Guide de déploiement des points d'accès REAP au niveau de la filiale

Contenu

Introduction

Ce document fournit les informations qui doivent être prises en compte quand vous déployez le Point d'accès de Distant-périphérie (REAP). Référez-vous au point d'accès Remote-Edge (REAP) avec des aps légers et à l'exemple Sans fil de configuration de contrôleurs LAN (WLCs) pour les informations de configuration de base REAP.

Remarque: La caractéristique REAP est prise en charge jusqu'à la version 3.2.215 WLC. De la release 4.0.155.5 WLC, cette fonctionnalité s'appelle Hybrid REAP (H-REAP) avec peu d'améliorations jusqu'à 7.0.x.x. De la release 7.2.103, cette caractéristique s'appelle FlexConnect.

Les Points d'accès basés sur traditionnels de Protocol de point d'accès léger de Cisco (LWAPP)

(aps), (également connus sous le nom de recouvrements), comme les 1010, 1020, et les gammes 1100 et 1200 aps qui exécutent la version de logiciel 12.3(7)JX ou ultérieures de Cisco IOS®, tiennent compte de la Gestion et du contrôle centraux par les contrôleurs LAN Sans fil de Cisco (WLCs). En outre, ces recouvrements permettent à des administrateurs pour accroître les contrôleurs comme seuls points d'agrégation Sans fil de données.

Tandis que ces recouvrements permettent à des contrôleurs pour exécuter la fonctionnalité avancée telle que QoS et application de liste de contrôle d'accès (ACL), la condition requise du contrôleur d'être un seul point d'entrée et de sortie pour tout le trafic de client sans fil peut gêner, plutôt que l'enable, la capacité de répondre convenablement aux besoins de l'utilisateur. Dans quelques environnements, tels que les bureaux distants, l'arrêt de toutes les données d'utilisateur aux contrôleurs peut prouver trop la bande passante intensive, particulièrement quand le débit limité est disponible au-dessus d'un lien WAN. En outre, où les liens entre les recouvrements et le WLCs sont à panne encline, de nouveau le terrain communal avec des liens WAN aux bureaux distants, l'utilisation des recouvrements qui se fondent sur WLCs pour l'arrêt de données d'utilisateur mène à la connexion sans fil divisée pendant des périodes de cas de panne du WAN.

Au lieu de cela, vous pouvez utiliser une architecture AP où l'avion traditionnel de contrôle LWAPP est accru afin d'effectuer des tâches, telles que la Gestion de configuration dynamique, mise à niveau de logiciel AP, et la détection Sans fil d'intrusion. Ceci permet aux données Sans fil pour rester local, et à l'infrastructure Sans fil pour être centralement géré et résilient au cas de panne du WAN.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Introduction d'architecture de 1030 REAP

Cisco 1030 REAP sépare l'avion de contrôle LWAPP du plan de données Sans fil afin de fournir la fonctionnalité distante. Des Cisco WLC sont encore utilisés pour le contrôle centralisé et la Gestion de la même manière que des recouvrements de militaire de carrière. La différence est que toutes les données d'utilisateur pont localement à AP. Access aux ressources en réseau local est mis à jour tout au long des cas de panne du WAN. La figure 1 montre une architecture de base REAP.

Figure 1 : Diagramme architectural de base REAP

Remarque: Voir l'annexe A pour une liste de différences de base dans la fonctionnalité REAP par rapport aux recouvrements traditionnels.

Quand REAP aps devrait-il être utilisé ?

Cisco 1030 REAP AP devrait être utilisé principalement dans ces deux conditions :

- Si le lien entre le RECOUVREMENT et le WLC est à panne encline, les 1030 REAP peuvent être utilisés pour permettre à des utilisateurs de sans fil l'accès aux données ininterrompu pendant la panne de lien.
- Si toutes les données d'utilisateur doivent être terminées localement, qui signifient au port de câble d'AP (par opposition à l'terminaison au contrôleur, car les données sont pour tous autres recouvrements), les 1030 REAP peuvent être utilisés pour tenir compte du contrôle central par l'intermédiaire de l'interface de contrôleur et/ou du système de contrôle sans fil (WCS). Ceci permet à des données pour rester local.

