

Solución de limitación de velocidad por usuario de LAN inalámbrica

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Configuración de Catalyst 6500](#)

[Configuración de regulación de microflujo](#)

[Ajuste de la Política de Regulación de Ancho de Banda](#)

[Lista blanca de recursos de directivas de ancho de banda](#)

[Políticas de microflujo IPv6](#)

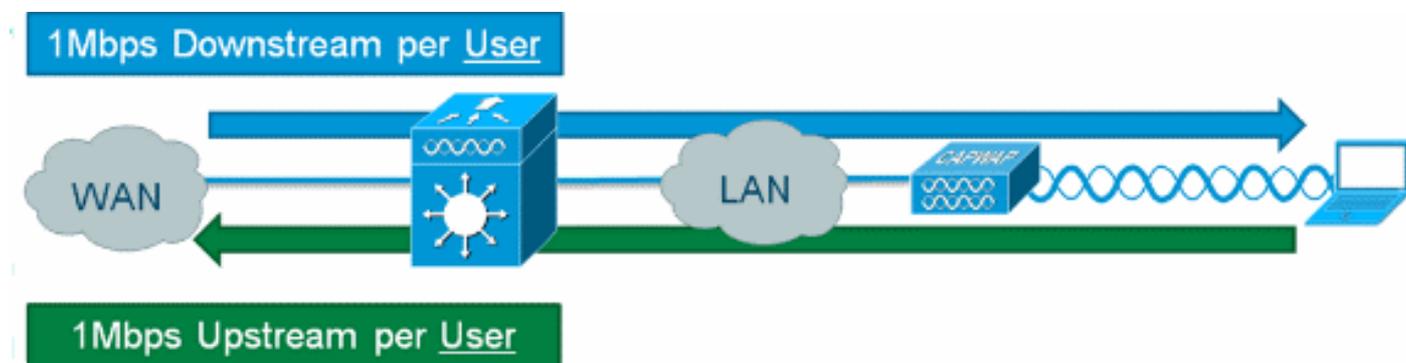
[Configuración del controlador basado en dispositivo \(2500, 4400, 5500\)](#)

[Configuración del controlador basado en módulos \(WiSM, WiSM2\)](#)

[Verificación de soluciones](#)

[Información Relacionada](#)

Introducción



Es posible proporcionar limitación de velocidad descendente por usuario para los usuarios de red inalámbrica en controladores Cisco Wireless LAN, pero añadir la regulación de microflujo de IOS a la solución permite la limitación de velocidad granular tanto en dirección ascendente como descendente. La motivación para implementar límites de velocidad por usuario en los rangos de protección de "cerdo" de ancho de banda es implementar modelos de ancho de banda por niveles para el acceso a la red del cliente y, en algunos casos, incluir en la lista blanca recursos concretos que están exentos de la regulación del ancho de banda como requisito. Además de limitar el tráfico IPv4 de la generación actual, la solución puede limitar la velocidad IPv6 por usuario. Esto protege la inversión.

Prerequisites

Requirements

La regulación de microflujo requiere el uso de un Supervisor 720 o posterior que ejecute una versión de Cisco IOS® Software Release 12.2(14)SX o posterior.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Controladores de LAN inalámbrica
- Puntos de acceso (AP)
- Cisco Catalyst Supervisor 720 o posterior

Convenciones

Consulte [Convenciones de Consejos Técnicos Cisco para obtener más información sobre las convenciones del documento.](#)

Configuración de Catalyst 6500

Configuración de regulación de microflujo

Complete estos pasos:

1. El uso de la regulación de tráfico de Microflow requiere en primer lugar la creación de una lista de control de acceso (ACL) para identificar el tráfico y aplicar una política de limitación. **Nota:** Este ejemplo de configuración utiliza la subred 192.168.30.x/24 para clientes inalámbricos.

```
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. Cree un mapa de clase que coincida con la ACL anterior.

```
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. La creación de un policy-map enlazará el ACL y el class-map creados anteriormente a una acción distinta que se aplicará al tráfico. En este caso, el tráfico se está acelerando a 1 Mbps en ambas direcciones. Una máscara de flujo de origen se utiliza en la dirección de flujo ascendente (cliente a AP) y una máscara de flujo de destino se utiliza en la dirección de flujo descendente (AP a cliente).

```
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
```

Para obtener más información sobre la configuración de la regulación de tráfico de Microflow, consulte [Limitación de velocidad basada en el usuario en Cisco Catalyst 6500.](#)

Ajuste de la Política de Regulación de Ancho de Banda

La sentencia de política dentro del policy-map es donde se configuran los parámetros reales *Bandwidth* (configurado en bits) y *Burst size* (configurado en bytes).

