H3Cアクセスコントローラ
WLANでのユーザー分離の設定

内容

ユーザー分離の構成

ユーザー分離について

ユーザー分離機能は、同じVLAN内で同じSSIDを使用するユーザーまたは同じVLAN内のユーザーのパケットを分離します。この機能により、ユーザーのセキュリティが向上し、デバイスの転送ストレスが軽減され、無線リソースの消費量が削減されます。

ユーザー分離のタイプ

ユーザーの分離には、次のタイプがあります。

- **SSIDベースのユーザー分離**: 同じVLAN内で同じSSIDを使用するワイヤレスユーザーを分離します。
- **VLANベースのユーザー分離**: 同じVLAN内の有線または無線ユーザーを分離します。

SSIDベースのユーザー分離

SSIDベースのユーザー分離は、ローカル転送モードと集中型転送モードの両方に適用できます。

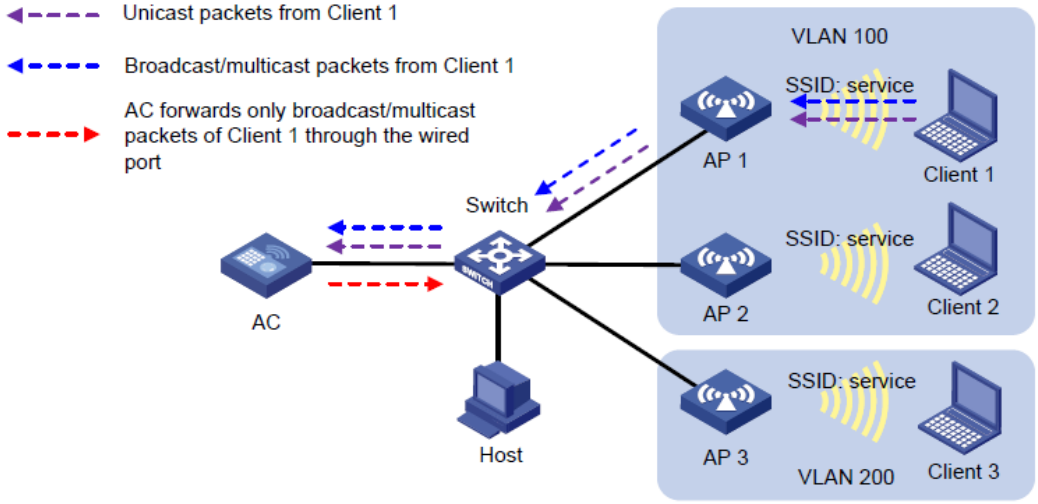
サービスに対してSSIDベースのユーザー分離がイネーブルになっている場合、デバイスは同じVLAN内のサービスを介してネットワークにアクセスするすべての無線ユーザーを分離します。

集中転送モードでのユーザー分離メカニズム

図1に示すように、ACはクライアントトラフィックを中央で転送します。クライアント1からクライアント3は、serviceという名前のサービスを使用して、AP1からAP3を介してWLANにアクセスします。クライアント1とクライアント2はVLAN100にあり、クライアント3はVLAN200にあります。AC上でサービスのためのユーザーの分離を有効にします。

- クライアント1はブロードキャストパケットまたはマルチキャストパケットをVLAN100で送信します。ACはパケットを受信すると、WLAN内のどのAPにも転送しません。ACはパケットを有線ポート経由でのみスイッチに転送します。
- クライアント1はユニキャストパケットをVLAN100のクライアント2に送信します。ACはパケットを受信すると、AP2に転送するのではなく廃棄します。