Là où la couverture ou la densité d'utilisateur exige plus de deux ou trois 1030 REAP aps à un site unique, considérez le déploiement des 2006 ou 2106 WLC. Ces contrôleurs peuvent prendre en charge jusqu'à 6 recouvrements de n'importe quel type. Ceci peut prouver plus financièrement viable, et fournit une version élaborée des fonctionnalités et caractéristiques par rapport à un déploiement réservé à la REAP.

Comme avec toute la gamme 1000 aps, 1030 couvertures simples AP approximativement 5,000 pieds carrés. Ceci dépend des caractéristiques de propagation de Radiofréquence (RF) à chaque site, et du nombre exigé d'utilisateurs de sans fil et de leurs besoins de débit. Dans la plupart des déploiements communs, une seule gamme 1000 AP peut prendre en charge 12 utilisateurs à 512kbps sur 802.11b et 12 utilisateurs à 2 mbps sur 802.11a, simultanément. Comme avec toutes les Technologies 802.11-based, l'accès au support est partagé. Par conséquent, quand plus d'utilisateurs joignent le point d'accès sans fil, le débit est partagé en conséquence. De nouveau, à mesure que la densité d'utilisateur augmente et/ou des conditions requises de débit montent, considérez l'ajout des gens du pays WLC pour sauvegarder sur le coût-par-utilisateur et pour augmenter la fonctionnalité.

Remarque: Vous pouvez configurer les 1030 REAP pour opérer identiquement à d'autres recouvrements. Par conséquent, quand WLCs sont ajoutés pour mesurer la taille des infrastructures WLAN des sites distants, des investissements existants REAP peuvent continuer à être accrus.

Déployez le REAP

Puisque les 1030 REAP est conçus pour être placés aux sites distants à partir de l'infrastructure WLC, les recouvrements traditionnels, de zéro-toucher de méthodes utilisés pour découvrir et joindre des contrôleurs (tels qu'option 43 DHCP) ne sont pas habituellement utilisés. Au lieu de cela, le RECOUVREMENT doit d'abord s'amorcer afin de permettre aux 1030 pour se connecter à un WLC de retour à un lieu d'exploitation principal.

L'amorçage est un processus où des recouvrements sont indiqués une liste de WLCs à laquelle ils peuvent se connecter. Une fois joint à un WLC simple, les recouvrements sont au courant de tous les contrôleurs au groupe de mobilité et équipés de toutes les informations requises pour joindre n'importe quel contrôleur dans le groupe. Référez-vous à déployer les contrôleurs LAN Sans fil de gamme de Cisco 440X pour plus d'informations sur des Groupes de mobilité, l'Équilibrage de charge, et la Redondance de contrôleur.

Afin d'exécuter ceci au lieu d'exploitation principal, tel qu'un Network Operations Center (centre d'exploitation du réseau) ou le centre de traitement des données, des REAP doit être connecté au réseau câblé. Ceci leur permet pour découvrir un WLC simple. Une fois joint à un contrôleur, les recouvrements téléchargent la version de système d'exploitation de RECOUVREMENT qui correspond à l'infrastructure WLAN. Puis, les adresses IP de tout le WLCs au groupe de mobilité sont transférées vers les aps. Ceci permet les aps, une fois mis sous tension à leurs sites distants, pour découvrir et joindre le moins contrôleur utilisé de leurs listes, si la connectivité IP est disponible.

Remarque: Option 43 DHCP et travail de consultation de Système de noms de domaine (DNS) avec des REAP, aussi bien. Référez-vous à déployer les contrôleurs LAN Sans fil de gamme de Cisco 440X pour les informations sur la façon dont configurer le DHCP ou les DN aux sites distants afin de permettre à des aps pour trouver les unités centrales de traitement.

