Uso di VLAN con apparecchiature wireless Cisco Aironet

Sommario

Introduzione

In questo documento viene fornito un esempio di configurazione per l'utilizzo di LAN virtuali (VLAN) con apparecchiature wireless Cisco Aironet.

Prerequisiti

Requisiti

Prima di provare questa configurazione, accertarsi di soddisfare i seguenti requisiti:

- Familiarità con le apparecchiature wireless Cisco Aironet
- Familiarità con i concetti di switching LAN per VLAN e trunking VLAN

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Access point Cisco Aironet e bridge wireless
- Switch Cisco Catalyst

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.

Prodotti correlati

Il lato switch di questa configurazione può essere utilizzato con uno dei seguenti componenti hardware o software:

- Catalyst 6x00/5x00/4x00 con CatOS o IOS
- Catalyst 35x0/37x0/29xx con IOS
- Catalyst 2900XL/3500XL con IOS

Convenzioni

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

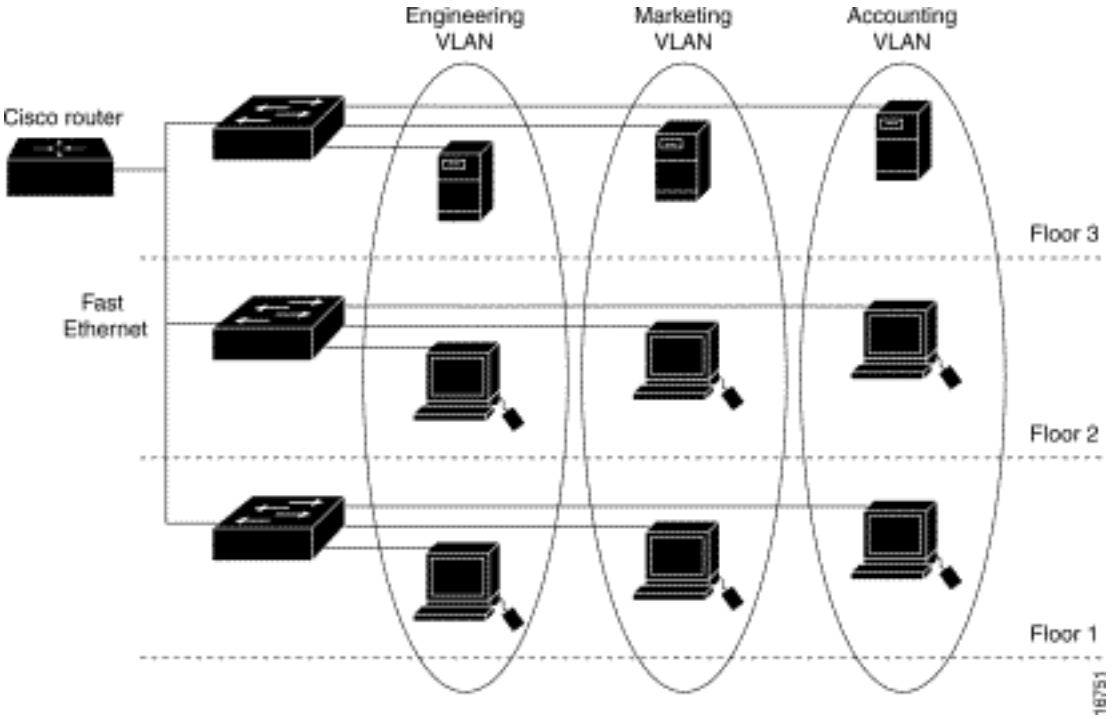
VLAN

Una VLAN è una rete commutata segmentata logicamente in base a funzioni, team di progetto o applicazioni anziché su base fisica o geografica. Ad esempio, tutte le workstation e i server utilizzati da un determinato team di workgroup possono essere connessi alla stessa VLAN, a prescindere dalle connessioni fisiche alla rete o dal fatto che possano interagire con altri team. Utilizzare le VLAN per riconfigurare la rete tramite il software anziché scollegare o spostare fisicamente i dispositivi o i cavi.

Una VLAN può essere interpretata come un dominio di broadcast che esiste in un set definito di switch. Una VLAN è costituita da un certo numero di sistemi terminali, host o apparecchiature di rete (ad esempio bridge e router), connessi da un singolo dominio di bridging. Il dominio di bridging è supportato su diverse apparecchiature di rete, ad esempio gli switch LAN, che operano tra loro tramite protocolli di bridging con un gruppo separato per ciascuna VLAN.

Quando si collega un dispositivo a uno switch Cisco Catalyst, la porta a cui è connesso il

dispositivo è un membro della VLAN 1. L'indirizzo MAC del dispositivo fa parte della VLAN 1. È possibile definire più VLAN su un singolo switch e configurare una porta dello switch sulla maggior parte dei modelli Catalyst come membro di più VLAN.



Quando il numero di porte in una rete supera la capacità della porta dello switch, è necessario collegare più switch allo chassis, che definisce un trunk. Il trunk non è un membro di alcuna VLAN, ma un canale sul quale il traffico passa per una o più VLAN.

Fondamentalmente, per configurare un access point in modo che si connetta a una VLAN specifica, è necessario configurare il relativo SSID in modo che riconosca tale VLAN. Poiché le VLAN sono identificate da un ID o da un nome VLAN, se l'SSID di un punto di accesso è configurato per riconoscere un ID o un nome VLAN specifico, viene stabilita una connessione alla VLAN. Una volta stabilita la connessione, i dispositivi client wireless associati che hanno lo stesso SSID possono accedere alla VLAN tramite il punto di accesso. La VLAN elabora i dati da e verso i client allo stesso modo in cui elabora i dati verso e da connessioni cablate. È possibile configurare fino a 16 SSID sul proprio punto di accesso per supportare fino a 16 VLAN. È possibile assegnare un solo SSID a una VLAN.

Per estendere le VLAN in una LAN wireless, aggiungere il tag IEEE 802.11Q al punto di accesso. I frame destinati a VLAN diverse vengono trasmessi dal punto di accesso in modalità wireless su SSID diversi con chiavi WEP diverse. Solo i client associati a tale VLAN ricevono i pacchetti. Al contrario, i pacchetti provenienti da un client associato a una determinata VLAN sono contrassegnati con 802.11Q prima di essere inoltrati alla rete cablata.

Ad esempio, i dipendenti e gli ospiti possono accedere contemporaneamente alla rete wireless di un'azienda ed essere amministrativamente separati. Una VLAN esegue il mapping a un SSID e il client wireless si collega al SSID appropriato. Nelle reti con bridge wireless, è possibile passare più VLAN attraverso il collegamento wireless per fornire connettività a una VLAN da postazioni diverse.

Se lo standard 802.1q è configurato sull'interfaccia Fast Ethernet di un punto di accesso, il punto di accesso invia sempre pacchetti keepalive sulla VLAN1 anche se la VLAN 1 non è definita sul punto di accesso. Di conseguenza, lo switch Ethernet si connette al punto di accesso e genera un messaggio di avviso. Non si verifica alcuna perdita di funzionalità sul punto di accesso o sullo

switch, ma il registro dello switch contiene messaggi privi di significato che possono causare il wrapping e la mancata visualizzazione di messaggi più importanti.

Questo comportamento crea un problema quando tutti gli SSID su un punto di accesso sono associati a reti mobili. Se tutti gli SSID sono associati a reti mobili, la porta dello switch Ethernet a cui è connesso il punto di accesso può essere configurata come porta di accesso. La porta di accesso viene normalmente assegnata alla VLAN nativa del punto di accesso, che non è necessariamente la VLAN1. In questo modo, lo switch Ethernet genera messaggi di avviso in cui si avvisa che il traffico con tag 802.1q viene inviato dal punto di accesso.

Se si disabilita la funzione keepalive, è possibile eliminare i messaggi in eccesso sullo switch.

