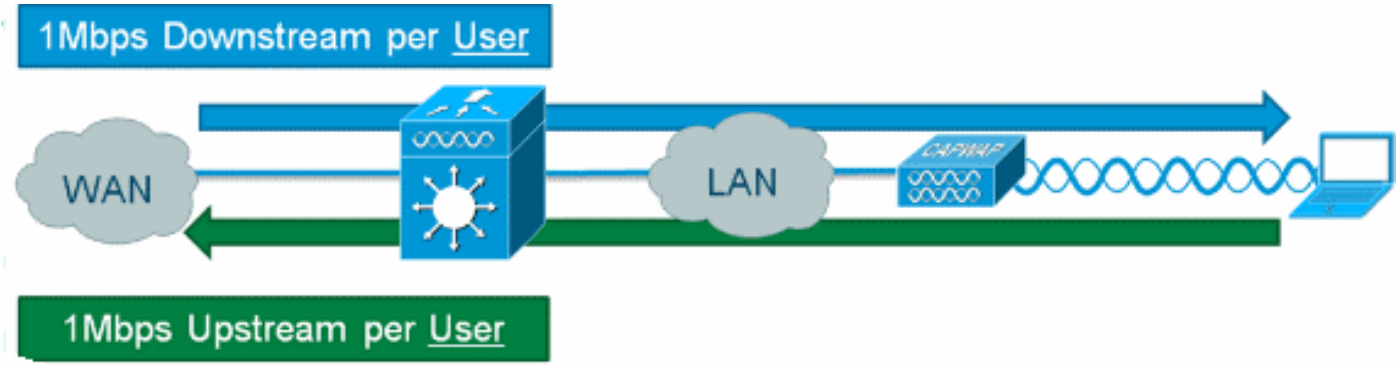
無線LAN每使用者速率限制解決方案

目錄

簡介



在Cisco無線LAN控制器上可為無線使用者提供下游每使用者速率限制，但將IOS微流管制新增到解決方案中可允許在上游和下游方向進行粒度速率限制。實施從頻寬「hog」保護到每使用者速率限制範圍的動機是為客戶網路訪問實施分層頻寬模型，在某些情況下，會根據需要將免除頻寬管制的特定資源列入白名單。除了限制當前生成的IPv4流量外，該解決方案還能夠限制每個使用者的IPv6速率。這提供了投資保護。

必要條件

需求

微流管制需要使用執行Cisco IOS®軟體版本12.2(14)SX或更新版本的管理引擎720或更新版本。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 無線LAN控制器
- 存取點(AP)
- Cisco Catalyst Supervisor 720或更高版本

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

Catalyst 6500組態

微流管制配置

請完成以下步驟：

1. 利用微流管制首先需要建立訪問控制清單(ACL)來識別流量，以便應用限制策略。**注意：**此配置示例對無線客戶端使用192.168.30.x/24子網。
```
ip access-list extended acl-wireless-downstream
permit ip any 192.168.30.0 0.0.0.255
ip access-list extended acl-wireless-upstream
permit ip 192.168.30.0 0.0.0.255 any
```
2. 建立要在上一個ACL上匹配的類對映。
```
class-map match-all class-wireless-downstream
match access-group name acl-wireless-downstream
class-map match-all class-wireless-upstream
match access-group name acl-wireless-upstream
```
3. 建立策略對映會將先前建立的ACL和類對映連結到要應用於流量的不同操作。在這種情況下，兩個方向的流量都被限製為1Mbps。在上游方向（客戶端到AP）使用源流掩碼，而在下游方向（AP到客戶端）使用目標流掩碼。
```
policy-map police-wireless-upstream
class class-wireless-upstream
police flow mask src-only 1m 187500 conform-action transmit exceed-action drop
policy-map police-wireless-downstream
class class-wireless-downstream
police flow mask dest-only 1m 187500 conform-action transmit exceed-action drop
```

有關配置微流策略的詳細資訊，請參閱Cisco Catalyst 6500中基於使用者的速率限制。

調整頻寬管制策略

策略對映中的policy語句是配置實際*Bandwidth*（以位為單位）和*Burst* size（以位元組為單位）引數的位置。

突發大小的好經驗法則是：

```
Burst = (Bandwidth / 8) * 1.5
```

範例：

此線路使用1Mbps（位）的速率：

```
police flow mask dest-only 1m 187500 conform-action transmit exceed-action drop
```

此線路使用5Mbps（位）的速率：

```
police flow mask dest-only 5mc 937500 conform-action transmit exceed-action drop
```

