstützt (hauptsächlich ACU7M und ACU10M)
- Aktualisierte Apple- und Samsung-Informationen für die lokale Geräteprofilierung auf dem 9800
- SGT-Unterstützung für Inline-Tagging für PortChannels
- Der Befehl "ip arp-limit rate" wurde hinzugefügt, um den ARP-Datenverkehr von Clients zu begrenzen.

Bengaluru - 17.6.2

- Der Grenzwert für bidirektionale Übertragungsraten kann jetzt in den lokalen FlexConnect-Switching-APs vollständig pro Client angewendet werden.
- Flex+Bridge Mesh-Unterstützung für 9124 APs
- 802.1X mit WebAuth-Unterstützung bei MAC-Filterausfällen

Bengaluru - 17.6.1

- Funktionen von Access Point und WiFi6:
 1. Konfiguration der globalen Tag-Persistenz auf dem WLC, die automatisch Tags auf die APs schreibt.
 2. Mesh EFT-Unterstützung auf Catalyst 9124
 3. Rest der Welt (-ROW)-Domänenunterstützung
 4. C-ANT9104-Antennenunterstützung sowie Konfiguration der Bandbreite und der Antennenanzahl auf dem WLC
 5. WLAN-Funkrichtlinie: Es kann konfiguriert werden, auf welchen 5-GHz-Slot-SSIDs gesendet werden sollen.
 6. Verschiedene Typen von SIA-Antennen können an denselben Access Point angeschlossen werden. Eine Bereitstellung, die jedoch nicht empfohlen wird.
 7. Kundenzuordnung von max. 9124 geändert von 255 zu 420
- Catalyst 9800 - Wireless-Innovationen
 1. Die mDNS-Funktion unterstützt jetzt die Hochverfügbarkeit, wenn der Controller im Peer-aktivierten oder deaktivierten Modus konfiguriert ist.
 2. Automatische Registrierung zufälliger MAC-Adressen in UDN-Umgebungen
 3. Dataplane-Paketprotokollierung
 4. Fallback für VLAN mit AAA-Überschreibung: Wenn das VLAN mit AAA-Überschreibung nicht auf dem Controller oder AP konfiguriert ist (für den FlexConnect LS-Modus), kann das VLAN aus dem Richtlinienprofil verwendet werden, wenn Fallback aktiviert ist.
 5. mDNS: FHRP-Unterstützung auf SDG für einen Service-Peer
 6. Geräteanalysen von Intel werden an das Cisco DNA Center weitergeleitet
 7. IPv6 Ready-Zertifizierung
 8. Die LDAP-Authentifizierung kann Attributzuordnungen verwenden, die die Verwendung

- anderer Felder als CN für den Benutzernamen zulassen (z. B. samAccountName).
- 9. Link-Lokales Bridging des Datenverkehrs nach dem Layer-3-Roaming
- 10. Über den Service-Port werden weitere Management-Protokolle unterstützt: SNMP, RADIUS, TACACS, Syslog, NTP, SSH, NETCONF, HTTPS, NetFlow
- 11. Device Classifier (Profiling) umfasst jetzt Daten aus Device Analytics
- 12. Nachdem eine HA SSO-Konfiguration unterbrochen wurde, behält der Standby-Modus die gleiche Konfiguration bei (mit Ausnahme des Herunterfahrens der Schnittstellen), anstatt die gesamte Konfiguration zu verlieren.
- Wartungsfreundlichkeit
 1. FQDN-Unterstützung für gRPC-Telemetrie
 2. Präzisere Gründe für das Löschen von Clients aus dem SANET-Prozess
 3. Einige CLIs wurden hinsichtlich des MAC-Adressformats konsistenter gestaltet (in Richtung xxxx.xxxx.xxxx)
 4. Sichere Boot-Einrichtung für ESXi, KVM, NFVIS und Microsoft Hyper-V
 5. Status der Standby-Schnittstelle über Aktiv über SNMP
 6. Syslog-Unterstützung für Wips
 7. Clients können nun durch IP-Adresse (Wireless Client IP-Adresse A.B.C.D deauthentifizieren) oder durch Benutzernamen (Wireless Client Benutzername Bob deauthentifizieren) deauthentifiziert werden
 8. Die Schlüsselvalidierung erfolgt nur für Beacons und Frames für die Abfrageantwort (nicht für alle Frames), wenn MFP aktiviert ist, um zu verhindern, dass Cisco APs als unautorisiert erkannt werden.
 9. "show ap name <ap-name> wlan vlan" zeigt jetzt die WLAN-VLAN-Zuordnung eines Access Points mit SSIDs für lokales FlexConnect-Switching
 10. Der AP-Webserver beendet die Unterstützung der TLS-Version vor TLS 1.2.
 11. Universelles AP-Priming auf Cat9100-APs deaktiviert.
- Neuer WLAN-Assistent in der Webbenutzeroberfläche