Se si ignorano punti secondari in questi concetti quando si distribuiscono VLAN con apparecchiature wireless Cisco Aironet, si possono verificare prestazioni impreviste, ad esempio:

- Impossibile limitare le VLAN consentite sul trunk a quelle definite sul dispositivo wirelessSe sullo switch sono definite le VLAN 1, 10, 20, 30 e 40, ma sull'apparecchiatura wireless sono definite solo le VLAN 1, 10 e 30, è necessario rimuovere le altre VLAN dalla porta dello switch trunk.
- Uso improprio della designazione di SSID infrastrutturaQuando si installano i punti di accesso, assegnare il SSID infrastruttura solo quando si utilizza un SSID in:dispositivi bridge per gruppi di lavoroaccess point ripetitorebridge non radiceÈ una configurazione errata designare il SSID dell'infrastruttura per un SSID con solo computer laptop wireless per i client e causa risultati imprevedibili.Nelle installazioni bridge è possibile avere un solo SSID infrastruttura. L'SSID dell'infrastruttura deve essere l'SSID correlato alla VLAN nativa.
- Utilizzo improprio o progettazione non corretta della designazione SSID modalità guestQuando si definiscono più SSID/VLAN su apparecchiature wireless Cisco Aironet, è possibile assegnare un (1) SSID come SSID in modalità guest con il broadcast SSID nei beacon radio 802.11. Gli altri SSID non vengono trasmessi. I dispositivi client devono indicare quale SSID connettere.
- Impossibile riconoscere che più VLAN e SSID indicano più subnet del modello OSI di livello 3Le versioni deprecate del software Cisco Aironet consentono di associare più SSID a una VLAN. Le versioni correnti no.
- Errori di routing o progettazioni non corrette del modello OSI Layer 3Ogni SSID e la relativa VLAN collegata devono avere un dispositivo di routing e alcune origini per indirizzare i client, ad esempio un server DHCP o l'ambito su un server DHCP.
- Comprensione errata o configurazione errata della VLAN nativaI router e gli switch che costituiscono l'infrastruttura fisica di una rete vengono gestiti in un metodo diverso rispetto ai PC client collegati all'infrastruttura fisica. La VLAN a cui appartengono queste interfacce di router e switch è chiamata VLAN nativa (per impostazione predefinita, VLAN 1). I PC client sono membri di una VLAN diversa, proprio come i telefoni IP sono membri di un'altra VLAN. L'interfaccia amministrativa del punto di accesso o del bridge (interfaccia BVI1) viene considerata e numerata come parte della VLAN nativa, a prescindere da quali VLAN o SSID passino attraverso il dispositivo wireless.

Importanza della VLAN nativa

Quando si usa una porta trunk IEEE 802.1Q, tutti i frame sono contrassegnati ad eccezione di quelli sulla VLAN configurata come "VLAN nativa" per la porta. I frame sulla VLAN nativa vengono

sempre trasmessi senza tag e normalmente ricevuti senza tag. Pertanto, quando un access point è collegato alla porta dello switch, la VLAN nativa configurata sull'access point deve corrispondere alla VLAN nativa configurata sulla porta dello switch.

Nota: In caso di mancata corrispondenza nelle VLAN native, i frame vengono scartati.

Questo scenario viene illustrato meglio con un esempio. Se la VLAN nativa sulla porta dello switch è configurata come VLAN 12 e sul punto di accesso, la VLAN nativa è configurata come VLAN 1, quando il punto di accesso invia un frame sulla VLAN nativa allo switch, lo switch considera il frame come appartenente alla VLAN 12 poiché i frame della VLAN nativa del punto di accesso non hanno tag. Ciò causa confusione nella rete e problemi di connettività. Lo stesso accade quando la porta dello switch inoltra un frame dalla VLAN nativa all'access point.

La configurazione della VLAN nativa diventa ancora più importante quando nella rete wireless è installato un Repeater AP. Non è possibile configurare più VLAN sui punti di accesso del ripetitore. I punti di accesso ripetitori supportano solo la VLAN nativa. Pertanto, la configurazione VLAN nativa sull'access point radice, la porta dello switch a cui è connesso l'access point e l'access point Repeater devono essere la stessa. In caso contrario, il traffico attraverso lo switch non passa da e verso il Repeater AP.

Un esempio di scenario in cui la mancata corrispondenza nella configurazione VLAN nativa del punto di accesso ripetitore può creare problemi è quello in cui vi è un server DHCP dietro lo switch a cui è connesso il punto di accesso radice. In questo caso, i client associati al punto di accesso ripetitore non ricevono un indirizzo IP dal server DHCP perché i frame (richieste DHCP nel nostro caso) della VLAN nativa del punto di accesso ripetitore (che non è la stessa del punto di accesso radice e dello switch) vengono scartati.

Inoltre, quando si configura la porta dello switch, *verificare che tutte le VLAN configurate sui punti di accesso siano consentite sulla porta dello switch.* Ad esempio, se le VLAN 6, 7 e 8 sono presenti sull'access point (rete wireless), le VLAN devono essere autorizzate sulla porta dello switch. A tale scopo, usare questo comando nello switch:

```
switchport trunk allowed vlan add 6,7,8
```

Per impostazione predefinita, una porta switchport configurata come trunk consente a tutte le VLAN di passare attraverso la porta trunk. Per ulteriori informazioni su come configurare la porta dello switch, consultare il documento sull'interazione con gli switch correlati.

Nota: anche consentire l'uso di tutte le VLAN sull'access point in alcuni casi può diventare un problema, in particolare se si tratta di una rete di grandi dimensioni. Ciò può determinare un elevato utilizzo della CPU negli access point. Eliminare le VLAN sullo switch in modo che solo il traffico VLAN a cui l'access point è interessato passi attraverso il access point per evitare un'elevata CPU.

VLAN sugli access point

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

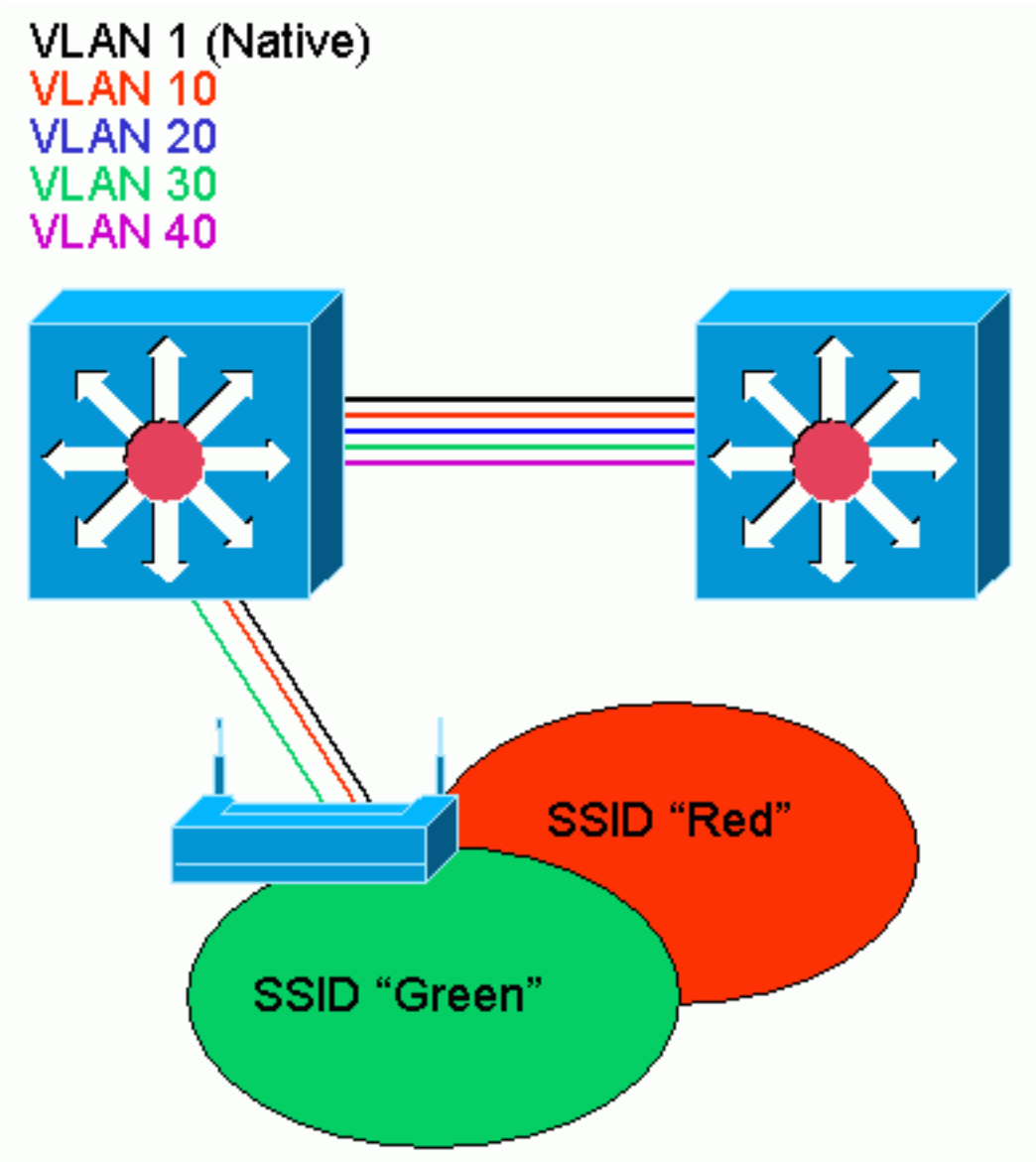
Nota: per ulteriori informazioni sui comandi menzionati in questo documento, usare lo strumento di

ricerca dei comandi (solo utenti registrati).

Nozioni base sui punti di accesso

In questa sezione vengono illustrati i concetti relativi alla distribuzione delle VLAN sui punti di accesso e viene fatto riferimento a questo diagramma di rete.

In questa rete di esempio, la VLAN 1 è la VLAN nativa e esistono le VLAN 10, 20, 30 e 40 e vengono trunkate su un altro chassis dello switch. Solo le VLAN 10 e 30 vengono estese al dominio wireless. La VLAN nativa è necessaria per fornire funzionalità di gestione e autenticazioni dei client.