図1 パケット転送パス



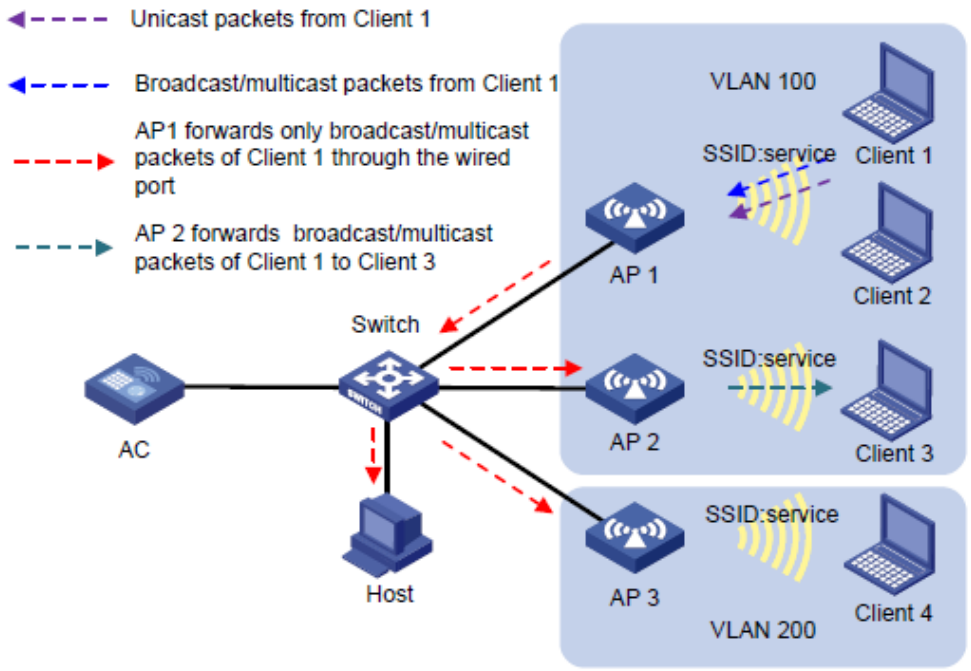
ローカル転送モードでのユーザー分離メカニズム

このメカニズムにより、同じAP上のワイヤレスクライアントが分離されます。

図2に示すように、APはクライアントに対してローカルトラフィック転送を実行します。クライアント1からクライアント4は、serviceという名前のサービスを使用してAP1からAP3を介してWLANにアクセスします。クライアント1からクライアント3はVLAN100にあり、クライアント4はVLAN200にあります。AP1のサービスでSSIDベースのユーザー分離を有効にします。

- クライアント1は、ブロードキャストパケットまたはマルチキャストパケットをVLAN100で送信します。
  - AP1はパケットを受信すると、ユーザー分離がイネーブルになっているため、パケットをクライアント2に転送しません。APは、AP2、AP3、およびホストを含む同じVLAN内の有線デバイスに対して、有線ポートを介してのみパケットを転送します。
  - AP2はパケットを受信すると、ユーザーの分離がAP2でディセーブルになっているため、パケットをクライアント3に転送します。
  - AP3はパケットを受信すると、クライアント1とクライアント4は異なるVLANにあるため、パケットをクライアント4に転送しません。
- クライアント1はユニキャストパケットをVLAN100のクライアント2に送信します。AP1はパケットを受信すると、クライアント2に転送するのではなく廃棄します。

図2 パケット転送パス



VLANベースのユーザー分離

VLANベースのユーザー分離は、ローカルおよび集中型の両方の転送モードに適用できます。表1は、有線ユーザーと無線ユーザーのトラフィックを分離するメカニズムを示しています。

表1VLANベースのユーザー分離メカニズム

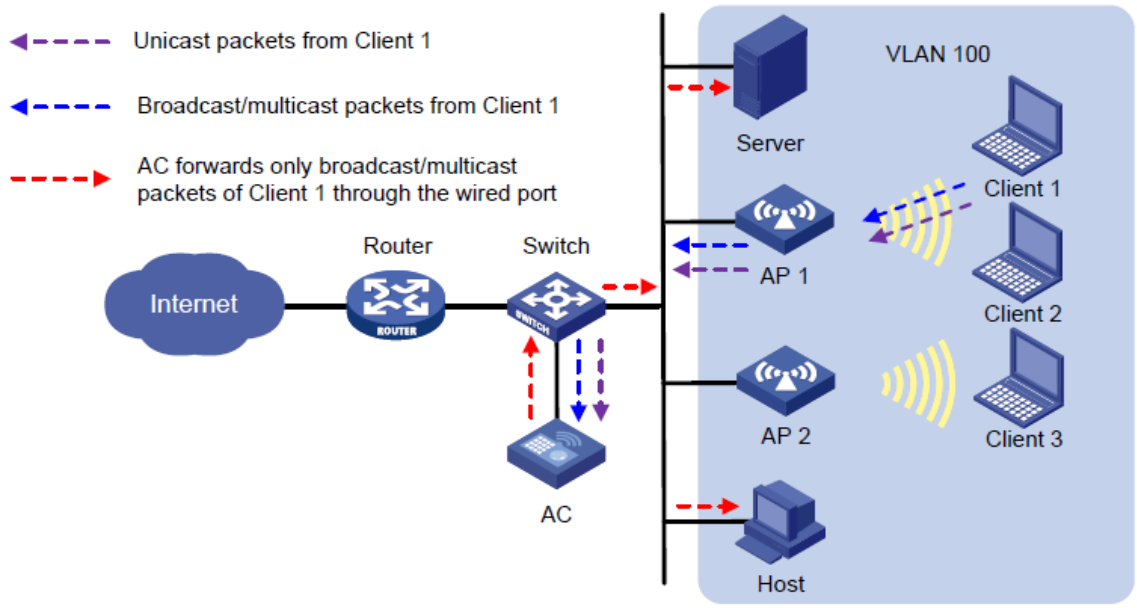
転送モード	受信ユニキャストパケット数	受信したブロードキャストパケットまたはマルチキャストパケット
集中型転送	ACはパケットを廃棄します。	ACは、パケットを有線ポートを介してVLAN内の有線ユーザーにだけ転送し、VLAN内の無線ユーザーには転送しません。
ローカル転送	FIT APはパケットを廃棄します。	FIT APはパケットを有線に転送しVLAN内のワイヤレスユーザーは、有線ポートを使用してパケットを転送します。ただし、APはパケットをVLAN内のローカルワイヤレスユーザーには転送しません。

