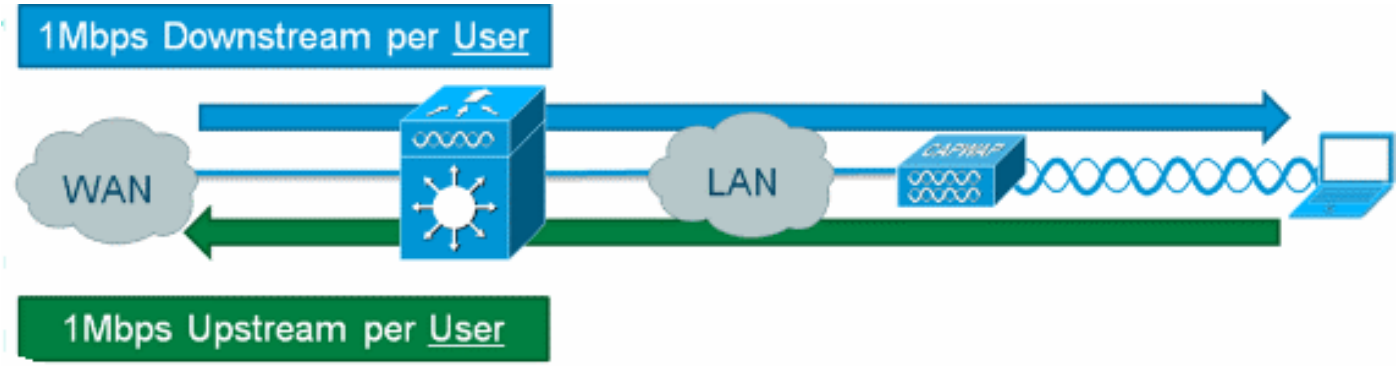
无线LAN每用户速率限制解决方案

目录

简介



在思科无线局域网控制器上可以为无线用户提供下行每用户速率限制，但解决方案中添加IOS微流管制允许在上游和下行方向进行精细的速率限制。实施从带宽“占用”保护到每用户速率限制范围的动机是为客户网络访问实施分层带宽模型，在某些情况下，会将免除带宽管制的特定资源列入白名单。除了限制当前一代的IPv4流量外，该解决方案还能够限制每用户IPv6速率。这提供了投资保护。

先决条件

要求

微流管制需要使用运行Cisco IOS®软件版本12.2(14)SX或更高版本的Supervisor 720或更高版本。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 无线 LAN 控制器
- 接入点 (AP)
- Cisco Catalyst Supervisor 720或更高版本

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

Catalyst 6500配置

微流管制配置

请完成以下步骤：

1. 使用微流管制首先需要创建访问控制列表(ACL)来识别流量，以便应用限制策略。**注意：**此配置示例对无线客户端使用192.168.30.x/24子网。
```
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. 创建与上一个ACL匹配的类映射。
```
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. 创建策略映射会将之前创建的ACL和类映射链接到要应用于流量的不同操作。在这种情况下，两个方向的流量都被限制为1Mbps。源流掩码用于上游方向（客户端到AP），目标流掩码用于下游方向（AP到客户端）。
```
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
```