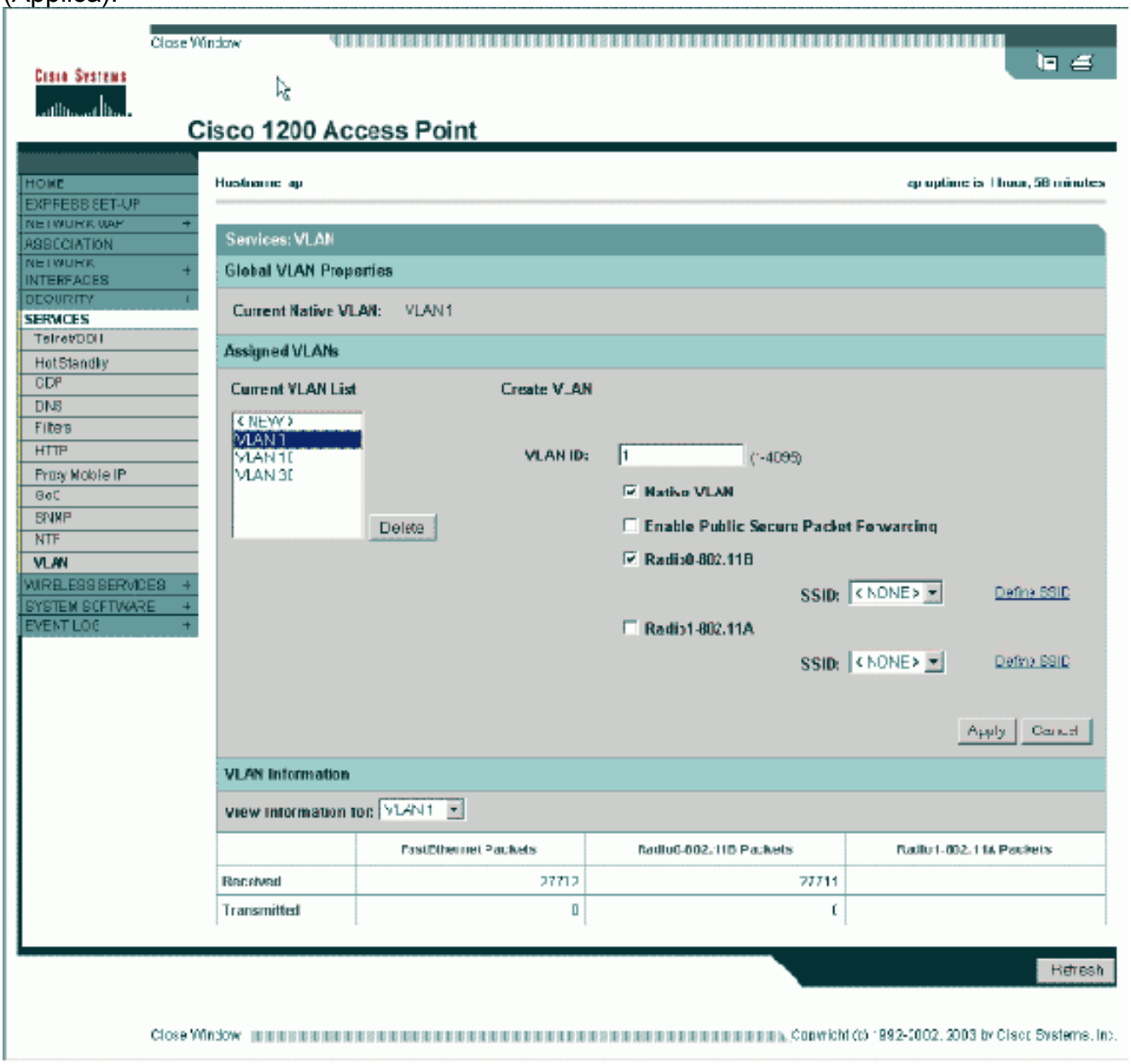


Configurazione Access Point

Per configurare il punto di accesso per le VLAN, attenersi alla seguente procedura:

1. Dalla GUI dell'access point, fare clic su Services > VLAN per selezionare **Services:** Pagina **VLAN** .Il primo passaggio consiste nella configurazione della VLAN nativa. Dall'elenco delle VLAN correnti, selezionare **Nuovo**.Immettere il numero VLAN della VLAN nativa nella casella ID VLAN. Il numero VLAN deve corrispondere alla VLAN nativa configurata sullo

switch.Poiché l'interfaccia BVI 1 è associata alla sottointerfaccia della VLAN nativa, l'indirizzo IP assegnato all'interfaccia BVI 1 deve trovarsi nella **stessa subnet IP** degli altri dispositivi dell'infrastruttura presenti sulla rete (ossia l'interfaccia SC0 su uno switch Catalyst con CatOS).Selezionare la casella di controllo della VLAN nativa.Selezionare le caselle di controllo relative all'interfaccia o alle interfacce radio a cui si applica la VLAN.Fare clic su **Apply**
(Applica).

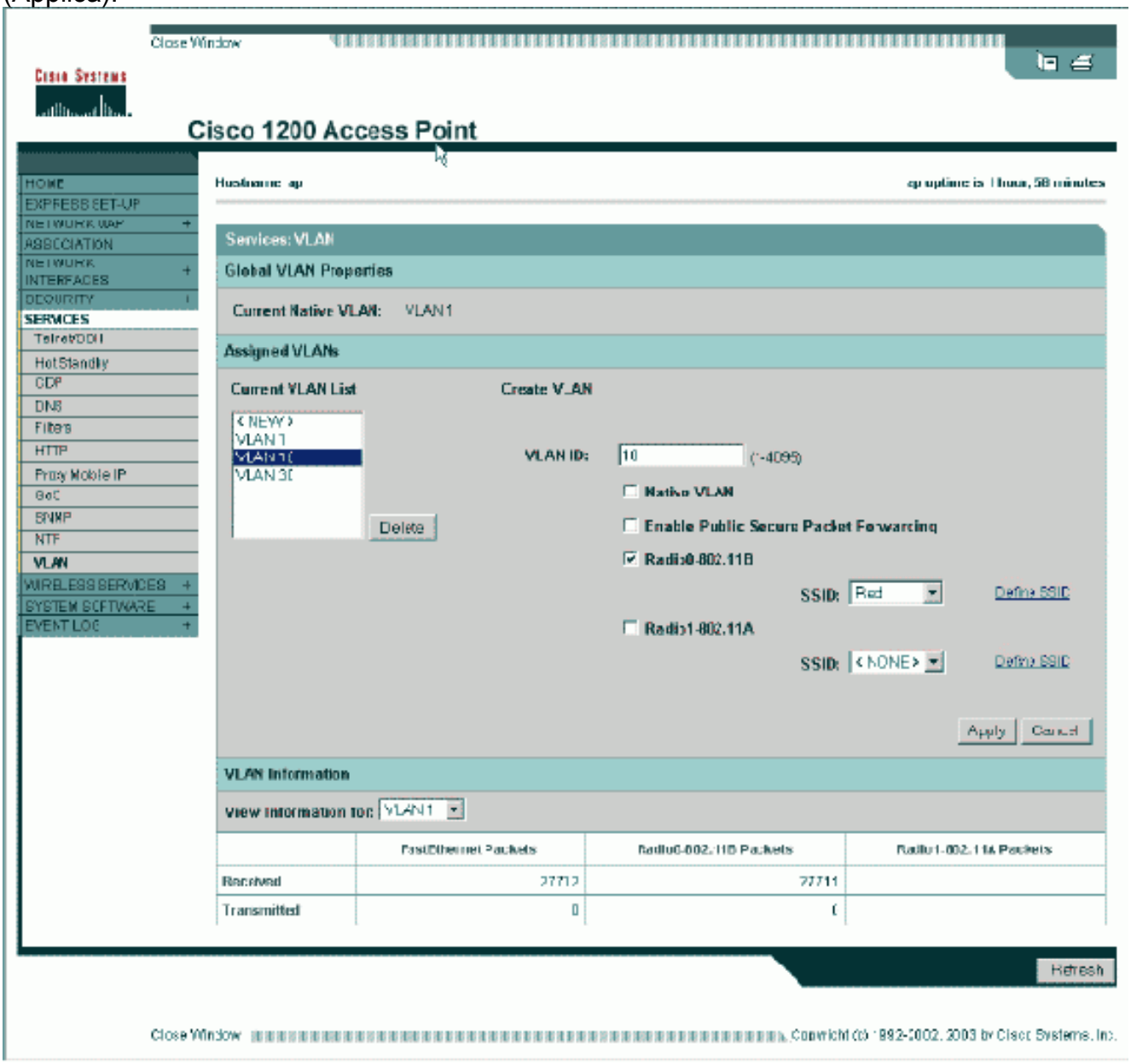


Oppure, dalla CLI, usare questi comandi:

```
AP# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
AP(config)# interface Dot11Radio0.1
AP(config-subif)# encapsulation dot1Q 1 native
AP(config-subif)# interface FastEthernet0.1
AP(config-subif)# encapsulation dot1Q 1 native
AP(config-subif)# end
AP# write memory
```

2. Per configurare altre VLAN, attenersi alla seguente procedura:Dall'elenco delle VLAN correnti, selezionare **Nuovo**.Immettere il numero VLAN della VLAN desiderata nella casella ID VLAN. Il numero VLAN deve corrispondere a una VLAN configurata sullo

switch.Selezionare le caselle di controllo relative all'interfaccia o alle interfacce radio a cui si applica la VLAN.Fare clic su **Apply**
(Applica).



