VLAN’s gebruiken met Cisco Aironet draadloze apparatuur

Inhoud

Inleiding

Dit document biedt een voorbeeldconfiguratie voor het gebruik van virtuele LAN’s (VLAN’s) met Cisco Aironet draadloze apparatuur.

Voorwaarden

Vereisten

Voordat u deze configuratie uitvoert, moet aan de volgende vereisten worden voldaan:

- Bekendheid met Cisco Aironet draadloze apparatuur
- Bekendheid met LAN-switchingconcepten van VLAN's en VLAN-trunking

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Aironet access points en draadloze bruggen
- Cisco Catalyst 6500 Switches

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Verwante producten

U kunt de hardwarekant van deze switch gebruiken met een van deze hardware of software:

- Catalyst 6x00/5x00/4x00 waarin CatOS of IOS wordt uitgevoerd
- Catalyst 350x00/37x00/29x switch die IOS-toepassingen ondersteunt
- Catalyst 2900XL/3500XL switch die IOS gebruikt

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

VLAN's

VLAN is een switched netwerk dat logisch gesegmenteerd is door functies, projectteams of applicaties in plaats van op een fysieke of geografische basis. Alle werkstations en servers die door een bepaald werkgroepteam worden gebruikt, kunnen bijvoorbeeld worden verbonden met hetzelfde VLAN, ongeacht hun fysieke verbindingen met het netwerk of het feit dat ze kunnen worden gekoppeld aan andere teams. Gebruik VLAN's om het netwerk via software aan te passen in plaats van de stekker fysiek uit het stopcontact te halen of de apparaten of draden te verplaatsen.

VLAN kan worden gezien als een uitzendingsdomein dat binnen een bepaalde reeks switches bestaat. VLAN bestaat uit een aantal eindsystemen, of hosts of netwerkapparatuur (zoals bruggen en routers), die door één overbruggingsdomein zijn aangesloten. Het overbruggingsdomein wordt ondersteund op diverse netwerkapparatuur, zoals LAN-switches, die onderling

overbruggingsprotocollen met een aparte groep voor elk VLAN bedienen.

Wanneer u een apparaat aansluit op een Cisco Catalyst-switch, is de poort waarop het apparaat is aangesloten een lid van VLAN 1. Het MAC-adres van dat apparaat is een onderdeel van VLAN 1. U kunt meerdere VLAN’s op één switch definiëren en u kunt op de meeste Catalyst-modellen een switch-poort configureren als lid van meerdere VLAN’s.

Wanneer het aantal poorten in een netwerk de poortcapaciteit van de switch overtreft, moet u meerdere switch-chassis onderling verbinden, waardoor een trunk wordt gedefinieerd. De trunk is geen lid van een VLAN, maar een geleider waarover verkeer voor een of meer VLAN’s passeert.

In fundamentele termen, is de sleutel in de configuratie van een toegangspunt om met een specifiek VLAN te verbinden zijn SSID te vormen om dat VLAN te erkennen. Omdat VLAN’s worden geïdentificeerd door een VLAN-id of een naam, volgt hieruit dat, als de SSID op een toegangspunt is geconfigureerd om een specifieke VLAN-id of -naam te herkennen, een verbinding met het VLAN tot stand is gebracht. Wanneer deze verbinding tot stand is gebracht, kunnen gekoppelde draadloze clientapparaten met dezelfde SSID via het toegangspunt toegang tot het VLAN krijgen. VLAN verwerkt gegevens van en naar de clients op dezelfde manier als het gegevens verwerkt van en naar bekabelde verbindingen. U kunt tot 16 SSID's configureren op uw access point, zodat u tot 16 VLAN's kunt ondersteunen. U kunt slechts één SSID aan een VLAN toewijzen.

U breidt VLAN’s uit naar een draadloos LAN wanneer u IEEE 802.11Q-tagbewustzijn toevoegt aan het access point. Frames die bestemd zijn voor verschillende VLAN’s worden draadloos via het toegangspunt verzonden op verschillende SSID’s met verschillende WEP-toetsen. Alleen de clients die aan dat VLAN zijn gekoppeld, ontvangen die pakketten. Omgekeerd worden pakketten die afkomstig zijn van een client die aan een bepaald VLAN is gekoppeld, 802.11Q getagd voordat ze naar het bekabelde netwerk worden doorgestuurd.

