Verwendung von VLANs mit Cisco Aironet Wireless Equipment

Inhalt

Einführung

Dieses Dokument enthält eine Beispielkonfiguration für die Verwendung virtueller LANs (VLANs) mit Cisco Aironet Wireless-Geräten.

Voraussetzungen

Anforderungen

Stellen Sie sicher, dass Sie diese Anforderungen erfüllen, bevor Sie versuchen, diese Konfiguration durchzuführen:

- Vertrautheit mit Cisco Aironet Wireless-Geräten
- Vertrautheit mit LAN-Switching-Konzepten von VLANs und VLAN-Trunking

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco Aironet Access Points und Wireless Bridges
- Cisco Catalyst-Switches

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Zugehörige Produkte

Sie können die Switch-Seite dieser Konfiguration mit einer der folgenden Hardware oder Software verwenden:

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

Konventionen

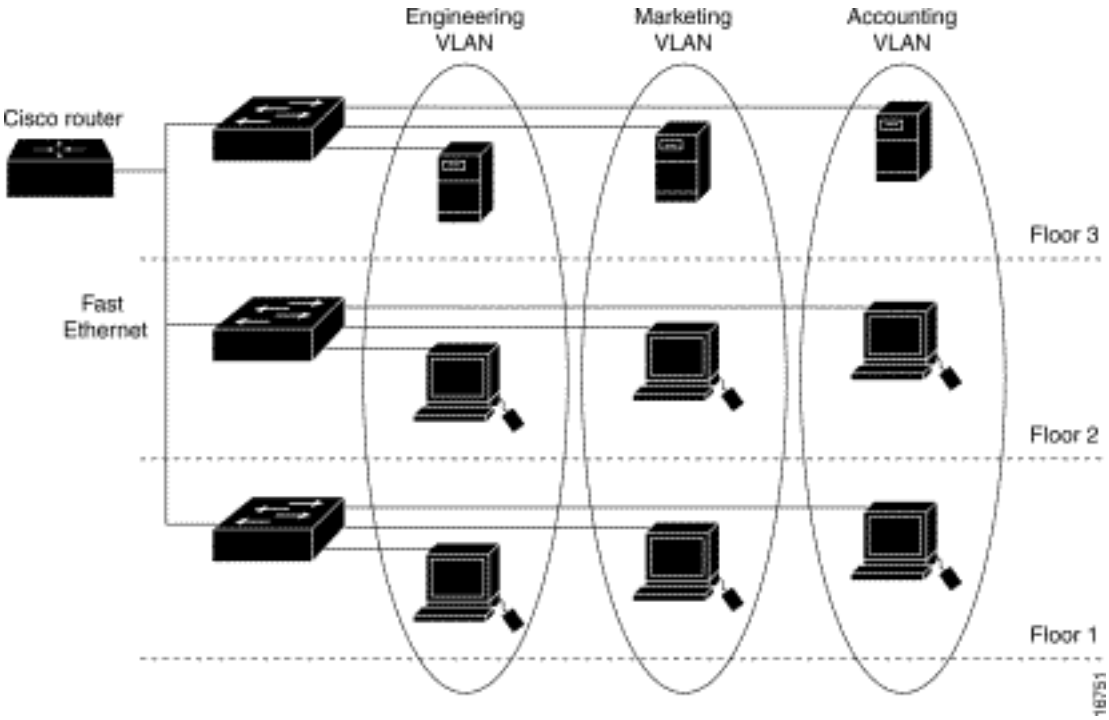
Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

VLANs

Ein VLAN ist ein Switch-Netzwerk, das logisch nach Funktionen, Projektteams oder Anwendungen und nicht auf physischer oder geografischer Basis segmentiert ist. Beispielsweise können alle Workstations und Server, die von einem bestimmten Arbeitsgruppenteam verwendet werden, mit demselben VLAN verbunden werden, unabhängig von ihren physischen Verbindungen zum Netzwerk oder der Möglichkeit, sie mit anderen Teams zu verbinden. Verwenden Sie VLANs, um das Netzwerk mithilfe von Software neu zu konfigurieren, anstatt die Geräte oder Kabel physisch zu trennen oder zu verschieben.

Ein VLAN kann als Broadcast-Domäne betrachtet werden, die innerhalb eines definierten Switch-Satzes existiert. Ein VLAN besteht aus einer Reihe von Endsystemen, entweder Hosts oder Netzwerkgeräte (wie Bridges und Router), die über eine einzige Bridge-Domäne verbunden sind. Die Bridging-Domäne wird von verschiedenen Netzwerkgeräten unterstützt, z. B. LAN-Switches, die Bridging-Protokolle zwischen ihnen mit einer separaten Gruppe für jedes VLAN betreiben.

Wenn Sie ein Gerät mit einem Cisco Catalyst-Switch verbinden, ist der Port, an den das Gerät angeschlossen ist, Teil von VLAN 1. Die MAC-Adresse dieses Geräts ist Teil von VLAN 1. Sie können mehrere VLANs auf einem einzigen Switch definieren und einen Switch-Port auf den meisten Catalyst-Modellen als Mitglied mehrerer VLANs konfigurieren.



Wenn die Anzahl der Ports in einem Netzwerk die Port-Kapazität des Switches übersteigt, müssen Sie mehrere Switch-Chassis miteinander verbinden, was einen Trunk definiert. Der Trunk ist kein Mitglied eines VLANs, sondern ein Kanal, über den der Datenverkehr für ein oder mehrere VLANs geleitet wird.

Grundsätzlich ist bei der Konfiguration eines Access Points für die Verbindung zu einem bestimmten VLAN die Konfiguration der SSID zur Erkennung dieses VLAN entscheidend. Da VLANs durch eine VLAN-ID oder einen Namen identifiziert werden, folgt daraus, dass eine Verbindung zum VLAN hergestellt wird, wenn die SSID eines Access Points so konfiguriert ist, dass sie eine bestimmte VLAN-ID oder einen bestimmten Namen erkennt. Wenn diese Verbindung hergestellt wird, können verknüpfte Wireless-Client-Geräte mit derselben SSID über den Access Point auf das VLAN zugreifen. Das VLAN verarbeitet Daten zu und von den Clients auf die gleiche Weise, wie Daten von und zu kabelgebundenen Verbindungen verarbeitet werden. Sie können bis zu 16 SSIDs auf Ihrem Access Point konfigurieren, sodass Sie bis zu 16 VLANs unterstützen können. Sie können einem VLAN nur eine SSID zuweisen.

Sie erweitern VLANs in ein WLAN, wenn Sie dem Access Point IEEE 802.11Q-Tag-Erkennung hinzufügen. Frames, die für verschiedene VLANs bestimmt sind, werden vom Access Point drahtlos auf verschiedenen SSIDs mit unterschiedlichen WEP-Schlüsseln übertragen. Nur die Clients, die diesem VLAN zugeordnet sind, empfangen diese Pakete. Pakete, die von einem Client stammen, der einem bestimmten VLAN zugeordnet ist, werden dagegen 802.11Q-markiert, bevor sie an das kabelgebundene Netzwerk weitergeleitet werden.

So können Mitarbeiter und Gäste gleichzeitig auf das Wireless-Netzwerk eines Unternehmens zugreifen und vom Administrator getrennt sein. Ein VLAN ist einer SSID zugeordnet, und der Wireless-Client wird der entsprechenden SSID zugeordnet. In Netzwerken mit Wireless Bridges können Sie mehrere VLANs über die Wireless-Verbindung weiterleiten, um die Verbindung zu einem VLAN von verschiedenen Standorten aus bereitzustellen.

Wenn 802.1q auf der FastEthernet-Schnittstelle eines Access Points konfiguriert ist, sendet der Access Point immer Keepalives für VLAN1, auch wenn VLAN 1 auf dem Access Point nicht definiert ist. Der Ethernet-Switch stellt somit eine Verbindung zum Access Point her und sendet eine Warnmeldung. Weder am Access Point noch am Switch gehen Funktionen verloren, aber das Switch-Protokoll enthält bedeutungslose Meldungen, die dazu führen können, dass wichtigere Meldungen umbrochen und nicht angezeigt werden.

Dieses Verhalten verursacht ein Problem, wenn alle SSIDs eines Access Points mit Mobilitätsnetzwerken verknüpft sind. Wenn alle SSIDs mit Mobilitätsnetzwerken verbunden sind, kann der Ethernet-Switch-Port, mit dem der Access Point verbunden ist, als Access-Port konfiguriert werden. Der Zugriffsport wird normalerweise dem nativen VLAN des Access Points zugewiesen, das nicht unbedingt VLAN1 ist. Dadurch generiert der Ethernet-Switch Warnmeldungen, die darauf hinweisen, dass Datenverkehr mit einem 802.1q-Tag vom Access Point gesendet wird.

Wenn Sie die Keepalive-Funktion deaktivieren, können Sie übermäßige Meldungen auf dem Switch entfernen.