集中転送モードでのユーザー分離メカニズム(ワイヤレスユーザーから受信したパケット)

図3に示すように、ACはクライアントトラフィックを中央で転送します。VLAN100のACでユーザーの分離を有効にします。

- クライアント1はブロードキャストパケットまたはマルチキャストパケットをVLAN100で送信します。ACはパケットを受信すると、WLAN内のどのAPにも転送しません。ACはパケットを有線ポート経由でのみスイッチに転送します。その後、スイッチはパケットを有線ホストおよびサーバに転送します。
- クライアント1はユニキャストパケットをVLAN100のクライアント3に送信します。ACはパケットを受信すると、AP2に転送するのではなく廃棄します。

図 3パケット転送パス

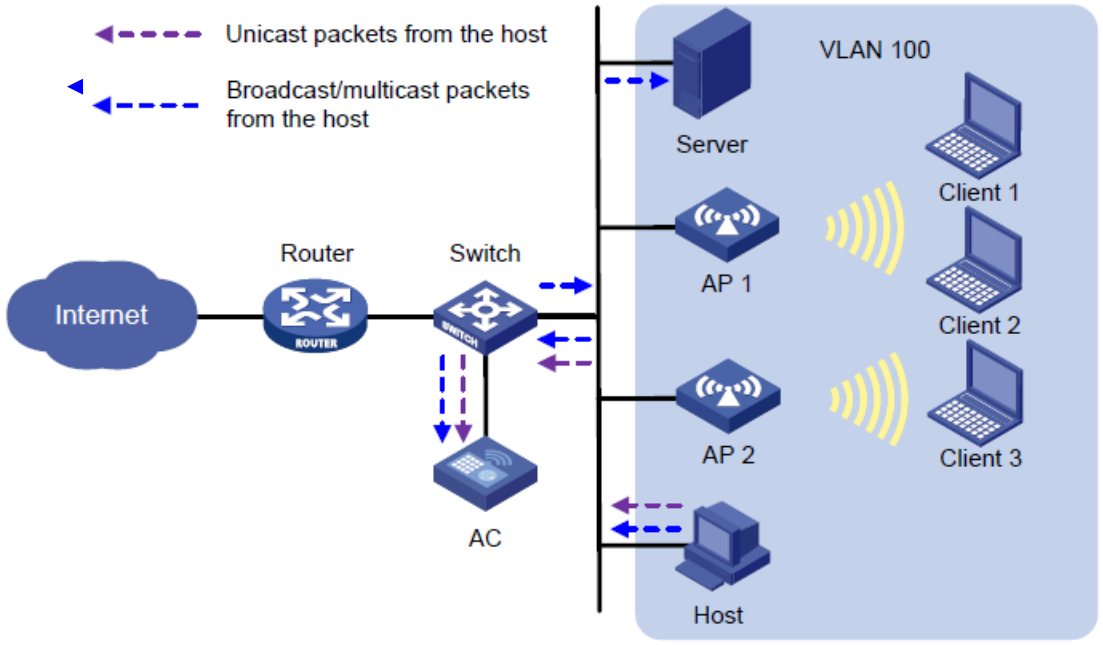


集中転送モードでのユーザー分離メカニズム(有線ユーザーから受信したパケット)

図4に示すように、ACはクライアントトラフィックを中央で転送します。VLAN100のACでユーザーの分離を有効にします。

- ホストはブロードキャストパケットまたはマルチキャストパケットをVLAN100で送信します。サーバおよびACはパケットを受信できます。ACはパケットを受信すると、WLAN内のAPに転送するのではなく、廃棄します。
- ホストはユニキャストパケットをVLAN100のクライアント3に送信します。ACはパケットを受信すると、AP2に転送するのではなく廃棄します。