Werknemers en gasten kunnen bijvoorbeeld tegelijkertijd toegang krijgen tot het draadloze netwerk van een bedrijf en administratief gescheiden zijn. Een VLAN wordt toegewezen aan een SSID en de draadloze client wordt als bijlage aan de juiste SSID toegevoegd. In netwerken met draadloze bruggen kunt u meerdere VLAN’s via de draadloze link doorgeven om verbinding met een VLAN te bieden vanaf afzonderlijke locaties.

Als 802.1q is geconfigureerd op de Fast Ethernet-interface van een access point, verstuurt het access point altijd keepalives op VLAN1, zelfs als VLAN 1 niet is gedefinieerd op het access point. Hierdoor maakt de Ethernet-switch verbinding met het toegangspunt en wordt een waarschuwingsbericht gegenereerd. Er is geen functieverlies op het toegangspunt of de switch, maar het switch logboek bevat betekenisloze berichten die kunnen veroorzaken dat belangrijkere berichten worden verpakt en niet gezien.

Dit gedrag leidt tot een probleem wanneer alle SSID's op een toegangspunt zijn gekoppeld aan mobiliteitsnetwerken. Als alle SSID's zijn gekoppeld aan mobiliteitsnetwerken, kan de Ethernet-switch waarmee het toegangspunt is verbonden, worden geconfigureerd als een toegangspoort. De toegangshaven wordt normaal toegewezen aan het native VLAN van het access point, dat niet noodzakelijk VLAN1 is. Hierdoor genereert de Ethernet-switch waarschuwingsberichten die melden dat verkeer met een 802.1q-tag wordt verzonden vanaf het toegangspunt.

U kunt de overmatige berichten op de switch verwijderen als u de functie keepalive uitschakelt.

Als u minder belangrijke punten in deze concepten negeert wanneer u VLAN's met Cisco Aironet draadloze apparatuur implementeert, kunt u onverwachte prestaties ervaren, bijvoorbeeld:

- De fout om toegestane VLAN's in de trunk te beperken tot de VLAN's die op het draadloze apparaat zijn gedefinieerd

  Als VLAN's 1, 10, 20, 30 en 40 op de switch zijn gedefinieerd, maar alleen VLAN's 1, 10 en 30 op de draadloze apparatuur zijn gedefinieerd, moet u de andere apparaten uit de trunkswitchpoort verwijderen.

- Misbruik van de benaming van infrastructuur-SSID

  Wanneer u toegangspunten installeert, wijs dan alleen de infrastructuur-SSID toe wanneer u een SSID gebruikt op:

  - werkgroepbridge-apparaten
  - repeater access points
  - niet-root-bruggen

  Het is een misconfiguratie om de infrastructuur SSID voor een SSID met slechts draadloze laptop computers voor cliënten aan te wijzen, en veroorzaakt onvoorspelbare resultaten.

  In bruginstallaties, kunt u slechts één infrastructuur SSID hebben. De infrastructuur SSID moet de SSID zijn die correleert met het native VLAN.

- Misbruik of onjuist ontwerp van de aanduiding van de gastmodus SSID

  Wanneer u meerdere SSID's/VLAN's definieert op Cisco Aironet draadloze apparatuur, kan één (1) SSID worden toegewezen als gastmodus SSID met de SSID-uitzending in 802.11-radiobakens. De andere SSID's worden niet uitgezonden. De clientapparaten moeten aangeven welke SSID wordt gebruikt voor de verbinding.

- Niet-herkenning dat meerdere VLAN's en SSID's wijzen op meerdere OSI Model Layer 3-subnetten

  Afkeurde versies van Cisco Aironet-software maken het mogelijk om meerdere SSID's aan één VLAN te binden. De huidige versies niet.

- OSI Model Layer 3-routerfouten of onjuiste ontwerpen

  Elke SSID en zijn verbonden VLAN moeten een routeringsapparaat en één of andere bron hebben om cliënten, bijvoorbeeld een server van DHCP of het werkingsgebied op een server van DHCP te richten.