Wenn Sie bei der Bereitstellung von VLANs mit Cisco Aironet Wireless-Geräten unbedeutende Punkte in diesen Konzepten ignorieren, können Sie beispielsweise von einer unerwarteten Leistung profitieren:

- Es wurden keine zulässigen VLANs auf dem Trunk auf die auf dem Wireless-Gerät definierten VLANs beschränkt.Wenn am Switch die VLANs 1, 10, 20, 30 und 40 definiert sind, aber nur die VLANs 1, 10 und 30 auf den Wireless-Geräten definiert sind, müssen die anderen vom Trunk-Switch-Port entfernt werden.
- Missbrauch der Benennung von Infrastruktur-SSIDWenn Sie Access Points installieren, weisen Sie die Infrastruktur-SSID nur dann zu, wenn Sie eine SSID verwenden:Workgroup Bridge-GeräteRepeater Access PointsNicht-Root-BridgesEs ist eine Fehlkonfiguration, die Infrastruktur-SSID für eine SSID festzulegen, bei der ausschließlich Wireless-Laptop-Computer für Clients verwendet werden, und führt zu unvorhersehbaren Ergebnissen.In Bridge-Installationen kann nur eine Infrastruktur-SSID verwendet werden. Bei der Infrastruktur-SSID muss es sich um die SSID handeln, die mit dem nativen VLAN korreliert.
- Missbrauch oder falsches Design der SSID-Kennzeichnung für den GastmodusWenn Sie mehrere SSIDs/VLANs auf Cisco Aironet Wireless-Geräten definieren, kann eine (1) SSID als Gast-Modus-SSID mit dem SSID-Broadcast in 802.11-Funkbaken zugewiesen werden. Die anderen SSIDs werden nicht übertragen. Die Client-Geräte müssen angeben, welche SSID angeschlossen werden soll.
- Keine Erkennung, dass mehrere VLANs und SSIDs auf mehrere Layer-3-Subnetze des OSI-Modells hinweisenVeraltete Versionen der Cisco Aironet-Software ermöglichen das Binden mehrerer SSIDs an ein VLAN. Aktuelle Versionen nicht.
- Layer-3-Routing-Fehler des OSI-Modells oder falsche DesignsJeder SSID und sein verknüpftes VLAN müssen über ein Routing-Gerät und eine Quelle verfügen, um Clients zu adressieren, z. B. einen DHCP-Server oder den Bereich auf einem DHCP-Server.
- Natives VLAN wird falsch verstanden oder falsch konfiguriertDie Router und Switches, aus denen sich die physische Infrastruktur eines Netzwerks zusammensetzt, werden anders verwaltet als die Client-PCs, die mit dieser physischen Infrastruktur verbunden sind. Das VLAN, zu dem diese Router- und Switch-Schnittstellen gehören, wird als natives VLAN (standardmäßig VLAN 1) bezeichnet. Client-PCs gehören einem anderen VLAN an, genau wie IP-Telefone einem anderen VLAN angehören. Die Verwaltungsschnittstelle des Access

Points oder der Bridge (Schnittstelle BVI1) wird als Teil des nativen VLAN betrachtet und nummeriert, unabhängig davon, welche VLANs oder SSIDs das Wireless-Gerät passieren.

Bedeutung des nativen VLAN

Wenn Sie einen IEEE 802.1Q-Trunk-Port verwenden, werden alle Frames mit Ausnahme der Frames im VLAN markiert, die als "natives VLAN" für den Port konfiguriert sind. Frames im nativen VLAN werden immer unmarkiert übertragen und werden normalerweise unmarkiert empfangen. Wenn also ein AP mit dem Switch-Port verbunden ist, muss das auf dem AP konfigurierte native VLAN mit dem auf dem Switch-Port konfigurierten nativen VLAN übereinstimmen.

Hinweis: Wenn in den nativen VLANs eine Diskrepanz auftritt, werden die Frames verworfen.

Dieses Szenario wird mit einem Beispiel besser erläutert. Wenn das native VLAN auf dem Switch-Port als VLAN 12 konfiguriert ist und auf dem WAP, wird das native VLAN als VLAN 1 konfiguriert. Wenn der WAP dann einen Frame auf seinem nativen VLAN an den Switch sendet, betrachtet der Switch den Frame als zu VLAN 12 zugehörig, da die Frames aus dem nativen VLAN des WAP nicht markiert sind. Dies führt zu Verwirrung im Netzwerk und zu Verbindungsproblemen. Das Gleiche geschieht, wenn der Switch-Port einen Frame von seinem nativen VLAN an den AP weiterleitet.

Die Konfiguration nativer VLANs ist umso wichtiger, wenn Sie im Wireless-Netzwerk einen Repeater-WAP einrichten. Sie können auf den Repeater-APs nicht mehrere VLANs konfigurieren. Repeater-APs unterstützen nur das native VLAN. Aus diesem Grund muss die native VLAN-Konfiguration auf dem Root-AP, dem Switch-Port, mit dem der AP verbunden ist, und dem Repeater-AP identisch sein. Andernfalls wird der durch den Switch laufende Datenverkehr nicht an den und vom Repeater-AP weitergeleitet.

Ein Beispiel für ein Szenario, in dem die Diskrepanz in der nativen VLAN-Konfiguration des Repeater-AP Probleme verursachen kann, ist der DHCP-Server hinter dem Switch, mit dem der Root-Access-Point verbunden ist. In diesem Fall erhalten die Clients, die dem Repeater-AP zugeordnet sind, keine IP-Adresse vom DHCP-Server, da die Frames (in unserem Fall DHCP-Anfragen) vom nativen VLAN des Repeater-AP (das nicht mit dem Root-Access-Point und dem Switch identisch ist) verworfen werden.

Wenn Sie den Switch-Port konfigurieren, *stellen Sie* außerdem sicher, *dass alle VLANs, die auf den APs konfiguriert sind, für den Switch-Port zugelassen sind.* Wenn beispielsweise die VLANs 6, 7 und 8 im WAP (Wireless Network) vorhanden sind, müssen die VLANs auf dem Switch-Port zugelassen werden. Dies kann mithilfe des folgenden Befehls im Switch erfolgen:

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

Standardmäßig ermöglicht ein als Trunk konfigurierter Switch-Port allen VLANs, den Trunk-Port zu passieren. Weitere Informationen zur Konfiguration des Switch-Ports finden Sie unter Interaktion mit verwandten Switches.

Hinweis: In einigen Fällen kann es auch zu Problemen kommen, wenn alle VLANs am Access Point zugelassen werden, insbesondere wenn es sich um ein großes Netzwerk handelt. Dies kann zu einer hohen CPU-Auslastung der APs führen. Bereinigen Sie die VLANs am Switch, sodass nur der VLAN-Datenverkehr, an dem der WAP interessiert ist, den WAP durchläuft, um eine hohe

CPU zu vermeiden.

VLANs auf Access Points

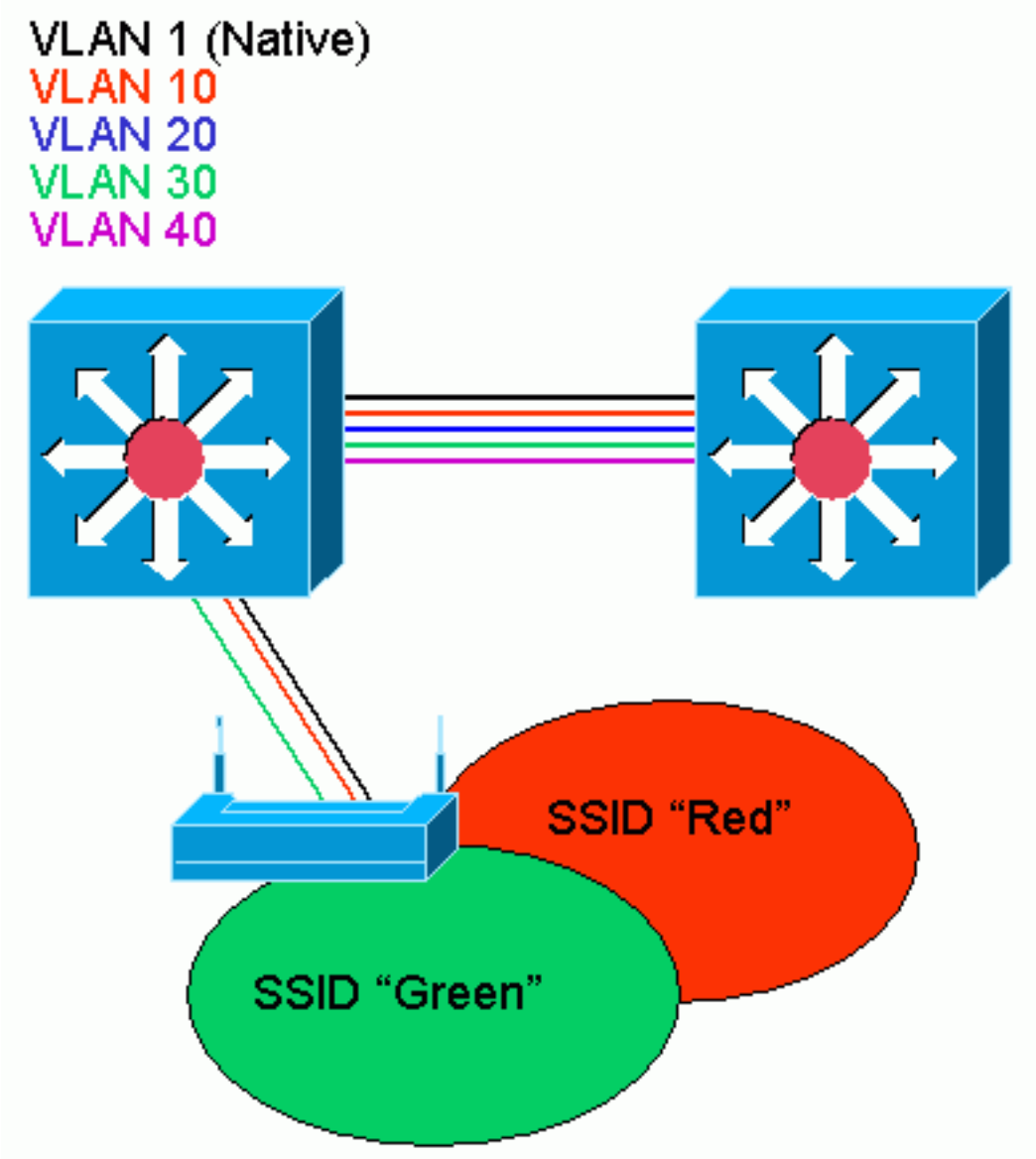
In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Hinweis: Um weitere Informationen zu den in diesem Dokument verwendeten Befehlen zu erhalten, verwenden Sie das Command Lookup Tool (nur registrierte Kunden).