Oppure, dalla CLI, usare questi comandi:

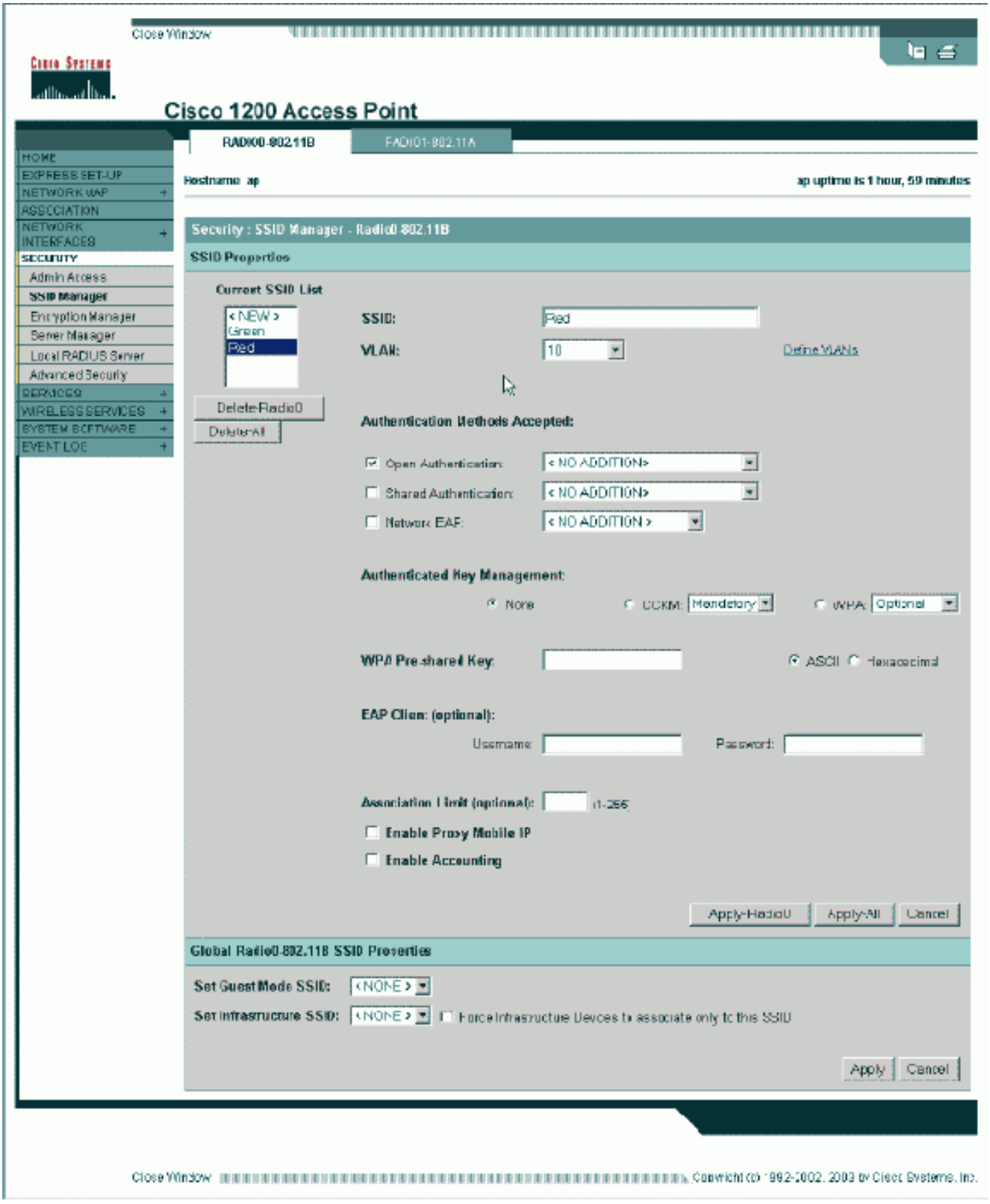
```
AP# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
AP(config)# interface Dot11Radio0.10
AP(config-subif)# encapsulation dot1Q 10
AP(config-subif)# interface FastEthernet0.10
AP(config-subif)# encapsulation dot1Q 10
AP(config-subif)# end
AP# write memory
```

Ripetere i passaggi da 2a a 2d per ciascuna VLAN desiderata o immettere questi comandi dalla CLI con le modifiche appropriate all'interfaccia secondaria e ai numeri di VLAN:

```
AP# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
AP(config)# interface Dot11Radio0.30
AP(config-subif)# encapsulation dot1Q 30
AP(config-subif)# interface FastEthernet0.30
AP(config-subif)# encapsulation dot1Q 30
AP(config-subif)# end
```

```
AP# write memory
```

3. Il passaggio successivo è associare le VLAN configurate agli SSID. A tale scopo, fare clic su **Protezione > Gestione SSID**.**Nota:** non è necessario associare tutte le VLAN definite sul punto di accesso a un SSID. Ad esempio, per motivi di sicurezza, la maggior parte delle installazioni di punti di accesso non associa un SSID alla VLAN nativa.Per creare un nuovo SSID, scegliere **Nuovo**.Immettere il SSID desiderato (con distinzione tra maiuscole e minuscole) nella casella SSID.Selezionare il numero di VLAN desiderato a cui associare il SSID dall'elenco a discesa.**Nota:** per mantenere il documento entro l'ambito previsto, la sicurezza per un SSID non viene affrontata.Fare clic su **Apply-RadioX** per creare il SSID sulla radio selezionata oppure su **Apply-all** per crearlo su tutte le radio.



In alternativa, dalla CLI, usare i seguenti comandi:

```
AP# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
AP(config)# interface Dot11Radio0
AP(config-if)# ssid Red
AP(config-if-ssid)# vlan 10
AP(config-if-ssid)# end
AP# write memory
```

4. Ripetere i passaggi da 3a a 3d per ogni SSID desiderato o immettere questi comandi dalla CLI con le modifiche appropriate allo SSID.

```
AP# configure terminal
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
AP(config)# interface Dot11Radio0
AP(config-if)# ssid Green
AP(config-if-ssid)# vlan 30
AP(config-if-ssid)# end
AP# write memory
```

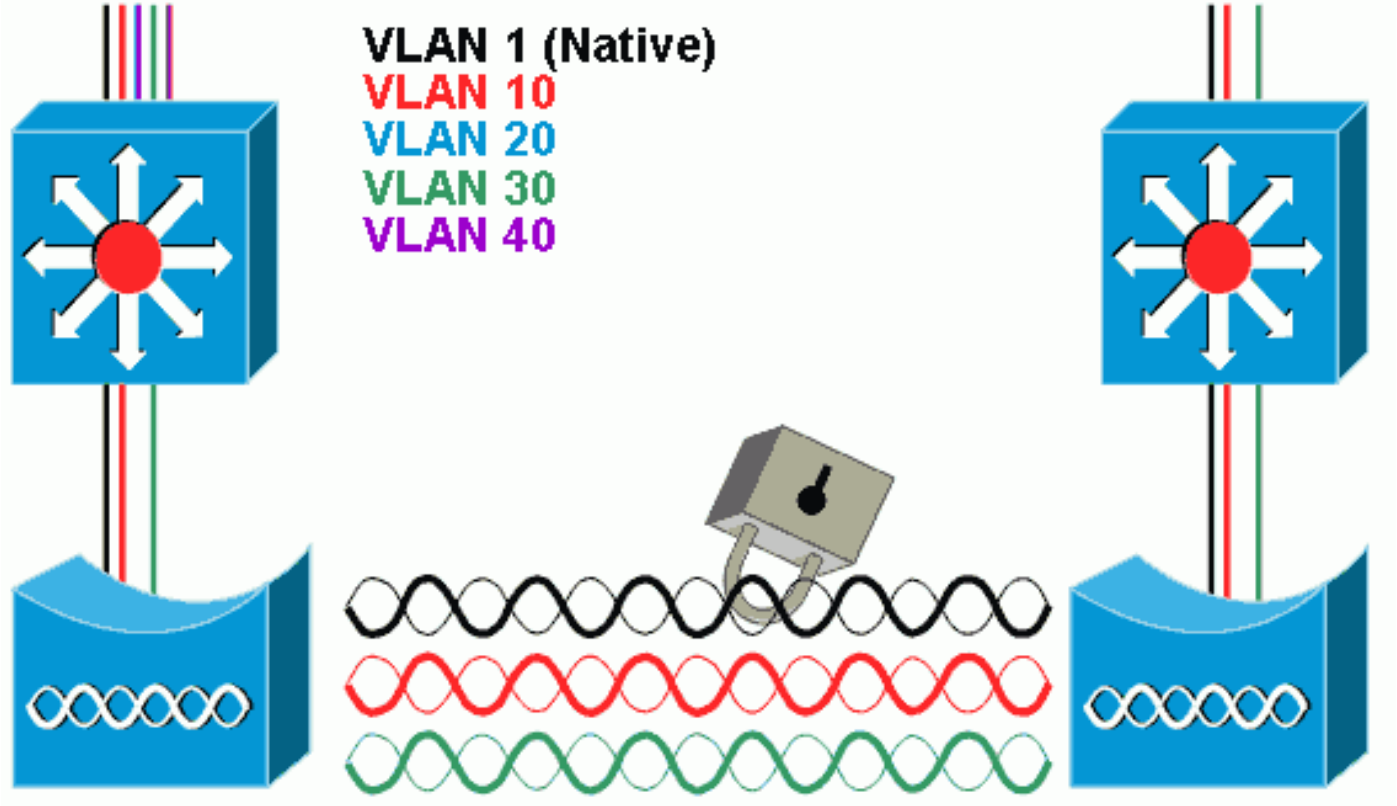
Nota: questi esempi non includono l'autenticazione. Per l'associazione dei client è necessaria una forma di autenticazione (Aperta, Rete-EAP).