Una buena regla general para el tamaño de ráfaga es:

$Burst = (Bandwidth / 8) * 1.5$

Ejemplo:

Esta línea utiliza una velocidad de 1 Mbps (bits):

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

Esta línea utiliza una velocidad de 5 Mbps (bits):

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

Lista blanca de recursos de directivas de ancho de banda

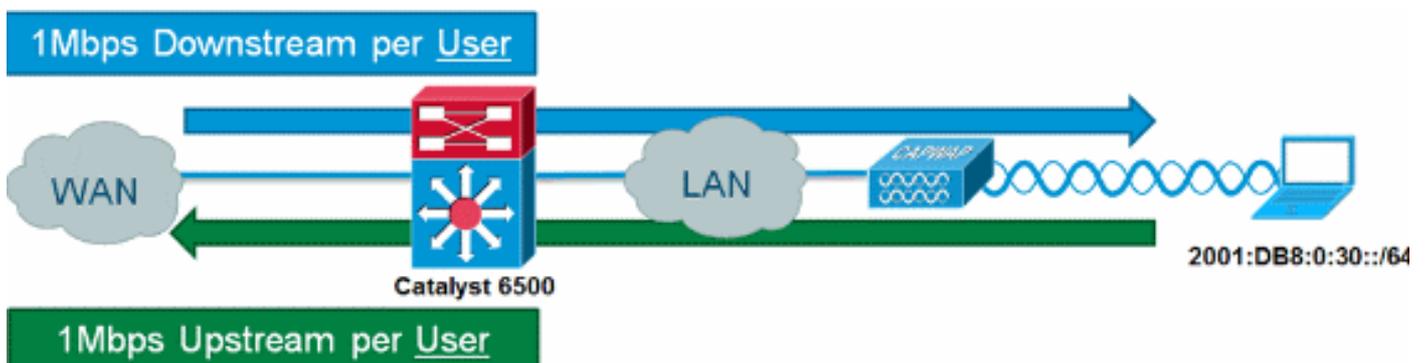
En algunos casos, ciertos recursos de red deben estar exentos de la regulación del ancho de banda, como un servidor de Windows Update o un dispositivo de corrección de estado. Además de los hosts, las listas blancas también se pueden utilizar para eximir subredes enteras de la regulación del ancho de banda.

Ejemplo:

Este ejemplo excluye al host 192.168.20.22 de cualquier limitación de ancho de banda cuando se comunica con la red 192.168.30.0/24.

```
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
```

Políticas de microflujo IPv6



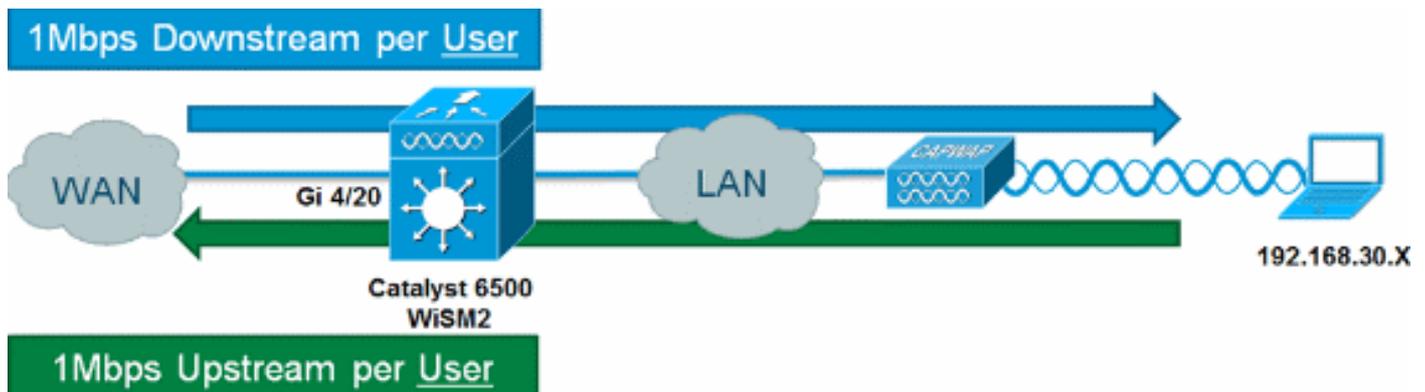
Complete estos pasos:

1. Agregue otra lista de acceso en Catalyst 6500 para identificar el tráfico IPv6 que se debe

end

Configuración del controlador basado en módulos (WiSM, WiSM2)

Para aprovechar la regulación de tráfico de Microflow en Catalyst 6500 con Wireless Service Module2 (WiSM2), la configuración debe ajustarse para utilizar calidad de servicio (QoS) basada en VLAN. Esto significa que la política de regulación de tráfico de Microflow no se aplica directamente a la interfaz de puerto (por ejemplo, Gi1/0/1), sino que se aplica a la interfaz VLAN.