Konzepte mit Access Points

In diesem Abschnitt werden Konzepte zur Bereitstellung von VLANs an Access Points erläutert. Außerdem wird auf dieses Netzwerkdiagramm verwiesen.

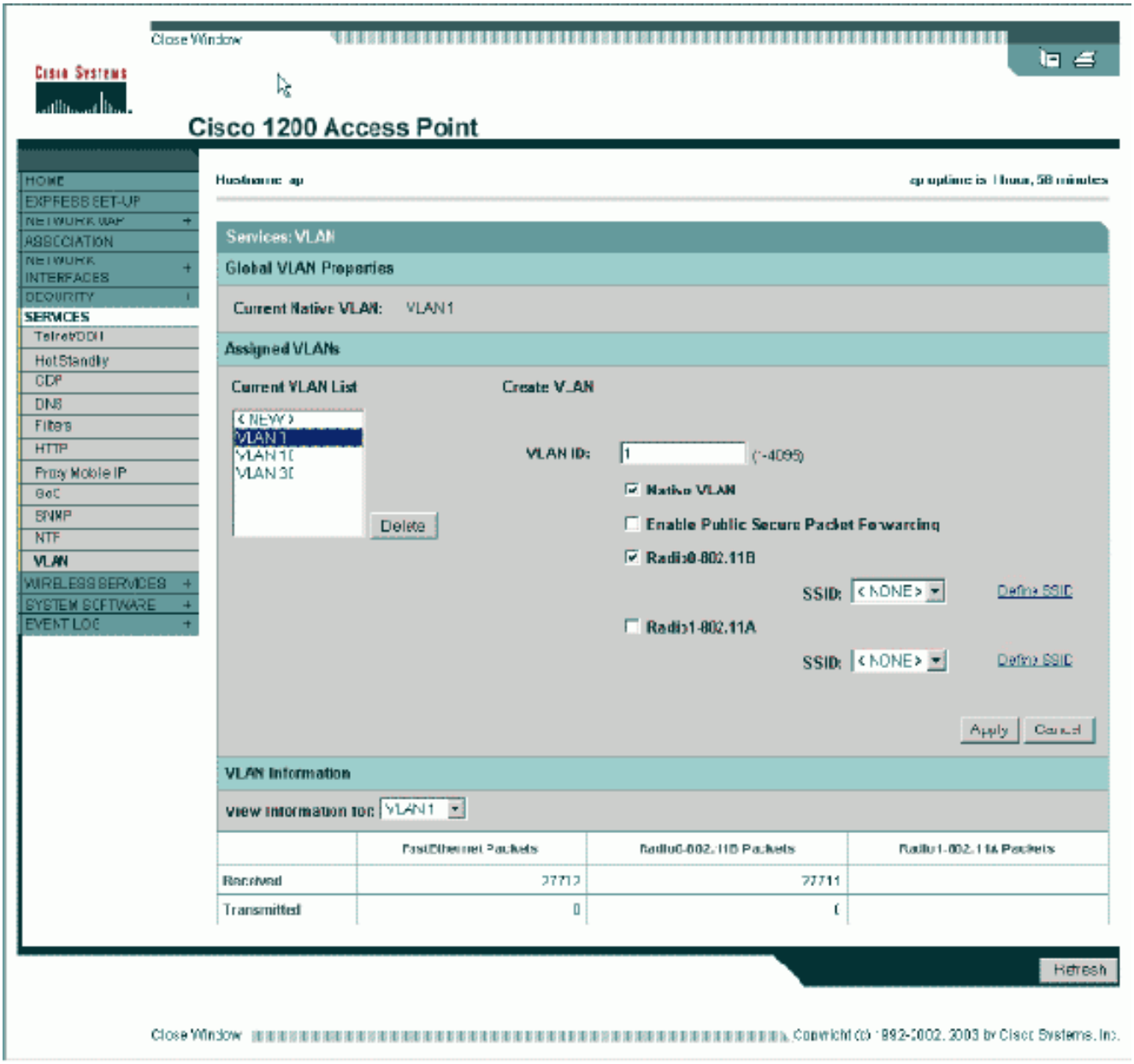
In diesem Beispielnetzwerk handelt es sich bei VLAN 1 um das native VLAN, und die VLANs 10, 20, 30 und 40 sind vorhanden und werden mit einem anderen Switch-Chassis verbunden. Nur die VLANs 10 und 30 werden in die Wireless-Domäne erweitert. Das native VLAN ist erforderlich, um Verwaltungsfunktionen und Client-Authentifizierungen bereitzustellen.



Access Point-Konfiguration

Gehen Sie wie folgt vor, um den Access Point für VLANs zu konfigurieren:

1. Klicken Sie in der AP-GUI auf Services > VLAN, um zu den **Services** zu navigieren: **VLAN-**Seite .Der erste Schritt besteht in der Konfiguration des nativen VLANs. Wählen Sie aus der aktuellen VLAN-Liste die Option **Neu**.Geben Sie im Feld VLAN ID (VLAN-ID) die VLAN-Nummer des nativen VLAN ein. Die VLAN-Nummer muss mit dem auf dem Switch konfigurierten nativen VLAN übereinstimmen.Da die Schnittstelle BVI 1 der Subschnittstelle des nativen VLAN zugeordnet ist, muss sich die der Schnittstelle BVI 1 zugewiesene IP-Adresse im **gleichen IP-Subnetz befinden** wie andere Infrastrukturgeräte im Netzwerk (d. h. die Schnittstelle SC0 auf einem Catalyst-Switch, der CatOS ausführt).Aktivieren Sie das Kontrollkästchen für das native VLAN.Aktivieren Sie Kontrollkästchen für die Funkschnittstelle oder Schnittstellen, auf die dieses VLAN angewendet wird.Klicken Sie auf **Übernehmen**.

