REAP-Implementierungsleitfaden für Zweigstellen

Inhalt

Einführung

Dieses Dokument enthält Informationen, die bei der Bereitstellung eines Remote-Edge Access Point (REAP) berücksichtigt werden müssen. Konfigurationsbeispiel für grundlegende REAP-Konfigurationsinformationen finden Sie im Remote-Edge AP (REAP) mit einfachen APs und Wireless LAN Controllern (WLCs).

Hinweis: Die REAP-Funktion wird bis WLC Release 3.2.215 unterstützt. Ab WLC Version 4.0.155.5 wird diese Funktionalität als Hybrid REAP (H-REAP) mit nur wenigen Erweiterungen bis 7.0.x.x bezeichnet. Ab Version 7.2.103 wird diese Funktion als FlexConnect bezeichnet.

Herkömmliche Cisco Lightweight Access Point Protocol (LWAPP)-basierte Access Points (APs),

auch LAPs genannt, wie die Access Points der Serien 1010, 1020 und 1100 und 1200, die die Cisco IOS® Software Version 12.3(7)JX oder höher ausführen, ermöglichen eine zentrale Verwaltung und Steuerung über die Cisco Wireless LAN Controller (WLCs). Diese LAPs ermöglichen es Administratoren außerdem, die Controller als einzelne Punkte der Wireless-Datenaggregation zu nutzen.

Diese LAPs ermöglichen es den Controllern, erweiterte Funktionen wie die QoS- und Zugriffskontrolllisten-Durchsetzung (ACLs) auszuführen. Die Anforderung, dass der Controller ein Eingangs- und Ausgangspunkt für den gesamten Wireless-Client-Datenverkehr sein muss, kann jedoch die Fähigkeit behindern, die Benutzeranforderungen angemessen zu erfüllen. In einigen Umgebungen, z. B. in Außenstellen, kann sich die Terminierung aller Benutzerdaten an Controllern als zu bandbreitenintensiv erweisen, insbesondere wenn über eine WAN-Verbindung ein begrenzter Durchsatz verfügbar ist. Wenn die Verbindungen zwischen LAPs und WLCs anfällig für Ausfälle sind, wie es auch bei WAN-Verbindungen mit Außenstellen der Fall ist, führt die Verwendung von LAPs, die WLCs für die Terminierung von Benutzerdaten verwenden, zu einer Unterbrechung der Wireless-Verbindungen während eines WAN-Ausfalls.

Stattdessen können Sie eine AP-Architektur verwenden, in der die traditionelle LWAPP-Kontrollebene verwendet wird, um Aufgaben wie dynamisches Konfigurationsmanagement, AP-Software-Upgrade und Wireless Intrusion Detection auszuführen. So können Wireless-Daten lokal bleiben und die Wireless-Infrastruktur zentral verwaltet und gegen WAN-Ausfälle geschützt werden.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

1030 REAP-Architektur - Einführung

Der Cisco REAP 1030 trennt die LWAPP-Kontrollebene von der Wireless-Datenebene, um Remote-Funktionen bereitzustellen. Cisco WLCs werden weiterhin für die zentrale Steuerung und Verwaltung wie reguläre LAPs verwendet. Der Unterschied besteht darin, dass alle Benutzerdaten lokal am Access Point überbrückt werden. Der Zugriff auf lokale Netzwerkressourcen wird bei WAN-Ausfällen aufrechterhalten. Abbildung 1 zeigt eine grundlegende REAP-Architektur.

Abbildung 1: Grundlegendes REAP-Architekturdiagramm

Hinweis: Eine Liste der grundlegenden Unterschiede bei der REAP-Funktionalität im Vergleich zu herkömmlichen LAPs finden Sie in Anhang A.

Wann sollten REAPs verwendet werden?

