Roaming WGB: Dettagli interni e configurazione

Sommario

Introduzione

Cisco Workgroup Bridge (WGB) è uno strumento molto utile per la progettazione e l'installazione di una rete wireless perché consente la mobilità dei dispositivi non wireless. WGB fornisce molti dettagli su roaming, accesso di sicurezza, ecc, che influiscono sugli scenari di distribuzione a seconda delle esigenze.

Nelle versioni 12.4(25d)JA e successive, Cisco ha introdotto una serie di comandi e modifiche per ottimizzare l'uso di WGB in ambienti di roaming ad alta velocità.

In questo documento vengono illustrati diversi aspetti del funzionamento di un WGB, inclusi i punti decisionali degli algoritmi di roaming, e viene spiegato come configurarlo per il modello di utilizzo previsto.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Soluzione Cisco Wireless LAN
- Cisco Workgroup Bridge

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Che cos'è un bridge per gruppi di lavoro?

Un WGB è fondamentalmente un punto di accesso (AP) configurato per operare come client wireless verso un'infrastruttura e per fornire connettività di layer 2 ai dispositivi connessi alla relativa interfaccia Ethernet.

Una distribuzione WGB tipica include i seguenti componenti:

- dispositivo WGB, in genere dotato di almeno un'interfaccia radio e un'interfaccia Ethernet
- Un'infrastruttura wireless, generalmente denominata root AP, che può essere autonoma o unificata.
- Uno o più dispositivi client cablati collegati al WGB. Questo documento non copre scenari con ruoli misti (una radio come WGB, una radio come root sullo stesso access point).

Esistono tre tipi principali di WGB:

- **WGB Cisco**: Cisco WGB è un qualsiasi access point basato su Cisco IOS® configurato come WGB (1130, 1240, 1250, ecc.). Questa modalità utilizza il protocollo IAPP per informare l'infrastruttura di rete dei dispositivi che il WGB ha appreso sulla propria interfaccia Ethernet. In questo caso, il controller WLC (Wireless LAN Controller) o l'access point principale ha la visibilità di layer 2 dei dispositivi "sporgenti" dal WGB.
- **WGB non Cisco:** Si tratta di un dispositivo di terze parti che funge da WGB e connette uno o

più dispositivi cablati all'infrastruttura wireless. Questi non supportano IAPP e consentono solo un singolo dispositivo cablato o forniscono un meccanismo di conversione degli indirizzi MAC, nascondendo tutti i client cablati dietro un singolo indirizzo MAC 802.11. Questi tipi di dispositivi richiedono una gestione speciale sui frame ARP (Address Resolution Protocol) e DHCP se l'infrastruttura è un WLC, a causa dei controlli di sicurezza e della gestione dei frame eseguiti sui controller.
- **Cisco AP configurato come "Universal WGB"**: Questa modalità sopprime il meccanismo IAPP, quindi il WGB può essere utilizzato per un'infrastruttura Cisco o per access point radice di terze parti. In questo caso, il WGB assume l'indirizzo del proprio client Ethernet, limitando a uno il numero di dispositivi dietro di esso.

La sezione successiva tratta dello scenario di un WGB Cisco utilizzato per un'infrastruttura autonoma o WLC.

Scenari di utilizzo

Esempi di utilizzo tipici di WGB includono:

- Collegamento di una stampante cablata alla rete
- Distribuzioni di produzione diverse, in cui non è possibile o pratico utilizzare un cavo per il dispositivo cablato
- Installazioni all'interno di veicoli, in cui il WGB fornisce connettività da un'auto, metropolitana, ecc, a una rete wireless esterna
- Telecamere cablate

Ciascun esempio presenta i propri requisiti in termini di:

- Larghezza di banda necessaria per supportare l'applicazione che verrà eseguita sull'infrastruttura wireless
- Tolleranza di ritardo roaming - Quanto tempo impiega il WGB per passare dall'attuale punto di accesso a quello successivo mentre il dispositivo è in movimento?
- Tolleranza tempo di inoltro: quanti frame vengono persi per ciascun roaming?

La stampante non si sposta molto, pertanto i requisiti di roaming sono inferiori. Un WGB montato sul treno, invece, deve essere regolato con precisione sul componente di roaming per assicurare un comportamento corretto mentre si muove.