Bengaluru - 17.5.1

- Funktionen von Access Point und WiFi6:
 1. Unterstützung der neuen C9124AX Access Point-Plattform
 2. Spektrumintelligenz für C9105AX
 3. Mehr 11ax OFDMA-Benutzer pro Übertragung an Catalyst 9105, 9115 und 9120 Access Points
 4. 11ac- und WiFi6-MU-MIMO-Unterstützung für C9105AX
 5. Client-lastbasierte EDCA-Parameter
 6. Möglichkeit zum Aktivieren oder Deaktivieren bestimmter Wi-Fi6-Funktionen pro SSID
- Catalyst 9800 - Wireless-Innovationen
 1. LAG-Unterstützung auf 9800-CL
 2. Unterstützung für MIC und LSC zum Beitritt zu demselben C9800 WLC
- Wartungsfreundlichkeit
 1. Standby-Überwachung
 2. Möglichkeit, die Verbindung von zufälligen MAC-Clients zu verbieten
 3. Überwachung der AP-CPU-Nutzung
 4. HA-Verbesserungen, wie z. B. automatische Upgrades des Standby-WLC, wenn das HA-Paar nicht dieselbe Version verwendet
 5. DHCP Relay : Passt die Einstellung der DHCP-Relay-Parameter wie Gateway-IP-Adresse, Option 82 und DHCP-Serveradresse an das Cisco AireOS-Verhalten an.
 6. Verfügbarer Port-Channel-Bereich von 1 bis 64
- Sicherheit und Ausfallsicherheit
 1. Easy PSK: WLAN-Client-Integration ohne Registrierung
 2. Unterstützung für Suite B 192-Bit-AVPs
 3. IP-Erreichbarkeitsprüfung des Standardgateways

4. Unterstützung von Zwischen-Zertifizierungsstellen für LSC-Zertifikate
5. Unterstützung für MIC- und LSC-APs, um die Verbindung zum Controller herzustellen
6. Unterstützung von DTLS durch mehrere Verschlüsselungsreihen
7. WPA(2)-PSK mit Unterstützung für Web-Authentifizierung bei MAC-Filterausfall
8. Zusätzliche Signaturen für Wips

Bengaluru - 17.4.1

- Wave1 Access Points (Cisco IOS-basiert) werden nicht mehr unterstützt (mit Ausnahme von IW3700)
- RLDP wird von dieser Version nicht mehr unterstützt.
- AP-Speicherinformationen werden jetzt gemeinsam genutzt
- Unterstützung für DHCP-Option 12 zum Festlegen des Hostnamens von Access Points
- Erweiterte Planungsanforderung für Clients
- Erkennung von getrennten Antennen
- Transparenz der Boot-Integrität
- Gateway-IP-Prüfung mit nativem IPV6
- "show ap image file summary" zeigt jetzt AP-Bilder an
- Unterstützung für OBSS-Paketerkennung
- Unterstützung für sich überschneidende IP-Adressen in Flex-Bereitstellungen
- Schnellere Erkennung von Gateway-Erreichbarkeitsverlusten
- RAP Ethernet-Verkettung
- Accounting-Sitzungs-ID wird in 802.1X unterstützt
- Unterstützung von Trennzeichen in der Unteroption "DHCP-Option 82 - Remote-ID"
- WIPS: konfigurierbarer Grenzwert für Unterstützung von Alarmen und Forensikerfassung
- Day0 CLI-Assistent
- Unterstützung für den Neustart aller APs, die einem Site-Tag zugeordnet sind, mit nur einem Klick.
- Syslog-Server können jetzt mit FQDN konfiguriert werden
- Smart Licensing mit Richtlinie
- Verbesserungen der Web-Benutzeroberfläche zur Überwachung der CPU- und Datenflugzeugauslastung
- TWT-Unterstützung für 9115 und 9120 APs hinzugefügt
- 9800 unterstützt die Konfiguration des RADIUS-Attributs mit Framed-MTU

Amsterdam - 17.3.5

- Der Befehl "ip arp-limit rate" wurde hinzugefügt, um den ARP-Datenverkehr von Clients zu begrenzen.

Amsterdam - 17.3.2

- Autorisierung von OfficeExtend Access Points über Seriennummer
- Administrator kann lokalen Zugriff auf die Office Extend Access Points-Benutzeroberfläche aktivieren oder deaktivieren
- BLE- und Assurance-Koexistenz auf dem Access Point ohne ICAP
- Smart Licensing mit Richtlinie
- TLS-Unterstützung für Telemetrie zur DNA Center Cloud
- Unterstützung überlappender Client-Subnetze in Flex-Bereitstellungen, nur für PSK und dot1x

Amsterdam - 17.3.1

- 802.11ax/Wi-Fi6
 - Das Cisco DNA Center Assurance Wi-Fi 6-Dashboard bietet eine visuelle Darstellung des Wireless-Netzwerks.