図4 パケット転送パス



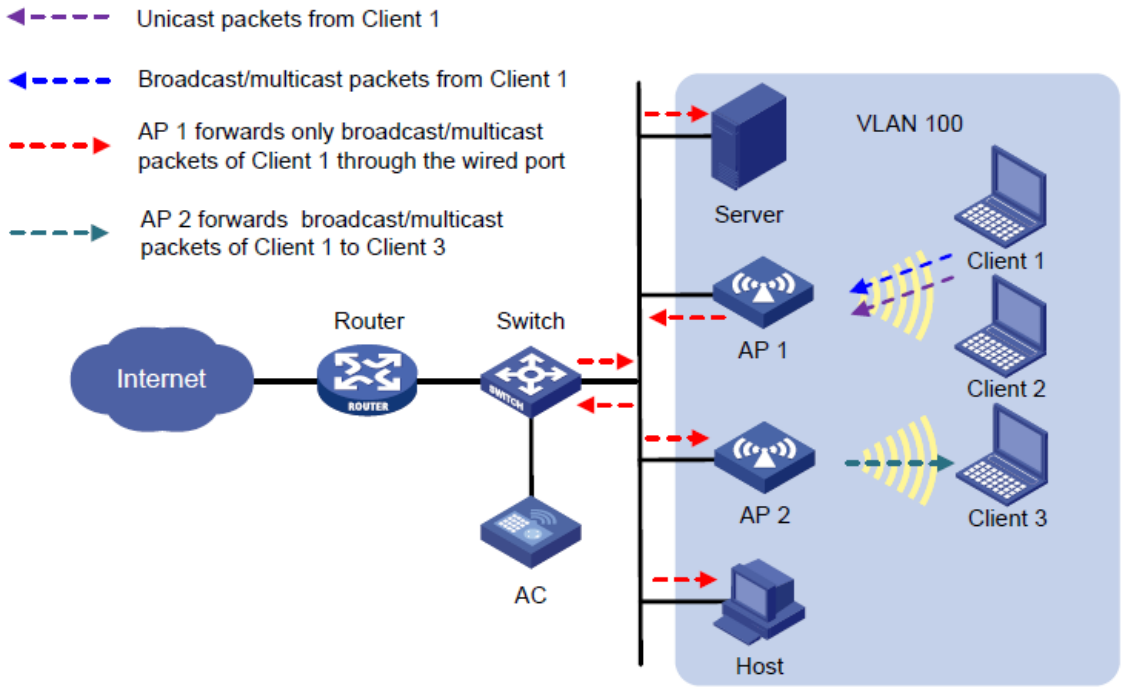
ローカル転送モードでのユーザー分離メカニズム(ワイヤレスユーザーから受信したパケット)

図5に示すように、AP1はクライアントに対してローカル転送を実行します。VLAN100に対してAP1でユー

ザー分離を有効にします。

- クライアント1は、ブロードキャストパケットまたはマルチキャストパケットをVLAN100で送信します。
  - AP1はパケットを受信すると、有線ポートを介してサーバ、AP2、およびVLAN100内のホストにパケットを転送します。ただし、ユーザーの分離がイネーブルになっているため、AP1はクライアント2にパケットを転送しません。
  - AP2はパケットを受信すると、ユーザーの分離がAP2でイネーブルになっていないため、パケットをクライアント3に転送します。
- クライアント1はユニキャストパケットをVLAN100のクライアント3に送信します。AP1はパケットを受信すると、AP2に転送するのではなく廃棄します。

