

Solution Sans fil de limitation de débit de Par-utilisateur de RÉSEAU LOCAL

ID de document : 113435

Mis à jour : FÉV 13, 2012



[PDF de téléchargement](#)



[Copie](#)

[_ Commentaires](#)

[Produits connexes](#)

- [Point d'accès Cisco Aironet 1200](#)
- [Contrôleurs sans fil de la gamme Cisco 5500](#)
- [Gamme Cisco Aironet 1260](#)
- [Point d'accès de la gamme Cisco Aironet 1250](#)
- [Gamme Cisco Aironet 1140](#)

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Conventions](#)

[Configuration de Catalyst 6500](#)

[Microflow maintenant l'ordre la configuration](#)

[Ajuster la bande passante maintenant l'ordre la stratégie](#)

[Ressources en Whitelisting du maintien de l'ordre de bande passante](#)

[Maintien de l'ordre de Microflow d'IPv6](#)

[\(2500, 4400, 5500\) configuration basée sur appliance de contrôleur](#)

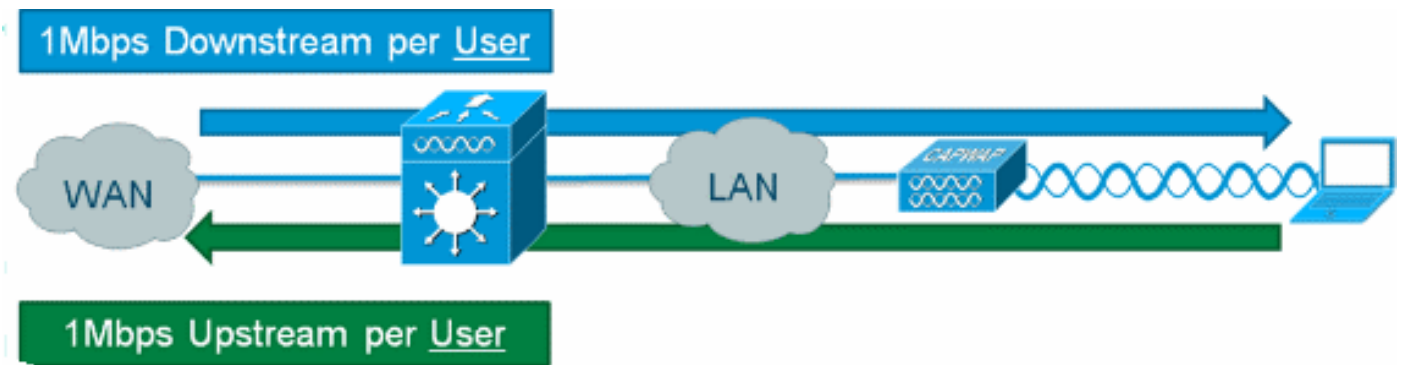
[\(WiSM, WiSM2\) configuration basée sur module de contrôleur](#)

[Vérification de solution](#)

[Informations connexes](#)

[Cisco relatif prennent en charge des discussions de la Communauté](#)

[Introduction](#)



Fournir une restriction du débit en aval par utilisateur sans fil est possible sur les contrôleurs de réseau local sans fil de Cisco, mais l'ajout de la surveillance IOS Microflow à la solution permet une limitation du débit granulaire en amont et en aval. La motivation pour mettre en application le par-utilisateur que la limitation de débit s'étend de la protection de « porc » de bande passante est d'implémenter les modèles à gradins de bande passante pour l'accès de réseau client, et dans certains cas, les ressources particulières en whitelist qui sont exemptes de la bande passante maintenant l'ordre comme condition requise. En plus d'étrangler le trafic de la génération actuelle d'ipv4, la solution est capable de la limitation de débit d'IPv6 de par-utilisateur. Ceci assure la protection de l'investissement.

Conditions préalables

Conditions requises

Le maintien de l'ordre de Microflow exige l'utilisation un superviseur de 720 ou de plus tard qui exécute une version de version de logiciel 12.2(14)SX ou ultérieures de Cisco IOS®.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Contrôleurs LAN Sans fil
- Points d'accès (aps)
- Superviseur 720 de Cisco Catalyst ou plus tard

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à [Conventions relatives aux conseils techniques Cisco](#).

Configuration de Catalyst 6500

Microflow maintenant l'ordre la configuration

Procédez comme suit :

1. L'utilisation de Microflow maintenant l'ordre d'abord exige qu'une liste de contrôle d'accès

(ACL) soit créée pour identifier le trafic afin d'appliquer une stratégie de étranglement. **Remarque:** Cet exemple de configuration utilise le sous-réseau

```
192.168.30.x/24 pour des clients sans fil.  
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. Créez un class-map pour apparier sur l'ACL précédent.

```
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 création d'un policy-map liera l'ACL et le class-map précédemment créés à une action distincte de s'appliquer au trafic. Dans ce cas le trafic est étranglé à 1Mbps dans les deux directions. Un masque de flux de source est utilisé dans la direction en amont (client à AP) et un masque de flux de la destination est utilisé dans la direction en aval (AP au client).

```
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
```

Pour plus d'informations sur configurer Microflow maintenant l'ordre, référez-vous à la [limitation de débit utilisateur Utilisateur dans le Cisco Catalyst 6500](#).

[Ajuster la bande passante maintenant l'ordre la stratégie](#)

L'instruction de stratégie dans le policy-map est où la bande passante réelle (configurée dans les bits) et des paramètres de *taille de rafale* (configurée dans les octets) sont configurés.