- Dynamische Tri-Radio-Unterstützung für 9130
- In dieser Version werden sowohl Uplink- als auch Downlink-Funktionen (UL OFDMA und DL OFDMA) für die orthogonale Frequenzaufteilung in dieser Version von den Cisco Catalyst 9130 APs unterstützt. Derzeit begrenzt auf die Unterstützung von acht Benutzern in einer DL OFDMA- oder UL OFDMA-Übertragung. In dieser Version werden 37 Benutzer in den Bandbreiten 80 MHz und 160 MHz unterstützt.
- Uplink Die Funktion "Multi-User Multiple Input, Multiple Output" (UL MU MIMO) wird in dieser Version von den Cisco Catalyst 9130 APs unterstützt.

Access Point-bezogene Funktionen

- Die Funktion "AP Audit Configuration" hilft bei der Erkennung von Synchronisierungsproblemen zwischen dem Controller und dem Access Point.
- Unterstützung für AP 9105
- Wi-Fi Direct-Unterstützung
- Die Erweiterung der Download-Zeit für AP-Images unterstützt mehrere Schieberegler für Steuerungspakete, die vom Controller zum AP übertragen werden.
- AP-Support-Paket: Sie können jetzt die Support-Paket-Informationen eines AP abrufen und an den Controller oder einen externen Server exportieren.
- Besonderheiten des IW3702:
 - AVC-Unterstützung auf IW3702
 - IW3702 kann nun seine Heizungen aktivieren oder deaktivieren
 - Unterstützung von Ethernet-Verkettung auf IW3702
 - Flexible Antennenanschlusskonfiguration
- Funktion für Spektrumintelligenz auf C9115
- Unterstützung externer Module
- gNMI-Konfigurationspersistenz
- IoT-Modulmanagement
- IPv6-Multicast-Filterung
- mDNS-Gateway-Unterstützung für Flex
- Hardwareunterstützung für DTLS-Verschlüsselung bei 9120 und 9115
- IGMPv3-Unterstützung auf COS-APs (Wave2- und 11ax-APs)

Controller-bezogene Funktionen

- BLE-Management auf dem Controller.
- Der Controller ermöglicht ein nahtloses Roaming zwischen demselben WLAN, das mit unterschiedlichen Richtlinienprofilen verknüpft ist.
- Eingebettetes Wireless auf Cat9k-Switches wird jetzt nicht sda (aber dennoch Fabric) unterstützt.
- Die PKI-Verwaltungsseite wurde erweitert und ermöglicht nun die Erstellung von CSRs und den Import von Zertifikaten.
- Zertifizierungsfunktionen für Hostpot 2.0 Release 3
- Webauthentifizierung und Webadministrator verfügen jetzt über separate Einstellungen für HTTP/HTTPS
- Mesh-Funktionen.
 - Mesh-Backhaul in 2,4 GHz.
 - Mesh-Hintergrundsuche außerhalb des Kanals
 - Verbesserte Mesh-Konvergenz.
- ARP-Proxy

- Der Controller behält die Client-Sitzung für 10 Sekunden bei, anstatt sie für einige Clients sofort zu löschen.
- Ein nicht autorisiertes Gerät, das mit 802.11w Protected Management Frames (PMF) aktiviert ist, ist nicht enthalten. Stattdessen wird das nicht autorisierte Gerät als "*Contained Pending*" (*Eingeschlossen, Ausstehend*) markiert, und es wird ein Alarm zur Wireless Service Assurance (WSA) ausgelöst, um über das Ereignis zu informieren.
- Ein Standby-WLC kann in einem HA SSO-Paar überwacht werden, indem die Redundanzmanagement-IP-Adresse erreicht wird.
- Mit der mobilen Anwendung Cisco User Defined Network (UDN) können Sie ein benutzerdefiniertes Netzwerk erstellen und den Zugriff auf Geräte einschränken, wenn diese nicht zur Freigabe des Netzwerks aufgefordert werden.
- SR-IOV kann in KVM- und ESXi-Umgebungen konfiguriert werden.
- Mit der Syslog-Unterstützung für Client-Statusänderungen können Sie Client-Details wie IP-Adressen, AP-Namen usw. verfolgen.
- Unterstützung für DS-Parametersätze: Die verwalteten APs verfügen nun in den Berichten für nicht autorisierte APs über zusätzliche Informationen zum DS-Parametersatz des erkannten nicht autorisierten APs.
- 2 zusätzliche WIPS-Angriffssignaturen.
- Vollständige Unterstützung von ISSU
- Individuelles Webauth TAR-Paket wird jetzt auch auf Standby-WLC kopiert
- Client-Details zeigen nun an, ob der Client eine universell verwaltete MAC-Adresse oder eine zufällige MAC-Adresse verwendet.
- Ab Version 17.3 können Vorlagen für hohen Durchsatz auf den Private Cloud-Instanzen des Cisco Catalyst 9800-CL Cloud Wireless Controller konfiguriert werden.
- Web-Benutzeroberfläche:
 - Dunkler Modus
 - AP-LED blinkt
 - AP-Supportpaket herunterladen
 - Optimierte PKI-Verwaltungsseite
 - OpenRoaming
 - Integrierte Wireless-Funktion auf 9000-Switch (nicht SDA)
 - Verbesserungen für Software-Upgrades
 - TRi-Funkkonfiguration
 - Überwachung der Gerätetemperatur im Dashboard