図5 パケット転送パス

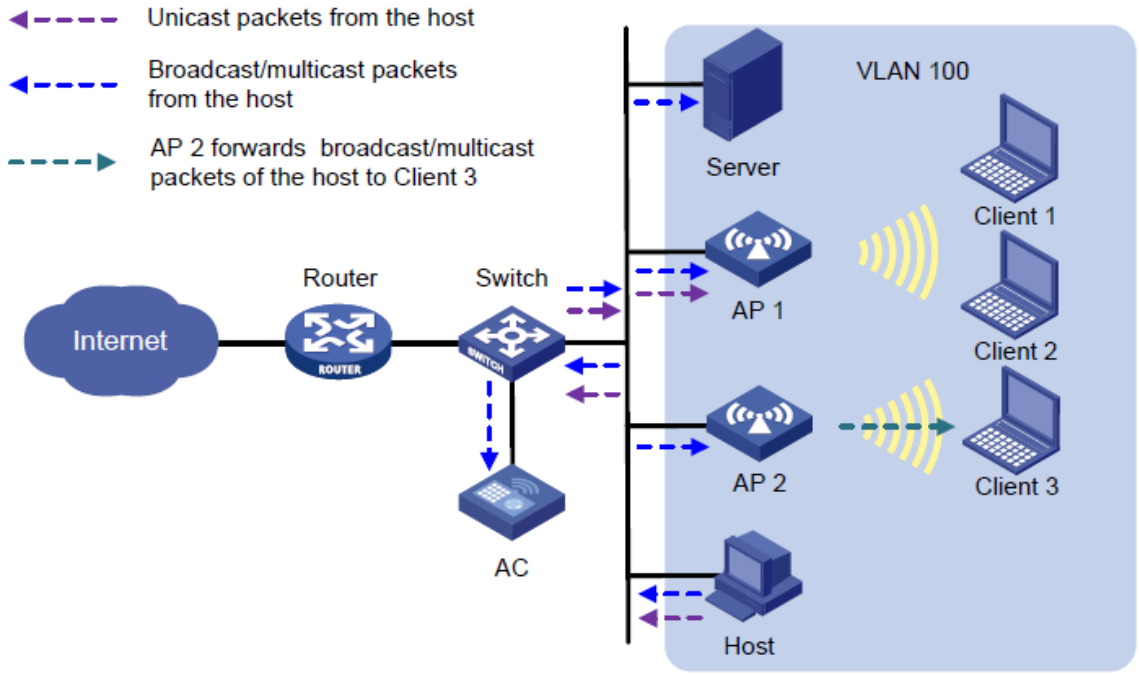


ローカル転送モードでのユーザー分離メカニズム(有線ユーザーから受信したパケット)

図6に示すように、AP1はクライアントに対してローカル転送を実行します。VLAN100のAP1でユーザーの分離を有効にします。

- ホストはブロードキャストパケットまたはマルチキャストパケットをVLAN100で送信します。サーバ、AC、AP1、およびAP2はパケットを受信できます。
  - AP1はパケットを受信すると、クライアント1およびクライアント2に転送するのではなく廃棄します。
  - AP2はパケットを受信すると、ユーザーの分離がAP2でイネーブルになっていないため、パケットをクライアント3に転送します。
- ホストはユニキャストパケットをVLAN100のクライアント1に送信します。AP1はパケットを受信すると、クライアント1に転送するのではなく廃棄します。

図6 パケット転送パス



SSIDベースのユーザー分離の有効化

1. システムビューに入ります。
   <AC>system-view
2. サービステンプレートビューを入力します。
   [AC] wlan service-template *service-template-name*
3. SSIDベースのユーザー分離をイネーブルにします。
   [AC-wlan-st-*service-template-name*] user-isolation enable
   デフォルトでは、SSIDベースのユーザー分離はディセーブルです。

VLANベースのユーザー分離の設定

制限事項およびガイドライン

VLANベースのユーザー分離は、集中型転送モードとローカル転送モードの両方に適用されます。

- **集中型転送モード**では、この機能をACに直接設定します。
- **ローカル転送モード**では、「手順」の項に示す順序でユーザー分離コマンド行を含む構成ファイルを準備する必要があります。次にACでmap-configurationコマンドを使用して、コンフィギュレーションファイルをAPに展開し、APのVLANベースのユーザー分離をイネーブルにします。コンフィギュレーションファイルの展開の詳細については、『WLAN Access Configuration Guide』を参照してください。

VLAN内のユーザーが外部ネットワークにアクセスできるようにするには、VLANベースのユーザー分離をイネーブルにする前に、VLANゲートウェイのMACアドレスを許可MACアドレスリストに割り当てます。

手順

1. システムビューに入ります。
   <AC>system-view
2. VLANのリストに許可MACアドレスリストを設定します。

[AC]user-isolation vlan *vlan-list* **permit-mac** *mac-list*

デフォルトでは、許可されたMACアドレスはVLANに設定されません。

デバイスは、指定したVLAN内の許可されたMACアドレスのユーザーによって送信されたユニキャスト、マルチキャスト、およびブロードキャストトラフィックを転送できます。さらに、他のユーザーから送信されたユニキャストトラフィックをこれらのユーザーに転送できます。

3. VLANリストのユーザー分離をイネーブルにします。

   [AC]user-isolation vlan *vlan-list* **enable [permit-unicast]**

   デフォルトでは、VLANのユーザー分離はディセーブルです。

4. (任意)有線ユーザーから無線ユーザーに送信されるブロードキャストおよびマルチキャストトラフィックを許可します。

   [AC]user-isolation permit-broadcast

   デフォルトでは、デバイスは有線ユーザーから送信されたブロードキャストまたはマルチキャストトラフィックを、ユーザー分離がイネーブルになっているVLAN内の無線ユーザーに転送しません。

ユーザーを分離するための表示および保守コマンド

任意のビューで表示コマンドを実行し、ユーザービューでコマンドをリセットします。

タスク	コマンド
VLANまたはすべてのVLANのユーザー分離統計情報を表示します。	**display user-isolation statistics [vlan** *vlan-id* **]**
VLANまたはすべてのVLANのユーザー分離統計情報をクリアします。	**reset user-isolation statistics [vlan** *lan-id* **]**

