

# 限制解决方案的无线局域网每用户速率

## 目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[Catalyst 6500配置](#)

[微流策略管理配置](#)

[调节带宽策略策略](#)

[从带宽管制的Whitelisting资源](#)

[IPv6微流策略管理](#)

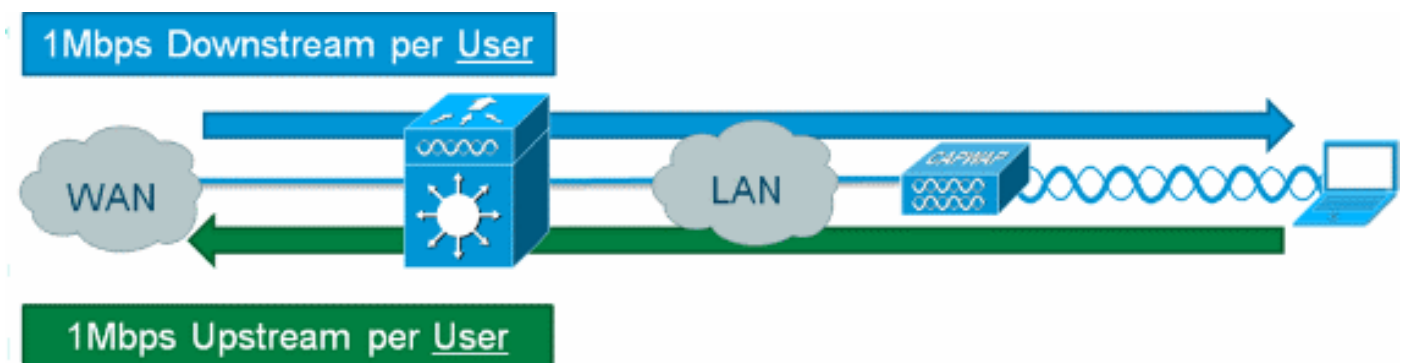
[基于设备的\(2500, 4400, 5500\)控制器配置](#)

[基于模块的\(WiSM, WiSM2\)控制器配置](#)

[解决方案验证](#)

[相关信息](#)

## 简介



提供限制下行每用户的速率为无线用户是可能的在Cisco无线LAN控制器，但是IOS微流策略管理的新增内容对解决方案的允许限制在两个上行和下行方向的粒状速率。实现的每用户速率限制动机范围自带宽“hog”保护是实现客户网络网络访问的有排列的带宽型号，和在某些情况下，从带宽管制是豁免作为需求的whitelist特定的资源。除限制的当前生成IPv4流量之外，解决方案能够每用户IPv6速率限制。此提供投资保护。

## 先决条件

### 要求

微流策略管理要求使用运行Cisco IOS软件版本12.2(14)SX或以上的Supervisor 720或以上。

### 使用的组件

本文档中的信息基于以下软件和硬件版本：

- 无线局域网控制器
- 接入点(AP)
- Cisco Catalyst Supervisor 720或以上

## 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

## 微流策略管理配置

完成这些步骤：

1. 使用微流策略管理首先要求访问控制表(ACL)创建识别流量为了运用一项限制的策略。**注意**：此配置示例使用192.168.30.x/24子网无线客户端。

```
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. 创建类映射匹配在上一个ACL。

```
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. 创建策略映射与一明显的操作适用将连接以前已创建ACL和类映射于流量。在这种情况下流量被抑制对在两个方向的1Mbps。来源流掩码用于上行方向(AP的客户端)，并且目的地流掩码用于下行方向(对客户端的AP)。

```
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
```