Der Cisco 1030 REAP AP sollte in erster Linie unter den folgenden beiden Bedingungen verwendet werden:

- Wenn die Verbindung zwischen LAP und WLC zu Ausfällen neigt, kann der REAP 1030 verwendet werden, um Wireless-Benutzern einen unterbrechungsfreien Datenzugriff bei Verbindungsausfällen zu ermöglichen.
- Wenn alle Benutzerdaten lokal terminiert werden müssen, d. h. am kabelgebundenen Port des Access Points (im Gegensatz zum Abschluss am Controller, wie es bei allen anderen LAPs der Fall ist), kann der REAP 1030 verwendet werden, um eine zentrale Steuerung über die Controller-Schnittstelle und/oder das Wireless Control System (WCS) zu ermöglichen. Dadurch können Daten lokal bleiben.

Wenn eine Abdeckung oder Benutzerdichte mehr als zwei oder drei 1030 REAPs an einem Standort erfordert, sollten Sie die Bereitstellung eines 2006- oder 2106-WLC in Betracht ziehen. Diese Controller können bis zu 6 LAPs aller Art unterstützen. Dies kann sich als finanziell tragfähiger erweisen und eine Reihe von Funktionen im Vergleich zu einer reinen REAP-Bereitstellung bieten.

Wie bei allen APs der Serie 1000 umfasst ein einzelner 1030 AP eine Fläche von ca. 5.000 Quadratmetern. Dies hängt von den Hochfrequenz-Verbreitungsmerkmalen an jedem Standort sowie von der erforderlichen Anzahl an Wireless-Benutzern und deren Durchsatzanforderungen ab. In den meisten gängigen Bereitstellungen kann ein einzelner Access Point der Serie 1000 12 Benutzer mit 512 Kbit/s auf 802.11b und 12 Benutzer gleichzeitig mit 2 Mbit/s auf 802.11a unterstützen. Wie bei allen 802.11-basierten Technologien wird auch der Medienzugriff freigegeben. Wenn also mehr Benutzer dem Wireless AP beitreten, wird der Durchsatz entsprechend gemeinsam genutzt. Wenn die Benutzerdichte zunimmt und/oder die Durchsatzanforderungen steigen, sollte ein lokaler WLC hinzugefügt werden, um Kosten pro Benutzer zu sparen und die Funktionalität zu erhöhen.

Hinweis: Sie können die 1030 REAPs so konfigurieren, dass sie identisch mit anderen LAPs funktionieren. Wenn WLCs hinzugefügt werden, um die Größe der WLAN-Infrastruktur von Remote-Standorten zu skalieren, können vorhandene REAP-Investitionen daher weiterhin genutzt werden.

REAP bereitstellen

Da der 1030 REAP so konzipiert ist, dass er an Remote-Standorten außerhalb der WLC-Infrastruktur platziert wird, werden die traditionellen, automatisierten LAPs zum Erkennen und Verbinden von Controllern (z. B. DHCP-Option 43) in der Regel nicht verwendet. Stattdessen muss die LAP zuerst aktiviert werden, damit die 1030 eine Verbindung zu einem WLC an einem

zentralen Standort herstellen kann.

Beim Priming werden LAPs eine Liste der WLCs zugewiesen, mit denen sie eine Verbindung herstellen können. Nach dem Beitritt zu einem einzigen WLC werden die LAPs über alle Controller in der Mobilitätsgruppe informiert und mit allen Informationen ausgestattet, die erforderlich sind, um einem Controller in der Gruppe beizutreten. Weitere Informationen zu Mobilitätsgruppen, Lastenausgleich und Controller-Redundanz finden Sie unter Bereitstellen der Cisco Wireless LAN-Controller der Serie 440X.