將頻寬策略中的資源列入白名單

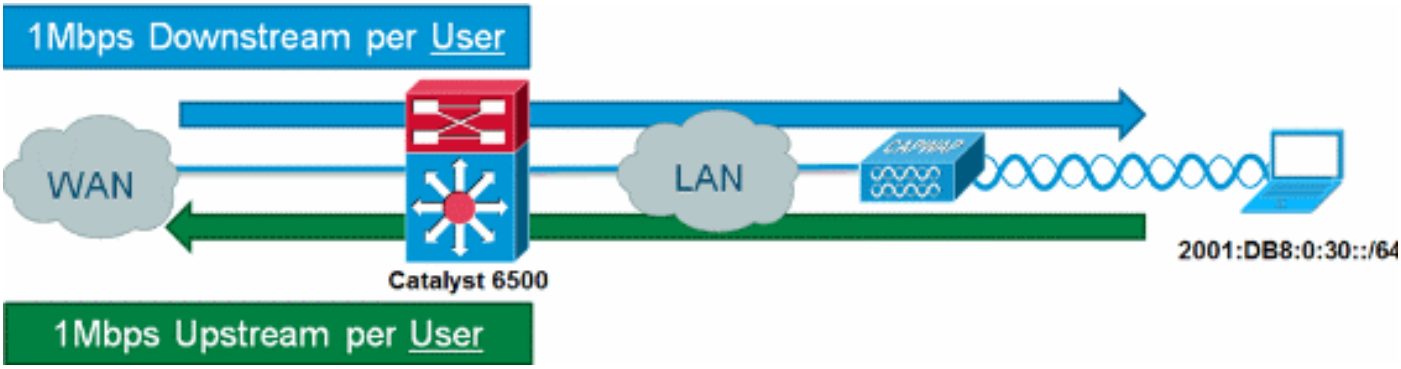
在某些情況下，某些網路資源應免於頻寬管制，例如Windows Update伺服器或狀態修正裝置。除主機外，白名單還可以用於使整個子網免於頻寬管制。

範例：

此範例在與192.168.30.0/24網路通訊時，將主機192.168.20.22排除在任何頻寬限制之外。

```
ip access-list extended acl-wireless-downstream
deny ip host 192.168.20.22 192.168.30.0 0.0.0.255
permit ip any 192.168.30.0 0.0.0.255
ip access-list extended acl-wireless-upstream
deny ip 192.168.30.0 0.0.0.255 host 192.168.20.22
permit ip 192.168.30.0 0.0.0.255 any
```

IPv6微流量管制



請完成以下步驟：

1. 在Catalyst 6500上新增另一個訪問清單以標識要限制的IPv6流量。

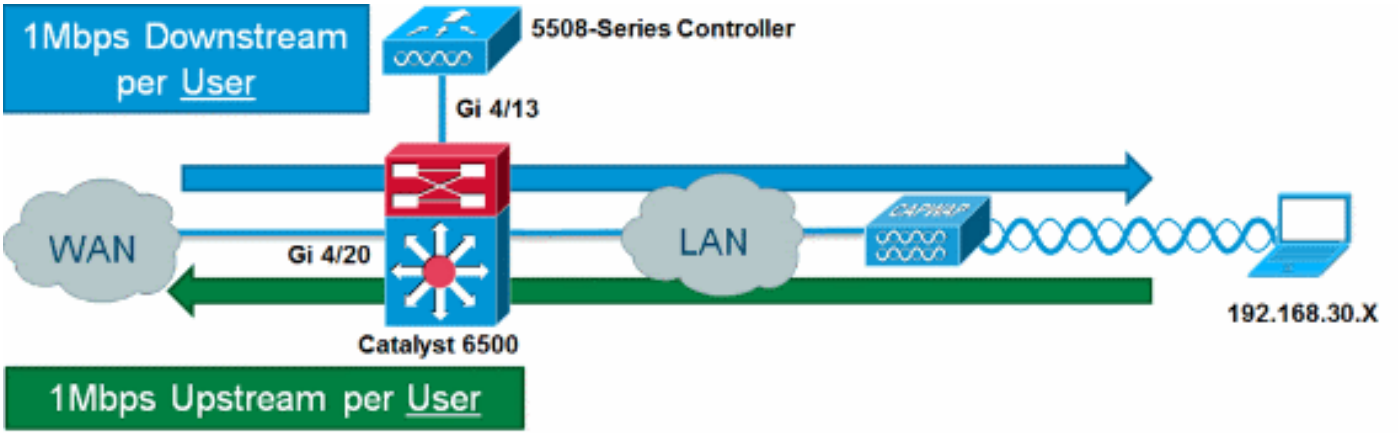
```
ipv6 access-list aclv6-wireless-downstream
permit ipv6 any 2001:DB8:0:30::/64
!
ipv6 access-list aclv6-wireless-upstream
permit ipv6 2001:DB8:0:30::/64 any
```

