

Del Wireless LAN tarifa por usuario que limita la solución

ID del Documento: 113435

Actualizado: De febrero el 13 de 2012



[Descarga PDF](#)



[Imprimir](#)

[Comentarios](#)

Productos Relacionados

- [Punto de acceso del Cisco Aironet 1200](#)
- [Cisco Wireless Controllers de la serie 5500](#)
- [Cisco Aironet de la serie 1260](#)
- [Punto de acceso del Cisco Aironet de la serie 1250](#)
- [Cisco Aironet de la serie 1140](#)

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Configuración del Catalyst 6500](#)

[Configuración de la regulación de microflujo](#)

[Ajuste de la política de establecimiento de políticas del ancho de banda](#)

[Recursos de Whitelisting del policing del ancho de banda](#)

[Regulación de microflujo del IPv6](#)

[\(2500, 4400, 5500\) configuración de controlador Dispositivo-basada](#)

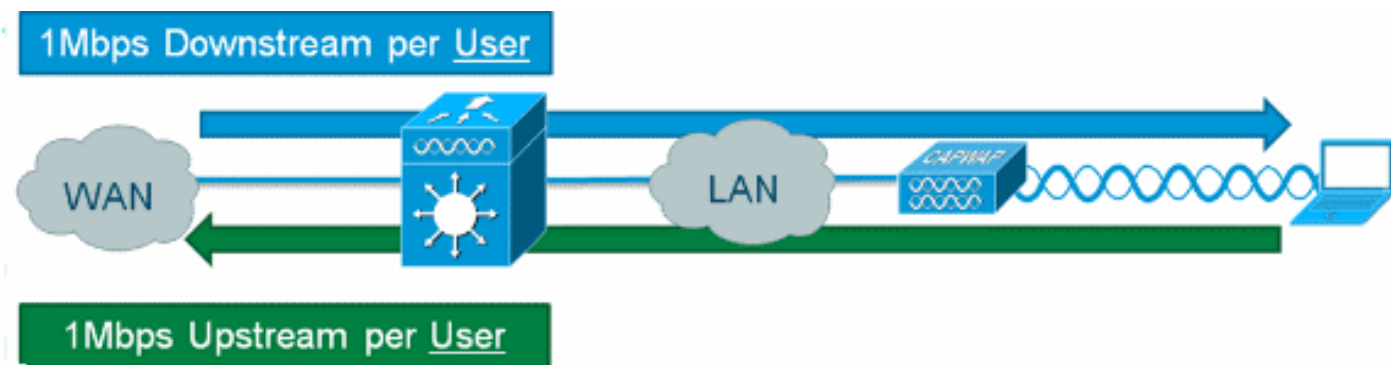
[\(WiSM, WiSM2\) configuración de controlador Módulo-basada](#)

[Verificación de la solución](#)

[Información Relacionada](#)

[Discusiones relacionadas de la comunidad del soporte de Cisco](#)

[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 por usuario la limitación de la tarifa se extiende de la protección del “cerdo” del ancho de banda es implementar los modelos con gradas del ancho de banda para el acceso de red del cliente, y en algunos casos, los recursos particulares del whitelist que están exentos del policing del ancho de banda como requisito. Además de estrangular el tráfico actual del IPv4, la solución es capaz por usuario de la limitación de la tarifa del IPv6. Esto proporciona la protección de la inversión.

prerrequisitos

Requisitos

La regulación de microflujo requiere el uso un supervisor de 720 o de más adelante que funcione con una versión del Software Release 12.2(14)SX o Posterior de Cisco IOS®.

Componentes Utilizados

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

- Reguladores del Wireless LAN
- (APS) de los Puntos de acceso
- Supervisor 720 del Cisco Catalyst o más adelante

Convenciones

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

Configuración del Catalyst 6500

Configuración de la regulación de microflujo

Complete estos pasos:

1. Utilizar la regulación de microflujo primero requiere que un Access Control List (ACL) esté

creado para identificar el tráfico para aplicar una directiva que estrangula. **Nota:** Este ejemplo de configuración utiliza la subred 192.168.30.x/24 para los clientes de red inalámbrica.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 clase-mapa para hacer juego en el 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. Crear un directiva-mapa conectará el ACL y el clase-mapa previamente creados a una acción distinta para aplicarse al tráfico. En este caso el tráfico se está estrangulando a 1Mbps en las ambas direcciones. Una máscara del flujo de la fuente se utiliza en la dirección ascendente (cliente al AP) y una máscara del flujo del destino se utiliza en la dirección descendente (AP al 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 más información sobre configurar la regulación de microflujo, refiera a la [tarifa basada en el usuario que limita en el Cisco Catalyst 6500](#).