- Onbegrepen of onjuist configureren van native VLAN

  Routers en switches die samen de fysieke netwerkinfrastructuur vormen, worden op een

andere manier beheerd dan de client-pc's die aan die fysieke infrastructuur zijn gekoppeld. VLAN deze router en switch interfaces zijn lid van wordt genoemd Native VLAN (door gebrek, VLAN 1). De PC's van de client zijn lid van een ander VLAN, net zoals IP-telefoons lid zijn van weer een ander VLAN. De beheerinterface van het toegangspunt of de brug (interface BVI1) wordt beschouwd als en genummerd als een deel van het native VLAN ongeacht welke VLAN's of SSID's door dat draadloze apparaat worden doorgegeven.

Significantie van Native VLAN

Wanneer u een IEEE 802.1Q trunkpoort gebruikt, worden alle frames getagd, behalve de frames op het VLAN die als "native VLAN" voor de poort zijn geconfigureerd. De kaders op inheems VLAN worden altijd overgebracht untagged en normaal ontvangen untagged. Daarom wanneer AP met de switchport wordt verbonden, moet het native VLAN dat op de AP is geconfigureerd overeenkomen met het native VLAN dat op de switchpoort is geconfigureerd.

Opmerking: als de native VLAN's niet overeenkomen, worden de frames verwijderd.

Dit scenario kan beter met een voorbeeld worden uitgelegd. Als het native VLAN op de switchport is geconfigureerd als VLAN 12 en op het AP, wordt het native VLAN geconfigureerd als VLAN 1, dan wanneer het AP een frame op zijn native VLAN naar de switch verzendt, beschouwt de switch het frame als behorend tot VLAN 12 aangezien de frames van het native VLAN van het AP niet zijn gelabeld. Dit veroorzaakt verwarring in het netwerk en resulteert in connectiviteitsproblemen. Het zelfde gebeurt wanneer de switchport een kader van zijn inheems VLAN aan AP door:sturen.

De configuratie van native VLAN wordt zelfs nog belangrijker wanneer u een Repeater AP-instelling hebt in uw draadloze netwerk. U kunt geen meerdere VLAN's configureren op de AP's van de repeater. Repeater AP's ondersteunen alleen het native VLAN. Daarom moeten de native VLAN-configuratie op de basis-AP, de switch-poort waarop de AP is aangesloten en de Repeater AP hetzelfde zijn. Anders gaat het verkeer door de switch niet over van en naar het toegangspunt van de repeater.

Een voorbeeld voor het scenario waar de wanverhouding in de configuratie van VLAN van de Repeater AP tot problemen kan leiden is wanneer er een server van DHCP achter de switch is waarmet wortelAP wordt verbonden. In dit geval ontvangen de clients die zijn gekoppeld aan het toegangspunt van de repeater geen IP-adres van de DHCP-server, omdat de frames (DHCP-verzoeken in ons geval) van het native VLAN van het toegangspunt van de repeater (dat niet hetzelfde is als het toegangspunt van de hoofdmap en de switch) worden verbroken.

Zorg er bij het configureren van de switch-poort ook voor dat alle VLAN's die op de AP's zijn geconfigureerd, op de switchpoort zijn toegestaan. Als VLAN's 6, 7 en 8 bijvoorbeeld bestaan op het AP (Wireless Network), moeten de VLAN's worden toegestaan op de switchpoort. Dit kan met deze opdracht in de switch worden gedaan:

<#root>

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

Door gebrek, staat een switchport die als trunk wordt gevormd alle VLAN's toe om door de trunkpoort te gaan. Raadpleeg Interactie met verwante Switches voor meer informatie over het configureren van de switchpoort.

Opmerking: het toestaan van alle VLAN's op het toegangspunt kan in bepaalde gevallen ook een probleem worden, met name als het om een groot netwerk gaat. Dit kan resulteren in een hoog CPU-gebruik op de AP's. Afdrukken van VLAN's op de switch zodat alleen het VLAN-verkeer waarin het toegangspunt is geïnteresseerd, door het toegangspunt wordt doorgegeven om een hoge CPU te voorkomen.