Complete estos pasos:

1. Configuración de WiSM para QoS basada en VLAN:

```
wism service-vlan 800
wism module 1 controller 1 allowed-vlan 30
wism module 1 controller 1 qos vlan-based
```

2. Aplique `policy-wireless-upstream` en la VLAN SVI del cliente:

```
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
```

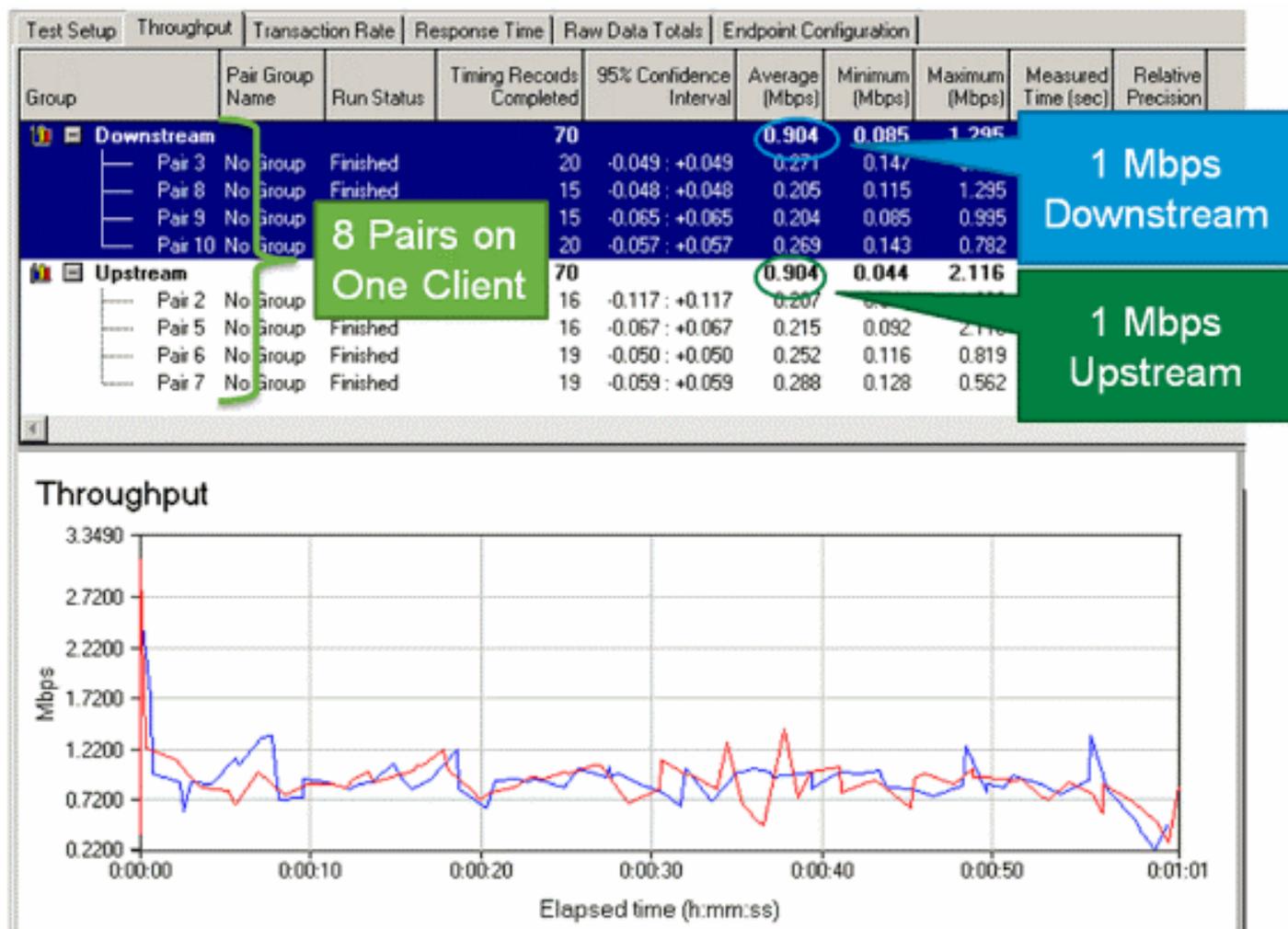
3. Aplique `policy-wireless-downstream` en los puertos LAN/WAN de enlace ascendente.

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

Verificación de soluciones

Uno de los principales requisitos de la limitación de velocidad por usuario es la capacidad de limitar todos los flujos que provienen de un usuario determinado y están destinados a él. Para verificar que la solución de regulación de tráfico de Microflow cumple con este requisito, IxChariot se utiliza para simular cuatro sesiones de descarga simultáneas y cuatro sesiones de carga simultáneas para un usuario en particular. Esto puede representar que alguien inicie una sesión FTP, navegue por la Web y vea una secuencia de vídeo mientras envía un correo electrónico con un archivo adjunto de gran tamaño, etc.

En esta prueba, IxChariot se configura con la secuencia de comandos "Processing.scr" utilizando el tráfico TCP para medir la velocidad del enlace mediante el tráfico acelerado. La solución de regulación de microflujo es capaz de reducir todos los flujos a un total de 1 Mbps de bajada y 1 Mbps de subida para el usuario. Además, todas las transmisiones utilizan aproximadamente el 25% del ancho de banda disponible (por ejemplo, 250 kbps por secuencia x 4 = 1 Mbps).



Nota: Debido a que la acción de regulación de tráfico de Microflow ocurre en la Capa 3, el resultado final para el rendimiento del tráfico TCP puede ser menor que la velocidad configurada debido a la sobrecarga del protocolo.

Información Relacionada

- [Soporte Técnico y Documentación - Cisco Systems](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).