关于配置微流策略管理的更多信息，参考[限制在Cisco Catalyst 6500的基于用户的速率](#)。

## 调节带宽策略策略

在策略映射内的策略语句是实际带宽(配置在位)，并且突发流量大小(配置在字节)参数配置。

突发流量大小的一好经验做法是：

$$\text{Burst} = (\text{Bandwidth} / 8) * 1.5$$

示例：

此线路使用每速率1Mbps (位)：

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

此线路使用每速率5Mbps (位)：

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

## 从带宽管制的Whitelisting资源

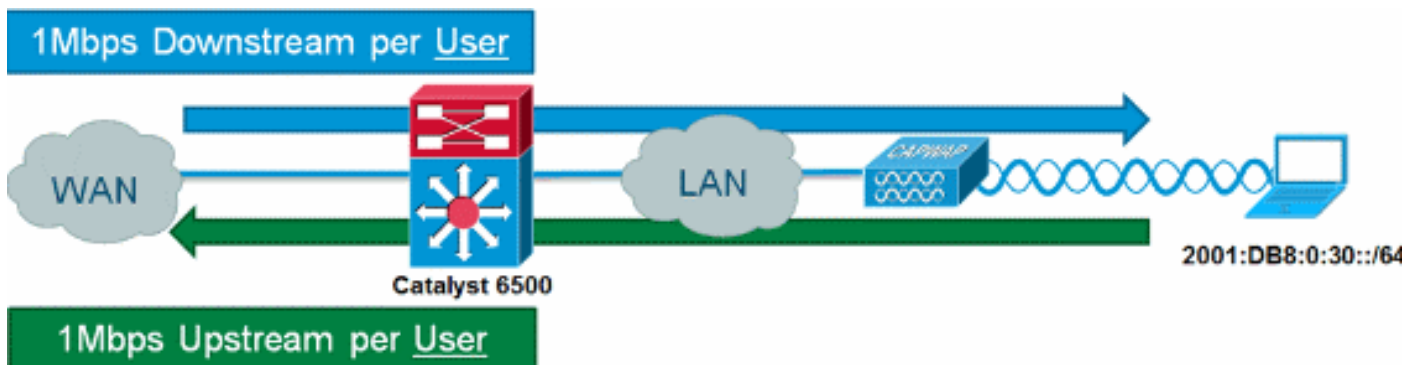
有时，某些网络资源应该是豁免从带宽管制例如Windows更新服务器或摆修正设备姿势。除主机之外，whitelisting可能也用于豁免从带宽管制的全部子网。