Sonstige Änderungen

- Für die Cisco Catalyst Wireless Controller der Serie 9800-CL sind jetzt 16 GB Festplatte erforderlich.
- Ab Cisco IOS XE Amsterdam 17.3.1 werden auf den folgenden Cisco Catalyst Wireless Controllern der Serie 9800 mehr Port-Channels unterstützt:
 - Cisco Catalyst Wireless Controller 9800-80: 1-40 bis 1-64
 - Cisco Catalyst Wireless Controller 9800-40: 1-4 bis 1-16

- Cisco Catalyst Wireless Controller 9800-L: 1-6 bis 1-14
- Ab Cisco IOS XE Amsterdam 17.3.1 darf der Name des Access Points nur noch bis zu 32 Zeichen lang sein.
- Beim Downgrade von Cisco IOS XE Amsterdam 17.3.1 auf eine frühere Version werden die Port-Channels ausgeblendet, für die ein höherer Bereich konfiguriert wurde.
- Bei Verwendung eines EoGRE-AAA-Proxys sind die AAA-Ports standardmäßig auf 1645 und 1646 festgelegt. Um diese Port-Konfiguration zu ändern, verwenden Sie den folgenden Befehl: `tunnel eogre interface tunnel-intf aaa proxy key key key-name auth-port auth_port acct-port acct_port`
- Der Mobility-Tunnel fällt aus und wird aktiviert, wenn SSO aufgrund eines Fehlers bei der Gateway-Prüfung ausgelöst wird.
- Zusätzliche Unterstützung für LED-Blinklicht bei Cisco Catalyst 9800 Wireless Controllern
- Das der GUI hinzugefügte Fenster Log Viewer (Protokollanzeige) zeigt radioaktive Ablaufverfolgungsprotokolle an.
- Neues Feld zum Anzeigen des AP-Konfigurationsstatus in der GUI hinzugefügt.
- Der Spaltenheader in der Erkennung von nicht autorisierten Elementen wurde von "MFP Required" in "PMF Required" geändert.
- Das Feld "Central Forwarding" (Zentrale Weiterleitung), das auf der Registerkarte "EoGRE > Tunnelprofile > Tunnelprofil bearbeiten > Allgemein" angezeigt wurde, wurde entfernt.

Diese MIBs wurden modifiziert.

- CISCO-LWAPP-AP-MIB.my
 - Folgende skalare Objekte wurden hinzugefügt:
 - cLApGlobalAPAuditBericht
 - cLApGlobalAPAuditReportInterval
 - Der Tabelle "cLApProfileEntry" wurden folgende Objekte hinzugefügt:
 - cLApProfilePersistentSsidBroadcastAktivieren
 - cLApProfilDhcpFallback
- CISCO-LWAPP-DOT11-CLIENT-CALIB-MIB.my
- CISCO-LWAPP-DOT11-CLIENT-MIB.my
- CISCO-LWAPP-DOT11-MIB.my
- CISCO-LWAPP-WLAN-SECURITY-MIB.my
- CISCO-WIRELESS-HOTSPOT-MIB.my
- CISCO-LWAPP-REAP-MIB.my

- CISCO-LWAPP-WLAN-MIB.my
 - cLWlanWifiDirectPolicyStatus: Dieser Richtlinienwert wurde hinzugefügt.
 - xconnectNichtZulassen

Amsterdam - 17.2.1

- 802.11ax/Wi-Fi6
 - Ziel-Aktivierungszeit
 - Dynamische Tri-Radio-Unterstützung für 9130
 - Spektrumanalyse mit DNAC
- Unterstützung für Hochleistungszugangspunkt IW6300
- Möglichkeit zum Deaktivieren/Aktivieren des opportunistischen Schlüssel-Caching
- Lokal geschaltete RLANs leiten Datenverkehr auch dann im lokalen Modus weiter, wenn der WLC nicht erreichbar ist.
- Multi-LAG-Unterstützung
- IPV6 QoS-Unterstützung (nicht AVC) in Flex Local Switching- und Fabric-Konfigurationen
- Fabric-in-a-Box mit externer Fabric-Edge-Unterstützung
- FT wird jetzt für lokales FlexConnect-Switching und lokale Authentifizierung unterstützt
- Möglichkeit zum Erstellen einer Mobilitätsdomänen-ID für die gemeinsame Nutzung von zwischengespeicherten Schlüsseln zwischen APs
- Für lokales FlexConnect-Switching wird jetzt DHCP unterstützt.
- HA SSO mit RMI : "ip default-gateway" ist nicht mehr erforderlich. Gateway-IP finden Sie in der Routing-Tabelle.
- Statistiken der BSSID-Zähler
- Unterstützung von OpenRoaming in der Kommandozeile
- Aironet IE wurde um den AP-Namen erweitert.
- Der Sensormodus wird vom Access Point nicht mehr unterstützt.
- Web-Benutzeroberfläche:
 - Unterstützung für Tri-Radio
 - Bericht zur intelligenten Client-Suche im Geräte-Ökosystem
 - Anzeige der SGT- und VN-Attribute