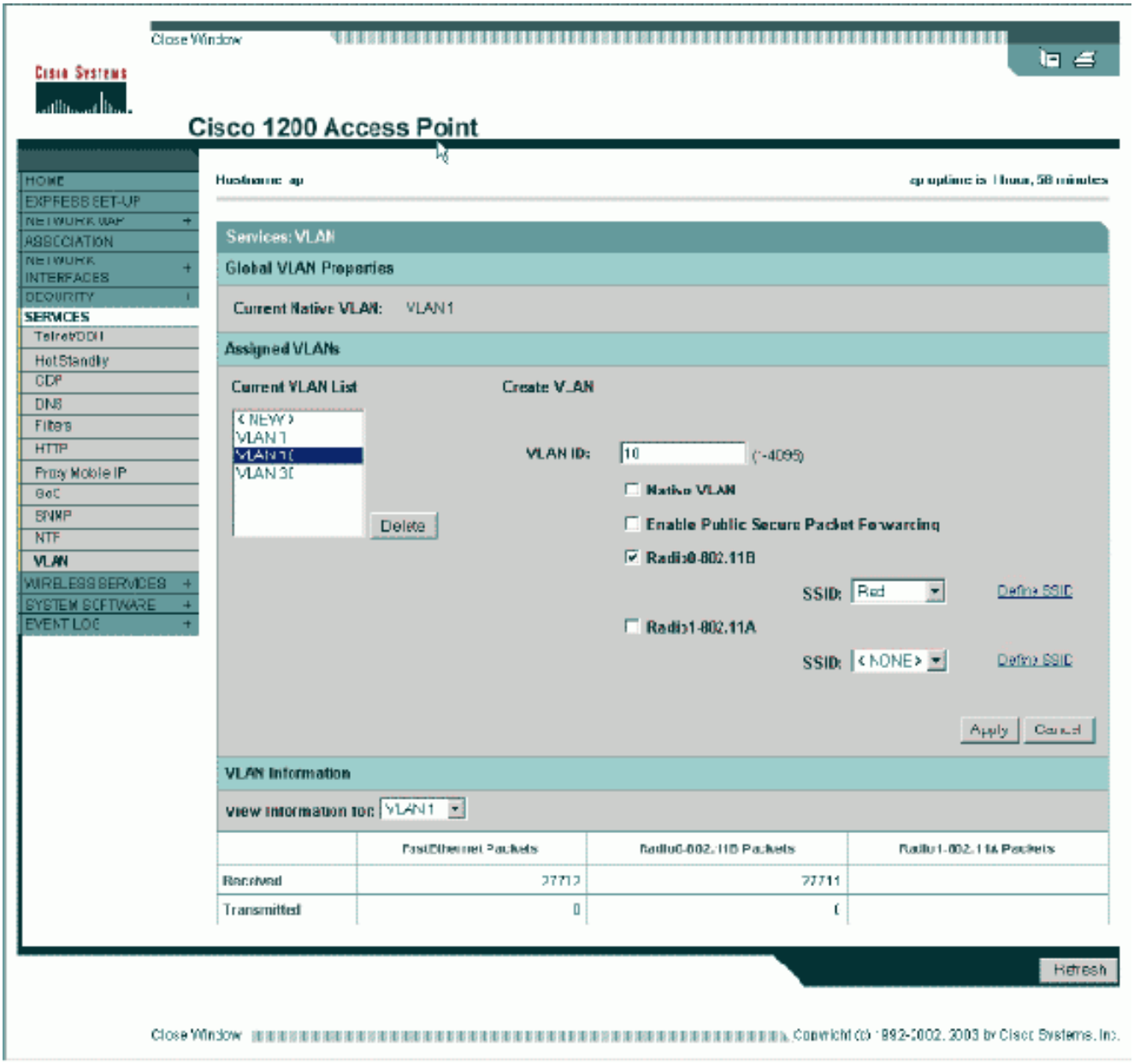


Oder geben Sie über die CLI die folgenden Befehle aus:

```
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. Um andere VLANs zu konfigurieren, gehen Sie wie folgt vor:Wählen Sie aus der aktuellen VLAN-Liste die Option **Neu**.Geben Sie im Feld VLAN ID (VLAN-ID) die VLAN-Nummer des gewünschten VLAN ein. Die VLAN-Nummer muss mit einem auf dem Switch konfigurierten VLAN übereinstimmen.Aktivieren Sie Kontrollkästchen für die Funkschnittstelle oder Schnittstellen, auf die dieses VLAN angewendet wird.Klicken Sie auf **Übernehmen**.



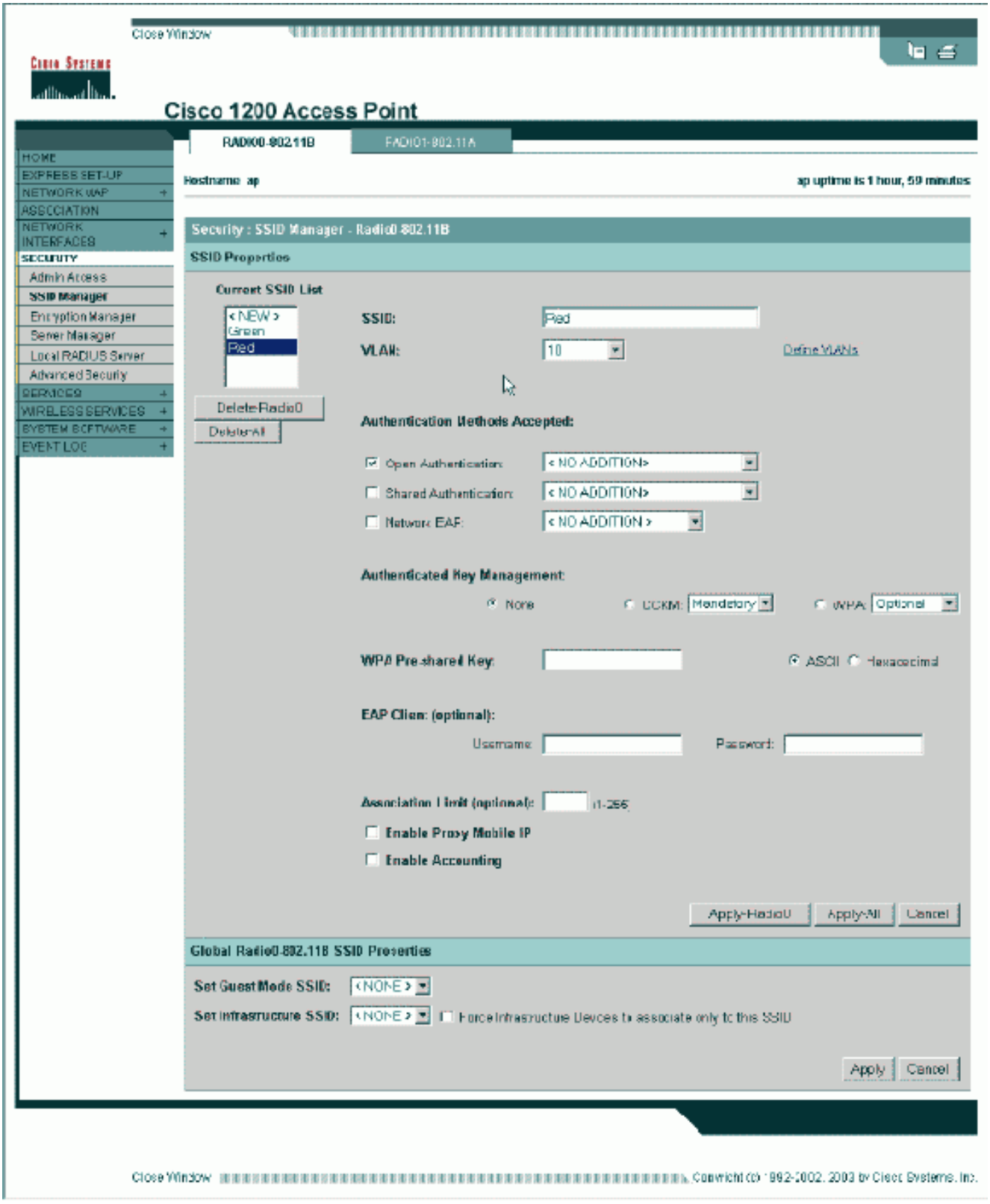
Oder geben Sie über die CLI die folgenden Befehle aus:

```
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
```

Wiederholen Sie die Schritte 2a bis 2d für jedes gewünschte VLAN, oder geben Sie diese Befehle über die CLI ein, wobei die Subschnittstelle und die VLAN-Nummern entsprechend geändert werden müssen:

```
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. Im nächsten Schritt werden die konfigurierten VLANs den SSIDs zugeordnet. Klicken Sie dazu auf **Sicherheit > SSID Manager**.**Hinweis:** Sie müssen nicht jedes auf dem Access Point definierte VLAN einer SSID zuordnen. Aus Sicherheitsgründen wird beispielsweise bei den meisten Access Point-Installationen keine SSID mit dem nativen VLAN verknüpft.Um eine neue SSID zu erstellen, wählen Sie **Neu**.Geben Sie die gewünschte SSID (Groß- und Kleinschreibung beachten) in das Feld SSID ein.Wählen Sie aus der Dropdown-Liste die gewünschte VLAN-Nummer aus, mit der diese SSID verknüpft werden soll.**Hinweis:** Um dieses Dokument im vorgesehenen Umfang zu behalten, wird die Sicherheit für eine SSID nicht berücksichtigt.Klicken Sie auf **Apply-RadioX**, um die SSID im ausgewählten Funkmodul zu erstellen, oder **Apply-all** (Alle anwenden), um sie auf allen Funkmodulen zu erstellen.



Führen Sie darüber hinaus folgende Befehle aus:

```
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. Wiederholen Sie die Schritte 3a bis 3d für jede gewünschte SSID, oder geben Sie diese Befehle über die CLI mit den entsprechenden Änderungen an der SSID ein.