Un flusso video può richiedere un'ampia larghezza di banda e quindi velocità di trasmissione dati wireless elevate. Tuttavia, un'applicazione di telemetria potrebbe richiedere solo pochi fotogrammi di tanto in tanto.

Èimportante che i requisiti siano definiti correttamente fin dall'inizio, in quanto influiscono non solo sulla configurazione del WGB, ma anche su come deve essere progettata l'infrastruttura wireless. Ad esempio, il posizionamento dei punti di accesso, la distanza, i livelli di alimentazione, le tariffe attivate e così via, influiscono sulle caratteristiche di roaming. Pertanto, tutti sono un punto cruciale se il roaming ad alta velocità è necessario.

In generale, è necessario conoscere i seguenti dettagli:

- Qual è la larghezza di banda necessaria per l'applicazione?
- Che cos'è la tolleranza del ritardo di roaming?
- L'applicazione è in grado di gestire correttamente le disconnessioni di rete? Esiste un

meccanismo di backup aggiuntivo?
- L'applicazione è in grado di gestire correttamente la perdita di pacchetti? (Anche con il design wireless migliore, ci si deve aspettare una percentuale di perdita di pacchetti.)

Il presente documento non fornisce dettagli su come progettare un ambiente RF per roaming ad alta velocità/esterni. Fare riferimento alla guida all'installazione di Mesh per esterni.

Roaming

Per un dispositivo wireless, il roaming è una parte fondamentale della sua funzionalità.

In sostanza, il roaming indica la capacità di passare da un punto di accesso all'altro, entrambi appartenenti alla stessa infrastruttura wireless.

Poiché il roaming richiede un cambiamento dall'access point corrente a quello successivo, ne consegue una disconnessione o un'interruzione del servizio. Questa disconnessione può essere minima. Ad esempio, meno di 200 ms in installazioni vocali o molto più lungo, anche secondi, se la sicurezza necessaria impone un'autenticazione completa su ogni evento di roaming.

Il roaming è necessario per consentire al dispositivo di trovare un nuovo elemento principale con un segnale che si spera migliori e di continuare ad accedere correttamente all'infrastruttura di rete. Allo stesso tempo, un numero eccessivo di roaming può causare disconnessioni multiple o mancanza di tempo per l'accesso. È importante che un dispositivo mobile, come un WGB, disponga di un buon algoritmo di roaming con capacità di configurazione sufficienti per adattarsi a diversi ambienti RF e alle diverse esigenze di dati.

Elementi del roaming

- **Trigger:** Ogni implementazione client dispone di uno o più trigger o eventi che, quando vengono soddisfatti, determinano lo spostamento del dispositivo in un altro punto di accesso padre. Esempi: perdita di beacon (il dispositivo non sente più i normali beacon provenienti dal punto di accesso), nuovi tentativi di caricamento dei pacchetti, livello del segnale, assenza di dati ricevuti, frame di deautenticazione ricevuti, bassa velocità di trasmissione dei dati in uso, ecc. I trigger possibili possono essere diversi dall'implementazione client a un'altra perché non sono completamente standardizzati. I dispositivi più semplici possono avere un set di trigger scadente, che causa problemi (client sticky) o roaming non necessari. WGB supporta tutti gli elementi precedenti descritti in precedenza.
- **Tempo di analisi:** Il dispositivo wireless (WGB) impiega del tempo a cercare potenziali genitori. Ciò implica normalmente l'utilizzo di canali diversi, l'esecuzione di probe attivi o l'ascolto passivo degli access point. Poiché la radio deve eseguire la scansione, questo significa che il WGB spende tempo per fare qualcosa di diverso dall'inoltro dei dati. A partire da questo tempo di analisi, il WGB può creare un set valido di elementi padre a cui è possibile eseguire il roaming.
- **Selezione padre:** Dopo il tempo di scansione, il WGB può controllare i potenziali padri, selezionare il migliore e attivare il processo di associazione/autenticazione. A volte, il punto di decisione può essere quello di rimanere nell'elemento padre corrente se non c'è un vantaggio significativo da un evento di roaming (ricordate che un roaming eccessivo può essere dannoso).
- **Associazione/Autenticazione:** Il WGB procede all'associazione al nuovo punto di accesso, che

normalmente copre entrambe le fasi di autenticazione e associazione 802.11, oltre al completamento della policy di sicurezza configurata sul SSID (WPA 2-PSK, CCKM, Nessuno, ecc.).
- **Ripristino inoltro traffico:** Il WGB aggiorna l'infrastruttura di rete dei client cablati noti tramite aggiornamenti IAPP dopo il roaming. Dopo questo punto, il traffico tra i client cablati e la rete riprende.

