ASR9000のQOS変更におけるDSCP値のトラブルシューティング

内容

概要

このドキュメントでは、Ciscoアグリゲーションサービスルータ(ASR)9000でQuality of Service(QOS)ポリシーの継承をトラブルシューティングする方法について説明します。物理ポートの入力ポリシー設定にDiffServコードポイント(DSCP)マーキングがある場合のルータの動作を示します。このポリシーは、その物理ポートの下にあるすべてのレイヤ2およびレイヤ3サブインターフェイスに適用されます。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- ASR9000でのレイヤ2バーチャルプライベートネットワーク(L2VPN)およびイーサネットサービスの設定

Cisco ASR 9000シリーズアグリゲーションサービスルータL2VPNおよびイーサネットサービスコンフィギュレーションガイド

- ASR9000のQuality of Service(QoS)設定

Cisco ASR 9000シリーズアグリゲーションサービスルータモジュラQoS設定ガイド

使用するコンポーネント

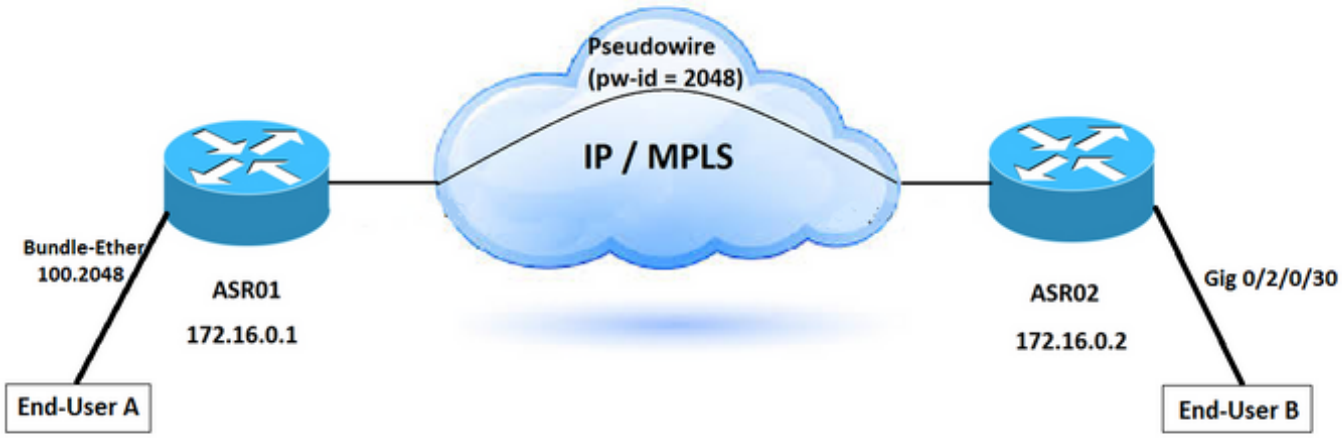
このドキュメントの情報は、Cisco ASR9000シリーズに基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

問題：一方向でのQOSのDSCP値の変更

パケットは一方向に再マーキングされます。Cisco ASR 9000上のポイントツーポイントレイヤ2(L2)接続を通過する際のQOSに新しいDifferentiated Services Code Point(DSCP)値が表示されます。L2接続は、MPLSネットワークを介して実装される疑似配線を介して設定されます。 このシナリオに関連するサブインターフェイスのDSCP値を変更する特別な設定はありません。元のパケットはユーザAから送信され、CS4としてDSCP値がマークされます。ただし、user-Bが受信したパケットは、AF41として設定されたDSCP値を示します。この問題は一方向、つまりAからBの方向でのみ発生します。

トポロジ



トラブルシュート

トラフィックはL2VPN接続を通過するため、ネットワーク内でDSCPの注釈が発生する場所を特定する必要があります。

パケットキャプチャは、DSCP値が変更された場所と方向を確認する方法の1つです。このシナリオでは、トラフィックは両方向からキャプチャされます。 ASR01からASR02への一方向で発生する問題を確認できます。 DSCP値は、ASR02に到達するとすぐに変更されます。パケットキャプチャは、ASR01ルータを離れた後にDSCP値が変更されたことを確認します。