```
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
```

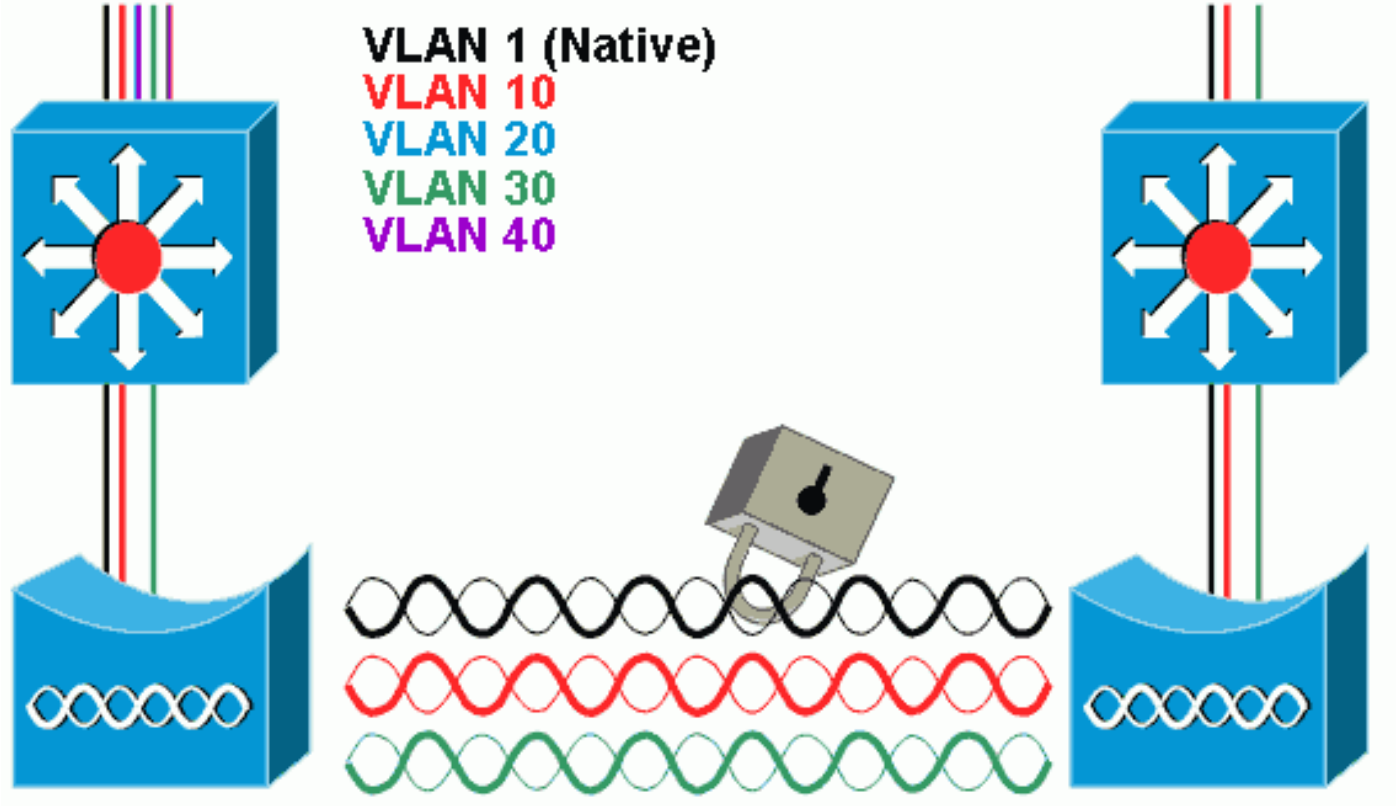
Hinweis: In diesen Beispielen ist keine Authentifizierung enthalten. Für die Zuordnung von Clients ist eine Authentifizierungsform (Open, Network-EAP) erforderlich.

VLANs auf Bridges

Konzepte zu Bridges

In diesem Abschnitt werden Konzepte zur Bereitstellung von VLANs auf Bridges erläutert. Außerdem wird auf dieses Netzwerkdiagramm verwiesen.

In diesem Beispielnetzwerk ist VLAN 1 das native VLAN, und die VLANs 10, 20, 30 und 40 sind vorhanden. Nur die VLANs 10 und 30 werden auf die andere Seite der Verbindung erweitert. Die Wireless-Verbindung ist verschlüsselt.

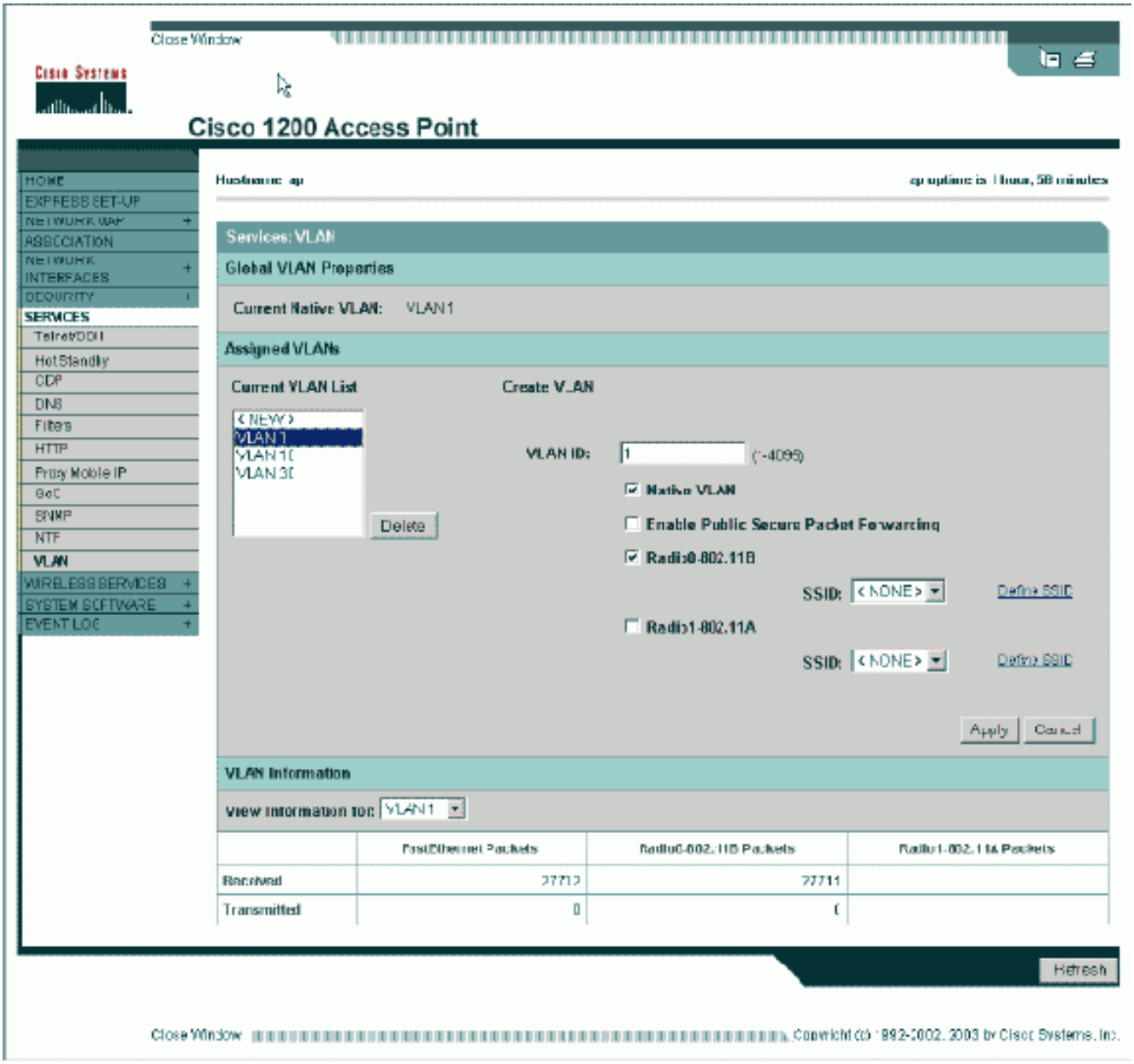


Um Daten zu verschlüsseln, die über die Funkverbindung übertragen werden, wenden Sie die Verschlüsselung nur auf die SSID des nativen VLAN an. Diese Verschlüsselung gilt für alle anderen VLANs. Bei der Bridge muss keinem VLAN ein separater SSID zugewiesen werden. Die VLAN-Konfigurationen sind auf den Root- und Nicht-Root-Bridges identisch.

Bridge-Konfiguration

Führen Sie zum Konfigurieren der Bridge für VLANs wie im Beispiel des Netzwerkdiagramms die folgenden Schritte aus:

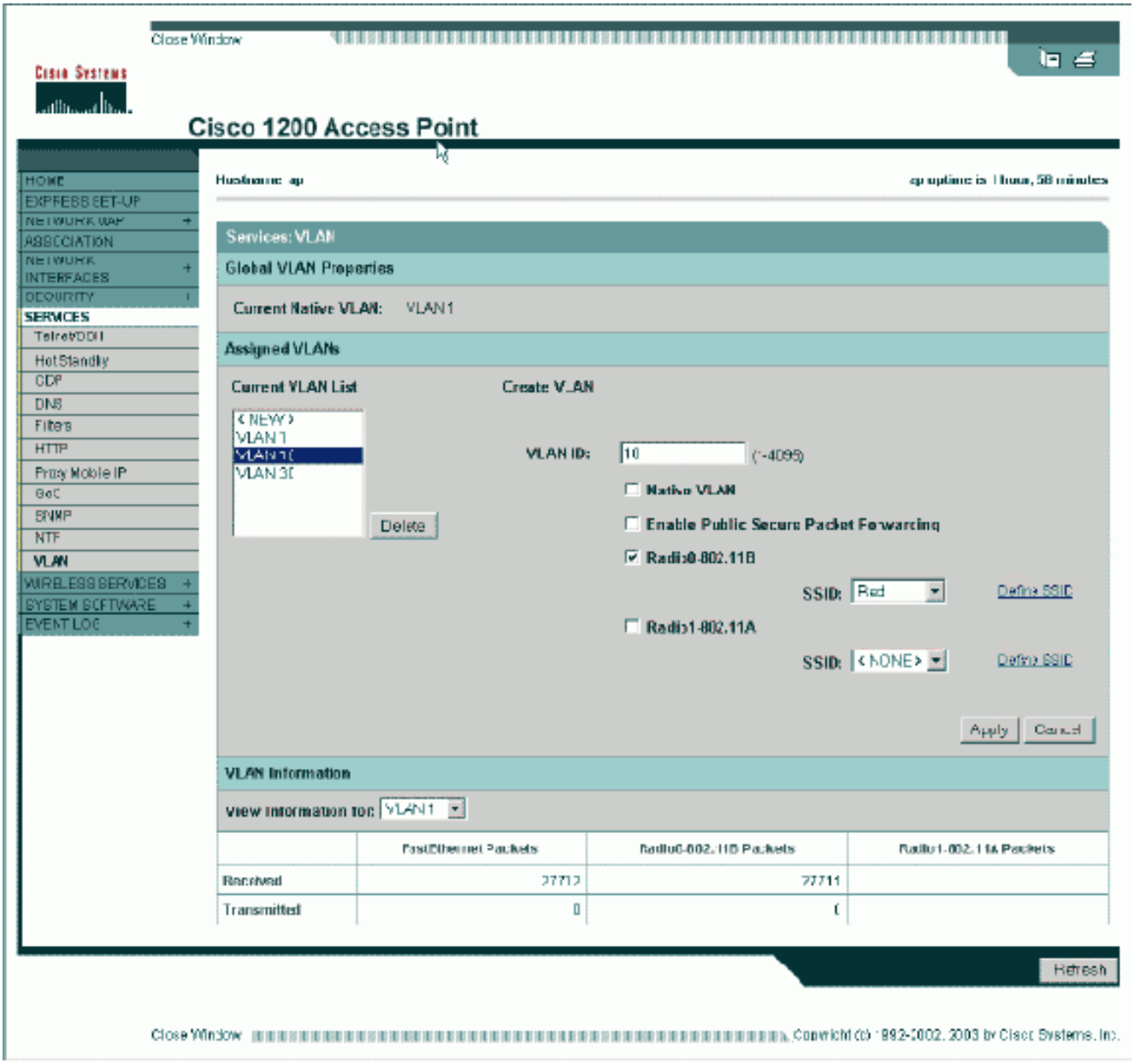
1. Klicken Sie in der AP-GUI auf **Services > VLAN**, um zu den **Services** zu navigieren**: VLAN-**SeiteDer erste Schritt besteht in der Konfiguration des nativen VLANs. Wählen Sie dazu **<Neu>** aus der Liste Aktuelles VLAN aus.Geben Sie im Feld VLAN ID (VLAN-ID) die VLAN-Nummer des nativen VLAN ein. Dies muss mit dem auf dem Switch konfigurierten nativen VLAN übereinstimmen.Da Schnittstelle BVI 1 der Subschnittstelle des nativen VLAN zugeordnet ist, muss sich die der Schnittstelle BVI 1 zugewiesene IP-Adresse im **gleichen IP-Subnetz** wie andere Infrastrukturgeräte im Netzwerk befinden (d. h. Schnittstelle SC0 auf einem Catalyst-Switch, der CatOS ausführt).Aktivieren Sie das Kontrollkästchen für das native VLAN.Klicken Sie auf **Übernehmen**.



Oder geben Sie über die CLI die folgenden Befehle aus:

```
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. Um andere VLANs zu konfigurieren, gehen Sie wie folgt vor:Wählen Sie aus der aktuellen VLAN-Liste die Option **Neu**.Geben Sie im Feld VLAN ID (VLAN-ID) die VLAN-Nummer des gewünschten VLAN ein. Die VLAN-Nummer muss mit einem auf dem Switch konfigurierten VLAN übereinstimmen.Klicken Sie auf **Übernehmen**.



Oder geben Sie über die CLI die folgenden Befehle aus:

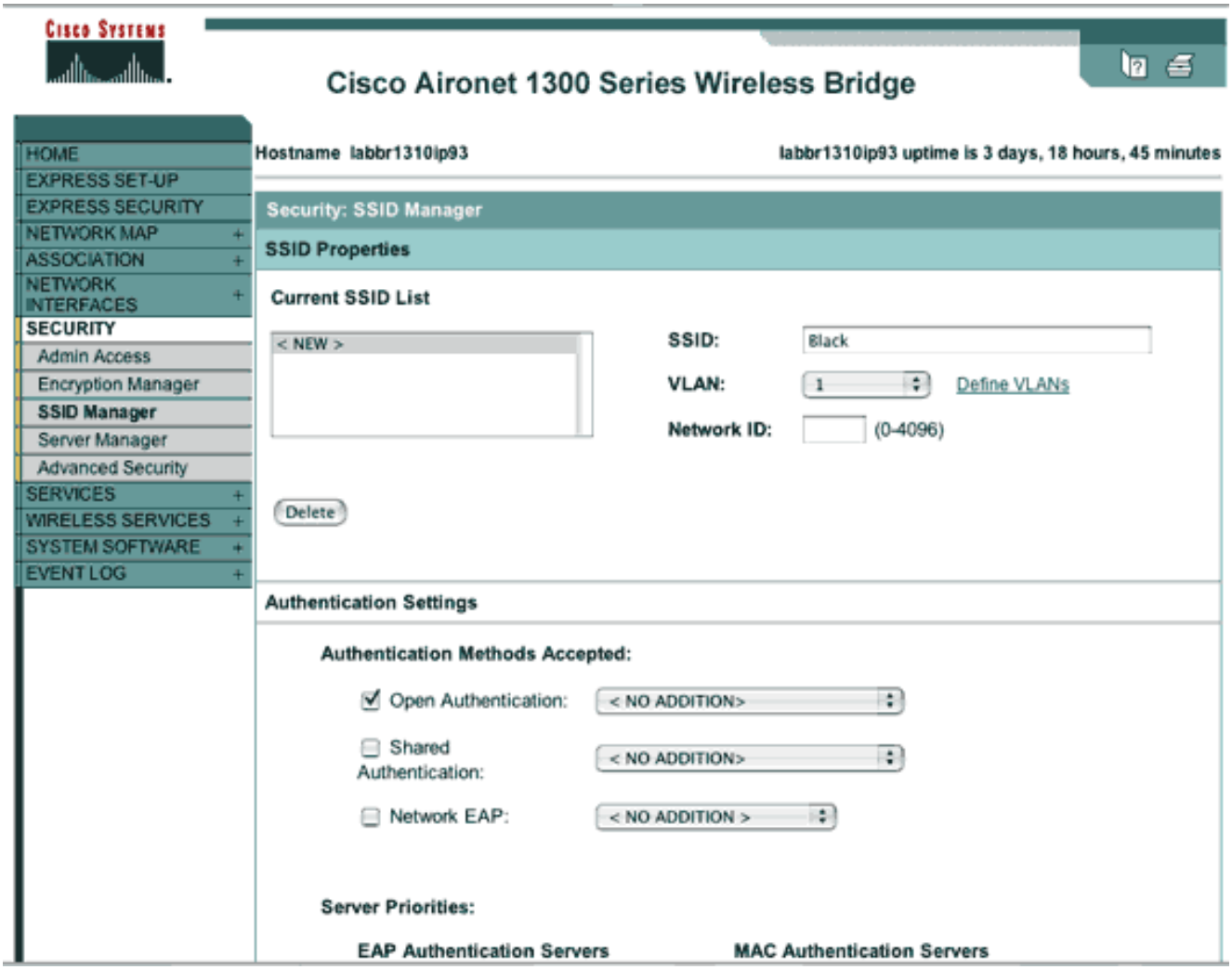
```
bridge# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
bridge(config)# interface Dot11Radio0.10
bridge(config-subif)# encapsulation dot1Q 10
bridge(config-subif)# interface FastEthernet0.10
bridge(config-subif)# encapsulation dot1Q 10
bridge(config-subif)# end
bridge#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

Wiederholen Sie die Schritte 2a bis 2c für jedes gewünschte VLAN, oder geben Sie die Befehle der CLI ein, wobei die Subschnittstelle und die VLAN-Nummern entsprechend geändert werden müssen.

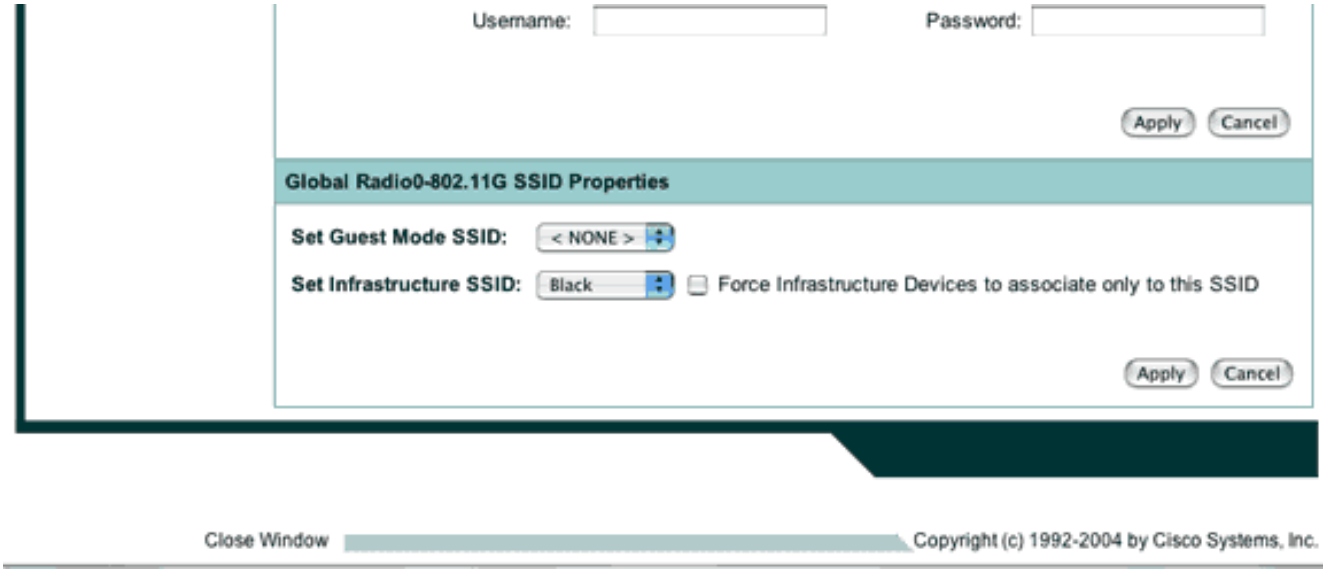
```
AP# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
bridge(config)# interface Dot11Radio0.30
```