Um dies an einem zentralen Standort, z. B. einem Network Operations Center (NOC) oder einem Rechenzentrum, zu ermöglichen, müssen REAPs mit dem kabelgebundenen Netzwerk verbunden werden. So können sie einen einzigen WLC erkennen. Nach dem Verbinden mit einem Controller laden die LAPs die LAP-Betriebssystemversion herunter, die der WLAN-Infrastruktur entspricht. Anschließend werden die IP-Adressen aller WLCs in der Mobilitätsgruppe an die APs übertragen. So können die APs beim Einschalten an ihren Remote-Standorten den am wenigsten genutzten Controller aus ihren Listen erkennen und ihm beitreten, sofern eine IP-Verbindung verfügbar ist.

Hinweis: Die DHCP-Option 43 und die DNS-Suche (Domain Name System) arbeiten auch mit REAPs zusammen. Informationen zur Konfiguration von DHCP oder DNS an Remote-Standorten finden Sie unter Deploying Cisco Wireless LAN Controllers der Serie 440X, um APs die Suche nach zentralen Controllern zu ermöglichen.

Zu diesem Zeitpunkt kann der 1030 bei Bedarf statische Adressen zugewiesen werden. Dadurch wird sichergestellt, dass das IP-Adressierungsschema mit dem Ziel-Remote-Standort übereinstimmt. Außerdem können WLCs-Namen eingegeben werden, um festzulegen, welche drei Controller jede LAP anschließen möchte. Wenn diese drei Ausfälle auftreten, ermöglicht die automatische Lastverteilungsfunktion von LWAPP der LAP, den am wenigsten geladenen Access Point aus der Liste der Controller im Cluster auszuwählen. Die Bearbeitung der LAP-Konfiguration kann über die WLC-Kommandozeilenschnittstelle (CLI), die Benutzeroberfläche oder einfach über das WCS erfolgen.

Hinweis: Für den Betrieb im Layer-3-LWAPP-Modus benötigen 1030 REAPs die WLCs, mit denen sie verbunden sind. Das bedeutet, dass den Controllern IP-Adressen zugewiesen werden müssen. Außerdem benötigen die WLCs einen DHCP-Server, der an jedem Remote-Standort verfügbar ist, oder statische Adressen müssen während des Pricing-Prozesses zugewiesen werden. Die in den Controllern integrierte DHCP-Funktion kann nicht verwendet werden, um Adressen für LAPs von 1030 oder deren Benutzer bereitzustellen.

Bevor Sie die 1030 LAPs ausschalten, um an Remote-Standorten ausgeliefert zu werden, stellen Sie sicher, dass für jeden 1030 der REAP-Modus eingestellt ist. Dies ist sehr wichtig, da die Standardeinstellung für alle LAPs die Ausführung regulärer, lokaler Funktionen ist und 1030-Geräte für die Ausführung von REAP-Funktionen festgelegt werden müssen. Dies kann auf LAP-Ebene über die CLI oder GUI des Controllers oder durch WCS-Vorlagen erfolgen.

Grundlegende REAP-Priming-Funktionen

Wenn 1030 REAPs mit einem WLC innerhalb der Mobilitätsgruppe verbunden sind, mit dem REAPs verbunden sind, wenn sie an Remote-Standorten aufgestellt werden, können diese Informationen bereitgestellt werden:

Erforderliche REAP-Einstellungen

- Eine Liste der IP-Adressen für den WLC in der Mobilitätsgruppe (wird automatisch bei Controller-/AP-Verbindung bereitgestellt)
- REAP-Modus (APs müssen für den Betrieb im REAP-Modus konfiguriert werden, um REAP-Funktionen auszuführen)

Optionale REAP-Einstellungen

- Statisch zugewiesene IP-Adressen (optionale Einstellungseingabe pro AP)
- Primäre, sekundäre und tertiäre WLC-Namen (optionale Einstellungsanzeigen auf AP-Basis oder über WCS-Vorlagen)
- AP-Name (optionale informative Einstellungsanzeige auf AP-Basis)
- Informationen zum AP-Standort (optionale Information Setting Input pro AP oder über WCS-Vorlagen)

Verbindungsanforderungen für REAP-zu-Controller

Wenn Sie REAPs bereitstellen möchten, müssen Sie sich einige grundlegende Anforderungen merken. Diese Anforderungen betreffen die Geschwindigkeit und Latenz der WAN-Verbindungen. REAP-LWAPP-Kontrolldatenverkehr durchläuft. Die 1030-LAP ist für die Verwendung über WAN-Verbindungen wie IP Security Tunnel, Frame Relay, DSL (nicht PPPoE) und Mietleitungen vorgesehen.