Guida alla configurazione - Criteri di protezione

Un aspetto importante per il roaming sui dispositivi mobili è costituito dalla politica di sicurezza che verrà implementata sull'infrastruttura. Ci sono diverse opzioni, ciascuna con punti buoni/cattivi. Questi sono i più importanti:

- **Aperta**: fondamentalmente nessuna protezione. Si tratta della politica più rapida e semplice. Il problema principale è quello di non limitare l'accesso non autorizzato all'infrastruttura e di non proteggere dagli attacchi, il che ne limita l'uso a scenari molto specifici. Ad esempio, le miniere dove non sono possibili attacchi esterni a causa della natura pura dell'installazione.
- **Autenticazione degli indirizzi MAC**: sostanzialmente lo stesso livello di sicurezza dell'autenticazione aperta, in quanto lo spoofing degli indirizzi MAC è un attacco banale. Non consigliato a causa del tempo aggiunto per completare la convalida MAC, che rallenta il roaming.
- **WPA2-PSK**: offre un buon livello di crittografia (AES-CCMP), ma la sicurezza dell'autenticazione dipende dalla qualità della chiave già condivisa. Per motivi di sicurezza, si consiglia una password di almeno 12 caratteri e casuale. Analogamente al metodo della chiave già condivisa, poiché la chiave viene utilizzata su più dispositivi, se la chiave viene compromessa la password deve essere modificata su tutte le apparecchiature. La velocità di roaming è accettabile, come avviene in 6 scambi di fotogrammi, ed è possibile calcolare quali saranno i limiti di tempo superiore/inferiore per il suo completamento perché non coinvolge alcuna apparecchiatura esterna (nessun server RADIUS, ecc.). In generale, questo metodo è quello preferito dopo aver bilanciato problemi e benefici.
- **WPA2 con 802.1x**: migliora il metodo precedente utilizzando una credenziale per dispositivo/utente, che può essere modificata singolarmente. Il problema principale è che per il roaming questo metodo non funziona correttamente quando il dispositivo è in movimento rapido o quando sono necessari tempi di roaming brevi. In generale, questo utilizza gli stessi 6 frame più lo scambio EAP che può essere tra 4 e fino. Dipende dal tipo EAP selezionato e dalle dimensioni del certificato. In genere, questa operazione richiede da 10 a 20 frame, più l'ulteriore ritardo dell'elaborazione del server radius.
- **WPA2+CCKM**: questo meccanismo offre una buona protezione, utilizza 802.1x per creare l'autenticazione iniziale, quindi esegue uno scambio rapido di soli 2 frame su ogni evento di roaming. Il tempo di roaming è estremamente rapido. Il problema principale è che nel caso di un roaming non riuscito, viene ripristinato lo stato 802.1x. Quindi, ricomincia a utilizzare CCKM dopo l'autenticazione. Se l'applicazione sul WGB può tollerare un tempo di roaming lungo occasionale in caso di problemi, può essere utilizzato come l'opzione migliore rispetto a PSK.

Questo documento non copre le tecnologie non consigliate che presentano problemi di sicurezza come LEAP, WPA-TKIP, WEP, ecc.

Configurazione di WPA2-PSK

Per quanto riguarda il WGB, è semplice da configurare. È necessario disporre della definizione SSID e della crittografia appropriata sulla radio.

```
dot11 ssid wgbpsk
vlan 32
authentication open
authentication key-management wpa version 2
wpa-psk ascii YourReallySecurePSK!
no ids mfp client

interface Dot11Radio0
ssid wgbpsk
encryption mode ciphers aes-ccm
station-role workgroup-bridge
```

Il nome SSID e la chiave già condivisa devono corrispondere all'infrastruttura di rete.