有关配置微流策略的详细信息，请参阅Cisco Catalyst 6500中基于用户的速率限制。

调整带宽管制策略

策略映射中的policy语句用于配置实际*Bandwidth*（以位配置）和*Burst* size（以字节配置）参数。

突发大小的一个好的经验法则是：

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

示例：

此线路使用1Mbps（位）的速率：

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

此线路使用5Mbps（位）的速率：

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

将资源从带宽管制列入白名单

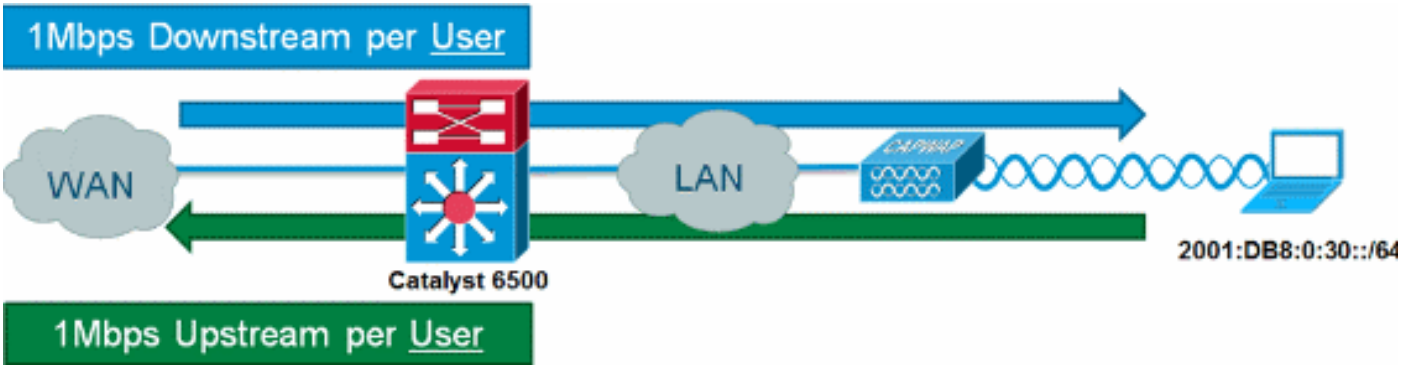
在某些情况下，某些网络资源应免于带宽管制，例如Windows Update服务器或状态补救设备。除主机外，白名单还可用于使整个子网免于带宽管制。

示例：

此示例将主机192.168.20.22排除在与网络192.168.30.0/24通信时的任何带宽限制。

```
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微流管制



请完成以下步骤：

1. 在Catalyst 6500上添加另一个访问列表，以标识要限制的IPv6流量。

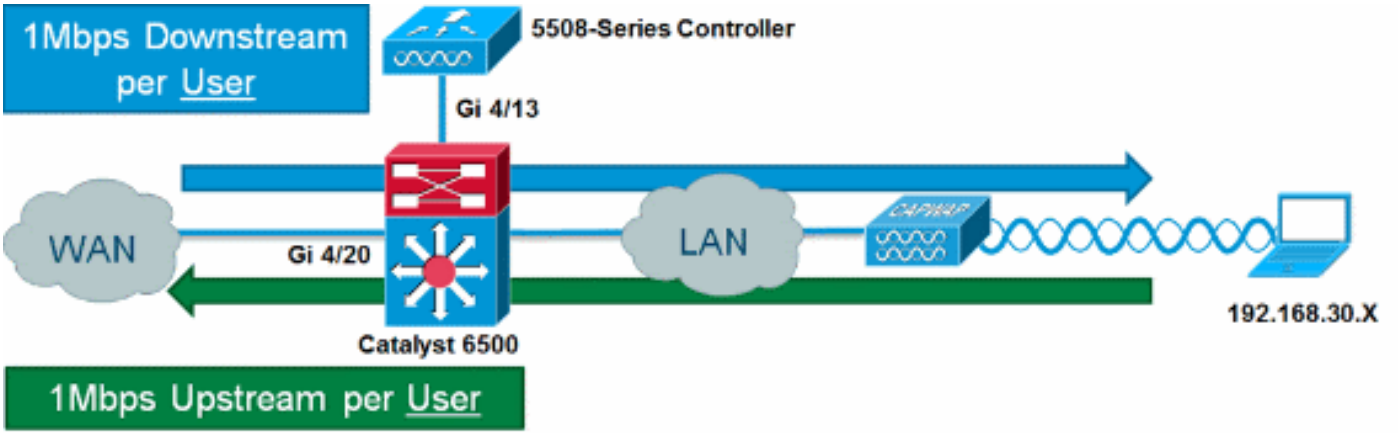
```
ipv6 access-list aclv6-wireless-downstream
permit ipv6 any 2001:DB8:0:30::/64
!
ipv6 access-list aclv6-wireless-upstream
permit ipv6 2001:DB8:0:30::/64 any
```

2. 修改类映射以包括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
```