Àce moment, les 1030 peuvent être donnés des adresses statiques si désirés. Ceci s'assure que le schéma d'adressage IP apparie le site distant de destination. En outre, des noms de WLCs peuvent être entrés afin de détailler que trois contrôleurs chaque RECOUVREMENT tenteront de connecter. Si l'échouer ces trois, la fonctionnalité automatique d'Équilibrage de charge de LWAPP laisse le RECOUVREMENT pour choisir AP moins-chargé de la liste restante de contrôleurs dans la batterie. L'éditer de la configuration de RECOUVREMENT peut être fait par l'interface de ligne de commande WLC (CLI) ou le GUI, ou avec la grande simplicité, par le WCS.

Remarque: 1030 REAP exigent le WLCs auquel ils se connectent pour fonctionner en mode de la couche 3 LWAPP. Ceci signifie que les contrôleurs doivent être donnés des adresses IP. En outre, le WLCs exigent d'un serveur DHCP d'être disponible à chaque site distant, ou des adresses statiques doivent être assignées pendant le procédé d'amorçage. La fonctionnalité DHCP incluse dans des contrôleurs ne peut pas être utilisée pour fournir des adresses aux recouvrements 1030s ou à leurs utilisateurs.

Avant que vous mettiez hors tension les 1030 recouvrements pour se transporter aux sites distants, assurez-vous que chaque 1030 est placés au mode REAP. C'est très important parce que tout le par défaut pour enroule est d'exécuter le militaire de carrière, la fonctionnalité locale, et le besoin 1030s d'être placé pour exécuter la fonctionnalité REAP. Ceci peut être fait au niveau de RECOUVREMENT par le contrôleur CLI ou GUI, ou avec la grande simplicité, par des modèles WCS.

Fonctions de base d'amorçage REAP

Après 1030 des REAP sont connectés à un WLC au sein du groupe de mobilité à où les REAP se connectent une fois placés aux sites distants, ces informations peuvent être fournis :

Configurations requises REAP

- Une liste d'adresses IP pour le WLC au groupe de mobilité (fourni automatiquement sur la connexion controller/AP)

- Mode REAP AP (des aps doivent être configurés pour fonctionner dans le mode REAP afin d'exécuter la fonctionnalité REAP)

Configurations facultatives REAP

- Adresses IP statiquement assignées (un paramètre facultatif entré sur une base par-AP)
- Noms primaire, secondaire, et tertiaire WLC (un paramètre facultatif entré sur une base par-AP ou par l'intermédiaire des modèles WCS)
- Nom AP (une configuration informationnelle facultative entrée sur une base par-AP)
- L'information d'emplacement AP (une configuration informationnelle facultative entrée sur une base par-AP ou par l'intermédiaire des modèles WCS)

Conditions requises de lien de REAP-à-contrôleur

Quand vous prévoyez de déployer des REAP, quelques exigences de base doivent être retrouvées. Ces conditions requises concernent la vitesse et la latence du trafic de contrôle des liens WAN REAP LWAPP traversera. Les 1030 RECOUVREMENTS sont destinés pour être utilisés à travers des liens WAN, tels que le tunnel de sécurité IP, le Relais de trames, le DSL (non PPPoE) et les lignes louées.

Remarque: 1030 l'implémentation REAP LWAPP assume un chemin de MTU de 1500 octets entre AP et le WLC. N'importe quelle fragmentation qui a lieu en transit en raison d'un MTU de l'octet sub-1500 mène aux résultats imprévisibles. Par conséquent, les 1030 RECOUVREMENTS pas approprié aux environnements, tels que le PPPoE, où les Routeurs fragmentent proactivement des paquets aux octets sub-1500.

La latence de lien WAN est particulièrement importante parce que tout les 1030 RECOUVREMENTS envoient, par défaut, des messages de pulsation de nouveau aux contrôleurs toutes les 30 secondes. Après que des messages de pulsation soient perdus, les recouvrements envoient 5 pulsations successives, une fois chaque seconde. Si aucun n'est réussi, le RECOUVREMENT détermine que la Connectivité de contrôleur est divisée et les 1030s retournent au mode REAP autonome. Tandis que les 1030 RECOUVREMENTS peuvent tolérer de grandes latences entre se et le WLC, il est nécessaire de s'assurer que la latence ne dépasse pas 100ms entre le RECOUVREMENT et le contrôleur. C'est dû aux temporisateurs de côté client qui limitent la durée de clients attendent avant que les temporisateurs déterminent une authentification ait manqué.