ユーザー分離の設定例

このドキュメントのAPモデルとシリアル番号は、例としてのみ使用されています。APモデルとシリアル番号のサポートは、ACモデルによって異なります。

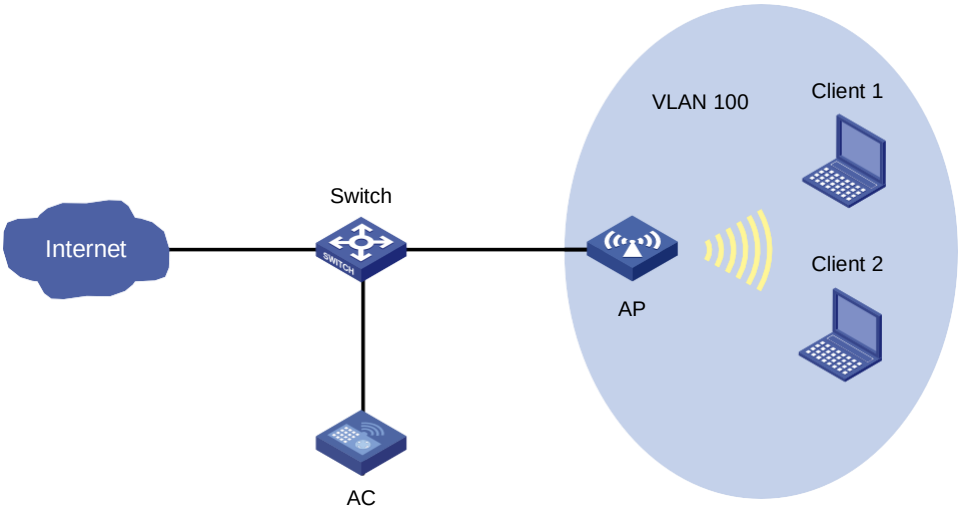
例:SSIDベースのユーザー分離の設定(集中型転送モード)

ネットワーク構成

図7に示すように、クライアント1とクライアント2は同じSSIDを使用してインターネットにアクセスします。ACはクライアントトラフィックを中央で転送します。

クライアントにインターネットアクセスを提供しながらクライアントを相互に分離するように、ACでユーザーの分離を設定します。

図7 ネットワーク図



手順

#サービステンプレートサービスを介してインターネットにアクセスするようにクライアント1およびクライアント2を設定します。詳細については、『WLAN Access Configuration Guide』の「WLAN access」および『AP and WT Management Configuration Guide』の「AP management」を参照してください(詳細は省略)。

#サービステンプレートサービスのSSIDベースのユーザー分離をイネーブルにします。

<AC> system-view

[AC] wlan service-template service

[AC-wlan-st-service] user-isolation enable

[AC-wlan-st-service] quit

設定の確認

#Client1とClient2がサービスserviceを使用してインターネットにアクセスできるが、互いにアクセスできないことを確認します(詳細は省略)。

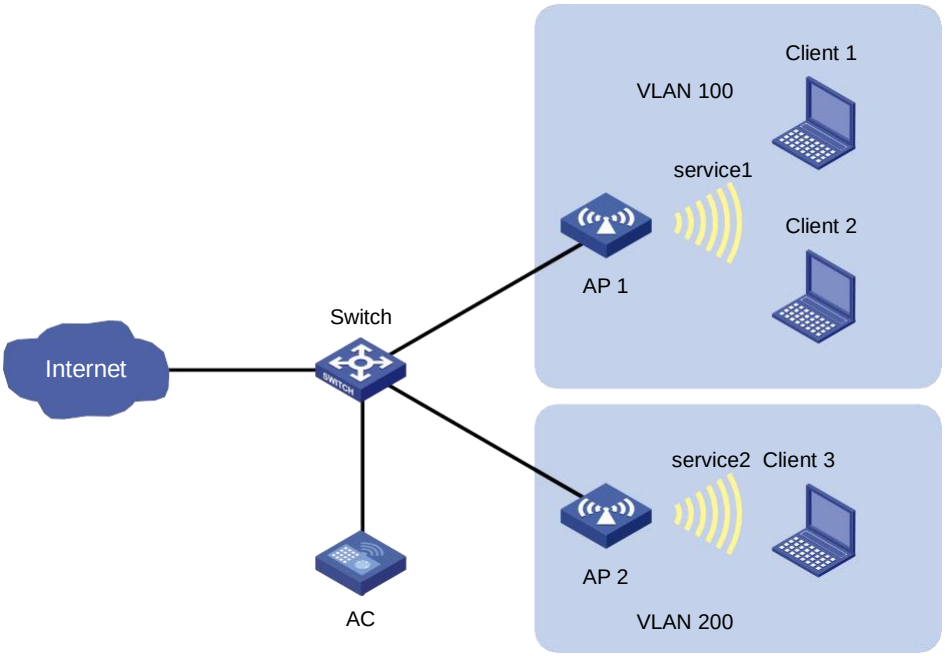
例:SSIDベースのユーザー分離の設定(ローカル転送モード)