Hinweis: Bei der REAP-LWAPP-Implementierung von 1030 wird von einem MTU-Pfad mit 1500 Byte zwischen dem Access Point und dem WLC ausgegangen. Jede Fragmentierung, die bei der Übertragung aufgrund einer MTU unter 1500 Byte stattfindet, führt zu unvorhersehbaren Ergebnissen. Daher ist die 1030 LAP nicht für Umgebungen wie PPPoE geeignet, in denen Router Pakete proaktiv auf weniger als 1500 Byte fragmentieren.

Die Latenz der WAN-Verbindungen ist besonders wichtig, da alle 1030 LAP standardmäßig Heartbeat-Nachrichten alle 30 Sekunden an Controller sendet. Wenn Heartbeat-Nachrichten verloren gehen, senden die LAPs einmal pro Sekunde fünf aufeinander folgende Heartbeats. Wenn keine erfolgreich ist, stellt die LAP fest, dass die Controller-Verbindung getrennt wird und die 1030er wieder in den eigenständigen REAP-Modus zurückkehren. Während die LAP 1030 große Latenzen zwischen sich selbst und dem WLC tolerieren kann, muss sichergestellt werden, dass die Latenz zwischen der LAP und dem Controller 100 ms nicht überschreitet. Dies liegt an clientseitigen Timern, die die Wartezeit der Clients einschränken, bevor die Timer feststellen, dass eine Authentifizierung fehlschlägt.

REAP-Einschränkungen

Obwohl der 1030-Access Point für die zentrale Verwaltung und Bereitstellung von WLAN-Services bei WAN-Verbindungsausfällen konzipiert wurde, gibt es einige Unterschiede zwischen den vom REAP angebotenen Diensten mit WLC-Anbindung und den Services, die er bereitstellen kann, wenn die Verbindung getrennt wird.

WLANs

Der REAP 1030 unterstützt zwar bis zu 16 WLANs (Wireless-Profile, die jeweils eine Service Set Identifier (SSID) sowie alle Sicherheits-, QoS- und anderen Richtlinien enthalten), jede mit einer

eigenen Multiple Basic Service Set ID (MBSSID). Der REAP 1030 kann jedoch nur das erste WLAN unterstützen, wenn die Verbindung mit einem Controller unterbrochen wird. In Zeiten eines WAN-Verbindungsausfalls werden alle WLANs außer den ersten außer Betrieb genommen. Daher sollte WLAN 1 als primäres WLAN vorgesehen werden, und die Sicherheitsrichtlinien sollten entsprechend geplant werden. Die Sicherheit in diesem ersten WLAN ist besonders wichtig, da bei einem Ausfall der WAN-Verbindung auch die Backend-RADIUS-Authentifizierung erforderlich ist. Der Grund hierfür ist, dass dieser Datenverkehr die LWAPP-Controllerebene passiert. Aus diesem Grund erhalten keine Benutzer Wireless-Zugriff.

Es wird empfohlen, für dieses erste WLAN eine lokale Authentifizierungs-/Verschlüsselungsmethode zu verwenden, z. B. den vorinstallierten Schlüsselbereich von Wi-Fi Protected Access (WPA-PSK). Wired Equivalent Privacy (WEP) ist ausreichend, wird jedoch wegen bekannter Sicherheitsschwachstellen nicht empfohlen.Wenn WPA-PSK (oder WEP) verwendet wird, können ordnungsgemäß konfigurierte Benutzer auch dann auf lokale Netzwerkressourcen zugreifen, wenn die WAN-Verbindung nicht verfügbar ist.