```
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. Ordnen Sie im SSID-Manager (unter dem Menüelement **Security > SSID Manager**) das native VLAN einer SSID zu.**Hinweis:** Bei der Bridge müssen Sie einem VLAN nur die SSID zuordnen, die mit dem nativen VLAN korreliert. Sie müssen diese SSID als Infrastruktur-SSID festlegen.Wählen Sie in der aktuellen SSID-Liste die Option **Neu**.Geben Sie die gewünschte SSID (Groß- und Kleinschreibung beachten) in das Feld SSID ein.Wählen Sie aus der Dropdown-Liste die VLAN-Nummer aus, die dem nativen VLAN entspricht.**Hinweis:** Um dieses Dokument im vorgesehenen Umfang zu behalten, wird die Sicherheit für eine SSID nicht berücksichtigt.Klicken Sie auf **Apply**, um die SSID im Funkmodul zu erstellen und dem nativen VLAN
zuzuordnen.



Blättern Sie zurück zum Ende der Seite, und wählen Sie unter **Global Radio0-802.11G SSID Properties** die **SSID** aus der Dropdown-Liste **Set Infrastructure SSID (Infrastruktur-SSID festlegen)** aus. Klicken Sie auf
Übernehmen.



Führen Sie darüber hinaus folgende Befehle aus:

```
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
```

Hinweis: Wenn VLANs verwendet werden, werden SSIDs unter der physischen Schnittstelle mit Dot11Radio und nicht unter einer logischen Subschnittstelle konfiguriert.**Hinweis:** In diesem Beispiel ist keine Authentifizierung enthalten. Die Root- und Non-Root-Bridges erfordern eine Authentifizierung (offen, Netzwerk-EAP usw.), um eine Verbindung herzustellen.

Verwenden eines RADIUS-Servers zum Zuweisen von Benutzern zu VLANs

Sie können Ihren RADIUS-Authentifizierungsserver so konfigurieren, dass Benutzer oder Benutzergruppen einem bestimmten VLAN zugewiesen werden, wenn sie sich beim Netzwerk authentifizieren. Weitere Informationen zu dieser Funktion finden Sie im Abschnitt Verwenden eines RADIUS-Servers zum Zuweisen von Benutzern zu VLANs im Dokument *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points, 12.4(3g)JA & 12.3(8)JEB*.

Verwenden eines RADIUS-Servers für die dynamische Zuweisung von Mobilitätsgruppen

Sie können auch einen RADIUS-Server konfigurieren, um Mobilitätsgruppen dynamisch Benutzern oder Benutzergruppen zuzuweisen. Dadurch müssen keine mehrere SSIDs auf dem Access Point konfiguriert werden. Stattdessen müssen Sie nur eine SSID pro Access Point konfigurieren. Weitere Informationen zu dieser Funktion finden Sie im Abschnitt Verwenden eines RADIUS-Servers für die dynamische Zuweisung von Mobilitätsgruppen im Dokument *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points, 12.4(3g)JA & 12.3(8)JEB*.

Konfiguration der Bridge-Gruppe für Access Points und Bridges

Im Allgemeinen erstellen Bridge-Gruppen segmentierte Switching-Domänen. Der Datenverkehr ist

auf Hosts innerhalb jeder Bridge-Gruppe beschränkt, jedoch nicht zwischen den Bridge-Gruppen. Der Switch leitet Datenverkehr nur zwischen den Hosts weiter, aus denen die Bridge-Gruppe besteht. Dadurch wird Broadcast- und Multicast-Datenverkehr (Flooding) auf diese Hosts beschränkt. Bridge-Gruppen reduzieren Netzwerküberlastungen und bieten zusätzliche Netzwerksicherheit, wenn sie Datenverkehr in bestimmte Bereiche des Netzwerks segmentieren.

Detaillierte Informationen finden Sie unter Bridging Overview.

In einem Wireless-Netzwerk werden Bridge-Gruppen auf den Wireless Access Points und Bridges konfiguriert, damit der Datenverkehr eines VLANs von Wireless-Medien an die kabelgebundene Seite und umgekehrt übertragen wird.

Führen Sie diesen Schritt von der AP-CLI aus, um Bridge-Gruppen auf dem Access Point/Bridge global zu aktivieren.

In diesem Beispiel wird die Bridge-Gruppe Nr. 1 verwendet.

AP(configure)#**Bridge** *1*

Hinweis: Sie können Ihre Bridge-Gruppen von 1 bis 255 nummerieren.

Konfigurieren Sie die Funkschnittstelle und die Fast Ethernet-Schnittstelle des Wireless-Geräts so, dass sie sich in derselben Bridge-Gruppe befinden. Dadurch wird ein Pfad zwischen diesen beiden verschiedenen Schnittstellen erstellt, und sie befinden sich für Tagging im selben VLAN. Die Daten, die von der Wireless-Seite über die Funkschnittstelle übertragen werden, werden an die Ethernet-Schnittstelle übertragen, an die das kabelgebundene Netzwerk angeschlossen ist, und umgekehrt. Mit anderen Worten: Funkschnittstellen und Ethernet-Schnittstellen, die derselben Bridge-Gruppe angehören, überbrücken die Daten zwischen ihnen.

In einem Access Point/Bridge muss pro VLAN eine Bridge-Gruppe vorhanden sein, damit der Datenverkehr vom Kabel zum Wireless-Netzwerk übertragen werden kann und umgekehrt. Je mehr VLAN-Verbindungen erforderlich sind, um Datenverkehr über das Wireless-Netzwerk weiterzuleiten, desto mehr Bridge-Gruppen werden benötigt.

Wenn Sie beispielsweise nur ein VLAN haben, um Datenverkehr über das Wireless-Netzwerk an die kabelgebundene Seite Ihres Netzwerks weiterzuleiten, konfigurieren Sie nur eine Bridge-Gruppe von der CLI des Access Points/Bridge aus. Wenn Sie über mehrere VLANs verfügen, um Datenverkehr vom Wireless-Netzwerk an die kabelgebundene Seite und umgekehrt weiterzuleiten, konfigurieren Sie Bridge-Gruppen für jedes VLAN an der Funkschnittstellen sowie die Fast Ethernet-Subschnittstelle.

1. Konfigurieren Sie die Bridge-Gruppe in der Wireless-Schnittstelle mithilfe des **Schnittstellenbefehls dot11radio** für die Bridge-Gruppe.Dies ist ein Beispiel.

```
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. Konfigurieren Sie die Bridge-Gruppe mit derselben Bridge-Gruppen-Nummer ("1" in diesem Beispiel) in der Fast Ethernet-Schnittstelle, sodass der VLAN 1-Datenverkehr über die Wireless-Schnittstelle an diese kabelgebundene Seite weitergeleitet wird und umgekehrt.