ネットワーク構成

図8に示すように、クライアント1とクライアント2は同じSSIDを使用してインターネットにアクセスします。APはローカルトラフィック転送を実行します。

クライアントにインターネットアクセスを提供しながらクライアントを相互に分離するように、AP1のユーザー分離を設定します。

図8 ネットワーク図



手順

#サービステンプレートservice1を介してインターネットにアクセスするようにClient1およびClient2を設定します。クライアントに対してローカルトラフィック転送を実行するようにAPを設定します。詳細については、『WLAN Access Configuration Guide』の「WLAN access」および『AP and WT Management Configuration Guide』の「AP management」を参照してください(詳細は省略)。

#サービステンプレートservice1のSSIDベースのユーザー分離をイネーブルにします。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] user-isolation enable

[AC-wlan-st-service1] quit

設定の確認

#Client1とClient2がサービスservice1を使用してインターネットにアクセスできるが、互いにアクセスできないことを確認します(詳細は省略)。

例:VLANベースのユーザー分離の設定(集中型転送モード)

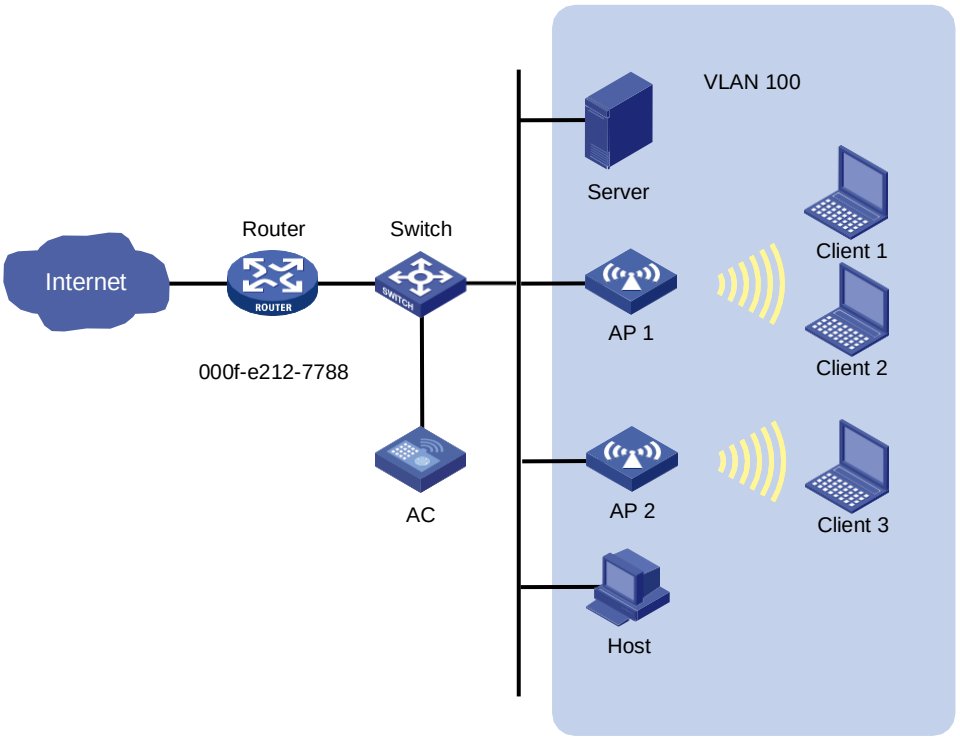
ネットワーク構成

図9に示すように、ACはクライアントトラフィックを中央で転送し、ルータはVLAN100内のデバイスのゲートウェイとして機能します。ゲートウェイのMACアドレスは000f-e212-7788です。

次の要件を満たすように、AC上のVLAN100のユーザー分離を設定します。

- クライアント1、クライアント2、クライアント3、ホスト、およびサーバはインターネットにアクセスできます。この目的のために、ゲートウェイのMACアドレスを許可MACアドレスリストに追加します。
- クライアント1がブロードキャストパケットを転送する場合、ホストとサーバだけがパケットを受信できます。
- クライアント1、クライアント2、およびクライアント3は、互いに到達できません。

図9 ネットワーク図



手順

#Client1、Client2、およびClient3を設定して、WLANを介してインターネットにアクセスします。詳細については、『WLAN Access Configuration Guide』の「WLAN access」および『AP and WT Management Configuration Guide』の「AP management」を参照してください(詳細は省略)。

#許可されるMACアドレスリストにゲートウェイのMACアドレスを割り当てます。

<AC> system-view

[AC] user-isolation vlan 100 permit-mac 000f-e212-7788

#VLAN100に対してVLANベースのユーザー分離をイネーブルにします。

[AC] user-isolation vlan 100 enable

設定の確認

#VLAN100内のクライアント1、クライアント2、クライアント3、ホスト、およびサーバがインターネットにアクセスできることを確認します(詳細は省略)。

#Client1からブロードキャストパケットを受信できるのはホストとサーバだけであることを確認します(詳細は表示されません)。

#Client1、Client2、およびClient3が相互に到達できないことを確認します(詳細は省略)。

例:VLANベースのユーザー分離の設定(ローカル転送モード)