2. 修改類對映以包括IPv6 ACL。

```
class-map match-any class-wireless-downstream
match access-group name aclv6-wireless-downstream
match access-group name acl-wireless-downstream
class-map match-any class-wireless-upstream
match access-group name aclv6-wireless-upstream
match access-group name acl-wireless-upstream
```

基於裝置的(2500、4400、5500)控制器配置

為了使用基於裝置的控制器（如5508系列）提供微流管制，配置過於簡單。控制器介面的配置方式與任何其它VLAN類似，而Catalyst 6500服務策略應用於控制器介面。



請完成以下步驟：

1. 在控制器的傳入連線埠上套用`police-wireless-upstream`。

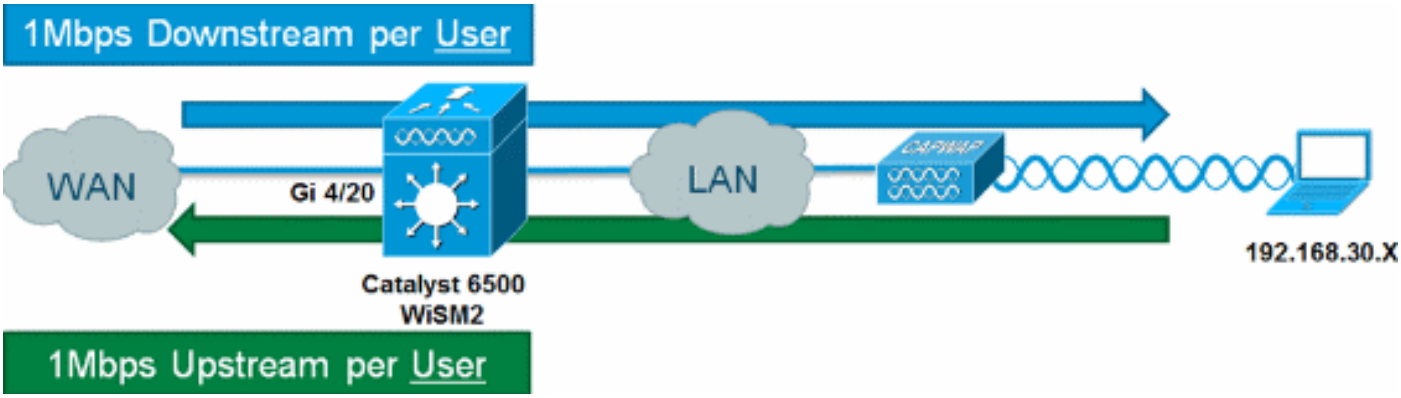
```
interface GigabitEthernet4/13
description WLC
switchport
switchport trunk allowed vlan 30
switchport mode trunk
service-policy input police-wireless-upstream
end
```

2. 在上行LAN/WAN埠上應用`policy-wireless-downstream`。

```
interface GigabitEthernet4/20
description WAN
switchport
switchport access vlan 20
switchport mode access
service-policy input police-wireless-downstream
end
```

基於模組的(WiSM、WiSM2)控制器配置

為了通過無線服務模組2(WiSM2)在Catalyst 6500上利用微流管制，必須調整配置以使用基於VLAN的服務品質(QoS)。這表示微流策略不直接應用於埠介面（例如Gi1/0/1），而是應用於VLAN介面。



請完成以下步驟：

1. 為基於VLAN的QoS配置WiSM:

```
wism service-vlan 800
```

```
wism module 1 controller 1 allowed-vlan 30
wism module 1 controller 1 qos vlan-based
```

2. 在客戶端VLAN SVI上應用`policy-wireless-upstream`：

```
interface Vlan30
description Client-Limited
ip address 192.168.30.1 255.255.255.0
ipv6 address 2001:DB8:0:30::1/64
ipv6 enable
service-policy input police-wireless-upstream
end
```