Limites REAP

Bien que les 1030 AP soit conçus pour être gérés centralement et pour fournir le service WLAN pendant les pannes de lien WAN, il y a quelques différences entre quels services le REAP offre avec la Connectivité WLC et ce qu'il peut fournir quand la Connectivité est divisée.

WLAN

Tandis que les 1030 REAP peuvent prendre en charge jusqu'à 16 WLAN (profils Sans fil qui contiennent un identifiant d'ensemble de services [SSID] chacun, avec toute la Sécurité, QoS, et d'autres stratégies), chacun avec son propre plusieurs ID d'ensemble des services de base (MBSSID), les 1030 REAP peut seulement prendre en charge le premier WLAN quand la

Connectivité avec un contrôleur est interrompue. Pendant des périodes de panne de lien WAN, tous les WLAN excepté le premier sont désarmés. Par conséquent, WLAN 1 devrait être destiné comme WLAN et stratégies de sécurité primaires devrait être prévu en conséquence. La Sécurité sur ce premier WLAN est particulièrement importante parce que si le lien WAN échoue, ainsi fait l'authentification principale de RAYON. C'est parce qu'un tel trafic traverse l'avion de contrôleur LWAPP. Par conséquent, on n'accorde aucun utilisateur l'accès Sans fil.

L'il est recommandé que une méthode d'authentification locale/cryptage, telle que la partie principale pré-partagée d'accès protégé par Wi-Fi (WPA-PSK), soit utilisé sur ce premier WLAN. Le Confidentialité équivalente aux transmissions par fil (WEP) suffit, mais n'est pas recommandé en raison des failles de la sécurité connues. Quand le WPA-PSK (ou le WEP) est utilisé, les utilisateurs correctement configurés peuvent encore accéder aux ressources en réseau local même si le lien WAN est en baisse.

Remarque: Toutes les méthodes basées sur rayon de Sécurité exigent des messages d'authentification d'être transmis à travers l'avion de contrôle LWAPP de nouveau au lieu d'exploitation principal. Par conséquent, tous les services basés sur rayon sont indisponibles pendant les cas de panne du WAN. Ceci inclut, mais n'est pas limité à, authentification MAC basée sur rayon, 802.1X, WPA, WPA2, et 802.11i.

Les 1030 REAP peuvent seulement résider sur un sous-réseau unique parce qu'il ne peut pas exécuter l'étiquetage du 802.1Q VLAN. Par conséquent, le trafic sur chaque SSID se termine sur le même sous-réseau sur le réseau câblé. Ceci signifie que tandis que le trafic Sans fil pourrait être segmenté au-dessus de l'air entre le SSID, le trafic d'utilisateur n'est pas séparé du côté de câble.

Sécurité

Les 1030 REAP peuvent fournir toutes les stratégies de sécurité de la couche 2 prises en charge par l'architecture BLÊME basée sur contrôleur de Cisco. Ceci inclut toute l'authentification de la couche 2 et les cryptages tape, comme le WEP, le 802.1X, le WPA, le WPA2, et le 802.11i. Comme indiqué précédemment, la plupart de ces stratégies de sécurité exigent la Connectivité WLC pour l'authentification principale. Le WEP et le WPA-PSK sont entièrement mis en application au niveau du AP et n'exigent pas l'authentification principale de RAYON. Par conséquent, même si le lien WAN est en baisse, les utilisateurs peuvent encore se connecter. La fonctionnalité offerte de liste d'exclusion de client à Cisco WLCis pris en charge avec les 1030 RECOUVREMENTS. Le filtrage MAC fonctionne sur les 1030 si la Connectivité de nouveau au contrôleur est disponible.

Remarque: Le REAP ne prend en charge pas WPA2-PSK quand AP est en mode autonome.