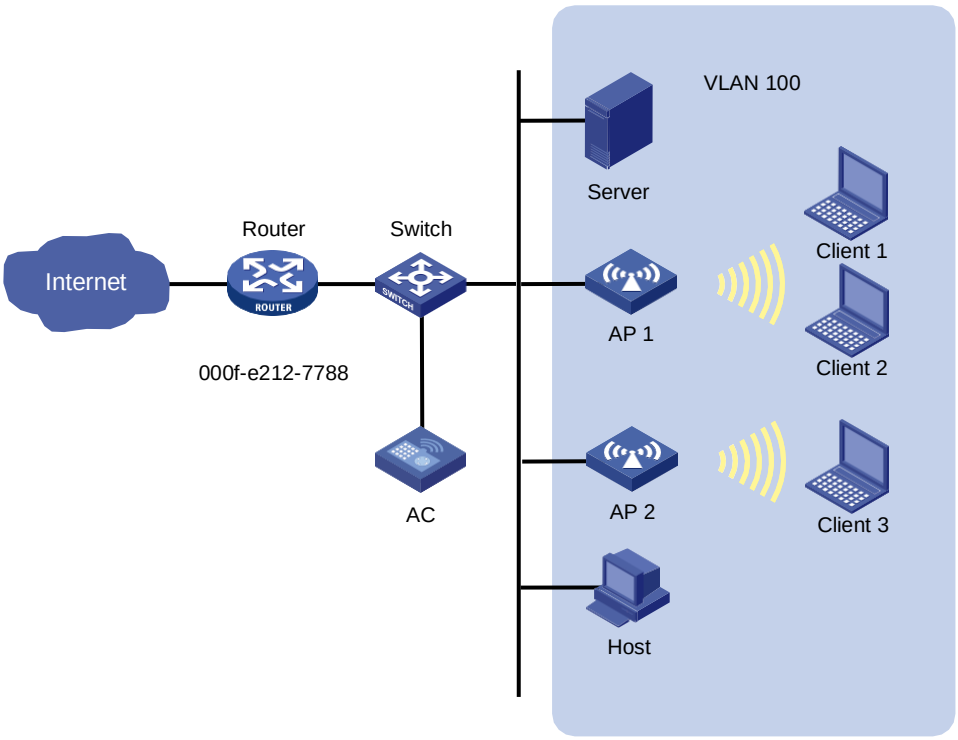
ネットワーク構成

図10に示すように、AP1はクライアントに対してローカルトラフィック転送を実行し、ルータはVLAN100内のデバイスのゲートウェイとして機能します。ゲートウェイのMACアドレスは000f-e212-7788です。

次の要件を満たすように、AP1でVLAN100のユーザー分離を設定します。

- クライアント1、クライアント2、クライアント3、ホスト、およびサーバはインターネットにアクセスできます。この目的のために、ゲートウェイのMACアドレスを許可MACアドレスリストに追加します。
- クライアント1がブロードキャストパケットを転送する場合、ホスト、サーバ、およびクライアント3だけがパケットを受信できます。
- Client1とClient2は互いに到達できません。

図 10ネットワーク図



手順

#Client1、Client2、およびClient3を設定して、WLANを介してインターネットにアクセスします。詳細については、『WLAN Access Configuration Guide』の「WLAN access」および『AP and WT Management Configuration Guide』の「AP management」を参照してください(詳細は省略)。

#設定ファイルapcfg.txtを作成し、次の順序でユーザー分離コマンド行を設定ファイルに追加します。ユーザー分離をイネーブルにするコマンドの前に、許可されたMACアドレスリストにゲートウェイMACアドレスを追加するコマンドを配置する必要があります。

<AC>system-view

[AC]user-isolation vlan100 permit-mac 000f-e212-7788

[AC]user-isolation vlan100 enable

#設定ファイルapcfg.txtをACにアップロードします(詳細は省略)。

#設定ファイルapcfg.txtをAP1に発行します。

<AC> system-view

[AC] wlan ap ap1 model WA4320i-ACN

[AC-wlan-ap-ap1] map-configuration apcfg.txt

設定の確認

#VLAN100内のクライアント1、クライアント2、クライアント3、ホスト、およびサーバがインターネットにアクセスできることを確認します(詳細は省略)。

#クライアント1からブロードキャストパケットを受信できるのは、ホスト、サーバ、およびクライアント3だけであることを確認します(詳細は省略)。

#クライアント1とクライアント2が相互に接続できないことを確認します(詳細は省略)。