VLAN's op access points

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

N.B.: Gebruik de Command Lookup Tool (alleen geregistreerde klanten) om extra informatie over de in dit document gebruikte opdrachten te vinden.

Concepten met access points

Deze sectie bespreekt concepten hoe u VLAN's op access points kunt implementeren en verwijst naar dit netwerkdiagram.

In dit voorbeeldnetwerk is VLAN 1 het native VLAN en bestaan VLAN's 10, 20, 30 en 40 en zijn trunked naar een ander switch-chassis. Alleen VLAN's 10 en 30 worden uitgebreid naar het draadloze domein. Native VLAN is vereist om beheermogelijkheden en clientverificaties te bieden.

Configuratie van access point

Voltooi de volgende stappen om het toegangspunt voor VLAN's te configureren:

1. Klik vanuit de AP GUI op Services > VLAN om naar de Services: VLAN-pagina te navigeren.

    a. De eerste stap is inheems VLAN te vormen. Selecteer in de lijst Huidige VLAN de optie Nieuw.

    b. Voer het VLAN-nummer van het native VLAN in het vak VLAN-id in. Het VLAN-nummer moet overeenkomen met het native VLAN dat op de switch is geconfigureerd.

    c. Omdat interface BVI 1 is gekoppeld aan de subinterface van het native VLAN, moet het IP-adres dat is toegewezen aan interface BVI 1 zich in hetzelfde IP-subnet bevinden als andere infrastructuurapparaten op het netwerk (dat wil zeggen, de interface SC0 op een Catalyst-switch die CatOS uitvoert).

    d. Selecteer checkbox voor het inheemse VLAN.

    e. Selecteer selectievakjes voor de radio-interface of interfaces waar dit VLAN van toepassing is.

f. Klik op Apply (Toepassen).

Of, van CLI, geef deze bevelen uit:

<#root>

```
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. Om andere VLAN's te configureren volgt u de volgende stappen:

a. Selecteer in de lijst Huidige VLAN de optie Nieuw.

b. Voer het VLAN-nummer van het gewenste VLAN in het vak VLAN-id in. Het VLAN-nummer moet overeenkomen met een VLAN dat op de switch is geconfigureerd.

c. Selecteer selectievakjes voor de radio-interface of interfaces waar dit VLAN van toepassing is.

d. Klik op Apply (Toepassen).

Of, van CLI, geef deze bevelen uit:

<#root>

```
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
```

e. Herhaal stap 2a tot en met 2d voor elk gewenst VLAN of voer deze opdrachten van de CLI in met de juiste wijzigingen in de subinterface en VLAN-nummers:

```
<#root>

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. De volgende stap is de geconfigureerde VLAN's te koppelen aan de SSID's. Klik hiervoor op Beveiliging > SSID Manager.

   Opmerking: u hoeft niet elk VLAN dat is gedefinieerd op het toegangspunt te koppelen aan

een SSID. Bijvoorbeeld, om veiligheidsredenen, associëren de meeste installaties van toegangspunten geen SSID met Inheems VLAN.

a. Kies Nieuw om een nieuwe SSID te maken.

b. Voer in het vak SSID de gewenste SSID (hoofdlettergevoeligheid) in.

c. Selecteer het gewenste VLAN-nummer om deze SSID aan te sluiten in de vervolgkeuzelijst.

   Opmerking: om dit document binnen het beoogde bereik te houden, wordt niet ingegaan op de beveiliging van een SSID.

d. Klik op Apply-RadioX om de SSID op de geselecteerde radio te maken of op Apply-all om de SSID op alle radio's te maken.

   Of van CLI, geef deze bevelen uit:

```
<#root>

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. Herhaal stap 3a tot en met 3d voor elke gewenste SSID of voer deze opdrachten in vanuit de CLI met de juiste wijzigingen in de SSID.