VLAN sui bridge

Concetti sui ponti

In questa sezione vengono illustrati i concetti relativi alla distribuzione di VLAN sui bridge e si fa riferimento a questo diagramma di rete.

In questa rete di esempio, la VLAN 1 è la VLAN nativa e esistono le VLAN 10, 20, 30 e 40. Solo le VLAN 10 e 30 vengono estese all'altro lato del collegamento. Il collegamento wireless è crittografato.

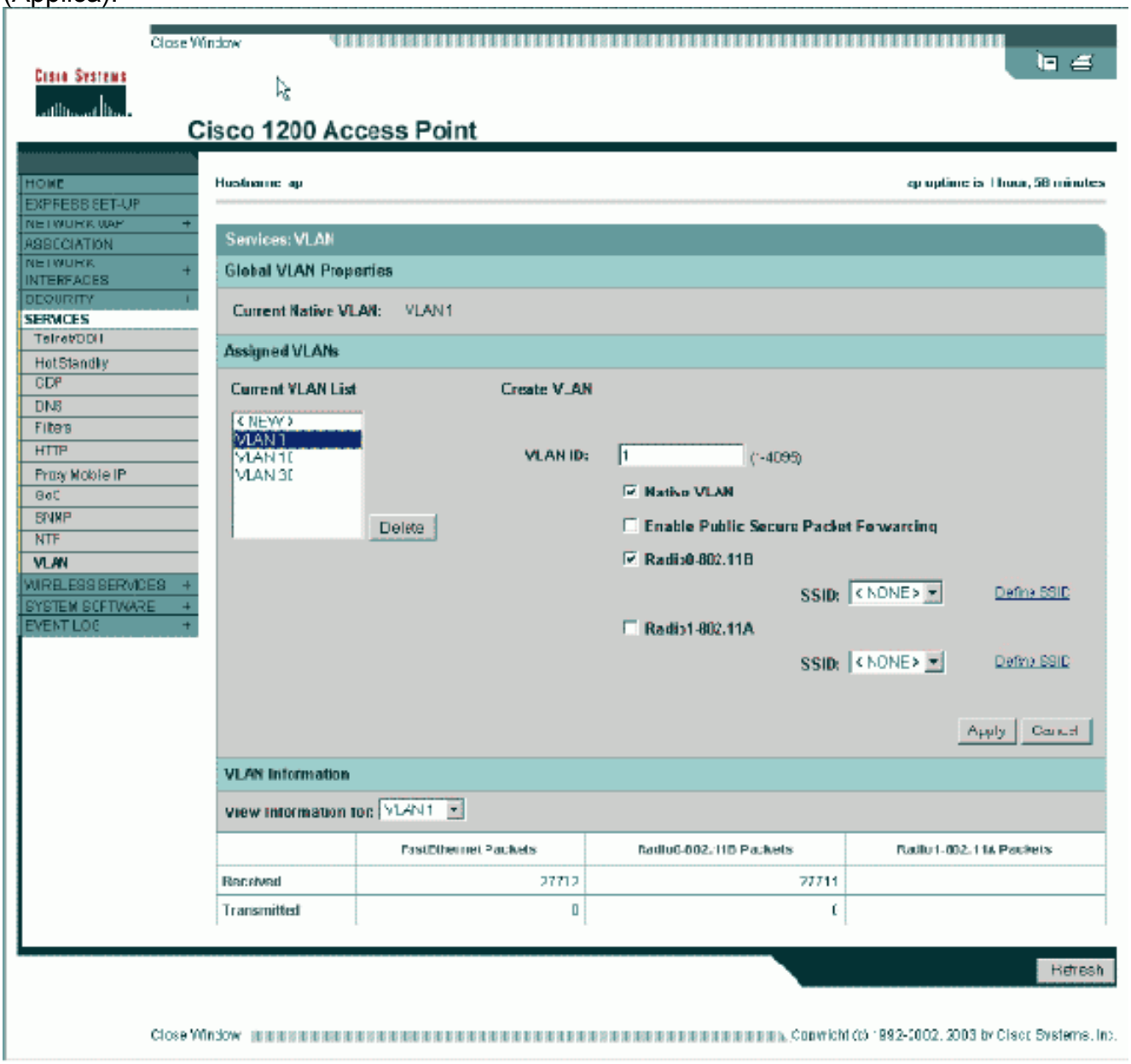


Per crittografare i dati che passano attraverso il collegamento radio, applicare la crittografia solo all'SSID della VLAN nativa. La crittografia viene applicata a tutte le altre VLAN. Quando si crea un bridge, non è necessario associare un SSID separato a ciascuna VLAN. Le configurazioni delle VLAN sono le stesse sui bridge radice e non radice.

Configurazione bridge

Per configurare il bridge per le VLAN, come nel diagramma di rete di esempio, attenersi alla seguente procedura:

1. Dalla GUI dell'access point, fare clic su **Services > VLAN** per selezionare **Services:** pagina **VLAN**.Il primo passaggio consiste nella configurazione della VLAN nativa. A tale scopo, selezionare **<New>** (Nuovo) dall'elenco delle VLAN correnti.Immettere il numero VLAN della VLAN nativa nella casella ID VLAN. Deve corrispondere alla VLAN nativa configurata sullo switch.Poiché l'interfaccia BVI 1 è associata alla sottointerfaccia della VLAN nativa, l'indirizzo IP assegnato all'interfaccia BVI 1 deve trovarsi nella **stessa subnet IP** degli altri dispositivi dell'infrastruttura presenti sulla rete (ad esempio, l'interfaccia SC0 su uno switch Catalyst con CatOS).Selezionare la casella di controllo della VLAN nativa.Fare clic su **Apply** (Applica).