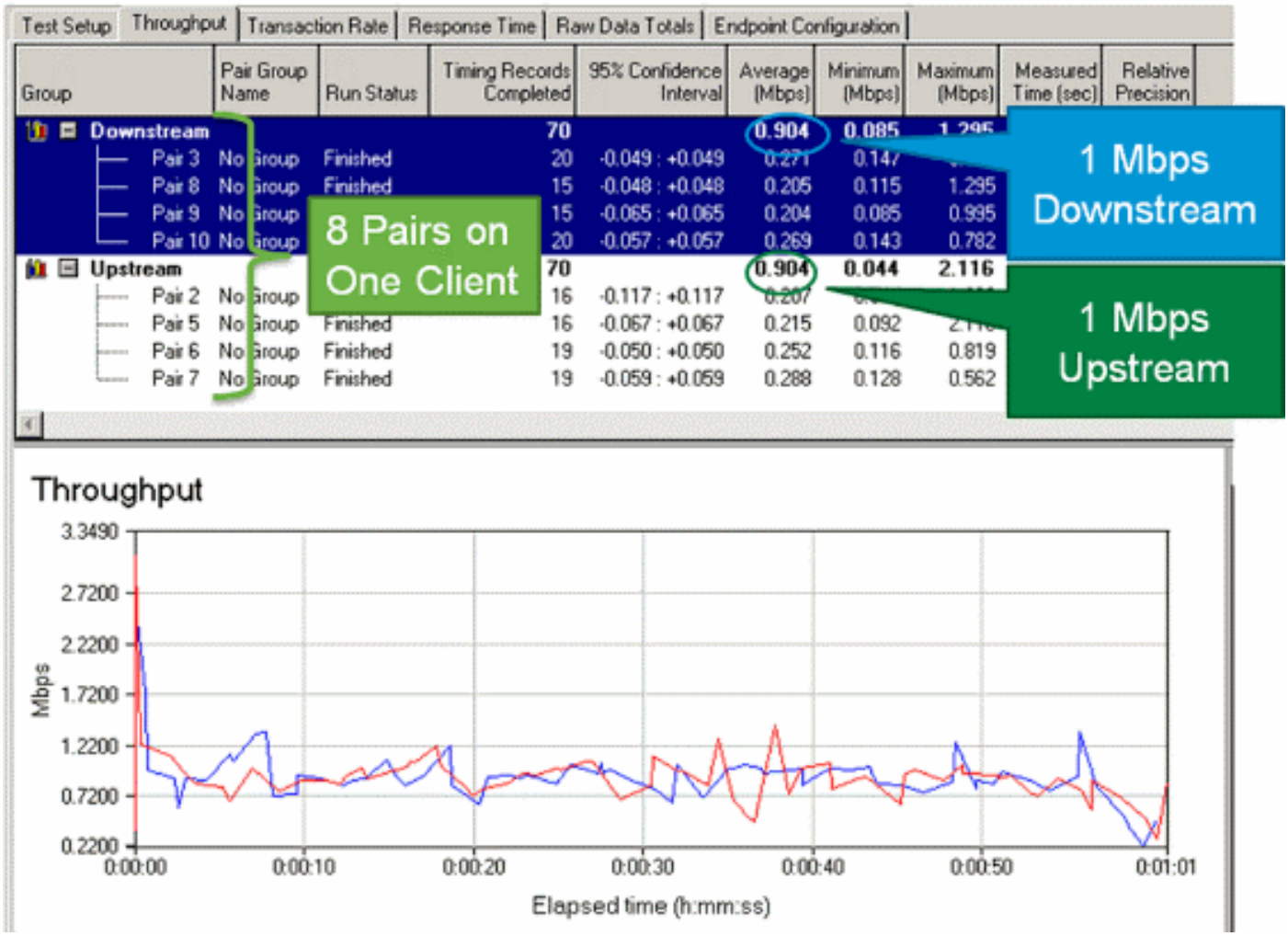
3. 在上行LAN/WAN埠上應用`policy-wireless-downstream`。

```
interface GigabitEthernet4/20
description WAN
switchport
switchport access vlan 20
switchport mode access
service-policy input police-wireless-downstream
end
```

解決方案驗證

每個使用者速率限制的主要要求之一是能夠限制所有來自特定使用者且目的地為特定使用者的流量。為了驗證Microflow管制解決方案是否符合此要求，IxChariot用於模擬特定使用者的四個同時下載作業階段和四個同時上傳作業階段。這可能表示有人啟動FTP會話、瀏覽Web和觀看影片流，同時傳送包含大型附件的電子郵件等。

在此測試中，IxChariot使用「Throughput.scr」指令碼配置了TCP流量，以便使用受限流量測量鏈路速度。Microflow管制解決方案能夠為使用者將所有流限製為總的下游1Mbps和上游1Mbps。此外，所有流都使用大約25%的可用頻寬（例如，每流250kbps x 4 = 1Mbps）。



注意：由於微流策略操作發生在第3層，因此TCP流量吞吐量的最終結果可能因協定開銷而低於配置的速率。

相關資訊

- [技術支援與文件 - Cisco Systems]

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。