Toutes les stratégies de sécurité de la couche 3 ne sont pas disponibles avec les 1030 RECOUVREMENTS. Ces stratégies de sécurité incluent l'authentification Web, l'arrêt basé sur contrôleur VPN, l'ACLs, et le blocage peer-to-peer, parce qu'elles sont mises en application au contrôleur. L'intercommunication VPN fonctionne pour les clients qui se connectent aux concentrateurs externes VPN. Cependant, la caractéristique de contrôleur qui permet seulement le trafic destiné pour un concentrateur spécifié VPN (intercommunication VPN seulement) ne fait pas.

Traduction d'adresses réseau (NAT)

WLCs auquel les REAP se connectent ne peut pas résider derrière des bornes NAT. Cependant,

les REAP aux sites de distants peuvent se reposer derrière une case NAT, si les ports utilisés pour LWAPP (ports UDP 12222 et 12223) sont expédiés au 1030s. Ceci signifie que chaque REAP doit avoir une adresse statique pour que la transmission du port fonctionne sûrement, et que seulement AP simple peut résider derrière chaque exemple NAT. La raison pour ceci est que seulement une instance de transfert de port unique peut exister par adresse IP NAT, qui signifie que seulement un RECOUVREMENT peut fonctionner derrière chaque service NAT aux sites distants. NAT linéaire peut fonctionner avec le multiple REAP parce que les ports LWAPP peuvent être expédiés pour chaque adresse IP externe à chaque adresse IP interne (adresse IP statique REAP).

Qualité de service (QoS)

La hiérarchisation de paquet basée sur des bits de la priorité 802.1p n'est pas disponible parce que le REAP ne peut pas exécuter l'étiquetage de 802.1Q. Ceci signifie que le Wi-Fi Multimedia (WMM) et 802.11e ne sont pas pris en charge. La hiérarchisation de paquet basée sur le SSID et le réseau de bases d'identité sont pris en charge. Cependant, l'affectation VLAN par l'intermédiaire du réseau basé sur identité ne fonctionne pas avec le REAP parce qu'elle ne peut pas exécuter l'étiquetage de 802.1Q.

Itinérance et Équilibrage de charge de client

Dans les environnements où plus qu'un REAP simple est présent et où la mobilité inter-AP est prévue, chaque RECOUVREMENT doit être sur le même sous-réseau. La mobilité de la couche 3 n'est pas prise en charge dans les 1030 RECOUVREMENTS. Typiquement, ce n'est pas une limite parce que les bureaux distants habituellement n'utilisent pas assez de recouvrements pour rendre nécessaire une telle flexibilité.

L'Équilibrage de charge agressif de client est équipé à travers tous les REAP dans les sites de plus qu'AP simple quand la Connectivité en amont de contrôleur est disponible (est seulement l'Équilibrage de charge est activé sur le contrôleur d'hôte).

Gestion des ressources radio (RRM)

Quand la Connectivité aux contrôleurs est présente, 1030 recouvrements reçoivent le canal et la puissance de sortie dynamiques du mécanisme RRM dans WLCs. Quand le lien WAN est en baisse, RRM ne fonctionne pas, et creuse des rigoles et des paramètres d'alimentation ne sont pas modifiés.

Détection escroc et fonctionnalité d'ID

L'architecture REAP prend en charge toute la signature escroc de détection et de détection d'intrusion (ID) qui apparie cela des recouvrements réguliers. Cependant, quand la Connectivité est perdue avec une unité centrale de traitement, toutes les informations recueillies ne sont pas partagées. Par conséquent, la visibilité dans les domaines rf des sites distants est perdue.

Résumé limite REAP

La table dans l'annexe B récapitule les capacités du REAP pendant le fonctionnement normal et quand la connexion au WLC à travers le lien WAN n'est pas disponible.