Configurazione di WPA2 con 802.1x

Si basa essenzialmente sulla configurazione precedente, con l'aggiunta di profili EAP e metodo di autenticazione:

```
dot11 ssid wlan1
authentication open eap eap
authentication network-eap eap
authentication key-management wpa version 2
dot1x credentials wgb
dot1x eap profile eapfast
no ids mfp client
eap profile eapfast
!--- This covers the EAP method type used on your network. method fast ! ! dot1x credentials wgb
!--- This is your WGB username/password. username cisco password 7 1511021F0725 interface
Dot11Radio0 encryption mode ciphers aes-ccm ssid wlan1
```

Configurazione di WPA2 con CCKM

Un solo passaggio sopra WPA2 con una sola modifica di minore entità: utilizzando il flag CCKM nella configurazione SSID. Ciò presuppone che la WLAN sia configurata per la CCKM solo sul lato WLC:

```
dot11 ssid wlan1
authentication open eap eap
authentication network-eap eap
authentication key-management cckm
dot1x credentials wgb
dot1x eap profile eapfast
no ids mfp client
```

Convalida del metodo utilizzato

Una rapida verifica sul WGB può segnalare la crittografia e la gestione delle chiavi in uso, ad

esempio, nella CCKM:

```
wgb-1260#sh dot11 associations al
Address           : 0024.97f2.75a0     Name             : lap1140-etsi-1
IP Address        : 192.168.40.10      Interface        : Dot11Radio 0
Device            : LWAPP-Parent      Software Version : NONE
CCX Version       : 5                  Client MFP       : Off

State             : EAP-Assoc          Parent           : -
SSID              : wlan1
VLAN              : 0
Hops to Infra     : 0                  Association Id   : 1
Tunnel Address    : 0.0.0.0
Key Mgmt type     : CCKM               Encryption       : AES-CCMP

Current Rate      : m7.-               Capability       : WMM ShortHdr ShortSlot
Supported Rates   : 48.0 54.0 m0. m1. m2. m3. m4. m5. m6. m7.
Voice Rates       : disabled           Bandwidth        : 20 MHz
Signal Strength   : -59  dBm           Connected for    : 72 seconds
Signal to Noise   : 41  dB            Activity Timeout : 8 seconds
Power-save        : Off                Last Activity    : 7 seconds ago
Apsd DE AC(s)     : NONE

Packets Input     : 12064              Packets Output   : 136
Bytes Input       : 2892798            Bytes Output     : 19514
Duplicates Rcvd   : 87                 Data Retries     : 8
Decrypt Failed    : 0                  RTS Retries      : 0
MIC Failed        : 0                  MIC Missing      : 0
Packets Redirected: 0                  Redirect Filtered: 0
```

Configurazione del roaming

Nel WGB è possibile modificare diversi parametri che influiscono sull'algoritmo di roaming.

Tentativi pacchetti

Per impostazione predefinita, il WGB ritrasmette un frame 64 volte. Se non viene riconosciuto correttamente (ACK) da un padre, presuppone che il padre non sia più valido e avvia un processo di scansione/roaming. Questo è un trigger di roaming "asincrono" perché può essere eseguito in qualsiasi momento in cui una trasmissione non riesce.

Il comando per configurare questa impostazione, va all'interno dell'interfaccia dot11 e richiede le opzioni seguenti:

```
packet retries NUM [drop]
```

Numero: È compreso tra 1 e 128, con un valore predefinito di 64. Un numero valido per un trigger di roaming rapido è in genere 32. L'utilizzo di un numero inferiore non è consigliabile nella maggior parte degli ambienti RF.

drop: Se non è presente, il WGB avvia un evento di roaming quando viene raggiunto il numero massimo di tentativi. Quando è presente, il WGB non inizia il nuovo roaming e utilizza altri trigger, come la perdita di beacon e il segnale.

Monitoraggio RSSI

WGB può implementare una scansione del segnale proattiva per l'elemento padre corrente e avviare un nuovo processo di roaming quando il segnale scende al di sotto del livello previsto.

Questo processo richiede due parametri:

- Un timer, che riattiva il processo di controllo ogni X secondi
- Livello RSSI, utilizzato per avviare un processo di roaming se il segnale corrente è inferiore a tale livello.

Ad esempio:

```
in d0
mobile station period 4 threshold 75
```

Il tempo non dovrebbe essere inferiore a quello impiegato dal WGB per completare un processo di autenticazione al fine di prevenire un "roaming a ciclo continuo" in alcune condizioni o di evitare un comportamento di roaming troppo aggressivo. In generale, dovrebbe essere testato per vedere cosa soddisfa le esigenze della domanda.

Per PSK può essere inferiore rispetto ai metodi basati su EAP (in genere 2 e 4 per applicazioni molto aggressive).