```
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
```

Hinweis: Wenn Sie eine Bridge-Gruppe auf der Funkschnittstelle konfigurieren, werden diese Befehle automatisch festgelegt.**Brückengruppe *1* Steuerung der Teilnehmerschleifebridge-Group *1* -Block-Unknown-Sourcekein Bridge-Group *1*-Source-Learningkeine Unicast-Flooding der Bridge-Gruppe *1*Bridge-Gruppe *1* - Spanning-DeaktiviertHinweis:** Wenn Sie eine Bridge-Gruppe auf der Fast Ethernet-Schnittstelle konfigurieren, werden diese Befehle automatisch festgelegt.**kein Bridge-Group *1*-Source-LearningBridge-Gruppe *1* - Spanning-Deaktiviert**

Integrated Routing and Bridging (IRB)

Integriertes Routing und Bridging ermöglicht das Routing eines bestimmten Protokolls zwischen gerouteten Schnittstellen und Bridge-Gruppen oder das Routing eines bestimmten Protokolls zwischen Bridge-Gruppen. Lokaler oder nicht routbarer Datenverkehr kann zwischen den Bridge-Schnittstellen in derselben Bridge-Gruppe überbrückt werden, während routingfähiger Datenverkehr an andere geroutete Schnittstellen oder Bridge-Gruppen weitergeleitet werden kann.

Mit integriertem Routing und Bridging können Sie Folgendes tun:

- Umschalten von Paketen von einer Bridge-Schnittstelle auf eine geroutete Schnittstelle
- Umschalten von Paketen von einer gerouteten Schnittstelle auf eine überbrückte Schnittstelle
- Switch-Pakete innerhalb derselben Bridge-Gruppe

Aktivieren Sie IRB auf den Wireless Access Points und Bridges, um Ihren Datenverkehr zwischen Bridge-Gruppen oder zwischen gerouteten Schnittstellen und Bridge-Gruppen weiterzuleiten. Sie benötigen einen externen Router oder einen Layer-3-Switch, um zwischen Bridge-Gruppen oder zwischen Bridge-Gruppen und gerouteten Schnittstellen weiterzuleiten.

Geben Sie diesen Befehl ein, um IRB im Access Point/Bridge zu aktivieren.

AP**(configure)#bridge-IRB**

Integriertes Routing und Bridging verwendet das Konzept einer virtuellen Bridge-Group-Schnittstelle (BVI), um Datenverkehr zwischen gerouteten Schnittstellen und Bridge-Gruppen oder zwischen Bridge-Gruppen weiterzuleiten.

Eine BVI ist eine virtuelle Schnittstelle innerhalb des Layer-3-Switch-Routers, die wie eine normale geroutete Schnittstelle funktioniert. Eine BVI unterstützt kein Bridging, stellt aber tatsächlich die entsprechende Bridge-Gruppe für geroutete Schnittstellen innerhalb des Layer-3-Switch-Routers dar. Sie verfügt über alle Attribute der Netzwerkschicht (wie z. B. eine Adresse der Netzwerkschicht und Filter), die für die entsprechende Bridge-Gruppe gelten. Die dieser virtuellen Schnittstelle zugewiesene Schnittstellennummer entspricht der Bridge-Gruppe, die diese virtuelle Schnittstelle darstellt. Diese Nummer ist die Verbindung zwischen der virtuellen Schnittstelle und der Bridge-Gruppe.

Führen Sie diese Schritte aus, um die BVI auf Access Points und Bridges zu konfigurieren.

1. Konfigurieren Sie die BVI, und weisen Sie der BVI die entsprechende Nummer der Bridge-

Gruppe zu. In diesem Beispiel wird der BVI die Bridge-Gruppe Nr. 1 zugewiesen.

```
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. Aktivieren Sie eine BVI, um routingfähige Pakete zu akzeptieren und weiterzuleiten, die von der entsprechenden Bridge-Gruppe empfangen wurden.

```
Ap(config)# bridge 1 route ip!---
!--- This example enables the BVI to accept and route the IP packet.
```

Es ist wichtig zu verstehen, dass Sie nur eine BVI für das Management-/native VLAN benötigen, in dem sich der WAP befindet (in diesem Beispiel VLAN 1). Sie benötigen für keine andere Subschnittstelle eine BVI, unabhängig davon, wie viele VLANs und Bridge-Gruppen Sie auf Ihrem AP/Bridge konfigurieren. Dies liegt daran, dass Sie den Datenverkehr in allen anderen VLANs (außer dem nativen VLAN) taggen und ihn über eine mit dot1q verbundene Schnittstelle an den Switch senden. Wenn Sie beispielsweise zwei VLANs im Netzwerk haben, benötigen Sie zwei Bridge-Gruppen, aber nur eine BVI-Verbindung zum Management-VLAN reicht in Ihrem Wireless-Netzwerk aus.Wenn Sie das Routing für ein bestimmtes Protokoll in der virtuellen Bridge-Gruppe-Schnittstelle aktivieren, werden Pakete, die von einer gerouteten Schnittstelle kommen, aber für einen Host in einer Bridge-Domäne bestimmt sind, an die virtuelle Bridge-Gruppe-Schnittstelle weitergeleitet und an die entsprechende Bridge-Schnittstelle weitergeleitet.Der gesamte an die virtuelle Bridge-Gruppe weitergeleitete Datenverkehr wird als überbrückter Datenverkehr an die entsprechende Bridge-Gruppe weitergeleitet. Der gesamte routbare Datenverkehr, der auf einer Bridge-Schnittstelle empfangen wird, wird an andere geroutete Schnittstellen geroutet, als käme er direkt von der virtuellen Bridge-Gruppe-Schnittstelle.Weitere Informationen zu Bridging und IRB finden Sie unter Configure Bridging (Bridging konfigurieren).

Interaktion mit verwandten Switches

In diesem Abschnitt erhalten Sie Informationen zur Konfiguration oder Verifizierung der Cisco Switches, die mit Cisco Aironet Wireless-Geräten verbunden sind.

Hinweis: Um weitere Informationen zu den in diesem Dokument verwendeten Befehlen zu erhalten, verwenden Sie das Command Lookup Tool (nur registrierte Kunden).

Switch-Konfiguration - Catalyst OS

Um einen Switch zu konfigurieren, der Catalyst OS zum Trunk-VLANs zu einem Access Point ausführt, lautet die Befehlssyntax **set trunk <*module #/port #*> on dot1q** und **set trunk <*module #/port #*> <*vlan list*>.**

Ein Beispiel aus dem Beispielnetzwerkdiagramm ist:

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

Switch-Konfiguration - IOS-basierte Catalyst-Switches

Geben Sie im Schnittstellenkonfigurationsmodus folgende Befehle ein, wenn Sie:

- Konfigurieren des Switch-Ports für Trunk-VLANs zu einem Access Point
- Auf einem Catalyst Switch, der IOS ausführt
- Das CatIOS umfasst u. a.:6 x 004 x 0035 x 0295 x

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

Hinweis: IOS-basierte Wireless-Geräte von Cisco Aironet unterstützen kein Dynamic Trunking Protocol (DTP), daher darf der Switch nicht versuchen, über das Protokoll zu verhandeln.

Switch-Konfiguration - Catalyst 2900XL/3500XL

Geben Sie im Schnittstellenkonfigurationsmodus diese Befehle ein, wenn Sie den Switch-Port zu Trunk-VLANs zu einem Access Point auf einem Catalyst 2900XL- oder 3500XL-Switch konfigurieren möchten, auf dem IOS ausgeführt wird:

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

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Überprüfen Sie die Wireless-Geräte.

- **show vlan**: Zeigt alle VLANs an, die derzeit auf dem Access Point konfiguriert sind, sowie deren Status.

```
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 dot1 Associations** - Zeigt Informationen zu verknüpften Clients pro SSID/VLAN an.

```
ap#show dot11 associations

802.11 Client Stations on Dot11Radio0:

SSID [Green] :

SSID [Red] :

Others:  (not related to any ssid)

ap#
```

Überprüfen des Switches

- Auf einem Catalyst OS-basierten Switch **show trunk <*module #/port #*>** - zeigt den Status eines Trunks an einem bestimmten Port an.

```
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)
```

- Auf einem IOS-basierten Switch zeigt **show interface fastethernet <*module #/port #*> trunk den Status eines Trunks an einer bestimmten Schnittstelle an**

```
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#
```

- Auf einem Catalyst Switch der Serie 2900XL/3500XL zeigt **show interface fastethernet <*module #/port #*> switchport** den Status eines Trunks auf einer bestimmten Schnittstelle an.

```
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#
```

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

- Konfigurieren von VLANs (Konfigurationshandbuch für Access Points)
- Konfigurieren von VLANs (Bridge-Konfigurationshandbuch)
- Technischer Trunking-Support
- Interaktion mit verwandten Switches
- Systemanforderungen für die Implementierung von Trunking
- Übersicht Bridging
- Beispiele für Wireless-Authentifizierungstypen in einem festkonfigurierten ISR
- Konfigurationsbeispiel für Wireless-Authentifizierungstypen auf festem ISR über SDM
- Konfigurationsbeispiel für Wireless LAN-Verbindungen mit einem ISR mit WEP-Verschlüsselung und LEAP-Authentifizierung
- Konfigurationsbeispiel für eine grundlegende WLAN-Verbindung
- Technischer Support und Dokumentation - Cisco Systems