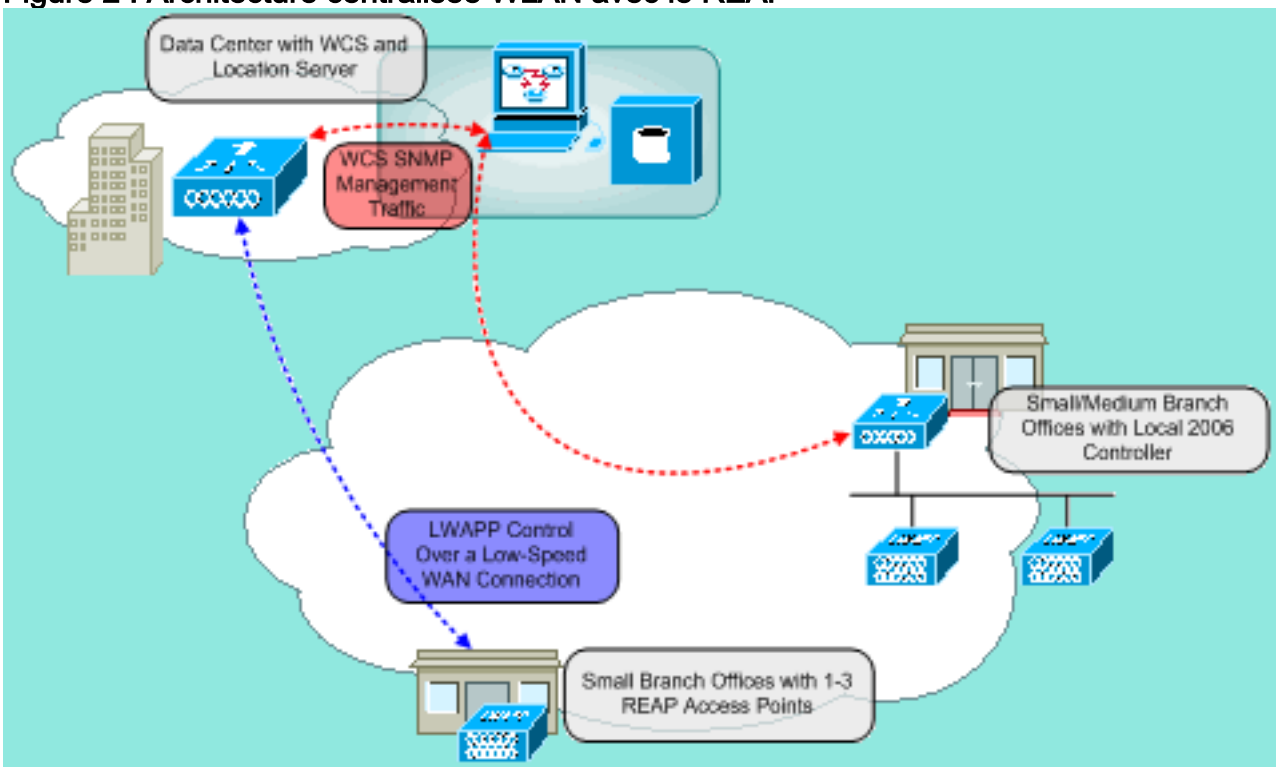
Gérez le REAP et l'architecture centrale WLAN

La Gestion de 1030 REAP n'est pas différente que celle des recouvrements réguliers et du WLCs. La Gestion et la configuration est tout faite au niveau du contrôleur, par le CLI de chaque contrôleur ou GUI de Web. Au niveau système la configuration et la visibilité de réseau est fournie par le WCS, où tous les contrôleurs et aps (REAP ou autrement) peuvent être gérés comme système unique. Quand la Connectivité de REAP-contrôleur est perturbée, des capacités de Gestion sont également perturbées.

Architecture centralisée WLAN avec le REAP

La figure 2 affiche comment chaque partie de l'architecture centralisée LWAPP fonctionne ensemble afin de répondre à un grand choix de besoins de réseau sans fil. Des services de Gestion et d'emplacement sont fournis centralement par le WCS et l'appliance de 2700 emplacements.

Figure 2 : Architecture centralisée WLAN avec le REAP



Annexe A

Quelles sont les différences principales entre l'architecture REAP et les recouvrements de militaire de carrière ?