Il livello RSSI viene espresso come un numero intero positivo, sebbene si tratti fondamentalmente di un livello misurato di -dBm normale. È consigliabile utilizzare un numero leggermente superiore al minimo necessario per garantire il corretto funzionamento della velocità dati. Ad esempio, se la velocità minima desiderata è 6 mbps, un RSSI di soglia di -87 dovrebbe essere sufficiente. Per una velocità di 48 mbps sono necessari -70 dBm, ecc.

Nota: questo comando può anche attivare il "roaming per variazione della velocità dei dati", che è troppo aggressivo. Per ottenere buoni risultati, esso deve essere utilizzato unitamente alla tariffa minima.

Velocità minima dei dati

A partire dalla versione 12.4(25d)JA, Cisco ha aggiunto un parametro configurabile per controllare quando il WGB deve attivare un nuovo evento di roaming, se la velocità dati corrente al padre è inferiore a un determinato valore.

Ciò è utile per garantire che venga mantenuto il limite inferiore di velocità desiderato per il supporto di applicazioni video o voce.

Prima che questo comando fosse disponibile, il WGB attivava frequentemente il roaming quando la velocità risultava essere inferiore all'ora precedente. Fondamentalmente negli orari X+1, se la velocità era inferiore al X-time precedente, il WGB ha avviato un processo di roaming. Nei log vengono visualizzati questi messaggi:

```
*Mar  1 00:36:43.490: %DOT11-4-UPLINK_DOWN: Interface Dot11Radio1, parent lost: Had to lower
data rate
```

Questa soluzione è troppo aggressiva e, in genere, l'unica soluzione è stata configurare una singola velocità dati sia in WGB che nei punti di accesso padre.

Ora, il modo consigliato è configurare sempre questo comando, ogni volta che si usa un comando

del periodo della stazione mobile:

```
in d0
mobile station  minimum-rate 2.0
```

In questo modo, il nuovo processo di roaming viene attivato solo se la velocità corrente è inferiore al valore configurato. In questo modo si riducono i roaming non necessari e si mantiene il valore della tariffa prevista.

Nota: il messaggio `"Doveva abbassare la velocità dati"` dovrebbe apparire anche con questa configurazione, proprio che ora dovrebbe essere visto solo se WGB era TX a una velocità inferiore a quella configurata, quando è stato attivato il periodo di controllo della stazione mobile.

Canali di scansione

Il WGB analizza tutti i "canali nazionali" durante un evento di roaming. Ciò significa che, a seconda del dominio radio, è possibile eseguire la scansione dei canali da 1 a 11 su una banda di 2,4 Ghz o da 1 a 13.

Ogni canale digitalizzato richiede del tempo. Su 802.11bg questo valore è di circa 10 a 13 ms. Su 802.11a, può essere fino a 150 ms se il canale è abilitato DFS (quindi non eseguire il probe, ma solo eseguire la scansione passiva).

Una buona ottimizzazione consiste nel limitare i canali digitalizzati in modo che utilizzino solo quelli in servizio nell'infrastruttura. Ciò è particolarmente importante in 802.11a, poiché l'elenco dei canali è molto ampio e il tempo per canale può essere lungo se DFS è in uso.

Quando si progetta un piano di canale per WGB/roaming, è necessario considerare tre punti:

- Per la banda a 2,4 GHz, cercate di aderire a 1/6/11 per ridurre al minimo le interferenze del canale laterale. Qualsiasi altra combinazione di canali con 4, ecc., è difficile da configurare correttamente dal punto di vista della radiofrequenza, senza aumentare le interferenze.
- L'utilizzo di una configurazione a canale singolo per tutti i punti di accesso è una buona idea dal punto di vista della scansione. Ciò ha senso solo se il numero totale di client da supportare è molto basso e non vi sono requisiti di larghezza di banda elevati. In questo modo il tempo di cambiamento della radio viene eliminato dal tempo di scansione. Tenere presente che questa opzione non consente di sfruttare i vantaggi di un numero limitato di ambienti, pertanto è consigliabile utilizzarla con cautela.
- Per la banda a 5,0 GHz, se possibile in base alle normative locali, l'utilizzo di canali interni non DFS (da 36 a 48) consente tempi di scansione più rapidi, in quanto WGB è in grado di probe attivamente ciascuno, invece di eseguire l'ascolto passivo per un tempo più lungo.