Hinweis: Alle RADIUS-basierten Sicherheitsmethoden erfordern, dass Authentifizierungsnachrichten über die LWAPP-Kontrollebene zurück an den zentralen Standort übertragen werden. Daher sind bei WAN-Ausfällen nicht alle RADIUS-basierten Services verfügbar. Dazu gehören u. a. die RADIUS-basierte MAC-Authentifizierung, 802.1X, WPA, WPA2 und 802.11i.

Der 1030 REAP kann sich nur in einem Subnetz befinden, da er kein 802.1q-VLAN-Tagging durchführen kann. Der Datenverkehr jeder SSID endet daher im gleichen Subnetz des kabelgebundenen Netzwerks. Das bedeutet, dass der Wireless-Datenverkehr zwischen den SSIDs zwar über die Luft segmentiert werden kann, der Benutzerdatenverkehr jedoch nicht auf der kabelgebundenen Seite getrennt wird.

Sicherheit

Der 1030 REAP kann alle Layer-2-Sicherheitsrichtlinien bereitstellen, die von der controllerbasierten WAN-Architektur von Cisco unterstützt werden. Dazu gehören alle Layer-2-Authentifizierungs- und Verschlüsselungstypen wie WEP, 802.1X, WPA, WPA2 und 802.11i. Wie bereits erwähnt, erfordern die meisten dieser Sicherheitsrichtlinien WLC-Verbindungen für die Backend-Authentifizierung. WEP und WPA-PSK sind auf AP-Ebene vollständig implementiert und erfordern keine RADIUS-Backend-Authentifizierung. Aus diesem Grund können Benutzer auch dann eine Verbindung herstellen, wenn die WAN-Verbindung unterbrochen ist. Die im Cisco WLC bereitgestellte Funktion für Client-Ausschlusslisten wird von der 1030 LAP unterstützt. MAC-Filterfunktionen auf dem 1030, wenn die Verbindung zurück zum Controller verfügbar ist.

Hinweis: Der REAP unterstützt WPA2-PSK nicht, wenn sich der Access Point im Standalone-Modus befindet.

Bei der LAP 1030 sind nicht alle Layer-3-Sicherheitsrichtlinien verfügbar. Zu diesen Sicherheitsrichtlinien gehören Webauthentifizierung, Controller-basierte VPN-Terminierung, ACLs und Peer-to-Peer-Blockierung, da sie am Controller implementiert werden. VPN-Passthrough funktioniert für Clients, die mit externen VPN-Konzentratoren verbunden sind. Die Controller-Funktion, die nur Datenverkehr zulässt, der für einen bestimmten VPN-Konzentrator bestimmt ist (nur VPN-Passthrough), ist jedoch nicht verfügbar.

Network Address Translation (NAT)

WLCs, mit denen REAPs verbunden sind, können sich nicht hinter NAT-Grenzen befinden. REAPs an Remote-Standorten können jedoch hinter einer NAT-Box sitzen, sofern die für LWAPP verwendeten Ports (UDP-Ports 1222 und 1223) an die 1030 weitergeleitet werden. Das bedeutet, dass jeder REAP über eine statische Adresse verfügen muss, damit die Port-Weiterleitung zuverlässig funktioniert, und dass sich hinter jeder NAT-Instanz nur ein einziger Access Point befinden kann. Der Grund hierfür ist, dass pro NAT-IP-Adresse nur eine Port Forwarding-Instanz vorhanden sein kann, d. h., dass nur eine LAP hinter jedem NAT-Service an Remote-Standorten arbeiten kann. One-to-One NAT kann mit mehreren REAPs verwendet werden, da die LWAPP-Ports für jede externe IP-Adresse an jede interne IP-Adresse (statische REAP-IP-Adresse) weitergeleitet werden können.