示例：

当通信与192.168.30.0/24网络时，此示例从所有带宽限制屏蔽主机192.168.20.22。

```
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微流策略管理



完成这些步骤：

1. 添加在Catalyst 6500的另一访问列表识别将被节流的IPv6流量。

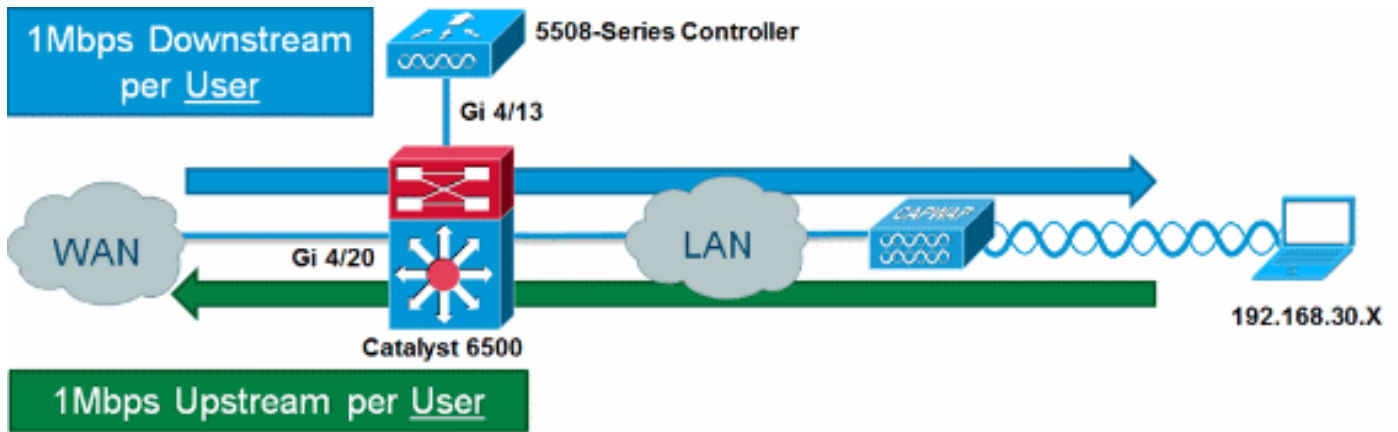
```
ipv6 access-list aclv6-wireless-downstream
permit ipv6 any 2001:DB8:0:30::/64
!
ipv6 access-list aclv6-wireless-upstream
permit ipv6 2001:DB8:0:30::/64 any
```

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

为了提供微流策略管理一个基于设备的控制器，例如5508系列，配置是单纯化的。而Catalyst 6500服务策略应用对控制器接口，控制器接口配置类似于其他VLAN。



完成这些步骤：

1. 应用在传入端口的police无线从控制器。

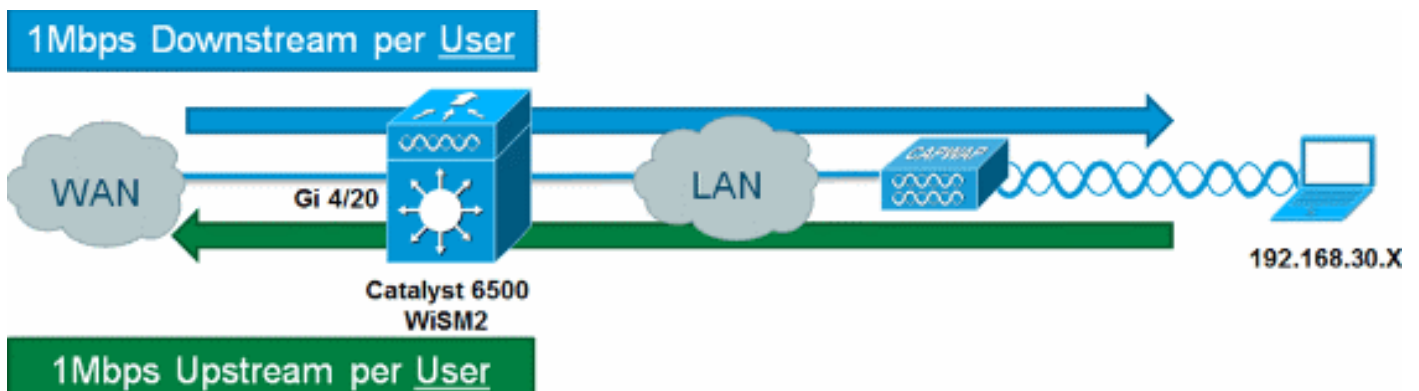
```
interface GigabitEthernet4/13
description WLC
switchport
switchport trunk allowed vlan 30
switchport mode trunk
service-policy input police-wireless-upstream
end
```

2. 应用在上行链路LAN/WAN端口的策略无线。

```
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

为了有效利用在Catalyst 6500的微流策略管理与无线服务Module2 (WiSM2)，必须调节配置使用基于vlan的服务质量(QoS)。这在VLAN接口意味着微流策略管理策略没有应用直接地对端口接口(例如，Gi1/0/1)，但是应用。