Il piano di canale utilizzato per la distribuzione potrebbe dover soddisfare altri requisiti. Utilizzare i consigli generali di progettazione RF.

Per configurare l'elenco dei canali di scansione:

```
in d0
mobile station scan 1 6 11
```

Nota: la stazione mobile viene visualizzata solo quando si utilizza il ruolo WGB sulla radio.

Nota: verificare che l'elenco di scansione WGB corrisponda all'elenco dei canali dell'infrastruttura. In caso contrario, il WGB non troverà gli access point disponibili.

Configura timer

A partire dalla versione 12.4(25a)JA, sono disponibili diversi nuovi comandi per ottimizzare il timer di ripristino quando viene rilevato un problema, disponibili solo quando l'access point è in modalità WGB.

```
wgb-1260(config)#workgroup-bridge timeouts ?

  assoc-response  Association Response time-out value
  auth-response   Authentication Response time-out value
  client-add      client-add time-out value
  eap-timeout     EAP Timeout value
  iapp-refresh    IAPP Refresh time-out value
```

In caso di risposta assoc, autenticazione-risposta, client-add, questi indicano per quanto tempo il WGB attende la risposta dell'access point padre, prima di considerare l'access point come inattivo e di provare il candidato successivo. I valori predefiniti sono 5 secondi, un tempo troppo lungo per alcune applicazioni. Il timer minimo è di 800 ms ed è consigliato per la maggior parte delle applicazioni mobili.

In eap-timeout, il WGB imposta un tempo massimo di attesa, fino al completamento del processo di autenticazione EAP completo. Questa procedura funziona dal punto di vista di un supplicant EAP per riavviare il processo se l'autenticatore EAP non risponde. Il valore predefinito è 60 secondi. Prestare attenzione a non configurare mai un valore inferiore al tempo effettivo necessario per completare un'autenticazione 802.1x completa. In genere, l'impostazione su 2-4 secondi è corretta per la maggior parte delle distribuzioni.

Per l'aggiornamento tramite iapp, per impostazione predefinita il WGB genera un aggiornamento in blocco IAPP nell'access point padre dopo il roaming per informare i client cablati noti. C'è una seconda ritrasmissione dopo l'associazione circa 10 secondi dopo. Questo timer consente di eseguire un "tentativo rapido" dell'operazione di massa IAPP dopo l'associazione per evitare che il primo aggiornamento IAPP sia stato perso a causa di RF o che le chiavi di crittografia non siano ancora installate nell'access point padre. Per gli scenari di roaming veloce, è possibile utilizzare 100 ms. Tuttavia, accertatevi che sia in uso un numero elevato di WGB. Ciò aumenta in modo significativo il numero totale di IAPP inviate all'infrastruttura dopo ogni roaming.

Esempio di valori aggressivi:

```
workgroup-bridge timeouts eap-timeout 4
workgroup-bridge timeouts iapp-refresh 100
workgroup-bridge timeouts auth-response 800
workgroup-bridge timeouts assoc-response 800
workgroup-bridge timeouts client-add 800
```

Questi sono stati testati correttamente negli scenari di distribuzione WGB mobile.

Altre ottimizzazioni WGB

Per gli scenari di distribuzione WGB è necessario prendere in considerazione altre modifiche di minore entità:

Correlato alla radio

- Riduci **tentativi rts** - **tentativi rts 32**. Ciò consente di risparmiare tempo RF in scenari aggressivi. Normalmente questo non è necessario.
- Tipo di antenna: Se si utilizza una singola antenna (nessuna diversità), è necessario configurare la radio per migliorare le prestazioni generali:

```
antenna transmit right-a
antenna receive right-a
```

La diversità delle antenne è auspicabile, ma non sempre possibile quando si installano fisicamente le antenne sul veicolo. La corretta selezione dell'antenna è fondamentale per il roaming. Un minimo di 2 dB può rappresentare un'enorme differenza rispetto ai tempi medi di roaming generale.

