

ID do Documento: 113435

Atualizado em: fevereiro 13, 2012

 [Transferência PDF](#)

 [Imprimir](#)

 [Feedback](#)

Produtos Relacionados

- [Access point do Cisco Aironet 1200](#)
- [Controladores sem fio Cisco série 5500](#)
- [Cisco Aironet série 1260](#)
- [Access point do Cisco Aironet série 1250](#)
- [Cisco Aironet série 1140](#)

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Configuração do Catalyst 6500](#)

[Configuração da vigilância de microfluxo](#)

[Ajustando a política de vigilância da largura de banda](#)

[Recursos de Whitelisting do policiamento da largura de banda](#)

[Vigilância de microfluxo do IPv6](#)

[\(2500, 4400, 5500\) configuração de controle Dispositivo-baseada](#)

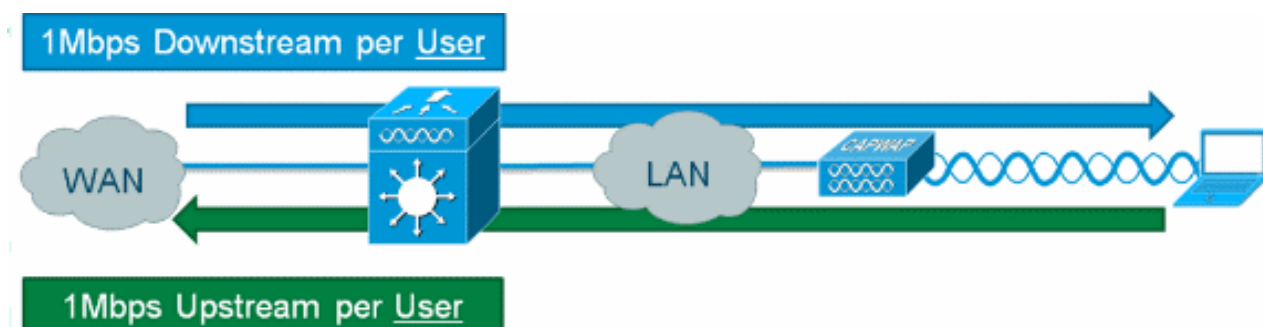
[\(WiSM, WiSM2\) configuração de controle Módulo-baseada](#)

[Verificação da solução](#)

[Informações Relacionadas](#)

[Cisco relacionado apoia discussões da comunidade](#)

Introdução



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 executar por usuário a limitação da taxa varia da proteção do “porco” da largura de banda é executar modelos estratificados da largura de banda para o acesso de rede cliente, e em alguns casos, os recursos específicos do whitelist que são isentos da largura de banda que policia como uma exigência. Além do que o tráfego de estrangulamento do IPv4 da geração atual, a solução é capaz da limitação da taxa do IPv6 do usuário per. Isto fornece a proteção de investimento.

Pré-requisitos

Requisitos

A vigilância de microfluxo exige o uso um supervisor de 720 ou de mais atrasado que execute uma versão do Software Release 12.2(14)SX ou Mais Recente de Cisco IOS®.

Componentes Utilizados

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

- Controladores do Wireless LAN
- Access point (AP)
- Supervisor 720 do Cisco catalyst ou mais atrasado

Convenções

Consulte as [Convenções de Dicas Técnicas da Cisco](#) para obter mais informações sobre convenções de documentos.

Configuração do Catalyst 6500

Configuração da vigilância de microfluxo

Conclua estes passos:

1. Utilizar a vigilância de microfluxo exige primeiramente que um Access Control List (ACL) esteja criado para identificar o tráfego a fim aplicar uma política de estrangulamento. **Nota:** Este exemplo de configuração usa a sub-rede 192.168.30.x/24 para clientes Wireless.
2. Crie um mapa de classe para combinar no ACL precedente.
3. Criar um mapa de política ligará o ACL previamente criado e o mapa de classe a uma ação distinta para aplicar-se ao tráfego. O tráfego está sendo estrangulado neste caso a 1Mbps nos ambos sentidos. Uma máscara do fluxo da fonte é usada na direção de upstream (cliente ao AP) e uma máscara do fluxo do destino é usada na direção fluxo abaixo (AP ao cliente).