基于设备的(2500、4400、5500)控制器配置

为了使用基于设备的控制器（如5508系列）提供微流管制，配置过于简单。控制器接口配置类似于任何其他VLAN，而Catalyst 6500服务策略应用于控制器接口。



请完成以下步骤：

1. 对来自控制器的传入端口应用police-wireless-upstream。

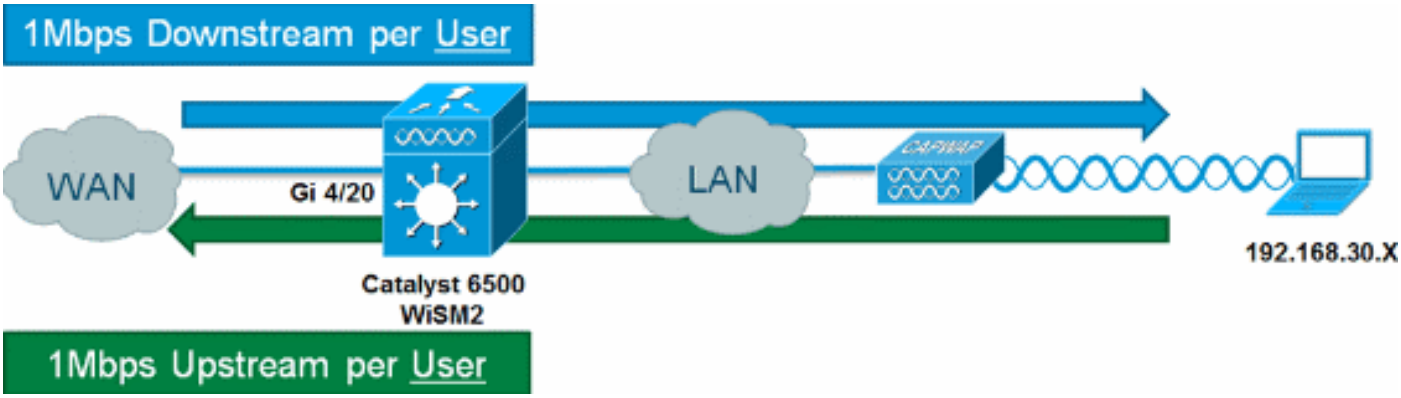
```
interface GigabitEthernet4/13
description WLC
switchport
switchport trunk allowed vlan 30
switchport mode trunk
service-policy input police-wireless-upstream
end
```

2. 在上行链路LAN/WAN端口上应用policy-wireless-downstream。

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

基于模块的(WiSM、WiSM2)控制器配置

为了通过无线服务模块2(WiSM2)在Catalyst 6500上利用微流管制，必须调整配置以使用基于VLAN的服务质量(QoS)。这意味着微流管制策略不直接应用于端口接口（例如Gi1/0/1），而是应用于VLAN接口。