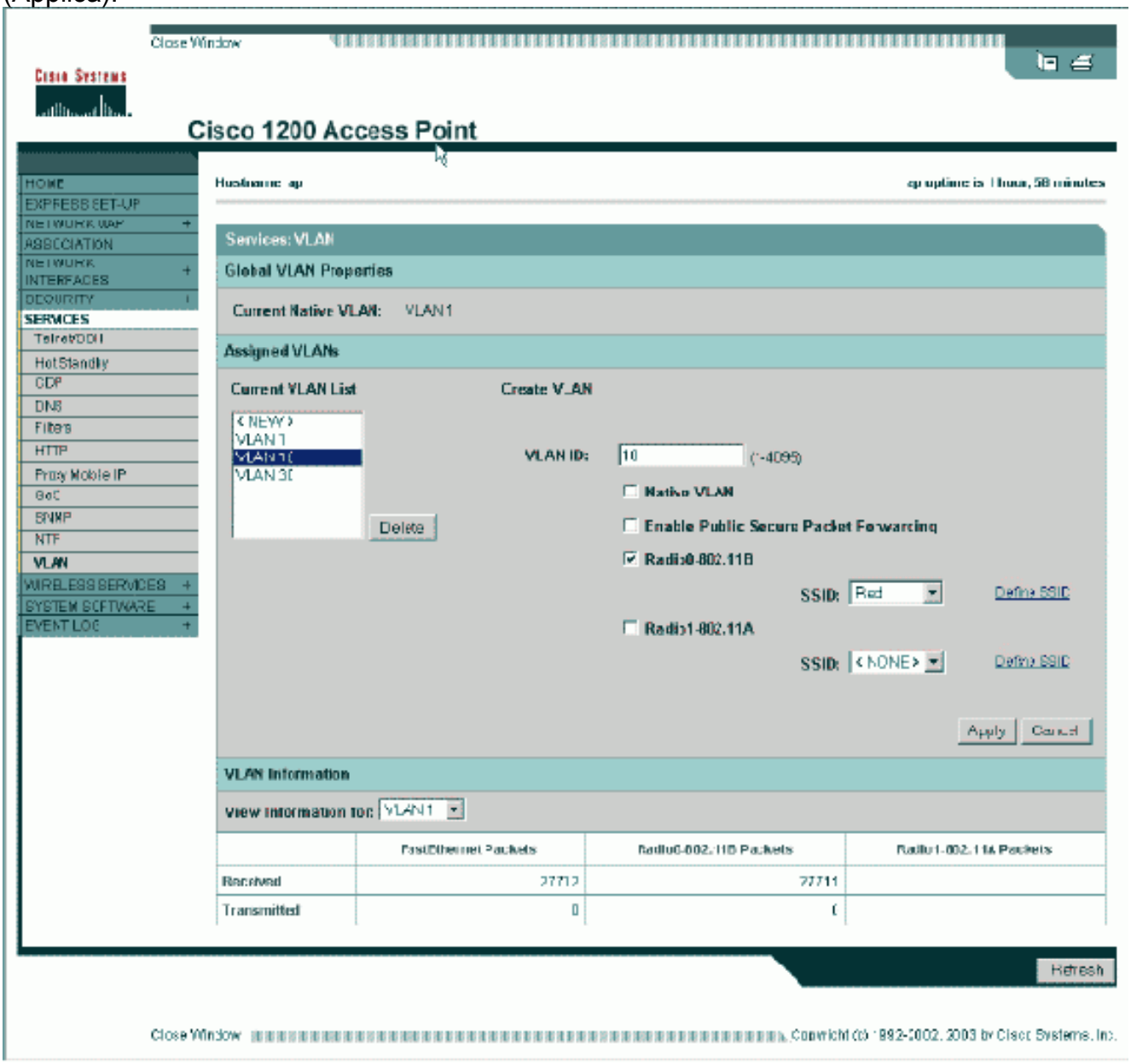


Oppure, dalla CLI, usare questi comandi:

```
bridge# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
bridge(config)# interface Dot11Radio0.1
bridge(config-subif)# encapsulation dot1Q 1 native
bridge(config-subif)# interface FastEthernet0.1
bridge(config-subif)# encapsulation dot1Q 1 native
bridge(config-subif)# end
bridge# write memory
```

2. Per configurare altre VLAN, attenersi alla seguente procedura:Dall'elenco delle VLAN

correnti, selezionare **Nuovo**.Immettere il numero VLAN della VLAN desiderata nella casella ID VLAN. Il numero VLAN deve corrispondere a una VLAN configurata sullo switch.Fare clic su **Apply**
(Applica).



Oppure, dalla CLI, usare questi comandi:

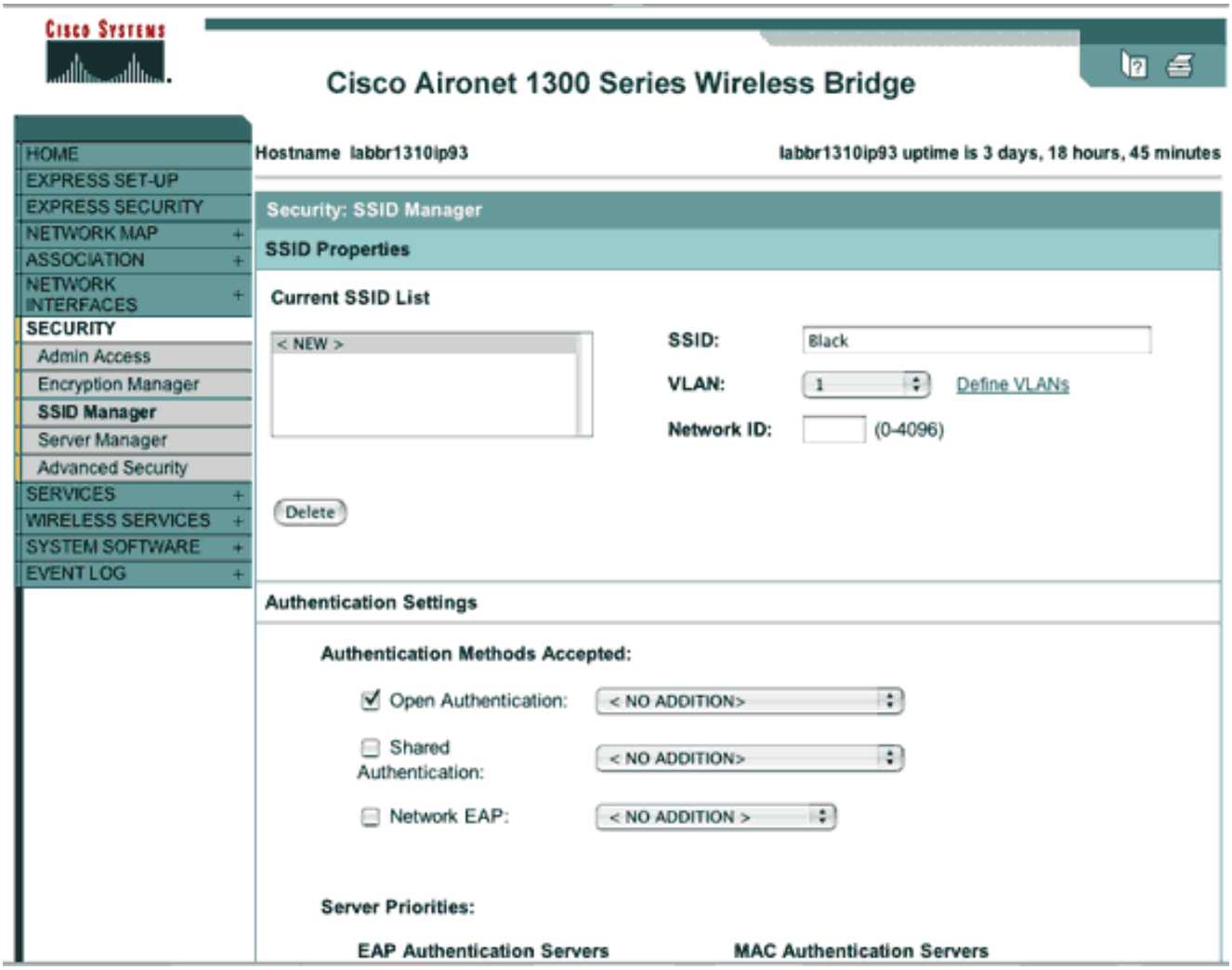
```
bridge# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
bridge(config)# interface Dot11Radio0.10
bridge(config-subif)# encapsulation dot1Q 10
bridge(config-subif)# interface FastEthernet0.10
bridge(config-subif)# encapsulation dot1Q 10
bridge(config-subif)# end
bridge# write memory
```

Ripetere i passaggi da 2a a 2c per ciascuna VLAN desiderata o immettere i comandi dalla CLI con le modifiche appropriate all'interfaccia secondaria e ai numeri di VLAN.

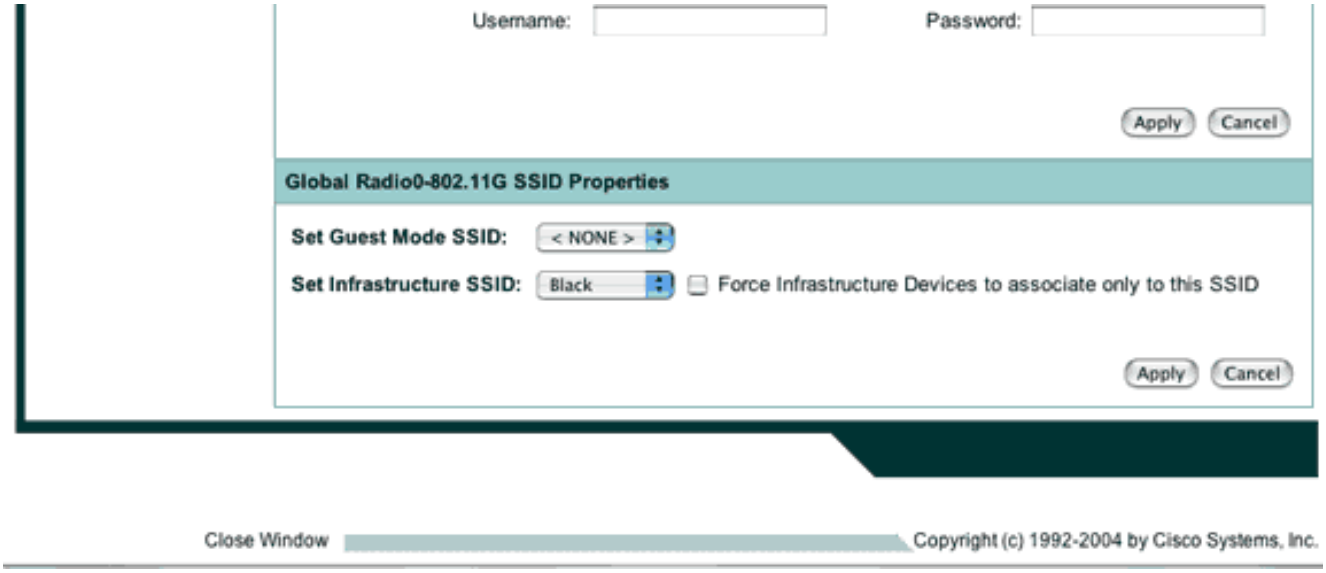
```
AP# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
bridge(config)# interface Dot11Radio0.30
bridge(config-subif)# encapsulation dot1Q 30
bridge(config-subif)# interface FastEthernet0.30
bridge(config-subif)# encapsulation dot1Q 30
```

```
bridge(config-subif)# end
bridge# write memory
```