- Si l'option 43 DHCP ou la résolution de DN n'est pas disponible aux sites distants, les 1030 doivent d'abord s'amorcer au bureau central. Puis, il est expédié au site de destination.
- Sur la panne de lien WAN, seulement le premier WLAN reste actif.Les stratégies de sécurité qui exigent le RAYON échoueront.L'authentification/cryptage qui utilise le WPA-PSK est recommandée pour des travaux WLAN 1. WEP, mais n'est pas recommandée.
- Aucun cryptage de la couche 3 (cryptage de couche 2 seulement)
- WLCs que les REAP connectent ne peut pas résider derrière des bornes NAT. Cependant,

les REAP mettent en boîte, si chaque adresse IP interne de la charge statique REAP a les deux ports LWAPP (12222 et 12223) expédiés à eux.**Remarque:** Adresse du port translation d'adresses) (de PAT/NAT avec la surcharge n'est pas pris en charge parce que le port de source du trafic LWAPP qui provient du RECOUVREMENT peut changer au fil du temps. Ceci casse l'association LWAPP. Le même problème peut surgir avec des réalisations NAT pour le REAP où l'adresse du port change, comme PIX/ASA pourrait, qui dépend de la configuration.

- Seulement les messages de contrôle LWAPP traversent le lien WAN.
- Le trafic de données pont au port Ethernet des 1030.
- Les 1030 RECOUVREMENTS n'exécutent pas l'étiquetage de 802.1Q (des VLAN). Par conséquent, le trafic Sans fil de tout le SSID se termine sur le même sous-réseau de câble.

Annexe B

Quelles sont les différences dans la fonctionnalité entre les modes REAP normaux et autonomes ?

		REAP (mode normal)	REAP (mode autonome)
Protocoles	Ipv4	Oui	Oui
	IPv6	Oui	Oui
	Tous autres protocoles	Oui (seulement si le client est également l'IP activé)	Oui (seulement si le client est également l'IP activé)
	Proxy ARP IP	Non	Non
WLAN	Nombre de SSID	16	1 (le premier)
	Affectation dynamique de canal	Oui	Non
	Contrôle d'alimentation dynamique	Oui	Non
	Équilibrage de charge dynamique	Oui	Non
VLAN	Plusieurs interfaces	Non	Non
	support de	Non	Non

	802.1Q		
Sécurité WLAN	Détection escroc AP	Oui	Non
	Liste d'exclusion	Oui	Oui (membres existants seulement)
	Blocage peer-to-peer	Non	Non
	Système de détection d'intrusion	Oui	Non
Degré de sécurité de la couche 2	Authentification MAC	Oui	Non
	802.1X	Oui	Non
	WEP (64/128/152bits)	Oui	Oui
	WPA-PSK	Oui	Oui
	WPA2-PSK	Oui	Non
	WPA-EAP	Oui	Non
	WPA2-EAP	Oui	Non
Degré de sécurité de la couche 3	Authentification Web	Non	Non
	IPsec	Non	Non
	L2TP	Non	Non
	Intercommunication VPN	Non	Non
	Listes de contrôle d'accès	Non	Non
QoS	Profils de QoS	Oui	Oui
	Liaison descendante QoS (files	Oui	Oui

	d'attente circulaires pesées)		
	support 802.1p	Non	Non
	contrats de bande passante de Par-utilisateur	Non	Non
	WMM	Non	Non
	802.11e (futur)	Non	Non
	Dépassement de profil de QoS d'AAA	Oui	Non
Mobilité	Intra-sous-réseau	Oui	Oui
	Inter-sous-réseau	Non	Non
DHCP	Serveur DHCP interne	Non	Non
	Serveur DHCP externe	Oui	Oui
Topologie	Lié directement (2006)	Non	Non

Informations connexes

- Exemple de configuration d'un point d'accès Remote-Edge (REAP) avec des points d'accès légers et des contrôleurs de réseau local sans fil
- Équilibrage de charge et mode secours des points d'accès dans les réseaux sans fil unifiés
- Déployer les Contrôleurs de LAN sans fil de la gamme Cisco 440X
- Exemple de configuration de base d'un contrôleur LAN sans fil et d'un point d'accès léger
- Support et documentation techniques - Cisco Systems