Registro correlato

- Per risparmiare alcuni millisecondi, ridurre il livello di registrazione della console agli errori: **registrazione degli errori della console**. Non disabilitarlo completamente perché potrebbe influire negativamente sulle prestazioni di roaming in alcune condizioni.
- Se possibile, usare telnet o ssh dal lato ethernet per raccogliere i debug o i log. L'impatto sulle prestazioni è molto inferiore rispetto alla registrazione dei debug sulla console: **debug del monitoraggio della registrazione**.
- Il comando per capire cosa sta succedendo per il punto di vista mobile WGB è **debug dot11 dot11 0 trace print uplink**. L'impatto sulla CPU è basso, ma non abilitare altre opzioni di debug se non indicato perché ciascuna di esse potrebbe aumentare il tempo di roaming totale.
- Provare a utilizzare il protocollo SNTP quando possibile. In questo modo viene mantenuto il tempo WGB alla sincronizzazione, che è estremamente utile per la risoluzione dei problemi.

Utilizzo MFP

- Le stampanti multifunzione possono essere utili dal punto di vista della protezione. Tuttavia, uno svantaggio è che in caso di errori di roaming, il WGB non accetta i frame di de-auth dall'elemento padre dell'access point per attivare un nuovo roaming se la chiave di crittografia tra entrambi è andata male per qualsiasi motivo.
- In questi rari scenari di errore, il WGB può impiegare fino a 5 secondi per attivare una nuova scansione, se l'attuale padre può essere ascoltato con un buon segnale RF. Esiste un meccanismo di rilevamento "catch-all" che WGB può attivare se non vengono ricevuti frame di dati validi durante tale periodo.
- Per impostazione predefinita, il WGB tenta di utilizzare l'interfaccia MFP del client se l'SSID ha WPA2 AES in uso.
- Si consiglia di disabilitare l'interfaccia MFP del client se sono necessari tempi di ripristino rapidi (WGB per reagire ai frame di default non protetti). Si tratta di un compromesso tra le esigenze di sicurezza e i tempi di ripristino rapidi. La decisione dipende dall'elemento più importante per lo scenario di distribuzione.

```
dot11 ssid wgbpsk
   no ids mfp client
```

EAP-TLS su WGB e "intervallo di salvataggio dell'orologio"

Fare riferimento alla sezione Synchronize IOS Supplicant Clocks and Save Time Setting to NVRAM delle note di versione per Cisco Aironet Access Point and Bridge per Cisco IOS versione 12.4(21a)JY.

Tenete presente che se si utilizza uWGB, l'uWGB potrebbe non avere mai la possibilità di eseguire una sincronizzazione sntp perché è in genere associato all'indirizzo MAC collegato e l'uWGB BVI non ha accesso alla rete. Pertanto, nel caso di un uWGB, si consiglia di ottenere almeno una buona sincronizzazione dell'orologio nella NVRAM al momento dell'installazione. Se il dispositivo di rete collegato ha la capacità di essere un'origine NTP (e un client aggiornato tramite la sua connessione WuGB), allora è possibile prendere in considerazione la sincronizzazione sntp uWGB da esso come un punto di riflessione NTP efficace.

Esempio di configurazione completa

```
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname wgb-1260
!
logging rate-limit console 9
logging console errors
!
clock timezone CET 1
no ip domain lookup
!
!
dot11 syslog
!
!
dot11 ssid wgbpsk
   vlan 32
   authentication open
   authentication key-management wpa version 2
   wpa-psk ascii 7 060506324F41584B56
   no ids mfp client
!
!
!
!
!
!
username Cisco password 7 13261E010803
!
!
bridge irb
!
!
interface Dot11Radio0
no ip address
no ip route-cache
!
encryption mode ciphers aes-ccm
!
ssid wgbpsk
```

```
!
antenna transmit right-a
antenna receive right-a
  packet retries 32
station-role workgroup-bridge
rts retries 32
mobile station scan 2412 2437 2462
mobile station minimum-rate 6.0
mobile station period 3 threshold 70
bridge-group 1
!

interface GigabitEthernet0
no ip address
no ip route-cache
duplex auto
speed auto
no keepalive
bridge-group 1
!
interface BVI1
ip address 192.168.32.67 255.255.255.0
no ip route-cache
!
ip default-gateway 192.168.32.1
no ip http server
no ip http secure-server

bridge 1 route ip

sntp server 192.168.32.1
clock save interval 1
workgroup-bridge timeouts eap-timeout 4
workgroup-bridge timeouts iapp-refresh 100
workgroup-bridge timeouts auth-response 800
workgroup-bridge timeouts assoc-response 800
workgroup-bridge timeouts client-add 800
```

Analisi di debug

In caso di problemi, è importante acquisire l'output del comando **debug dot11 dot11 0 trace print uplink** come primo passaggio. In questo modo si ottiene una buona visualizzazione di ciò che accade durante il processo di roaming.