3. Da Gestione SSID (nella voce di menu **Sicurezza > Gestione SSID**), associare la VLAN nativa a un SSID.**Nota:** quando si crea un bridge, l'unico SSID da associare a una VLAN è quello correlato alla VLAN nativa. È necessario designare questo SSID come SSID infrastruttura.Dall'elenco SSID corrente, selezionare **Nuovo**.Immettere il SSID desiderato (con distinzione tra maiuscole e minuscole) nella casella SSID.Selezionare il numero di VLAN correlato alla VLAN nativa dall'elenco a discesa.**Nota:** per mantenere il documento entro l'ambito previsto, la sicurezza per un SSID non viene affrontata.Fare clic su **Apply** (Applica) per creare l'SSID sulla radio e associarlo alla VLAN nativa.



Scorrere fino alla fine della pagina e in **Proprietà SSID Global Radio0-802.11G** selezionare **SSID** dall'elenco a discesa **Imposta SSID infrastruttura**. Fare clic su **Apply** (Applica).



In alternativa, dalla CLI, usare i seguenti comandi:

```
AP# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
AP(config)# interface Dot11Radio0
AP(config-if)# ssid Black
AP(config-if-ssid)# vlan 1
AP(config-if-ssid)# infrastructure-ssid
AP(config-if-ssid)# end
AP# write memory
```

Nota: quando le VLAN sono in uso, gli SSID sono configurati nell'interfaccia fisica Dot11Radio e non in alcuna sottointerfaccia logica.**Nota:** questo esempio non include l'autenticazione. I bridge radice e non radice richiedono una forma di autenticazione (Open, Network-EAP, ecc.) per essere associati.

Uso di un server RADIUS per assegnare gli utenti alle VLAN

Èpossibile configurare il server di autenticazione RADIUS in modo che assegni utenti o gruppi di utenti a una VLAN specifica quando eseguono l'autenticazione sulla rete. Per informazioni su questa funzione, fare riferimento alla sezione Uso di un server RADIUS per assegnare gli utenti alle VLAN nel documento *Cisco IOS Software Configuration Guide for Cisco Aironet Access Point, 12.4(3g)JA e 12.3(8)JEB*.

Utilizza un server RADIUS per l'assegnazione di gruppi di mobilità dinamica

Èinoltre possibile configurare un server RADIUS per assegnare dinamicamente gruppi di mobilità a utenti o gruppi di utenti. In questo modo non è più necessario configurare più SSID sul punto di accesso. È invece necessario configurare un solo SSID per punto di accesso. Per informazioni su questa funzione, fare riferimento alla sezione Using a RADIUS Server for Dynamic Mobility Group Assignment del documento *Cisco IOS Software Configuration Guide for Cisco Aironet Access Point, 12.4(3g)JA e 12.3(8)JEB*.

Configurazione gruppo di bridge su punti di accesso e bridge

In generale, i gruppi di bridge creano domini di switching segmentati. Il traffico è limitato agli host all'interno di ciascun gruppo di bridge, ma non tra i gruppi di bridge. Lo switch inoltra il traffico solo tra gli host che compongono il gruppo di bridge, limitando il traffico broadcast e multicast (flooding)

solo a quegli host. I gruppi di bridge riducono la congestione della rete e forniscono ulteriore sicurezza di rete quando segmentano il traffico verso alcune aree della rete.

Per informazioni dettagliate, fare riferimento a Panoramica bridging.

In una rete wireless, i gruppi di bridge sono configurati sui punti di accesso e sui bridge wireless in modo che il traffico di dati di una VLAN possa essere trasmesso dai supporti wireless al dispositivo cablato e viceversa.

Eseguire questo passaggio dalla CLI dell'access point per abilitare i gruppi di bridge a livello globale sul punto di accesso/bridge.

In questo esempio viene utilizzato il numero di gruppo-ponte 1.

Ap(configure)#**bridge** ***1***

Nota: è possibile numerare i gruppi di bridge da 1 a 255.

Configurare l'interfaccia radio e l'interfaccia Fast Ethernet del dispositivo wireless in modo che si trovino nello stesso gruppo bridge. In questo modo viene creato un percorso tra queste due interfacce diverse che si trovano nella stessa VLAN ai fini del tagging. Di conseguenza, i dati trasmessi dal lato wireless attraverso l'interfaccia radio vengono trasmessi all'interfaccia Ethernet a cui è collegata la rete cablata e viceversa. In altre parole, le interfacce radio ed Ethernet che appartengono allo stesso gruppo bridge in realtà collegano i dati tra loro.

In un punto di accesso/bridge, è necessario avere un gruppo di bridge per VLAN in modo che il traffico possa passare dal cavo al wireless e viceversa. Maggiore è la VLAN che deve trasmettere il traffico sulla rete wireless, più gruppi di bridge sono necessari.

Ad esempio, se si ha solo una VLAN per trasmettere il traffico dal lato wireless al lato cablato della rete, configurare un solo gruppo di bridge dalla CLI dell'access point/bridge. Se si hanno più VLAN per passare il traffico dal lato wireless a quello cablato e viceversa, configurare i gruppi di bridge per ciascuna VLAN all'interfaccia secondaria radio e all'interfaccia secondaria Fast Ethernet.

1. Configurare il gruppo bridge nell'interfaccia wireless con il comando **bridge group** dot11radio interface.Questo è un esempio.
```
AP# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
AP(config)# interface Dot11Radio0.1
Ap(config-subif)# encapsulation dot1q 1 native
Ap(config-subif)# bridge group 1 !--- Here "1" represents the bridge group number.
ap(config-subif)# exit
```

2. Configurare il gruppo di bridge con lo stesso numero di gruppo di bridge ("1" nell'esempio) nell'interfaccia Fast Ethernet in modo che il traffico della VLAN 1 venga passato dall'interfaccia wireless a questo lato cablato e viceversa.
```
Ap(config)# interface fastEthernet0.1
Ap(config-subif)# encapsulation dot1q 1 native
Ap(config-subif)# bridge group 1 !--- Here "1" represents the bridge group number.
Ap(config-subif)# exit
```

   Nota: quando si configura un gruppo bridge sull'interfaccia radio, questi comandi vengono impostati automaticamente.**bridge-group** ***1*** **subscriber-loop-controlbridge-group** ***1*** **block-**

known-sourcenessun bridge-group *1* source-learningno bridge-group *1* unicast-floodingbridge-group *1* spanning-disabledNota: quando si configura un gruppo bridge sull'interfaccia Fast Ethernet, questi comandi vengono impostati automaticamente.**nessun bridge-group *1* source-learningbridge-group *1* spanning-disabled**

IRB (Integrated Routing and Bridging)

Il routing e il bridging integrati consentono di indirizzare un protocollo specifico tra interfacce con routing e gruppi di bridge o di indirizzare un protocollo specifico tra gruppi di bridge. Il traffico locale o non instradabile può essere collegato tra le interfacce con bridging nello stesso gruppo di bridge, mentre il traffico instradabile può essere indirizzato ad altre interfacce o gruppi di bridge con routing

Con il routing e il bridging integrati è possibile:

- Commutazione di pacchetti da un'interfaccia con bridging a un'interfaccia con routing
- Commutazione di pacchetti da un'interfaccia instradata a un'interfaccia con bridging
- Pacchetti di switch nello stesso gruppo di bridge

Abilitare il protocollo IRB sui punti di accesso wireless e sui bridge per indirizzare il traffico tra gruppi di bridge o tra interfacce instradate e gruppi di bridge. Per effettuare il routing tra i gruppi di bridge o tra i gruppi di bridge e le interfacce con routing, è necessario un router esterno o uno switch di layer 3.

Utilizzare questo comando per abilitare il protocollo IRB nell'access point/bridge.

AP**(configure)#bridge irb**

Il routing e il bridging integrati usano il concetto di interfaccia virtuale bridge-gruppo (BVI) per indirizzare il traffico tra interfacce con routing e gruppi di bridge o tra gruppi di bridge.