```
<#root>

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
```

N.B.: Deze voorbeelden omvatten geen verificatie. Er is een bepaalde vorm van verificatie (Open, Network-EAP) vereist voor de clients die u wilt koppelen.

VLAN's op bruggen

Concepten op bruggen

Deze sectie bespreekt concepten met betrekking tot hoe u VLAN's op bruggen kunt implementeren en verwijst naar dit netwerkdiagram.

In dit voorbeeldnetwerk is VLAN 1 het native VLAN en VLAN's 10, 20, 30 en 40 bestaan. Alleen VLAN's 10 en 30 worden uitgebreid naar de andere kant van de link. De draadloze link is versleuteld.

Als u gegevens wilt versleutelen die via de radioverbinding worden doorgegeven, moet u alleen codering toepassen op de SSID van het native VLAN. Deze codering is van toepassing op alle andere VLAN's. Wanneer u overbrugt, is er geen behoefte om afzonderlijke SSID met elk VLAN te associëren. VLAN-configuraties zijn hetzelfde op zowel de root- als niet-root-bruggen.

Bridge-configuratie

Voltooi de volgende stappen om de brug voor VLAN's te configureren, zoals in het voorbeeldnetwerkdiagram:

1. Klik vanuit de AP GUI op Services > VLAN om naar de pagina Services: VLAN te navigeren.

    a. De eerste stap is het configureren van het native VLAN. Kies <New> uit de huidige VLAN-lijst om dit te doen.

    b. Voer het VLAN-nummer van het native VLAN in het vak VLAN-id in. Dit moet overeenkomen met het native VLAN dat op de switch is geconfigureerd.

    c. Omdat interface BVI 1 is gekoppeld aan de subinterface van het native VLAN, moet het IP-adres dat is toegewezen aan interface BVI 1 zich in hetzelfde IP-

subnetwerkknooppunt bevinden als andere infrastructuurapparaten op het netwerk (bijv. interface SC0 op een Catalyst-switch met CatOS.)

d. Selecteer checkbox voor het inheemse VLAN.

e. Klik op Apply (Toepassen).

Of, van CLI, geef deze bevelen uit:

<#root>

```
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. Om andere VLAN's te configureren volgt u de volgende stappen:

a. Selecteer in de lijst Huidige VLAN de optie Nieuw.

b. Voer het VLAN-nummer van het gewenste VLAN in het vak VLAN-id in. Het VLAN-nummer moet overeenkomen met een VLAN dat op de switch is geconfigureerd.

c. Klik op Apply (Toepassen).

Of, van CLI, geef deze bevelen uit:

<#root>

```
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
```

d. Herhaal stap 2a tot en met 2c voor elk gewenst VLAN of voer de opdrachten van de CLI in met de juiste wijzigingen in de subinterface en VLAN-nummers.

<#root>

```
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. Vanuit de SSID Manager (onder de menuoptie Security > SSID Manager) koppelt u het native VLAN aan een SSID.

Opmerking: wanneer u overbrugt, is de enige SSID die u met een VLAN moet associëren, die correleert met het native VLAN. U moet deze SSID aanwijzen als de infrastructuur-SSID.

a. Selecteer in de lijst Huidige SSID de optie Nieuw.

b. Voer in het vak SSID de gewenste SSID (hoofdlettergevoeligheid) in.

c. Selecteer het VLAN-nummer dat correleert met het inheemse VLAN in de vervolgkeuzelijst.

   Opmerking: om dit document binnen het beoogde bereik te houden, wordt niet ingegaan op de beveiliging van een SSID.

d. Klik op Toepassen om de SSID op de radio te maken en deze te koppelen aan het native VLAN.

e. Scroll terug naar de onderkant van de pagina en selecteer onder Global Radio0-802.11G SSID Properties de SSID uit de vervolgkeuzelijst Set Infrastructure SSID. Klik op Apply (Toepassen).

   Of van CLI, geef deze bevelen uit:

```
<#root>

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
```

   Opmerking: wanneer VLAN's in gebruik zijn, worden SSID's geconfigureerd onder de fysieke Dot11Radio-interface, niet onder enige logische subinterface.

Opmerking: dit voorbeeld bevat geen verificatie. De root en niet-root-bruggen vereisen een of andere vorm van verificatie (Open, Network-EAP, enz.) om aan te kunnen koppelen.

Gebruik een RADIUS-server om gebruikers aan VLAN's toe te wijzen

U kunt uw RADIUS-verificatieserver configureren om gebruikers of groepen gebruikers toe te wijzen aan een specifiek VLAN wanneer ze zich verifiëren bij het netwerk. Raadpleeg voor informatie over deze functie het gedeelte Een RADIUS-server gebruiken om gebruikers toe te wijzen aan VLAN's van het document Cisco IOS-softwareconfiguratiegids voor Cisco Aironet access points, 12.4(3g)JA en 12.3(8)JEB.

Gebruik een RADIUS-server voor Dynamic Mobility Group Assignment

U kunt ook een RADIUS-server configureren om dynamisch mobiliteitsgroepen toe te wijzen aan gebruikers of gebruikersgroepen. Dit elimineert de noodzaak om meerdere SSID's op het access point te configureren. In plaats daarvan hoeft u slechts één SSID per access point te configureren. Raadpleeg voor informatie over deze functie het gedeelte Een RADIUS-server gebruiken voor de toewijzing van Dynamic Mobility Group in het document Cisco IOS-softwareconfiguratiegids voor Cisco Aironet access points, 12.4(3g)JA en 12.3(8)JEB.

Configuratie van bridgegroep op access points en bruggen

In het algemeen maken bridgegroepen gesegmenteerde switchingdomeinen. Het verkeer is beperkt tot hosts binnen elke bruggroep, maar niet tussen de bruggroepen. De switch forwards verkeer alleen tussen de hosts die samen de bruggroep vormen, die broadcast en multicast verkeer (overstroming) beperkt tot alleen die hosts. De bruggroepen verlichten netwerkcongestie en verstrekken extra netwerkveiligheid wanneer zij verkeer aan bepaalde gebieden van het netwerk segmenteren.

Raadpleeg Overbruggingsoverzicht voor gedetailleerde informatie.

In een draadloos netwerk zijn bridgegroepen geconfigureerd op de draadloze access points en bruggen zodat het gegevensverkeer van een VLAN wordt verzonden van draadloze media naar de bekabelde kant en vice versa.

Voer deze stap uit vanaf de CLI van het toegangspunt om bruggroepen wereldwijd op het toegangspunt/de brug in te schakelen.

Dit voorbeeld gebruikt het bridge-group nummer 1.

AP (configureren)#bridge 1

Opmerking: U kunt uw bruggroepen van 1 tot 255 nummeren.

Configureer de radio-interface en de Fast Ethernet-interface van het draadloze apparaat om in dezelfde bridge-groep te zijn. Dit maakt een pad tussen deze twee verschillende interfaces en ze zijn in hetzelfde VLAN voor coderingsdoeleinden. Dientengevolge, worden de gegevens die van

de draadloze kant door de radio interface worden overgebracht overgebracht naar de Ethernet interface waarop het getelegrafeerde netwerk wordt aangesloten en vice versa. Met andere woorden, radio- en Ethernet-interfaces die tot dezelfde bruggroep behoren, overbruggen in feite de gegevens tussen hen.

In een access point/bridge hebt u één bruggroep per VLAN nodig zodat het verkeer van de draad naar de radio kan overgaan en vice versa. Hoe meer VLAN u hebt dat verkeer over de radio moet overgaan, hoe meer bruggroepen die nodig zijn.

Als u bijvoorbeeld slechts één VLAN hebt om verkeer over de draadloze naar de bekabelde kant van uw netwerk door te geven, configureer dan slechts één bruggroep vanaf de CLI van de AP/bridge. Als u meerdere VLAN's hebt om verkeer van de draadloze naar de bekabelde kant en vice versa door te geven, configureer dan bridgegroepen voor elk VLAN op de subinterface van de radio, evenals voor de Fast Ethernet-subinterface.

1. Configureer de bruggroep in de draadloze interface met de opdracht van de bruggroep dot11radio interface.

   Hierna volgt een voorbeeld.

   <#root>

   ```
   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. Configureer de bruggroep met hetzelfde bruggroepnummer ("1" in dit voorbeeld) in de Fast Ethernet-interface zodat VLAN 1-verkeer over de draadloze interface wordt doorgegeven aan deze bekabelde kant en vice versa.