[Ajuste de la política de establecimiento de políticas del ancho de banda](#)

La declaración de directiva dentro del directiva-mapa es donde el ancho de banda real (configurado en los bits) y se configuran los parámetros del *tamaño de ráfaga* (configurado en los bytes).

Una buena regla práctica para el tamaño de ráfaga es:

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

Ejemplo:

Este líneas utilizas un índice de 1Mbps (bits):

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

Este líneas utilizas un índice de 5Mbps (bits):

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

[Recursos de Whitelisting del policing del ancho de banda](#)

En algunos casos, ciertos recursos de red deben estar exentos del policing del ancho de banda tal como un dispositivo del servidor de Windows Update o de la corrección de la postura. Además de los host, el whitelisting se puede también utilizar para eximir las toda la subredes del policing del ancho de banda.

Ejemplo:

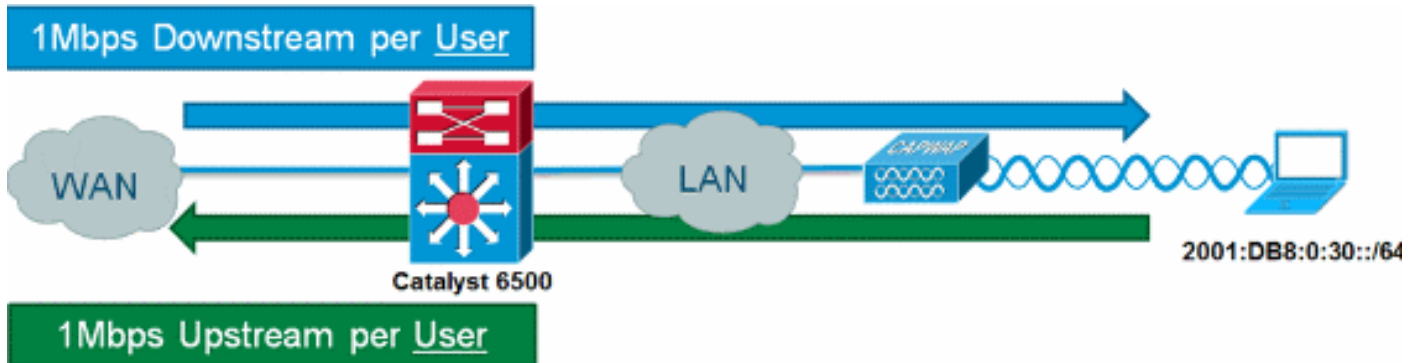
Este ejemplo excluye el host 192.168.20.22 de cualquier limitación de ancho de banda al comunicar con la red 192.168.30.0/24.

```

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

```

Regulación de microflujo del IPv6



Complete estos pasos:

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

```

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. Modifique el clase-mapa para incluir el IPv6 ACL.

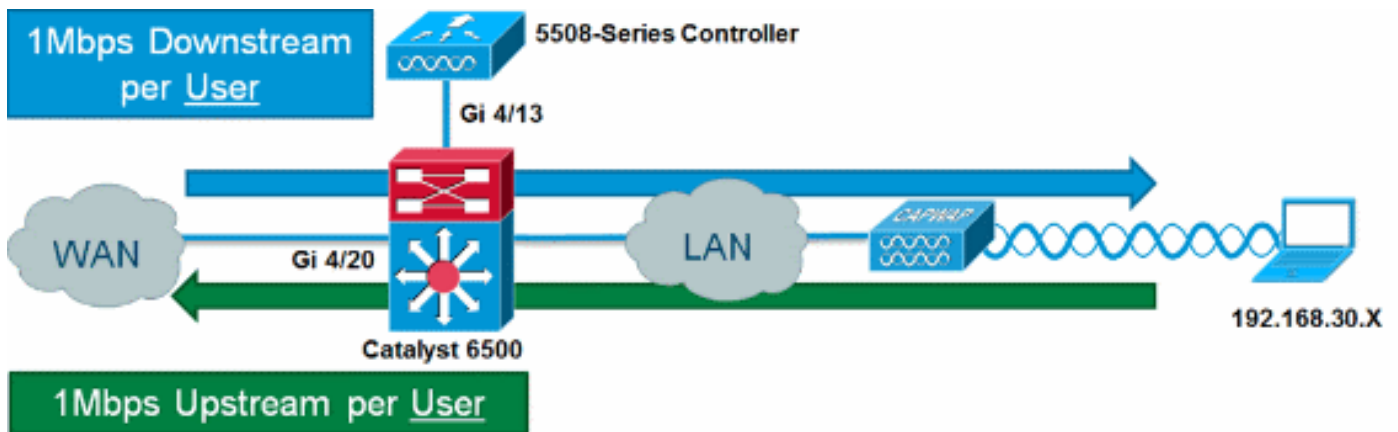
```

