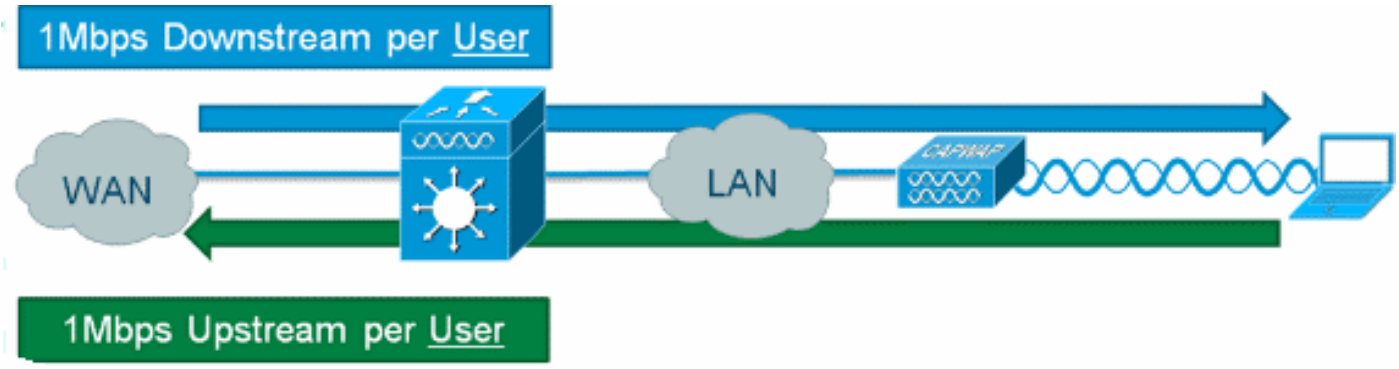
Solução de Limitação de Taxa por Usuário de LAN Sem Fio

Contents

Introduction



Fornecer o limite de taxa de downstream por usuário para usuários wireless é possível nos Controllers de LAN Wireless da Cisco, mas a adição de policiamento do IOS Microflow à solução permite um limite de taxa granular nos sentidos de upstream e downstream. A motivação para implementar intervalos de limitação de taxa por usuário da proteção "hog" de largura de banda é implementar modelos de largura de banda em camadas para o acesso à rede do cliente e, em alguns casos, colocar na lista branca recursos específicos que estão isentos da vigilância de largura de banda como um requisito. Além de controlar o tráfego IPv4 da geração atual, a solução é capaz de limitar a taxa de IPv6 por usuário. Isso fornece proteção ao investimento.

Prerequisites

Requirements

A vigilância de microfluxo requer o uso de um Supervisor 720 ou posterior que execute uma versão do Cisco IOS® Software Release 12.2(14)SX ou posterior.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Controladores de LAN sem fio
- Pontos de acesso (APs)
- Cisco Catalyst Supervisor 720 ou posterior

Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Configuração do Catalyst 6500

Configuração de vigilância de microfluxo

Conclua estes passos:

1. O uso da vigilância de microfluxo requer primeiro que uma lista de controle de acesso (ACL) seja criada para identificar o tráfego para aplicar uma política de limitação.**Observação:** este exemplo de configuração usa a sub-rede 192.168.30.x/24 para clientes sem fio.
```
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. Crie um mapa de classe para corresponder à 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. A criação de um mapa de políticas vinculará a ACL e o mapa de classes criados anteriormente a uma ação distinta a ser aplicada ao tráfego. Nesse caso, o tráfego está sendo regulado para 1Mbps em ambas as direções. Uma máscara de fluxo de origem é usada na direção upstream (cliente para AP) e uma máscara de fluxo de destino é usada na direção downstream (AP para 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 obter mais informações sobre como configurar a vigilância de microfluxo, consulte Limitação de Taxa Baseada no Usuário no Cisco Catalyst 6500.

Ajustando a política de vigilância de largura de banda

A instrução de política no mapa de política é onde os parâmetros *Bandwidth* real (configurado em

bits) e *Burst* size (configurado em bytes) são configurados.

Uma boa regra prática para o tamanho de intermitência é:

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

Exemplo:

Essa linha usa uma taxa de 1Mbps (bits):

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

Essa linha usa uma taxa de 5 Mbps (bits):

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

Recursos de whitelisting da vigilância de largura de banda

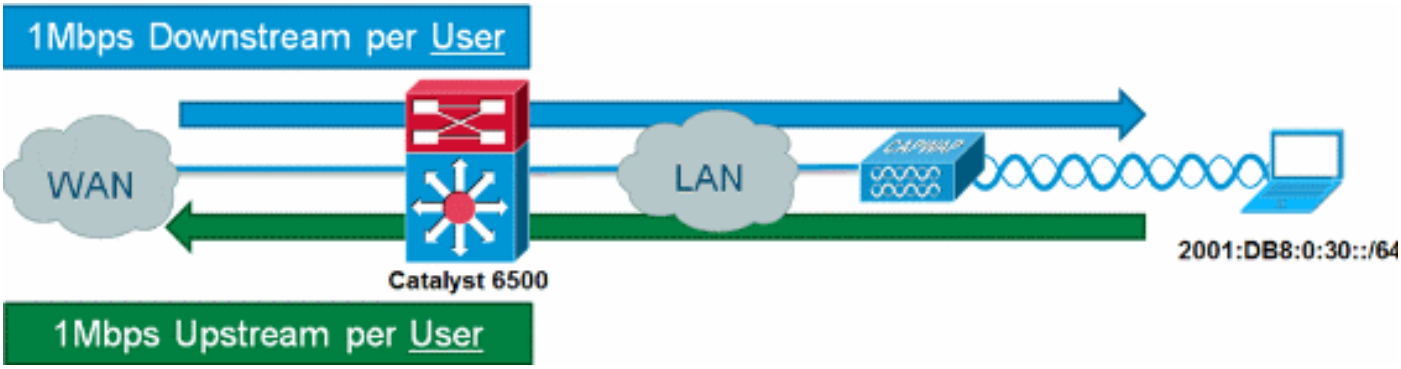
Em alguns casos, determinados recursos de rede devem ser isentos da vigilância de largura de banda, como um servidor Windows Update ou um dispositivo de correção de postura. Além dos hosts, a lista branca também pode ser usada para isentar sub-redes inteiras da vigilância de largura de banda.

Exemplo:

Este exemplo exclui o host 192.168.20.22 de qualquer limitação de largura de banda durante a comunicação com a rede 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
```

Vigilância de microfluxo IPv6



Conclua estes passos:

1. Adicione outra lista de acesso no Catalyst 6500 para identificar o tráfego IPv6 a ser acelerado.

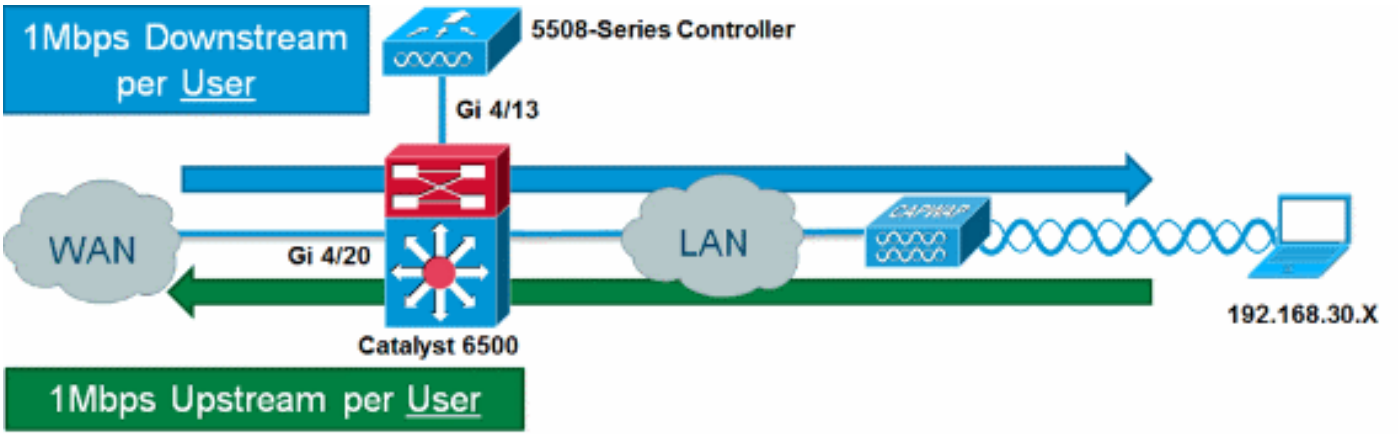
```
ipv6 access-list aclv6-wireless-downstream
permit ipv6 any 2001:DB8:0:30::/64
!
ipv6 access-list aclv6-wireless-upstream
permit ipv6 2001:DB8:0:30::/64 any
```

2. Modifique o mapa de classe para incluir a ACL IPv6.

```
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
```

Configuração do controlador baseada em dispositivo (2500, 4400, 5500)

Para fornecer vigilância de Microflow com um controlador baseado em dispositivo, como a série 5508, a configuração é simplista. A interface do controlador é configurada de forma semelhante a qualquer outra VLAN, enquanto a política de serviço do Catalyst 6500 é aplicada à interface do controlador.