   <#root>

   ```
   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
```

Opmerking: wanneer u een bruggroep op de radio-interface vormt, worden deze opdrachten automatisch ingesteld.

- bridge-groep 1 Subscriber-loop-besturing
- bridge-groep 1 blok-onbekende-bron
- geen bridge-group 1 brononderwijs
- geen bridge-groep 1 unicast-overstroming
- bridge-groep 1 overspannen-uitgeschakeld

Opmerking: wanneer u een bruggroep configureert op de Fast Ethernet-interface, worden deze opdrachten automatisch ingesteld.

- geen bridge-group 1 brononderwijs
- bridge-groep 1 overspannen-uitgeschakeld

Geïntegreerde routing en bridging (IRB)

Geïntegreerde routing en bridging maakt het mogelijk om een specifiek protocol tussen routed interfaces en bridgegroepen te routeren, of een specifiek protocol tussen bridgegroepen te routeren. Lokaal of unroutable verkeer kan worden overbrugd tussen de overbrugde interfaces in dezelfde bruggroep, terwijl routable verkeer naar andere routed interfaces of bridgegroepen kan worden geleid

Met geïntegreerde routing en bridging kunt u dit doen:

- Switch-pakketten van een overbrugde interface naar een routeringsinterface
- Switch-pakketten van een routeringsinterface naar een overbrugde interface
- Switch-pakketten binnen dezelfde bruggroep

Schakel IRB in op de draadloze access points en bruggen om uw verkeer tussen bruggroepen of tussen gerouteerde interfaces en bruggroepen te leiden. U hebt een externe router of een Layer 3-switch nodig om tussen bruggroepen of tussen bruggroepen en routed interfaces te kunnen

routeren.

Geef deze opdracht uit om IRB in het toegangspunt/de brug in te schakelen.

AP(configureren)#bridge irb

Geïntegreerde routing en bridging maakt gebruik van het concept van een Bridge-Group Virtual Interface (BVI) om verkeer tussen gerouteerde interfaces en bruggroepen of tussen bruggroepen te routeren.

Een BVI is een virtuele interface binnen Layer 3-switch die werkt als een normale routeringsinterface. Een BVI ondersteunt geen overbrugging, maar vertegenwoordigt in feite de correspondent bridge group to routed interfaces binnen de Layer 3 switch router. Het heeft alle eigenschappen van de netwerklaag (zoals een adres en filters van de netwerklaag) die op de correspondentbruggroep van toepassing zijn. Het interfacenummer dat aan deze virtuele interface is toegewezen, komt overeen met de bruggroep die deze virtuele interface vertegenwoordigt. Dit nummer is het verband tussen de virtuele interface en de bruggroep.

Voer deze stappen uit om de BVI te configureren op access points en bruggen.

1. Configureer de BVI en wijs het correspondentnummer van de bruggroep toe aan de BVI. Dit voorbeeld wijst bruggroep nummer 1 aan BVI toe.

<#root>

```
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. Schakel een BVI in om routable pakketten te accepteren en te routeren die worden ontvangen van zijn correspondent bridge-groep.

<#root>