Questo è un esempio di padre corrente come candidato:

```
 Sep 27 11:42:38.797: %DOT11-4-UPLINK_DOWN: Interface Dot11Radio0, parent lost: Signal strength
too low
 Sep 27 11:42:38.797: CDD051F1-0 Uplink: Lost AP, Signal strength too low
```

Questo è il trigger per il segnale basso raggiunto. Dipende dal comando X threshold Y della stazione mobile. Il primo messaggio viene sempre inviato alla console, il secondo fa parte delle tracce di debug uplink. Non è un problema, ma fa parte del normale processo WGB.

```
 Sep 27 11:42:38.798: CDD052C7-0 Uplink: Wait for driver to stop
```

Il processo di uplink forza l'eliminazione di una coda radio prima di avviare una scansione del canale. Questa operazione può richiedere da alcuni millisecondi a diversi secondi, a seconda dell'utilizzo del canale e della profondità della coda. I frame dati non sono scaduti. I frame vocali hanno un confronto temporale fatto, quindi dovrebbero essere scartati più velocemente. In

ambienti rumorosi potrebbe essere osservato un certo ritardo.

```
 Sep 27 11:42:38.798: CDD05371-0 Uplink: Enabling active scan
 Sep 27 11:42:38.799: CDD05386-0 Uplink: Scanning
```

Questa è la scansione effettiva del canale in corso. Parcheggia la radio per circa 10-13 ms per canale configurato.

```
 Sep 27 11:42:38.802: CDD064CD-0 Uplink: Rcvd response from 0021.d835.ade0 channel 1 3695
```

Elenco delle risposte di richiesta ricevute. Il primo numero è il canale, il secondo è il microsecondo impiegato per riceverlo.

```
 Sep 27 11:42:38.808: CDD078F1-0 Uplink: Compare1 0021.d835.ade0 - Rssi 58dBm, Hops 0, Count 0,
load 0
 Sep 27 11:42:38.809: CDD07929-0 Uplink: Compare2 0021.d835.cce0 - Rssi 46dBm, Hops 0, Count 0,
load 0
```

Confronto effettivo eseguito nei dettagli seguenti:

```
 Sep 27 11:42:38.809: CDD07BDB-0 Uplink: Same as previous, send null data packet
```

Selezione padre

```
 Sep 27 11:42:38.809: CDD07BF7-0 Uplink: Done
 Sep 27 11:42:38.808: %DOT11-4-UPLINK_ESTABLISHED: Interface Dot11Radio0,
 Associated To AP AP1 0021.d835.ade0 [None WPAv2 PSK]Roaming completed.
```

Èil punto in cui il roaming è "finito". Il traffico riprende non appena i frame IAPP vengono elaborati dal padre.

Informazioni di confronto padre

```
 Sep 27 14:16:47.590: F515B1FF-0 Uplink: Compare1 0021.d835.7620 - Rssi 60dBm, Hops 0, Count 0,
load 3
 Sep 27 14:16:47.591: F515B238-0 Uplink: Compare2 0021.d835.e8b0 - Rssi 58dBm, Hops 0, Count -1,
load 0
```

Il confronto 1 stampa il conteggio delle associazioni effettive -1 (pertanto il valore WGB non viene incluso nel numero). Se l'access point "corrente" è ancora quello associato, vengono eseguiti gli hop e il caricamento effettivi.

Il comando compare2 visualizza le differenze. Per questo è possibile vedere un numero negativo. Se il numero di test è maggiore di quello corrente, verrà visualizzato negativo.

In base al numero di associazioni, al carico, alla differenza di segnale e al valore soglia mobile correnti, il WGB potrebbe selezionare o meno un nuovo elemento padre.

Il confronto viene sempre eseguito tra due punti di accesso e l'access point selezionato sostituisce quello corrente per l'iterazione successiva. Pertanto, alcune decisioni possono essere dovute a RSSI su un loop o ad altri fattori sul test successivo.

Informazioni correlate

- Come utilizzare un WGB IOS con autenticazione EAP-TLS in una rete wireless unificata Cisco
- Documentazione e supporto tecnico – Cisco Systems