完成这些步骤：

1. 配置基于vlan的QoS的WiSM：

```
wism service-vlan 800
```

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

## 2. 应用在客户端VLAN SVI的策略无线：

```
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
```

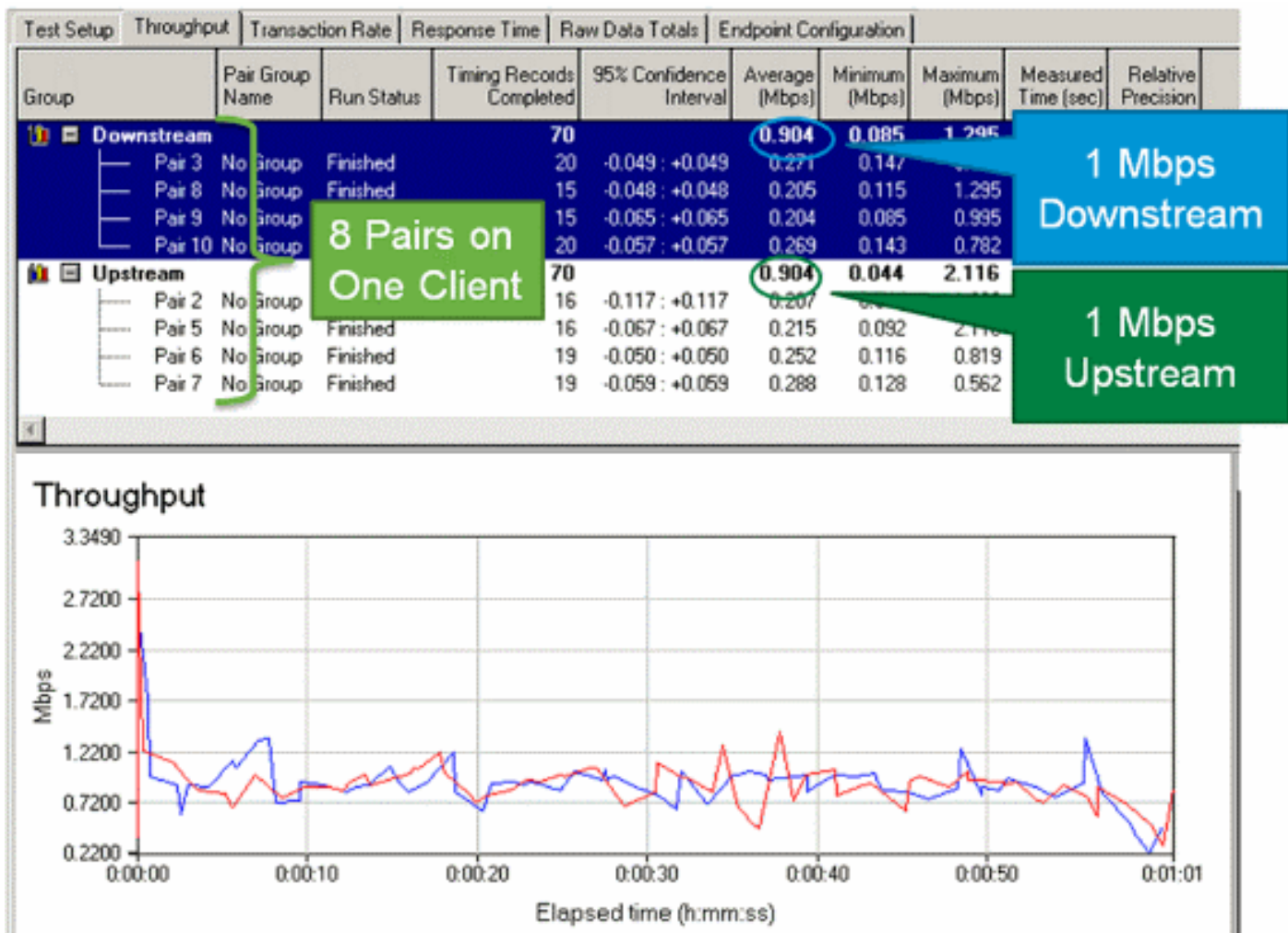
## 3. 应用在上行链路LAN/WAN端口的策略无线。

```
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

其中一个每用户速率限制的主要需求是能力对特定用户限制来自的所有流和注定。为了验证微流策略管理解决方案达到此需求，IxChariot用于模拟四同时下载会话和四同时加载会话特定用户的。这能代表启动FTP会话，浏览Web和观看视频流，当发送一电子邮件用一个大附件时等等的某人。

使用被抑制的流量，在此测验中IxChariot配置与“Throughput.scr”脚本使用TCP数据流为了测量链路的速度。微流策略管理解决方案能节流所有数据流下来到总共1Mbps下行和1Mbps上行用户的。另外，所有数据流使用大致25%可用的带宽(例如，250kbps每数据流x 4 = 1Mbps)。



注意：由于微流策略管理操作发生在第3层，TCP数据流吞吐量的最终结果比配置速率可以是较少由于协议开销。

## 相关信息

- [技术支持和文档 - Cisco Systems](#)