Amsterdam - 17.1.1s

- Hohe Verfügbarkeit (AP SSO)
 - Redundanz-Management-Schnittstelle
 - Gateway-Verifizierung
 - LACP-Unterstützung für HA SSO (LACP wurde bereits im Standalone-WLC unterstützt)
- 11ax/WiFi 6
 - BSS-Färbung (noch keine OBSS-PD)
 - FastLocate auf 9120
 - IPV6-RA-Weiterleitung bei kabelgebundenem Gast
 - Unterstützung von OpenDNS auf IPv6 und Flexconnect
 - IPv6-Unterstützung für verschlüsselte Datenverkehrsanalyse
 - Flex/Fabric AVC auf IPv6
 - Flexconnect lokale Authentifizierung auf IPv6
 - CMX- und DNA Spaces over IPv6 NMSP-Unterstützung
 - IPv6 Assurance und Netconf
 - UDPlite-Unterstützung für Capwapv6-Tunnel
- Neue Hardware
 - Unterstützung für IW3700 und IW6300 AP

- 9800-CL-Unterstützung auf HyperV
- Unterstützung für integrierte Wireless Controller auf Catalyst Access Points (EWC-AP)
- Unterstützung für Mesh (Bridge-Modus) auf allen Indoor Wave 2 APs
- Flex+Bridge-Modus-Unterstützung (außer für Wi-Fi6-APs)
- 9800-L Performance-Lizenzunterstützung
- aWischt
- Facebook Express Wi-Fi
- Unterstützung von VLAN-Außerkräftsetzung nach Gast-Authentifizierung (LWA und CWA)
- Mobility-Tunnel-Unterstützung für WLCs hinter NAT
- QoS-Richtlinienänderung für Wireless-Clients ohne Trennung der Verbindung
- Netzwerk : Samsung Analytics
- Privates Netzwerk von Benutzern
- Verfolgung von AP-Up-/Down-Ereignissen innerhalb der RADIUS-Accounting
- iPSK Peer-to-Peer-Blockierung
- mDNS advanced (Richtlinie unter VLAN, mdns unter RLAN, Erweiterung für Standortfilterung, mdns auf AP, mdns für kabelgebundenen Gast)
- SGACL-Unterstützung für Wireless-Gastzugriff mit Anker
- Smart License verbesserte Nachverfolgung der AP-Identität zur Vermeidung doppelter Zählungen
- Client-Multi-Auth für Gast: L2 (dot1x,PSK) + L3 (LWA/CWA)-Authentifizierungskombinationsunterstützung mit Gast-Anker
- TLS 1.2-Unterstützung für lokale EAP-Authentifizierung
- Flexible lokale Switching-Unterstützung für DNS-URL-Filter-ACLs vor und nach der Authentifizierung
- Erweiterte URL-Filter (pro URL Zulassen/Verweigern von Aktionen) nur für Flex Local Switching
- DNS-Unterstützung für Netzwerkservices wie Radius

Gibraltar - 16.12.4a

Keine neuen Funktionen in dieser Version

Gibraltar - 16.12.3

Ab dieser Version funktionieren nur noch unterstützte SFPs. Wenn Sie einen nicht unterstützten SFP verwenden, funktioniert der Port nicht.

Gibraltar - 16.12.2t

Keine neuen Funktionen.

Gibraltar - 16.12.2s

- Unterstützung für 9120AX und 9130-AXI AP
- Default-policy-tag bearbeitbar: Automatische Zuordnung von WLAN-ID 1-16 zu Standard-Policy-Profil deaktiviert