Quality of Service (QoS)

Die Paketpriorisierung basierend auf 802.1p-Prioritätsbits ist nicht verfügbar, da der REAP kein 802.1q-Tagging durchführen kann. Dies bedeutet, dass Wi-Fi Multimedia (WMM) und 802.11e nicht unterstützt werden. Paketpriorisierung basierend auf SSID und Identity Bases Networking wird unterstützt. Die VLAN-Zuweisung über identitätsbasierte Netzwerke funktioniert jedoch nicht mit dem REAP, da 802.1q-Tagging nicht ausgeführt werden kann.

Roaming und Client-Lastenausgleich

In Umgebungen, in denen mehr als ein einzelner REAP vorhanden ist und eine Mobilität zwischen den APs erwartet wird, muss jede LAP im gleichen Subnetz sein. Layer-3-Mobilität wird in der LAP 1030 nicht unterstützt. In der Regel ist dies keine Einschränkung, da Außenstellen in der Regel nicht über genügend LAPs verfügen, um eine solche Flexibilität zu erfordern.

Wenn Upstream-Controller-Verbindungen verfügbar sind, wird für alle REAPs an Standorten mit mehr als einem Access Point ein aggressiver Client-Lastenausgleich bereitgestellt (nur der Lastenausgleich ist auf dem Host-Controller aktiviert).

Radio Resource Management (RRM)

Wenn eine Verbindung zu Controllern besteht, erhalten 1030 LAPs eine dynamische Kanal- und Stromausgabe vom RRM-Mechanismus in WLCs. Wenn die WAN-Verbindung ausfällt, funktioniert das RRM nicht, und die Kanal- und Energieeinstellungen werden nicht geändert.

Erkennung nicht autorisierter APs und IDS-Funktionen

Die REAP-Architektur unterstützt alle Signaturen zur Erkennung von unautorisierten Zugriffen und zur Identifizierung von Sicherheitsrisiken (IDS), die mit denen regulärer LAPs übereinstimmen. Wenn jedoch die Verbindung mit einem zentralen Controller unterbrochen wird, werden alle erfassten Informationen nicht gemeinsam genutzt. Die Transparenz der RF-Domänen von Remote-Standorten geht daher verloren.

Zusammenfassung der REAP-Einschränkung

In der Tabelle in Anhang B sind die Funktionen des REAP während des normalen Betriebs und wenn keine WLC-Verbindung über die WAN-Verbindung verfügbar ist, zusammengefasst.