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

```

(2500, 4400, 5500) configuración de controlador Dispositivo-basada

Para proporcionar la regulación de microflujo con un regulador dispositivo-basado, tal como las 5508 Series, la configuración es simplista. La interfaz del regulador es similar configurado a cualquier otro VLAN, mientras que la política de servicio del Catalyst 6500 se aplica a la interfaz del regulador.



Complete estos pasos:

1. Aplique la policía-Tecnología inalámbrica-conexión en sentido ascendente en el puerto entrante del regulador.

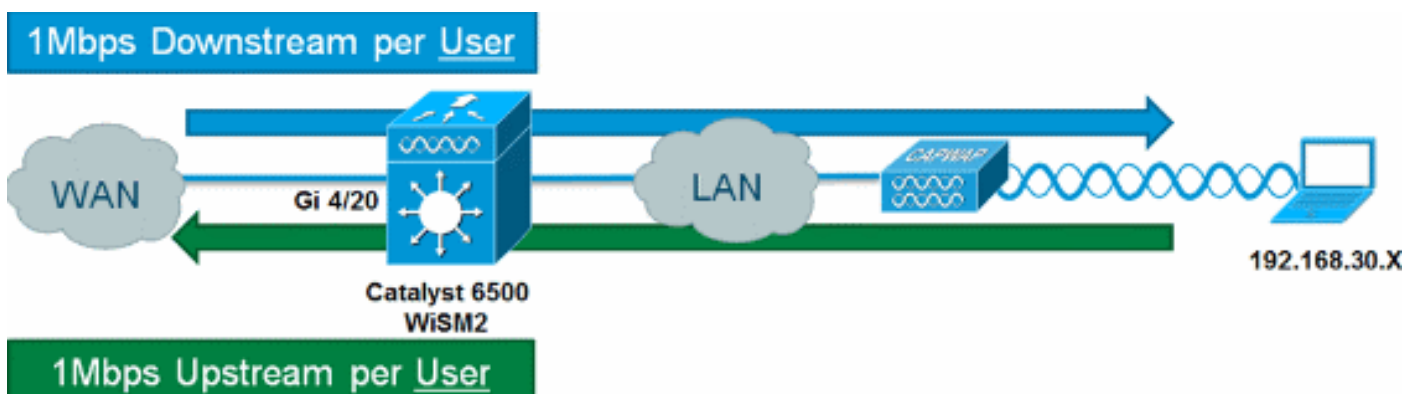
```
interface GigabitEthernet4/13
description WLC
switchport
switchport trunk allowed vlan 30
switchport mode trunk
service-policy input police-wireless-upstream
end
```

2. Aplique la directiva-Tecnología inalámbrica-rio abajo en los puertos del uplink LAN/WAN.

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

(WiSM, WiSM2) configuración de controlador Módulo-basada

Para leverage la regulación de microflujo en el Catalyst 6500 con el servicio de red inalámbrica Module2 (WiSM2), la configuración se debe ajustar para utilizar el Calidad de Servicio (QoS) VLAN basado. Esto significa que la directiva de la regulación de microflujo no está aplicada directamente a la interfaz de puerto (por ejemplo, Gi1/0/1), pero se aplica en la interfaz VLAN.



Complete estos pasos:

1. Configure el WiSM para QoS VLAN basado:


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

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

2. Aplique la directiva-Tecnología inalámbrica-conexión en sentido ascendente en el VLA N 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
```