Para obter mais informações sobre de configurar a vigilância de microfluxo, refira a [taxa USER-baseada que limita no Cisco catalyst 6500](#).

Ajustando a política de vigilância da largura de banda

A declaração de política dentro do mapa de política é onde a largura de banda real (configurada nos bit) e os parâmetros do *tamanho de intermitência* (configurado nos bytes) são configurados.

Um bom princípio básico para o tamanho de intermitência é:

Exemplo:

Este usos de linha uma taxa de 1Mbps (bit):

Este usos de linha uma taxa de 5Mbps (bit):

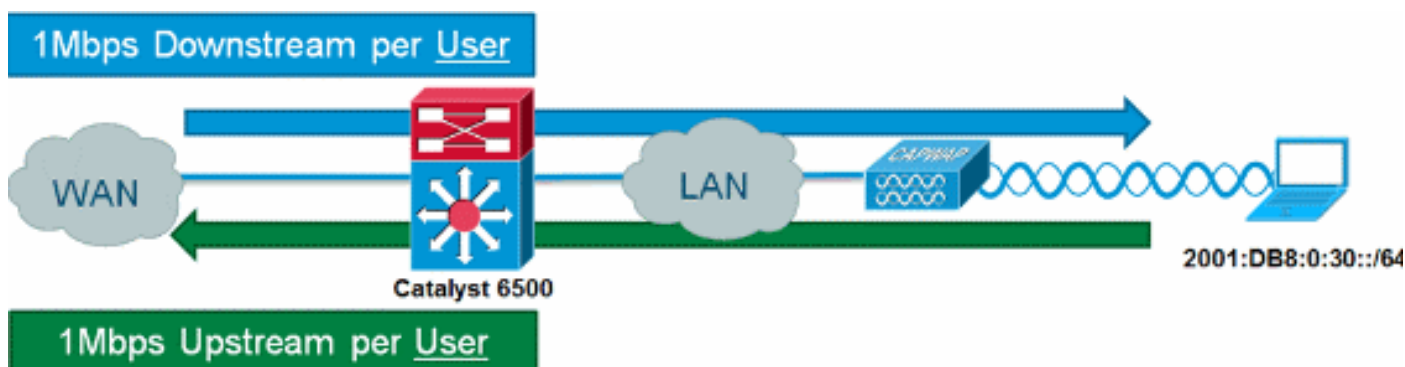
Recursos de Whitelisting do policiamento da largura de banda

Em alguns casos, determinados recursos de rede devem ser isentos da largura de banda que policia como um dispositivo do server de Windows Update ou da remediação da postura. Além do que anfitriões, whitelisting pode igualmente ser usado para isentar sub-redes inteiras do policiamento da largura de banda.

Exemplo:

Este exemplo exclui o host 192.168.20.22 de toda a limitação de largura de banda ao comunicar-se com a rede 192.168.30.0/24.

Vigilância de microfluxo do IPv6



Conclua estes passos:

1. Adicionar uma outra lista de acessos no Catalyst 6500 para identificar o tráfego do IPv6 a ser estrangulado.
2. Altere o mapa de classe para incluir o IPv6 ACL.