Un BVI è un'interfaccia virtuale all'interno del router dello switch di layer 3 che funziona come un'interfaccia di routing normale. Un BVI non supporta il bridging ma in realtà rappresenta il gruppo di bridge corrispondente alle interfacce indirizzate all'interno del router dello switch di layer 3. Dispone di tutti gli attributi a livello di rete (come l'indirizzo e i filtri a livello di rete) che si applicano al gruppo di bridge corrispondente. Il numero di interfaccia assegnato a questa interfaccia virtuale corrisponde al gruppo di bridge rappresentato da questa interfaccia virtuale. Questo numero è il collegamento tra l'interfaccia virtuale e il gruppo di bridge.

Eseguire questa procedura per configurare il BVI sui punti di accesso e sui bridge.

1. Configurare la BVI e assegnare il numero corrispondente del gruppo di bridge alla BVI. In questo esempio viene assegnato il numero di gruppo di bridge 1 al BVI.
   ```
   Ap(configure)#interface BVI 1
   AP(config-if)#ip address 10.1.1.1 255.255.0.0 !--- Assign an IP address to the BVI.
   Ap(config-if)#no shut
   ```

2. Abilitare una BVI ad accettare e indirizzare i pacchetti indirizzabili ricevuti dal suo gruppo di bridge corrispondente.
   ```
   Ap(config)# bridge 1 route ip!---
   !--- This example enables the BVI to accept and route the IP packet.
   ```
   Èimportante capire che è necessaria solo una VLAN di gestione/VLAN nativa in cui si trova l'access point (nell'esempio, VLAN 1). Non è necessario un BVI per altre sottointerfacce, a

prescindere dal numero di VLAN e gruppi di bridge configurati sull'access point/bridge. Infatti, è possibile assegnare un tag al traffico in tutte le altre VLAN (ad eccezione della VLAN nativa) e inviarlo allo switch tramite un'interfaccia trunking dot1q sul lato cablato. Ad esempio, se sulla rete sono presenti 2 VLAN, sono necessari due gruppi di bridge, ma nella rete wireless è sufficiente un solo BVI corrispondente alla VLAN di gestione.Quando si abilita il routing per un determinato protocollo sull'interfaccia virtuale del gruppo di bridge, i pacchetti provenienti da un'interfaccia instradata, ma destinati a un host in un dominio con bridging, vengono instradati all'interfaccia virtuale del gruppo di bridge e vengono inoltrati all'interfaccia con bridging corrispondente.Tutto il traffico instradato all'interfaccia virtuale del gruppo di bridge viene inoltrato al gruppo di bridge corrispondente come traffico con bridging. Tutto il traffico instradabile ricevuto su un'interfaccia con bridging viene instradato ad altre interfacce instradate come se provenisse direttamente dall'interfaccia virtuale del gruppo di bridge.Per ulteriori informazioni sul bridging e l'IRB, consultare il documento sulla configurazione del bridging.

Interazione con gli switch correlati

In questa sezione vengono presentate le informazioni necessarie per configurare o verificare la configurazione degli switch Cisco che si connettono alle apparecchiature wireless Cisco Aironet.

Nota: per ulteriori informazioni sui comandi menzionati in questo documento, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Configurazione switch - Sistema operativo Catalyst

Per configurare uno switch con sistema operativo Catalyst in modo che esegua il trunk delle VLAN su un punto di accesso, la sintassi del comando è set trunk <*modulo #/porta #*> ***sul punto1q*** e **set trunk <*modulo #/porta #*> <*elenco vlan*>**.

Di seguito è riportato un esempio di diagramma di rete:

```
set trunk 2/1 on dot1q
set trunk 2/1 1,10,30
```

Configurazione switch: switch Catalyst basato su IOS

In modalità di configurazione interfaccia, immettere questi comandi se si desidera:

- Configurazione della porta dello switch per il trunk delle VLAN su un punto di accesso
- Su uno switch Catalyst con IOS
- CatIOS include, tra l'altro:6x004x0035 x 0295x

```
switchport mode trunk
switchport trunk encapsulation dot1q
switchport nonegotiate
switchport trunk native vlan 1
switchport trunk allowed vlan add 1,10,30
```

Nota: le apparecchiature wireless Cisco Aironet basate su IOS non supportano il protocollo DTP (Dynamic Trunking Protocol), quindi lo switch non deve tentare di negoziarlo.

Configurazione dello switch - Catalyst 2900XL/3500XL

In modalità di configurazione interfaccia, immettere questi comandi se si desidera configurare la porta dello switch per il trunk delle VLAN su un punto di accesso su uno switch Catalyst 2900XL o 3500XL con IOS:

```
switchport mode trunk
switchport trunk encapsulation dot1q
switchport trunk native vlan 1
switchport trunk allowed vlan 1,10,30
```

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Verifica dell'apparecchiatura wireless

- **show vlan**: visualizza tutte le VLAN attualmente configurate sul punto di accesso e il relativo stato

```
ap#show vlan

Virtual LAN ID:  1 (IEEE 802.1Q Encapsulation)

   vLAN Trunk Interfaces:  FastEthernet0.1
Dot11Radio0.1
Virtual-Dot11Radio0.1

 This is configured as native Vlan for the following interface(s) :
FastEthernet0
Dot11Radio0
Virtual-Dot11Radio0

   Protocols Configured:   Address:          Received:        Transmitted:
        Bridging        Bridge Group 1          36954                  0
        Bridging        Bridge Group 1          36954                  0

Virtual LAN ID:  10 (IEEE 802.1Q Encapsulation)

   vLAN Trunk Interfaces:  FastEthernet0.10
Dot11Radio0.10
Virtual-Dot11Radio0.10

   Protocols Configured:   Address:          Received:        Transmitted:
        Bridging        Bridge Group 10          5297                  0
        Bridging        Bridge Group 10          5297                  0
        Bridging        Bridge Group 10          5297                  0

Virtual LAN ID:  30 (IEEE 802.1Q Encapsulation)

   vLAN Trunk Interfaces:  FastEthernet0.30
Dot11Radio0.30
```

```
Virtual-Dot11Radio0.30

   Protocols Configured:   Address:          Received:        Transmitted:
        Bridging        Bridge Group 30          5290                  0
        Bridging        Bridge Group 30          5290                  0
        Bridging        Bridge Group 30          5290                  0

ap#
```

- **show dot11 association**: visualizza le informazioni sui client associati, per SSID/VLAN

```
ap#show dot11 associations

802.11 Client Stations on Dot11Radio0:

SSID [Green] :

SSID [Red] :

Others:  (not related to any ssid)

ap#
```

Verifica dello switch

- Su uno switch Catalyst basato sul sistema operativo, **show trunk <*modulo #/porta #*>**: visualizza lo stato di un trunk su una determinata porta

```
Console> (enable) show trunk 2/1
* - indicates vtp domain mismatch
Port      Mode         Encapsulation  Status        Native vlan
--------  -----------  -------------  ------------  -----------
 2/1      on           dot1q          trunking      1

Port      Vlans allowed on trunk
--------  ---------------------------------------------------------------
 2/1      1,10,30

Port      Vlans allowed and active in management domain
--------  ---------------------------------------------------------------
 2/1      1,10,30

Port      Vlans in spanning tree forwarding state and not pruned
--------  ---------------------------------------------------------------
 2/1      1,10,30
Console> (enable)
```

- Su uno switch con IOS, **show interface fastethernet <*modulo #/porta #*> trunk** : restituisce lo stato di un trunk su una determinata interfaccia

```
2950g#show interface fastEthernet 0/22 trunk

Port        Mode         Encapsulation  Status        Native vlan
Fa0/22      on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/22      1,10,30

Port        Vlans allowed and active in management domain
Fa0/22      1,10,30

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/22      1,10,30
2950gA#
```

- Su uno switch Catalyst 2900XL/3500XL, **show interface fastethernet <*modulo #/porta #*>**

switchport: visualizza lo stato di un trunk su una determinata interfaccia

```
cat3524xl#show interface fastEthernet 0/22 switchport
Name: Fa0/22
Switchport: Enabled
Administrative mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Disabled
Access Mode VLAN: 0 ((Inactive))
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: 1,10,30,1002-1005
Trunking VLANs Active: 1,10,30
Pruning VLANs Enabled: 2-1001

Priority for untagged frames: 0
Override vlan tag priority: FALSE
Voice VLAN: none
Appliance trust: none
Self Loopback: No
wlan-cat3524xl-a#
```

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Informazioni correlate

- Configurazione delle VLAN (Guida alla configurazione dei punti di accesso)
- Configurazione delle VLAN (Guida alla configurazione del bridge)
- Supporto tecnico Trunking
- Interazione con gli switch correlati
- Requisiti di sistema per l'implementazione del trunking
- Panoramica sul bridging
- Tipi di autenticazione wireless su una configurazione ISR fissa Esempio
- Tipi di autenticazione wireless su ISR fisso tramite configurazione SDM
- Esempio di connettività LAN wireless tramite un ISR con crittografia WEP e autenticazione LEAP
- Esempio di configurazione della connessione base della LAN wireless
- Documentazione e supporto tecnico – Cisco Systems