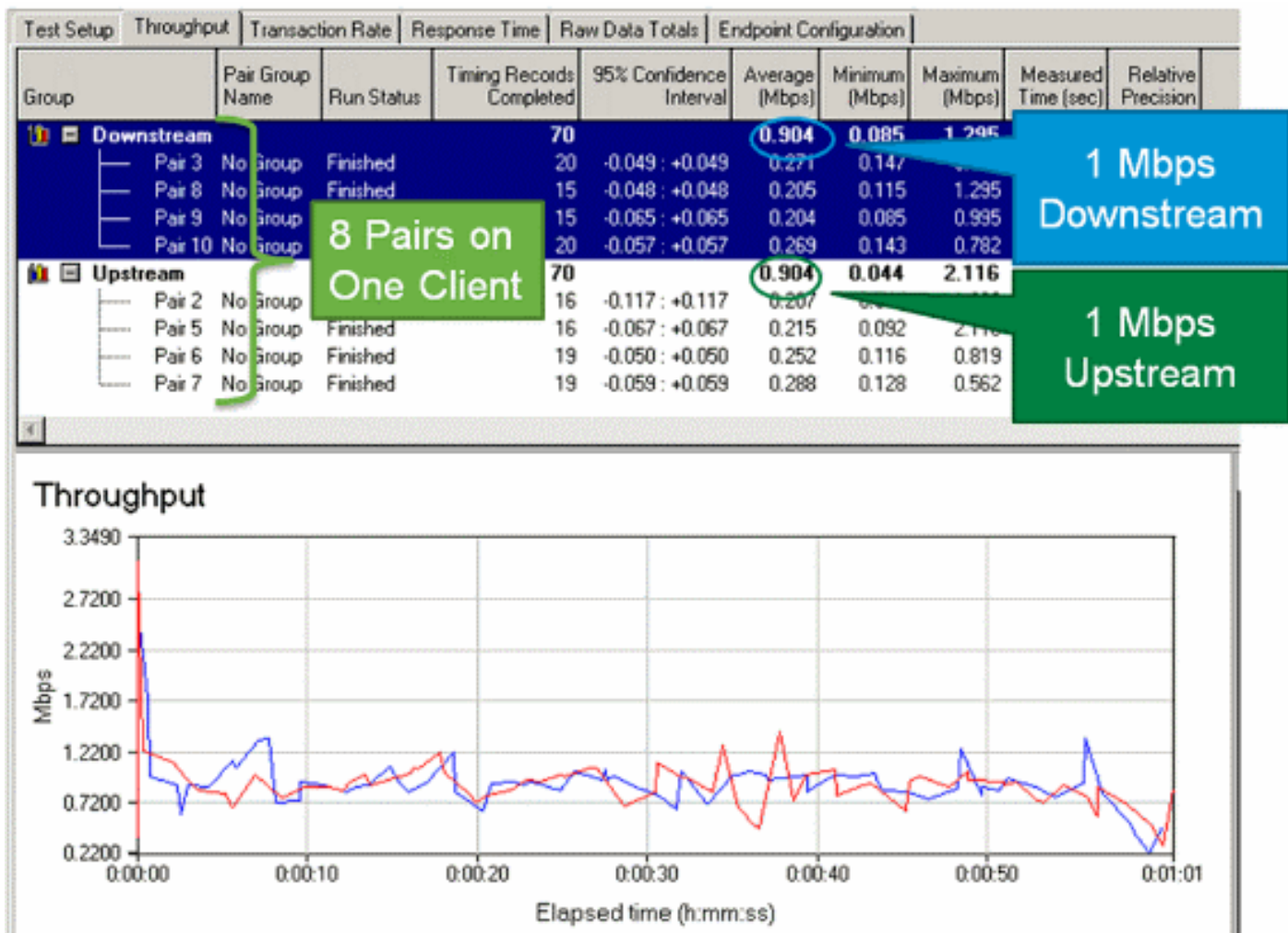
3. Aplique la directiva-Tecnología inalámbrica-rio abajo en los puertos del uplink

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

Verificación de la solución

Uno de los requisitos principales por usuario de la limitación de la tarifa es la capacidad de limitar todos los flujos que vienen de y destinado a un usuario determinado. Para verificar que la solución de la regulación de microflujo cumpla este requisito, IxChariot se utiliza para simular cuatro sesiones simultáneas de la descarga y cuatro sesiones simultáneas de la carga para un usuario determinado. Esto puede representar alguien que inicia a una sesión FTP, hojeando la red y mirando un secuencia de video mientras que envía un correo electrónico con una conexión grande, el etc.

En esta prueba IxChariot se configura con el script "Throughput.scr" usando tráfico TCP para medir la velocidad del link usando el tráfico estrangulamiento. La solución de la regulación de microflujo puede estrangular todas las secuencias abajo a un total de conexión en sentido ascendente 1Mbps rio abajo y 1Mbps para el usuario. Además, todas las secuencias utilizan el áspero 25% del ancho de banda disponible (por ejemplo, 250kbps por la secuencia x 4 = 1Mbps).



Nota: Porque la acción de la regulación de microflujo ocurre en la capa 3, el resultado final para tráfico TCP la producción puede ser menos que la velocidad configurada debido a la tara de protocolo.

Información Relacionada

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

¿Era este documento útil? [Sí](#) [ningún](#)

Gracias por su feedback.

[Abra un caso de soporte](#) (requiere un [contrato de servicios con Cisco](#).)

Discusiones relacionadas de la comunidad del soporte de Cisco

[La comunidad del soporte de Cisco](#) es un foro para que usted haga y conteste a las preguntas, las sugerencias de la parte, y colabora con sus pares.

Refiera a los [convenios de los consejos técnicos de Cisco](#) para la información sobre los convenios usados en este documento.

Actualizado: De febrero el 13 de 2012

ID del Documento: 113435