Gibraltar - 16.12.1t

- Verhindert, dass 9120AX und 9130AXI mit 9800 verbunden werden

Gibraltar - 16.12.1

- Hardware
 - Unterstützung für 9800-L
 - Unterstützung für 1840 AP
 - Unterstützung der Google Cloud-Plattform als Public Cloud-Betreiber
- Unterstützung für -P-Domäne
- vMotion-Unterstützung für Esxi
- BLE-USB-Dongle-Unterstützung
- WPA 3
- Unterstützung für Hostpot 2.0
- Kabelgebundener Gast
- Erweiterte Unterstützung für Public Cloud (bis zu 6.000 APs)
- OFDMA-Unterstützung für Catalyst 9100 APs
- Flexibler Multiband-Betrieb durch Wi-Fi Alliance
- MFP-Unterstützung
- Airtime Fairness auf Mesh
- Checker-Fenster für Best Practices auf der WLC-Weboberfläche
- Einrichtung von Wireless-Client-Sitzungen mit Kalenderprofil verweigern
- IPv6-Unterstützung für Fabric-Modus-Clients und ACL vor und nach der Authentifizierung
- IPv6 Multicast-to-Unicast
- Unterstützung für IPv6 Prime-Infrastruktur
- Sicherheitsoptimierter permissiver Linux-Modus
- RadioActive-Ablaufverfolgung jetzt über die Webbenutzeroberfläche verfügbar
- RadioActive verfolgt eine IP-Adresse einer Multicast-Gruppe.
- Zurücksetzen auf vorherige Versionen zulassen ("show install rollback")
- FIPS-Zertifizierung
- LACP für Standalone-WLC

Gibraltar - 16.11.1

- Hardware
 - Unterstützung für Wi-Fi6-Zugangspunkte der Modelle 9115, 9117, 9120 und 11ax
 - Integrierte Wireless-Unterstützung für Catalyst 9400, Catalyst 9500 (insbesondere für 16.11.1c)
- mDNS-Gateway/Proxy-Unterstützung auf dem 9800 WLC
- Bidirektionale Ratenbegrenzung mit AAA-Aufhebung
- PAT-Unterstützung auf CAPWAP für den Beitritt von Remote-APs (hinter NAT/PAT)
- Upgrade-Funktion für AP-Gerätepaket
- AP SMU-Upgrade pro Standort oder AP-Modell
- Lobbybotschafter
- LAG-Unterstützung auf APs für den Flexconnect-Modus
- EoGRE-Unterstützung
- DHCP auf Root-Mesh-APs mit NAT-Unterstützung
- Unterstützung für BLE-Funkmodule in APs
- Lokale Webauth (LWA)-Unterstützung für IPv6-ACLs auf Flex
- Mesh-CAC
- Guestshell auf Appliances [9800-40/9800-80]
- RESTCONF Configuration Management Protocol (RESTCONF)
- Servicelevel-Zugriffskontrolllisten für NETCONF und RESTCONF
- RadioActive Tracing für den NMSP-Prozess mithilfe der CMX-IP-Adresse
- Mobilitätsprotokollstatistiken auf dem 9800 über den Befehl "show wireless stats mobility messages"
- AP nach Gruppen neu starten
- Aktualisierungsseite für Webbenutzeroberfläche unterstützt jetzt SFTP-Option
- Passiver Client in SDA
- Unterstützung für MAC-Adresse als Filter im Packet Tracer

- Richtlinienklassifizierungs-Engine
- Aktionsprofil für UNBEKANNTE Geräte mit lokaler Profilierung:

Gibraltar - 16.10.1

Dies ist die erste Version, die 9800-Controller unterstützt.

- Unterstützte Plattformen
 - 9800-40 (einschließlich SFP-Unterstützung für RP-Port, USB 3.0-Unterstützung)
 - 9800-80
 - 9800-CL auf ESXi, KVM, ENCS(NFviS)
 - 9800-CL auf AWS
 - 9800-SW - Fabric-Unterstützung auf Cat9300
- AP-Modi
 - Lokal
 - FlexConnect
 - Brücke (Mesh)
 - Sniffer
 - Überwachung
 - OEAP-Unterstützung
- Allgemein
 - CAPWAP-Fragmentierung
 - Daten-DTLS
 - Wireless-Management-Schnittstelle
 - Management über Wireless
 - Zulassung (20 Ländercodes unterstützt)
 - Smart License-Unterstützung
 - Spezifizierte Lizenzreservierung
 - L2-Port-Channel
 - L3-Zugriffsliste
 - WLC zum Generieren des 2048-Bit-RSA-Schlüssels
 - CSR-Zertifikate
 - Lokal signiertes PKI-Zertifikat (LSC)
 - Rechtmäßiges Abfangen: AAA-Attribute
 - Standby-Client
 - Webserver
 - Bring Your Own Device (BYOD)
 - Verschlüsselte Verkehrsanalyse (ETA)
 - Unterstützung der Erstellung dynamischer Telemetrie-Abonnements
 - Best Practices mit Fehlerbehebung
 - Plug-and-Play-Verbesserungen
 - Day 0-Assistent
 - Migrationstool für die Bereitstellung bestehender Private und Public Clouds über die vEWLC-Benutzeroberfläche und eigenständige Anwendungen
 - Smart Call Home
 - Stadion-Vision
 - Integrierte Paketerfassung
 - Packet Tracer für die Datenebene
 - TrustSec SGT: SGACL und Inline-Tagging bei WLC
 - Wireless-Übertragung