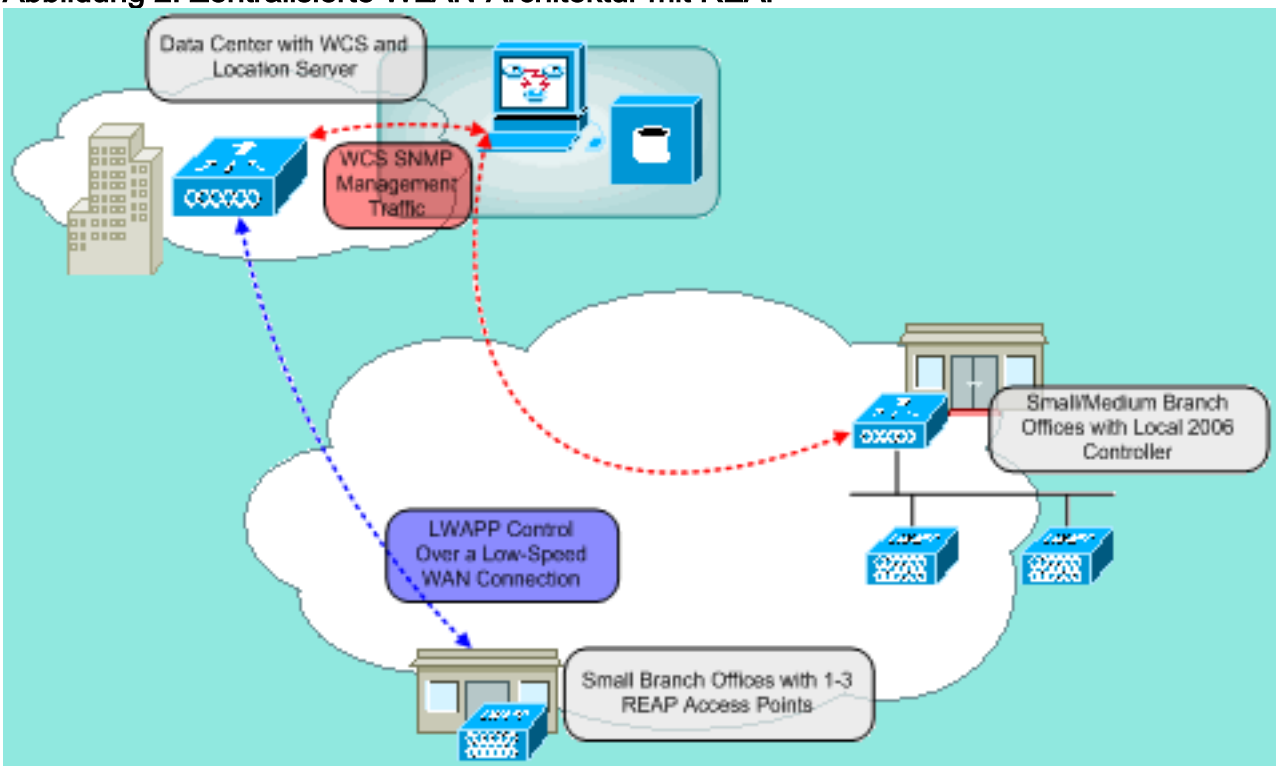
Verwaltung von REAP und zentraler WLAN-Architektur

Das 1030 REAP-Management unterscheidet sich nicht von dem regulärer LAPs und WLCs. Verwaltung und Konfiguration erfolgen auf Controller-Ebene, entweder über die CLI der einzelnen Controller oder über die Web-GUI. Die systemweite Konfiguration und Netzwerktransparenz erfolgt über das WCS, wo alle Controller und APs (REAP oder andere) als ein System verwaltet werden können. Wenn die REAP-Controller-Verbindung unterbrochen wird, werden auch die Verwaltungsfunktionen unterbrochen.

Zentralisierte WLAN-Architektur mit REAP

Abbildung 2 zeigt, wie die einzelnen Komponenten der zentralisierten LWAPP-Architektur zusammenarbeiten, um eine Vielzahl von Wireless-Netzwerkanforderungen zu erfüllen. Verwaltungs- und Standortdienste werden zentral über das WCS und die 2700 Location Appliance bereitgestellt.

Abbildung 2: Zentralisierte WLAN-Architektur mit REAP



Anhang A

Worin bestehen die Hauptunterschiede zwischen der REAP-Architektur und regulären LAPs?

- Wenn die DHCP-Option 43 oder die DNS-Auflösung an Remote-Standorten nicht verfügbar ist, muss der 1030 zuerst in der Zentrale gepriesen werden. Anschließend wird es an den Zielstandort ausgeliefert.
- Bei einem Ausfall der WAN-Verbindung bleibt nur das erste WLAN aktiv.Sicherheitsrichtlinien, die RADIUS erfordern, schlagen fehl.Für WLAN 1 wird die Authentifizierung/Verschlüsselung mit WPA-PSK empfohlen. WEP funktioniert, wird jedoch nicht empfohlen.
- Keine Layer-3-Verschlüsselung (nur Layer-2-Verschlüsselung)
- WLCs, mit denen REAPs verbunden sind, können sich nicht hinter NAT-Grenzen befinden. REAPs können jedoch mit der Maßgabe, dass jede interne statische REAP-IP-Adresse beide LWAPP-Ports (1222 und 1223) an sie weitergeleitet hat.**Hinweis:** Port Address Translation

(PAT)/NAT mit Überladung wird nicht unterstützt, da sich der Quellport des von der LAP stammenden LWAPP-Datenverkehrs mit der Zeit ändern kann. Dadurch wird die LWAPP-Zuordnung unterbrochen. Das gleiche Problem kann auch bei NAT-Implementierungen für REAP auftreten, wenn sich die Port-Adresse ändert, z. B. PIX/ASA, was von der Konfiguration abhängt.