『Cisco ASR 9000シリーズアグリゲーションサービスルータモジュラQuality of Service(QoS)コンフィギュレーションガイド』に従って、アクセスコントロールリスト(ACL)、プロトコルの一致、IP優先順位、DSCP、IPパケットのMultiprotocol Label Switching(MPLS)experimental bits(EXP)フィールド、またはClass of Service(CoS)など、1台のルータ内のトラフィックフロー

を識別するためのいくつかの方法が実行されます。

トラフィックをマーキングするには、IP Type of Service(ToS)バイトにIP PrecedenceまたはDSCPビットを設定します。

設定の確認

根本的な原因を見つけるには、設定を確認します。

ステップ 1：L2VPN設定を確認します。

```
ASR01- Config:
==============
l2vpn
router-id 172.16.0.1
pw-class TEST
encapsulation mpls
protocol ldp
!
bridge group DSCP-TEST
bridge-domain DSCP-TEST
mtu 9216
interface Bundle-Ether100.2048
!
vfi DSCP-TEST
neighbor 172.16.0.2 pw-id 2048
pw-class TEST
!

ASR02- Config:
============
l2vpn
router-id 172.16.0.2

pw-class TEST
encapsulation mpls
protocol ldp
!
bridge group DSCP-TEST
bridge-domain DSCP-TEST
mtu 9216
interface GigabitEthernet0/2/0/30.2048
!
vfi DSCP-TEST
neighbor 172.16.0.1 pw-id 2048
pw-class TEST
```

ステップ 2：インターフェイス設定を確認します。

バンドルインターフェイス100には入力サービスポリシーが設定されており、このポリシーはエンドユーザに接続され、異なるL2VPNサービスに対して複数のトラフィックを伝送します。トラフィックを区別するには、サブインターフェイスを設定し、トラフィックのタイプごとに固有のVLANを使用します。

```
ASR01- Interface Configuration:
================================
RP/0/RSP0/CPU0:ASR1# show running-config interface gigabitEthernet 0/1/0/4
```

```
Thu Jun 1 13:17:37.642 AEST
interface GigabitEthernet0/1/0/4
description "TO User-A-TEST"
bundle id 100 mode active
mtu 9192
!
RP/0/RSP0/CPU0:ASR1# show running-config interface Bundle-Ether100.2048
Thu Jun 1 13:17:43.438 AEST
interface Bundle-Ether100.2048 l2transport
encapsulation dot1q 2048 second-dot1q any
mtu 9216
!
RP/0/RSP0/CPU0:ASR1# show running-config interface gigabitEthernet 0/1/0/4.2048
Thu Jun 1 13:17:43.438 AEST
interface GigabitEthernet0/1/0/4.2048 l2transport
encapsulation dot1q 2048 second-dot1q any
mtu 9216
!
RP/0/RSP0/CPU0:ASR1# show running-config interface Bundle-Ether100
Thu Jun 1 13:20:43.438 AEST
interface Bundle-Ether100
description "To User-A"
mtu 9216
service-policy input INPUT   <<< ========================
service-policy output OUTPUT
bundle maximum-active links 1

ASR02: Interface Configuration:
============================

RP/0/RSP0/CPU0:ASR2#show running-config interface gigabitEthernet 0/2/0/30.2048
Thu Jun 1 15:25:06.742 AEST
interface GigabitEthernet0/2/0/30.2048 l2transport
encapsulation dot1q any
rewrite ingress tag push dot1q 2048 symmetric
mtu 9216
monitor-session span ethernet
!

RP/0/RSP0/CPU0:ASR2#show running-config interface gigabitEthernet 0/2/0/30
Thu Jun 1 15:25:00.516 AEST
interface GigabitEthernet0/2/0/30
description "To User-B"
mtu 9216
monitor-session span ethernet
speed 1000
transceiver permit pid all
!
```