- DNS-ACL, FQDN-Auth-ACL, URL-Filterung
- Programmierbarkeit und Telemetrie
- Netzwerkservices
 - DNS
 - RADIUS (einschließlich RADIUS-Auswahl nach Bereich)
 - Ping
 - Telnet
 - SSH
 - HTTP
 - NTP
 - SNMP
 - Syslogs (einschließlich Unterstützung für die Konfiguration von Syslog-Hosts nach Hostnamen)
- WLAN
 - Neues Konfigurationsmodell
 - Zentrale Authentifizierung (WPA/WPA2, EAP-FAST/EAP-PEAP, WPA2-PSK)
 - Statisches WEP
 - WPA-PSK/TKIP
 - MAB
 - LDAP
 - Sicheres LDAP
 - CCKM
 - Multi-PSK (MPSK)-Sicherheit für SSIDs mit bis zu 5 Schlüsseln pro SSID
 - Autorisierungsänderung (CoA)
 - Multiple-Auth-Methoden (PSK+LWA/CWA, MAB+iPSK+LWA, do1x+LWA) - nur für Nicht-Gast-Clients (Fremd-/Anker-Clients).
- WLAN Erweitert
 - Client-Lastenausgleich
 - Client-Grenzwert
 - P2P-Blockierung
 - Bandauswahl
 - 802,11h
 - 11 W
 - 11r
 - 11 V (BSS-Übergang, Leerlaufzeitüberschreitung, gerichteter Multicast-Dienst)
 - P2P-Client-Unterstützung
 - AAA-Außerkräftsetzung
 - VLAN-Gruppierung
 - IP Source Guard v4/v6
- DHCP
 - Interner DHCP-Server
 - IP-Diebstahl
 - DHCP-Relay (einschließlich Option 82)
 - DHCP-Option 82 (AP-Name-SSID, AP-Greifname, Flex-Greifname, AP-Standort, AP MAC, AP-Name + VLAN, AP eth MAC),
 - DHCP-Suboption 5, 151/152 (Cisco IOS- und COS-APs)
 - DHCP am AP mit NAT (nur IPv4)
 - DHCP-opt. 60 + Anbietername
- Lokaler Modus/Zentrales Switching
 - Lokaler Modus: Open Auth + MAB
 - Lokaler Modus: WPA/WPA2-PSK/802.1x
 - Lokaler Modus: LWA/CWA
 - Lokaler Modus: Client IPv6
 - Lokaler Modus: RF-Gruppierung/TPC/DCA/CHD
 - Lokaler Modus: 802.11k

- Lokaler Modus: ACL
- Lokaler Modus: RxSoP
- Lokaler Modus: Smart Roaming
- Lokaler Modus: Clean Air
- Lokaler Modus: EDRRM
- Lokaler Modus: XoR
- Lokaler Modus: SXPv4-Unterstützung für WLC
- DNAC Automatisierungs- und Assurance-Workflow für Lokal
- FlexConnect
 - Zentrales Switching/Zentrales DHCP
 - Effizientes FlexConnect (FC)-Image-Upgrade
 - Telearbeiter
 - TrustSec:SGT-Inline-Tagging für Flex-Modus
 - Ethernet-Fallback
 - Ethernet-VLAN-Tag am AP
 - Split-Tunnel, NAT-PAT, Radius-Fallback, zentrales DHCP (lokale SW)
 - Client V6
 - Proxy ARP
 - Remote-LAN-Unterstützung (RLAN) für 1815
 - TrustSec SGT: SGACL und Inline-Tagging für Flex
 - Flex AP über NAT an WLC. Bei Verbindungsunterbrechung fungiert der flexible Access Point als lokaler DHCP-Server.
 - DNAC Automatisierungs- und Assurance-Workflow für Flex
- Mesh
 - Beste Auswahl für übergeordnete Elemente - einfache Berechnung, übergeordnete Entscheidung, SNR-Glättung, Schleifenvermeidung, bevorzugte übergeordnete Elemente
 - Mehrere RAPs
 - RRM auf 5-GHz-RAP
 - GPS-Unterstützung für Außenbereiche
 - Bereitstellungsmodi: Wireless-Backhaul, universeller Zugriff, Wireless-Punkt-zu-Multipoint-Bridging, P-P-Bridging
 - Lokal signierte Zertifikate (LSC)
 - Verschiedene Authentifizierungsmechanismen - MAC-Adresse, RADIUS, PSK, LSC
- WGB
 - WGB mit mehreren VLANs (Bergbaufunktion)
 - Universeller WGB
 - Hochgeschwindigkeits-Roaming (WGB und WLC)
 - Statischer Anker WGB
- RF/RRM/Nicht autorisiert
 - RF-Gruppierung
 - Dynamische Kanalzuweisung (DCA)
 - Transmit Power Control (TPC)
 - Erkennung von Abdeckungslochern
 - Rx-SOP
 - EDCA-Parameter
 - 11ac - 80 MHz
 - FRA
 - XOR
 - Dynamic Band Selection (DBS)
 - Unterstützung von 3. Funkmodulen
 - Aktivierungs-/Deaktivierungsraten pro SSID
 - DFS- und Nicht-DFS-Kanalsuche
 - Energiesparmodus (U-APSD)
 - Client-Link