```
Ap(config)#

bridge 1 route ip!---


!--- This example enables the BVI to accept and route the IP packet.
```

Het is belangrijk om te begrijpen dat u alleen een BVI nodig hebt voor het beheer/native VLAN waarin het AP zich bevindt (in dit voorbeeld VLAN 1). U hebt geen BVI nodig voor een andere subinterface, ongeacht hoeveel VLAN's en bruggroepen u op uw AP/bridge configureert. Dit komt doordat u het verkeer in alle andere VLAN's (behalve het native VLAN) labelt en naar de switch stuurt via een dot1q trunked interface naar de bekabelde kant. Als u bijvoorbeeld 2 VLAN's op uw netwerk hebt, hebt u twee bruggroepen nodig, maar slechts één BVI-correspondent voor het beheer VLAN is voldoende in uw draadloze netwerk.

Wanneer u routing voor een bepaald protocol op de virtuele interface van de bruggroep inschakelt, worden pakketten die afkomstig zijn van een routeringsinterface, maar bestemd zijn voor een host in een overbrugd domein, naar de virtuele interface van de bruggroep verstuurd en naar de correspondent overbrugde interface verstuurd.

Al verkeer dat aan de virtuele interface van de bruggroep wordt verpletterd wordt door:sturen aan de overeenkomstige bruggroep als overbrugd verkeer. Al routable verkeer dat op een overbrugde interface wordt ontvangen wordt aan andere gerouteerde interfaces gerouteerd alsof het direct van de virtuele interface van de bruggroep komt.

Raadpleeg Overbrugging configureren voor meer gedetailleerde informatie over overbrugging en IRB.

Interactie met verwante Switches

In deze sectie wordt u gepresenteerd met de informatie om de configuratie van de Cisco-switches die verbinding maken met Cisco Aironet draadloze apparatuur te configureren of te verifiëren.

N.B.: Gebruik de Command Lookup Tool (alleen geregistreerde klanten) om extra informatie over de in dit document gebruikte opdrachten te vinden.

Switch-configuratie—Catalyst 9500 OS

Om een switch te configureren waarin Catalyst OS wordt uitgevoerd naar trunk VLAN's naar een access point, wordt de opdrachtsyntaxis ingesteld op trunk <module #/poort #> op dot1q en ingesteld trunk <module #/poort #> <VLAN list>.

Een voorbeeld van aan het diagram van het steekproefnetwerk, is:

<#root>

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

Switch configuratie-IOS gebaseerde Catalyst Switches

Voer in de interfaceconfiguratiemodus deze opdrachten in als u:

- Configureer de switchport naar trunk-VLAN's naar een access point
- Op een Catalyst switch waarop IOS wordt uitgevoerd
- CatIOS omvat, maar is niet beperkt tot:
    - 6x00
    - 4x00
    - 35 x 0
    - 295 x

<#root>

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

Opmerking: op IOS gebaseerde Cisco Aironet draadloze apparatuur ondersteunt Dynamic Trunking Protocol (DTP) niet, dus de switch moet niet proberen om dit te bespreken.

Switch configuratie—Catalyst 2900XL/3500XL

Voer in de interfaceconfiguratiemodus deze opdrachten in als u de switchport naar trunk-VLAN's wilt configureren voor een access point op een Catalyst 2900XL of 3500XL switch die IOS uitvoert:

<#root>

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

Verifiëren

Gebruik deze sectie om te controleren of uw configuratie goed werkt.

Controleer de draadloze apparatuur

- toon VLAN—toont alle VLAN's die momenteel op het access point zijn geconfigureerd, en hun status

<#root>

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#

- toon dot11 vereniging-toont informatie over geassocieerde cliënten, per SSID/VLAN

<#root>

ap#

```
show dot11 associations

802.11 Client Stations on Dot11Radio0:

SSID [Green] :

SSID [Red] :

Others:  (not related to any ssid)

ap#
```

Controleer de Switch

- Op een Catalyst OS-gebaseerde switch toont trunk <module #/port #>—de status van een trunk op een bepaalde poort

<#root>

```
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)
```

- Op een IOS-gebaseerde switch toont u de status van een trunk-interface Fast Ethernet <module #/port #> met een bepaalde interface

<#root>

```
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#
```

- Op een Catalyst 2900XL/3500XL switch toont de interfacepoort fasteEthernet <module #/poort #> switchpoort—de status van een trunk op een bepaalde interface

<#root>

```
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#
```

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

Gerelateerde informatie

- VLAN's configureren (configuratiehandleiding voor access point)
- VLAN's configureren (configuratiehandleiding voor bridge)

- Technische ondersteuning voor trunking
- Interactie met verwante Switches
- Systeemvereisten voor implementatie van trunking
- Overzicht van overbrugging
- Draadloze verificatietypen op een vast ISR-configuratievoorbeeld
- Draadloze verificatietypen op vaste ISR-doorlatende SDM-configuratievoorbeeld
- Configuratie-voorbeeld van draadloze LAN-connectiviteit met een ISR met WEP-encryptie en LEAP-verificatie
- Configuratievoorbeeld van eenvoudige wireless LAN-verbinding
- Technische ondersteuning en documentatie – Cisco Systems

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.