ステップ 3：サービスポリシー設定を確認します。

この設定は、CS4としてマークされたパケットに一致し、AF41に注釈を付けるビデオトラフィック用のポリシーマップがあることを示しています。

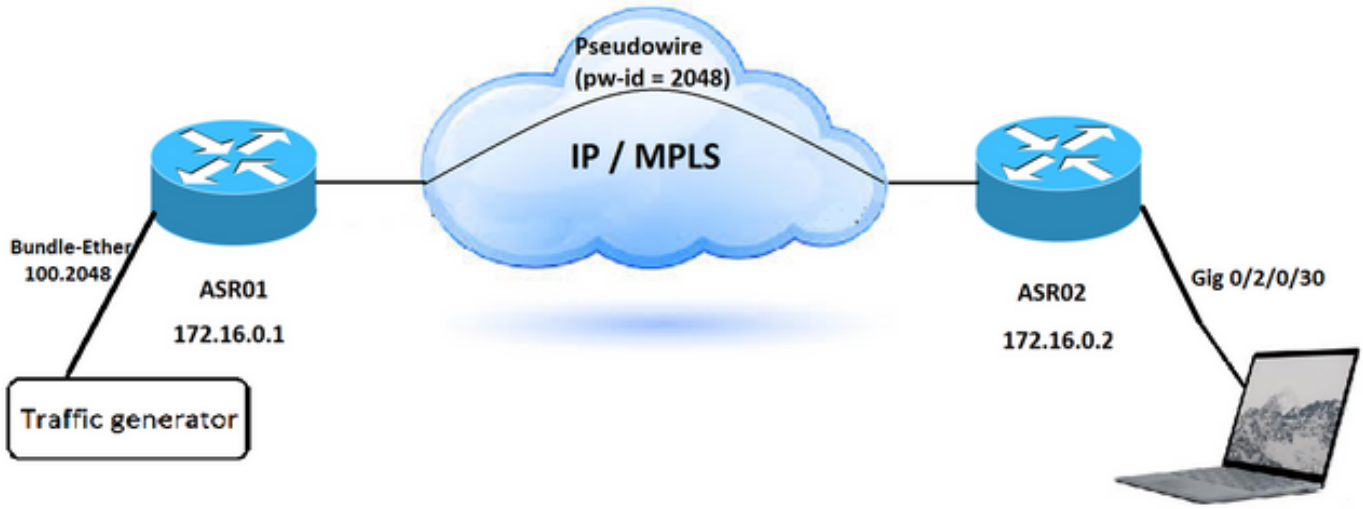
さらに、このポリシーは、異なるVLANタグを持つ別のL2VPNサービスに対して設定されます。ただし、この条件はメインバンドルインターフェイスに適用され、この条件を満たすすべての入力トラフィックに影響します。

```
policy-map INPUT
class CS4
set dscp af41
```

```
!
class-map match-any CS4
description Video Traffic
match cos 4
end-class-map
!
policy-map OUTPUT
class DSCP
set cos 4
priority level 2
police rate percent 33
conform-action transmit
exceed-action drop
!
class-map match-any DSCP
description Video Traffic
match dscp af41
end-class-map
```

ラボでのテストシナリオの再作成

ラボで同じシナリオを再作成し、このサービスポリシー設定が着信トラフィックのDSCP値にどのように影響するかを確認できます。



ステップ 1：サービスポリシーを使用せずに同様のシナリオを設定し、宛先でパケットをキャプチャします。

DSCP値は着信トラフィックに対してCS4に設定され、宛先では同じままです。

```
Ethernet II, Src: XeroxCor_00:0a:00 (00:00:01:00:0a:00), Dst: CiscoInc_e2:05:be
(18:ef:63:e2:05:be)
    Destination: CiscoInc_e2:05:be (18:ef:63:e2:05:be)
    Source: XeroxCor_00:0a:00 (00:00:01:00:0a:00)
    Type: IPv6 (0x86dd)
Internet Protocol Version 6, Src: 2020::1, Dst: 2020::2
    0110 .... = Version: 6
    .... 1000 0000 .... .... .... .... .... = Traffic class: 0x80 (DSCP: CS4, ECN: Not-ECT) <<
============
    .... .... .... 0000 0000 0000 0000 0000 = Flow label: 0x00000
    Payload length: 20
```