- wIPS Auto SPT (Switch Port Tracing) - Prime obligatorisch
- Nicht autorisiert/RLDP - ein Controller
- Nicht autorisiert pro AP
- Airtime-Berechtigung
- CleanAir
- Spektrumintelligenz auf 18xx APs
- Flexibles DFS
- AP
 - AP-Priorität
 - AP - Lokale Authentifizierung intern
 - Lokale AP-Authentifizierung extern
 - Hochladen von AP-Absturzdateien
 - AP-CDP
 - AP-Image-Vorabdownload
 - AP-NTP
 - AP-Authentifizierungsliste
 - AP-Paket-Dump
 - AP-LAG (Lokaler Modus)
 - TCP-MSS-Anpassung (lokaler Modus, FlexConnect- und Fabric-Modus)
 - AP-Filter
 - AP-Bereitstellungs-PnP
 - DNS- und AP-Domäne auf APs mit statischer IP-Adresse angeben
 - AUX-Ethernet-Port aktiviert auf Wave 2-APs für Downstream-Geräteverbindungen
- Mobilität
 - IRCM
 - Gastzugriff
 - L2-Mobilität (Einzelinstanz) Open Auth
 - L2-Mobility-MAB/dot1x
 - L2 Mobility LWA/CWA
 - L3-Mobility OpenAuth
 - L3-Mobilität Dot1x, MAB
 - L3-Mobility-CWA, LWA
 - Sicherheitsprofilaktualisierungen für Ankeranwendungsfälle (GS-Funktion)
 - Apple L3-Mobilität
 - Roaming für statischen Client
 - Automatische Ankerunterstützung für DNS-basierte ACL
- Gast
 - Gast-Anker
 - Interne/Externe Webauth
 - CWA
 - Redundante Guest Anker-Gruppen
 - Webauth bei MAC-Fehler
 - Nahtloses Roaming in WebAuth ausstehend
 - Unterstützung von Foreign Map
- Hohe Verfügbarkeit
 - HA AP und Client SSO [kein RMI, keine Gateway-Prüfung, kein Remote-Zugriff auf den Standby-Service-Port]
 - HA - N+1-Redundanz für integrierte Wireless-Switches (9800-SW)
 - Prozessneustart und Patching-Unterstützung für integrierte Wireless-Funktionen auf Switches (9800-SW)
 - SMU + Rolling AP-Upgrade
 - N+1 Rolling AP-Upgrade für vollständige Controller-Image-Aktualisierung

- QoS/Sprache/Video
 - Voice-over-Wireless
 - Automatische QoS
 - Sprachmobilität
 - QoS - BSSID
 - QoS - Client
 - QoS - Fastlane
 - SDN-QoS
 - QoS-TCLAS, SIP
 - QoS SIP Voice Call Snooping
 - SIP-CAC
 - Punkt1P-Markierungen
 - Ungefähre faire Bandbreite
 - Diagnose der Sprachfunktionen
 - Sprachmetriken
 - Video-CAC
- AVC/Profilierung
 - NBAR-Protokollerkennung
 - Flexibles NetFlow
 - Application Visibility and Control (AVC)
 - Native Profilierung
 - Dynamisches Protokollpaket-Upgrade
- Multicast/mDNS
 - Multicast - IPv4
 - Multicast - L2-Roaming (eine Instanz)
 - VLAN-Auswahl und L2/L3-Multicast-Optimierung
 - Medien-Streaming (MC2UC)
- IPV6
 - Natives IPv6
 - IP Source Guard V6
 - Webauth IPv6
 - IPv6-Client - Mobilität/Roaming
 - IPv6-Client - SDA Wireless (nur)
 - IPV6-Multicast-Multicast
 - Interner IPv6-DHCP-Server
 - AP-Teilnahme an Public Cloud über Cisco Cloud Connect PnP-Workflow
 - AP Teilnahme an Private Cloud über Cisco DNA-Center PnP-Workflow oder über reguläre DHCP/DNS/Priming-Option
- Location (Standort)
 - NMSP
 - Hyperlokation
 - Probe RSSI und Standort
 - Unterstützung für CMX Cloud
 - NMSP-Unterstützung für CleanAir
 - RFID-Tag-Unterstützung
 - Hyperlocation - CMX, HA und AP-Filterung

- Hyperlocation-Unterstützung - Fabric-Modi
- SDA
 - Unterstützung für Over-the-Top (OTT)/Flex
 - 1800s Sensor-Unterstützung
 - DNAC Automatisierungs- und Assurance-Workflow für Fabric
 - SDA IRCM
 - NetFlow-Unterstützung Fabric Edge
 - Sichere Kontrollebene
 - Ein WLC für mehrere Fabric-Domänen (MAP-Server pro AP-Gruppe)
 - AP-Unterstützung für Außenbereiche
 - iCAP-Unterstützung für AP4800

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.