- Nur LWAPP-Kontrollnachrichten durchlaufen die WAN-Verbindung.
- Der Datenverkehr wird am Ethernet-Port des 1030 überbrückt.
- Die LAP 1030 führt keine 802.1Q-Tagging (VLANs) durch. Aus diesem Grund endet der Wireless-Datenverkehr aller SSIDs im selben kabelgebundenen Subnetz.

Anhang B

Worin bestehen die Funktionsunterschiede zwischen dem normalen und dem eigenständigen REAP-Modus?

		REAP (Normalmodus)	REAP (Standalone-Modus)
Protokolle	IPv4	Ja	Ja
	IPv6	Ja	Ja
	Alle anderen Protokolle	Ja (nur wenn der Client auch IP aktiviert ist)	Ja (nur wenn der Client auch IP aktiviert ist)
	IP-Proxy-ARP	Nein	Nein
WLAN	Anzahl der SSIDs	16	1 (der erste)
	Dynamische Kanalzuweisung	Ja	Nein
	Dynamische Stromüberwachung	Ja	Nein
	Dynamischer Lastenausgleich	Ja	Nein
VLAN	Mehrere Schnittstellen	Nein	Nein
	802.1Q-Unterstützung	Nein	Nein
WLAN-Sicherheit	Erkennung nicht autorisierter APs	Ja	Nein
	Ausschlussli	Ja	Ja (nur

	ste		vorhandene Mitglieder)
	Peer-to-Peer-Blockierung	Nein	Nein
	Intrusion Detection System	Ja	Nein
Layer-2-Sicherheit	MAC-Authentifizierung	Ja	Nein
	802.1x	Ja	Nein
	WEP (64/128/152 Bit)	Ja	Ja
	WPA-PSK	Ja	Ja
	WPA2-PSK	Ja	Nein
	WPA-EAP	Ja	Nein
	WPA2-EAP	Ja	Nein
Layer-3-Sicherheit	Webauthentifizierung	Nein	Nein
	IPsec	Nein	Nein
	L2TP	Nein	Nein
	VPN-Passthrough	Nein	Nein
	Zugriffskontrolllisten	Nein	Nein
QoS	QoS-Profile	Ja	Ja
	Downlink-QoS (gewichtete Round-Robin-Warteschlangen)	Ja	Ja
	802.1p-Unterstützung	Nein	Nein
	Verträge mit benutzerspezifischer Bandbreite	Nein	Nein
	WMM	Nein	Nein
	802.11e (künftig)	Nein	Nein
	Überschreiben des AAA-QoS-Profils	Ja	Nein

Mobilität	Intra-Subnetz	Ja	Ja
	Inter-Subnetz	Nein	Nein
DHCP	Interner DHCP-Server	Nein	Nein
	Externer DHCP-Server	Ja	Ja
Topologie	Direkte Verbindung (2006)	Nein	Nein

Zugehörige Informationen

- Remote-Edge AP (REAP) mit einfachen APs und WLCs (Wireless LAN Controller) - Konfigurationsbeispiel
- AP-Lastenausgleich und AP-Fallback in Unified Wireless Networks
- Bereitstellung der Cisco Wireless LAN Controller der Serie 440X
- Grundlegende Konfigurationsbeispiel für Wireless LAN Controller und Lightweight Access Point
- Technischer Support und Dokumentation - Cisco Systems