请完成以下步骤：

1. 为基于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. 在客户端VLAN SVI上应用`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
```

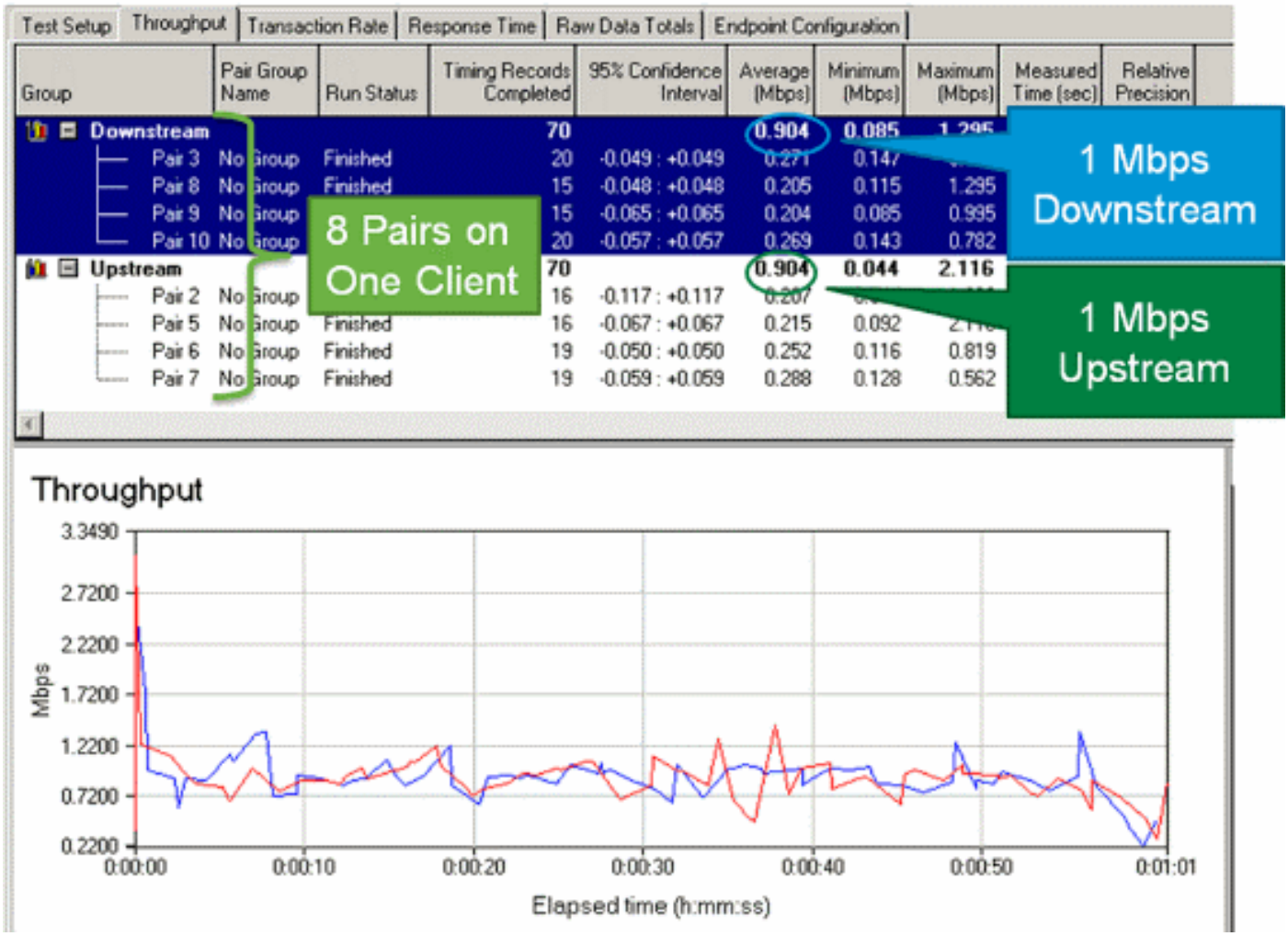
3. 在上行链路LAN/WAN端口上应用`policy-wireless-downstream`。

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

解决方案验证

每用户速率限制的主要要求之一是能够限制所有来自和发往特定用户的流量。为了验证Microflow策略解决方案是否满足此要求，IxChariot用于模拟特定用户的四个同步下载会话和四个同步上传会话。这可能表示有人启动FTP会话、浏览Web和观看视频流，同时发送包含大型附件的电子邮件等。

在本测试中，IxChariot使用“Throughput.scr”脚本配置了TCP流量，以便使用受限流量测量链路速度。Microflow策略解决方案能够将所有流限制为总下行速度为1Mbps，上行速度为1Mbps。此外，所有数据流使用大约25%的可用带宽（例如，每流250kbps x 4 = 1Mbps）。



注意：由于微流管制操作发生在第3层，因此TCP流量吞吐量的最终结果可能由于协议开销而低于配置的速率。

相关信息

- [技术支持和文档 - Cisco Systems]

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。