Conclua estes passos:

1. Aplique `police-wireless-upstream` na porta de entrada do controlador.

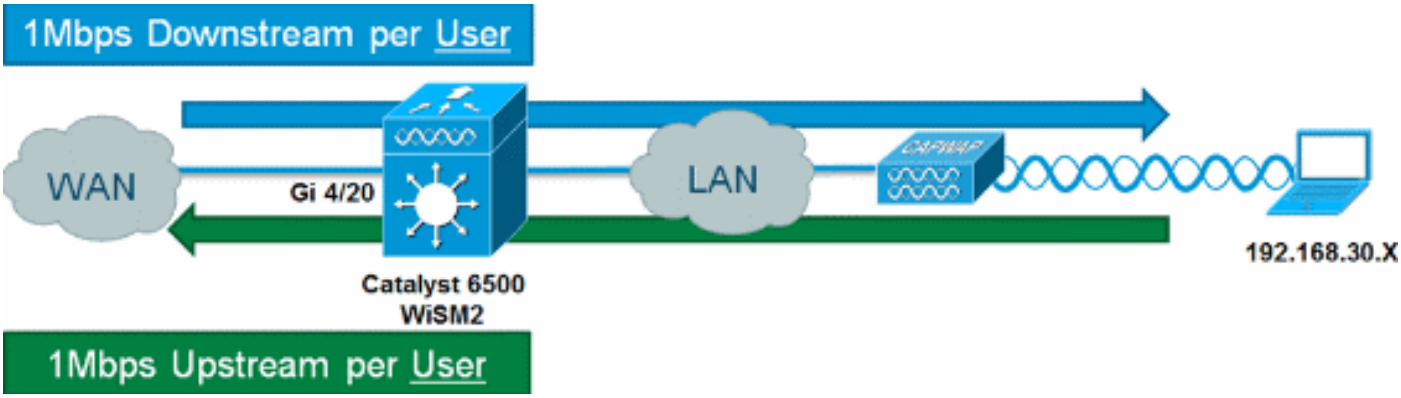
```
interface GigabitEthernet4/13
description WLC
switchport
switchport trunk allowed vlan 30
switchport mode trunk
service-policy input police-wireless-upstream
end
```

2. Aplique `policy-wireless-downstream` nas portas de uplink LAN/WAN.

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

Configuração do controlador baseado em módulo (WiSM, WiSM2)

Para aproveitar a vigilância de microfluxo no Catalyst 6500 com o Wireless Service Module2 (WiSM2), a configuração deve ser ajustada para usar Qualidade de Serviço (QoS) baseada em VLAN. Isso significa que a política de vigilância de microfluxo não é aplicada diretamente à interface da porta (por exemplo, Gi1/0/1), mas é aplicada à interface VLAN.



Conclua estes passos:

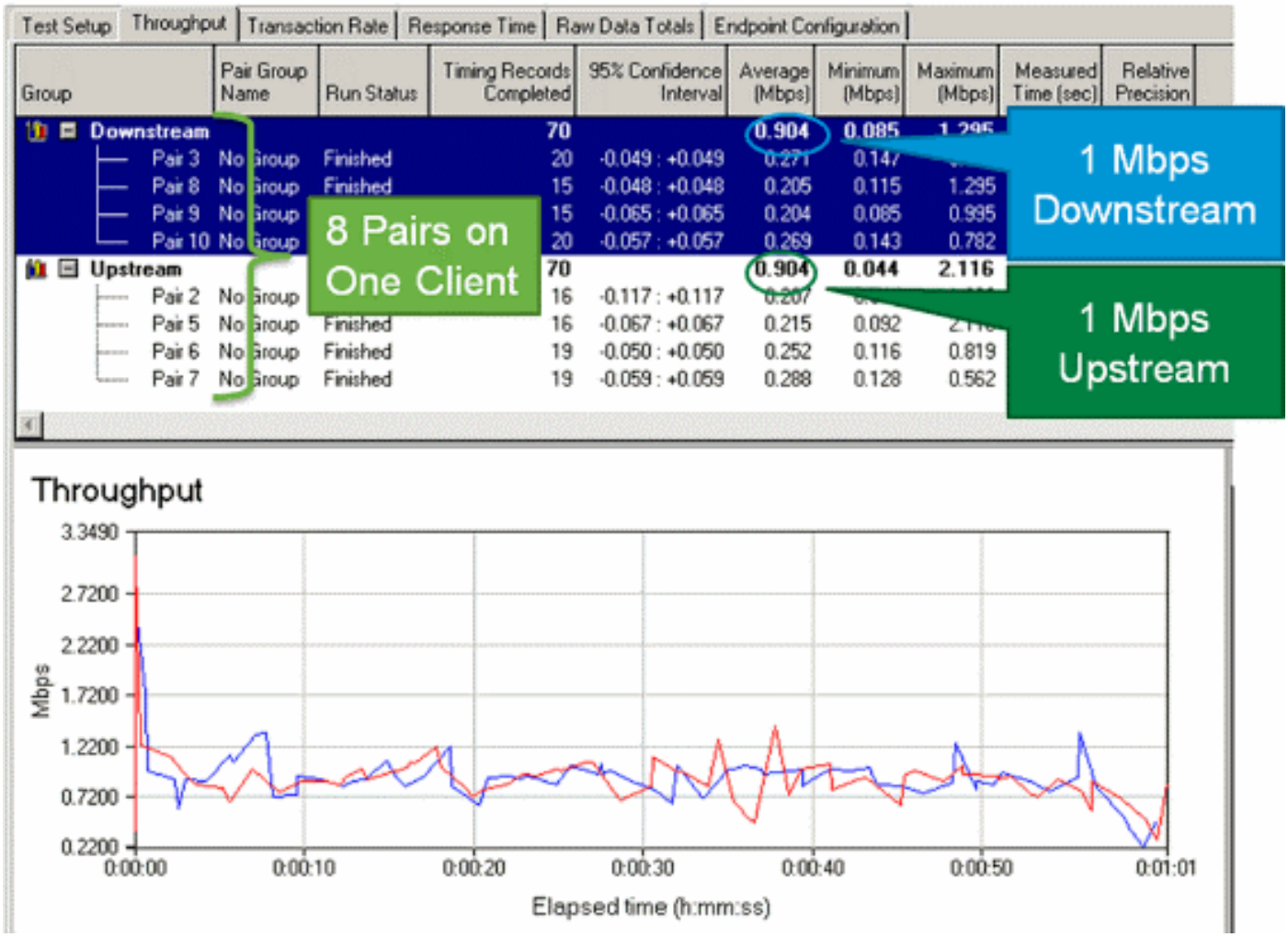
1. Configure o WiSM para QoS baseado em VLAN:
```
wism service-vlan 800
wism module 1 controller 1 allowed-vlan 30
wism module 1 controller 1 qos vlan-based
```
2. Aplique `policy-wireless-upstream` no SVI da VLAN do cliente:
```
interface Vlan30
description Client-Limited
ip address 192.168.30.1 255.255.255.0
ipv6 address 2001:DB8:0:30::1/64
ipv6 enable
service-policy input police-wireless-upstream
end
```
3. Aplique `policy-wireless-downstream` nas portas de uplink LAN/WAN.
```
interface GigabitEthernet4/20
description WAN
switchport
switchport access vlan 20
switchport mode access
service-policy input police-wireless-downstream
end
```

Verificação da solução

Um dos principais requisitos de limitação de taxa por usuário é a capacidade de limitar todos os fluxos que vêm e se destinam a um usuário específico. Para verificar se a solução de vigilância Microflow atende a esse requisito, o IxChariot é usado para simular quatro sessões simultâneas de download e quatro sessões simultâneas de upload para um usuário específico. Isso pode representar alguém iniciando uma sessão FTP, navegando na Web e assistindo a um fluxo de vídeo ao enviar um e-mail com um anexo grande, etc.

Neste teste, o IxChariot é configurado com o script "Throughput.scr" usando o tráfego TCP para medir a velocidade do link usando o tráfego acelerado. A solução de vigilância de microfluxo é

capaz de reduzir todos os fluxos para um total de 1Mbps downstream e 1Mbps upstream para o usuário. Além disso, todos os fluxos usam aproximadamente 25% da largura de banda disponível (por exemplo, 250 kbps por fluxo x 4 = 1 Mbps).



Observação: como a ação de vigilância de microfluxo ocorre na Camada 3, o resultado final do throughput do tráfego TCP pode ser menor que a taxa configurada devido à sobrecarga do protocolo.

Informações Relacionadas

- Suporte Técnico e Documentação - Cisco Systems

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.