(2500, 4400, 5500) configuração de controle Dispositivo-baseada

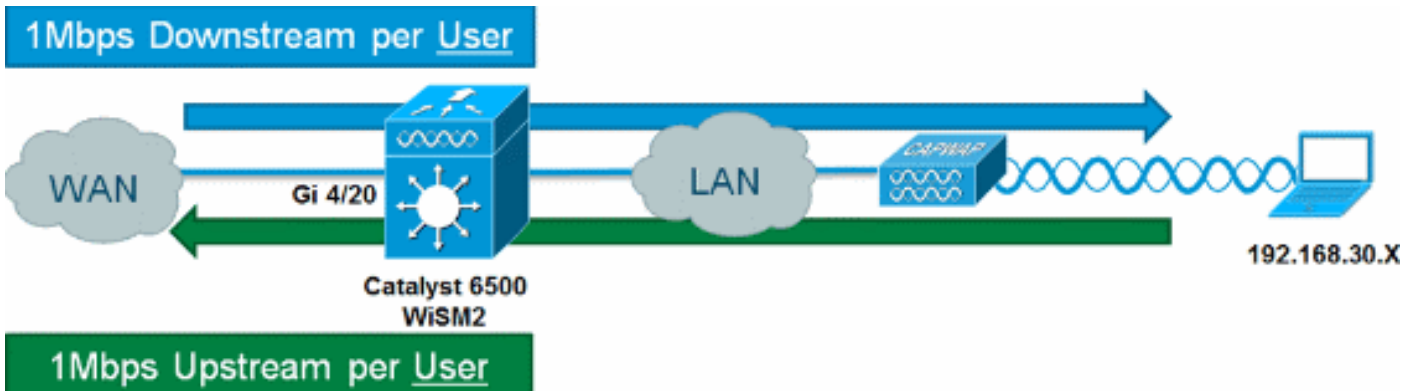
A fim fornecer a vigilância de microfluxo um controlador dispositivo-baseado, tal como o 5508 Series, a configuração é simplista. A relação do controlador é similar configurado a todo o outro VLAN, quando a política de serviços do Catalyst 6500 for aplicada à relação do controlador.

Conclua estes passos:

1. Aplique o política-Sem fio-rio acima na porta de recebimento do controlador.
2. Aplique o política-Sem fio-rio abaixo nas portas do uplink LAN/WAN.

(WiSM, WiSM2) configuração de controle Módulo-baseada

A fim leverage a vigilância de microfluxo no Catalyst 6500 com o serviço Wireless Module2 (WiSM2), a configuração deve ser ajustada para usar o Qualidade de Serviço (QoS) com base em VLAN. Isto significa que a política da vigilância de microfluxo não está aplicada diretamente à interface de porta (por exemplo, Gi1/0/1), mas é aplicado na interface de VLAN.



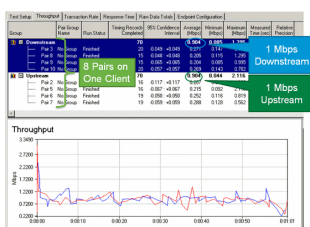
Conclua estes passos:

1. Configurar o WiSM para QoS com base em VLAN:
2. Aplique o política-Sem fio-rio acima no cliente VLAN SVI:
3. Aplique o política-Sem fio-rio abaixo nas portas do uplink LAN/WAN.

Verificação da solução

Uma das exigências principais da limitação da taxa do usuário per. é a capacidade para limitar todos os fluxos que vêm de e destinado a um usuário particular. A fim verificar que a solução da vigilância de microfluxo cumpre esta exigência, IxChariot é usado para simular quatro sessões simultâneas da transferência e quatro sessões simultâneas da transferência de arquivo pela rede para um usuário particular. Isto pode representar alguém que lança uma sessão de FTP, consultando a Web e olhando um fluxo de vídeo ao enviar um email com um grande acessório, etc.

Neste teste IxChariot é configurado com o script "Throughput.scr" usando o tráfego TCP a fim medir a velocidade do link usando o tráfego estrangulado. A solução da vigilância de microfluxo pode estrangular para baixo todos os córregos a um total de 1Mbps rio abaixo e de 1Mbps rio acima para o usuário. Além, todos os córregos usam aproximadamente 25% da largura de banda disponível (por exemplo, 250kbps pelo córrego x 4 = 1Mbps).



Nota: Porque a ação de vigilância de microfluxo ocorre na camada 3, o resultado final para a taxa de transferência de tráfego TCP pode ser menos do que a taxa configurada devido à carga adicional de protocolo.

[Informações Relacionadas](#)

- [Suporte Técnico e Documentação - Cisco Systems](#)

Era este documento útil? [Sim nenhum](#)

Obrigado para seu feedback.

[Abra um caso de suporte](#) (exige um [contrato de serviço Cisco](#).)

Cisco relacionado apoia discussões da comunidade

[Cisco apoia a comunidade](#) é um fórum para que você faça e responda a perguntas, sugestões da parte, e colabora com seus pares.

Refira [convenções dos dicas técnicas da Cisco](#) para obter informações sobre as convenções usadas neste documento.

Atualizado em: fevereiro 13, 2012

ID do Documento: 113435