ステップ 2：トラフィックジェネレータに接続されたインターフェイスの入力方向に同じサービ

スポリシーを適用します。

ステップ 3： 2種類のトラフィックを生成します。1つはDSCP値がCS4に設定され、もう1つは他のDSCP値に設定されています。

ASR02の後でキャプチャされたパケットは次を示します。

着信トラフィックのDSCP値がCS4に設定されている場合、宛先で受信されたパケットにはDSCP値としてAF41が表示されます。ただし、サービスポリシーの基準に一致しない他のDSCP値を設定した場合、パケットのDSCP値は宛先に到達しても同じままになります。

```
Ethernet II, Src: XeroxCor_00:0a:00 (00:00:01:00:0a:00), Dst: CiscoInc_e2:05:be
(18:ef:63:e2:05:be)

    Destination: CiscoInc_e2:05:be (18:ef:63:e2:05:be)

    Source: XeroxCor_00:0a:00 (00:00:01:00:0a:00)

    Type: IPv6 (0x86dd)

Internet Protocol Version 6, Src: 2020::1, Dst: 2020::2

    0110 .... = Version: 6

    .... 1000 1000 .... .... .... .... .... = Traffic class: 0x88 (DSCP: AF41, ECN: Not-ECT) <<
============

    .... .... .... 0000 0000 0000 0000 0000 = Flow label: 0x00000

    Payload length: 20
```

解決方法

ASR01デバイスのバンドルインターフェイス（バンドル100）で設定された入力サービスポリシーは、基準に一致するパケットのDSCP値を書き換えます。CS4値を検索し、AF41で再マーキングします。したがって、この問題を解決するには、入力サービスポリシーを削除する必要があります。

ポリシーの継承については、『モジュラQoSサービスパケット分類の設定』ドキュメントで説明されています。ポリシーマップが物理ポートに適用されると、その物理ポートの下にあるすべてのレイヤ2およびレイヤ3サブインターフェイスにポリシーが適用されます。

これは、ASR 9000のデフォルトのマーキング動作です。

VLANタグまたはMPLSラベルが入力または出力インターフェイスに追加されると、CoSおよびEXPのデフォルト値がそれらのタグおよびラベルに移動します。その後、ポリシーマップに基づいてデフォルト値を上書きできます。CoSおよびEXPのデフォルト値は、システムへの入力時にパケット内の信頼できるフィールドに基づきます。ルータは、パケットタイプと入力インターフェイスの転送タイプ（レイヤ2またはレイヤ3）に基づいて、特定のフィールドの暗黙的な信頼を実装します。

デフォルトでは、ルータはポリシーマップが設定されていない場合、IP優先順位またはDSCPを変更しません。

ルータのデフォルトの動作は次のとおりです。

- xconnectやbridge-domainなどの入力または出力レイヤ2インターフェイスでは、入力インターフェイスに追加されるすべてのフィールドに対して最も外側のCoS値が使用されます。レイヤ2の書き換えのために追加されるVLANタグがある場合、着信する最も外側のCoS値が新しいVLANタグに使用されます。MPLSラベルが追加されると、MPLSタグのEXPビットにCoS値が使用されます。
- 入力または出力レイヤ3インターフェイス（IPv4またはIPv6パケット用に重み付けされたルーテッドまたはラベル）では、3つのDSCPビットと優先順位ビットが着信パケットで識別されます。MPLSパケットでは、EXPビットの最も外側のラベルが識別され、この値は入力インターフェイスで追加される新しいフィールドに使用されます。MPLSラベルが追加されると、新しく追加されたMPLSタグのEXPビットに、識別された優先順位、DSCP、またはMPLS EXP値が使用されます。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。