Une bonne règle empirique pour la taille de rafale est :

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

Exemple :

Cette ligne utilisations par débit de 1Mbps (bits) :

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

Cette ligne utilisations par débit de 5Mbps (bits) :

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

[Ressources en Whitelisting du maintien de l'ordre de bande passante](#)

Dans certains cas, certaines ressources de réseau devraient être exemptes de la bande passante maintenant l'ordre comme une appliance de serveur de Windows Update ou de correction de posture. En plus des hôtes, whitelisting peut également être utilisé pour exempter des sous-réseaux entiers du maintien de l'ordre de bande passante.

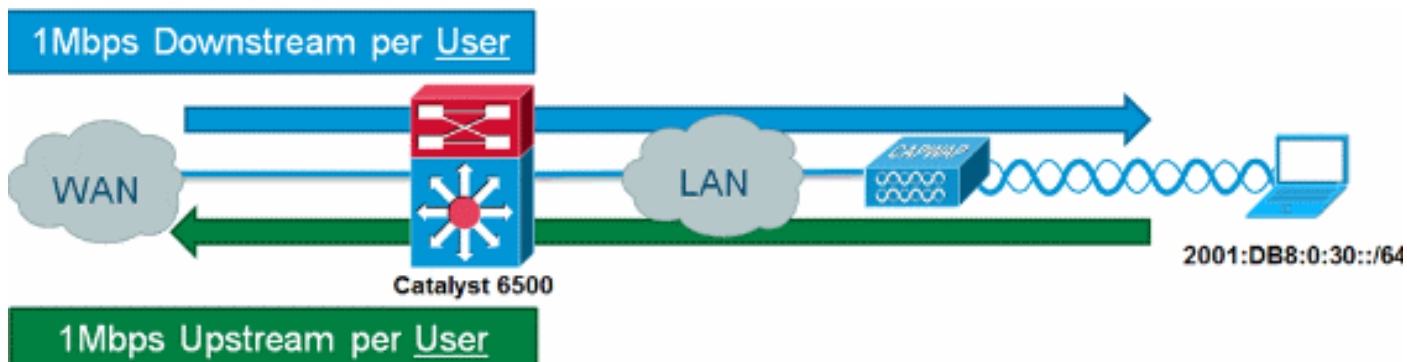
Exemple :

Cet exemple exclut l'hôte 192.168.20.22 de n'importe quelle limite de bande passante en communiquant avec le réseau 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
```

Maintien de l'ordre de Microflow d'IPv6



Procédez comme suit :

1. Ajoutez une autre liste d'accès sur le Catalyst 6500 pour identifier le trafic d'IPv6 à étrangler.

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

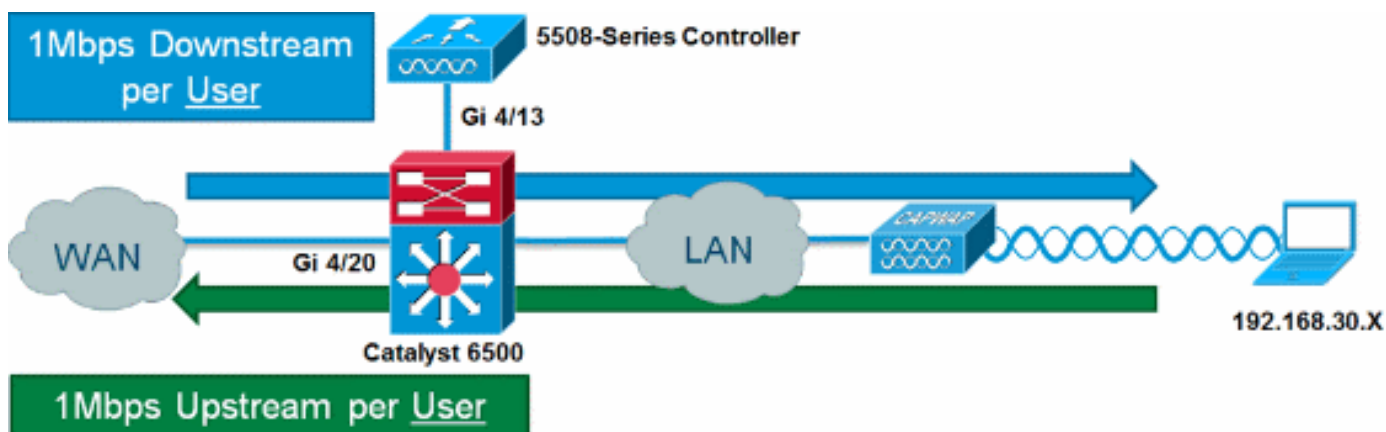
```
ipv6 access-list aclv6-wireless-upstream
permit ipv6 2001:DB8:0:30::/64 any
```

2. Modifiez le class-map pour inclure l'ACL d'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
```

(2500, 4400, 5500) configuration basée sur appliance de contrôleur

Afin de fournir à Microflow maintenant l'ordre un contrôleur basé sur appliance, tel que la gamme 5508, la configuration est simpliste. L'interface de contrôleur est semblable configuré à n'importe quel autre VLAN, alors que la stratégie de service de Catalyst 6500 est appliquée à l'interface de contrôleur.



Procédez comme suit :

1. Appliquez le `police-radio-en amont` sur le port d'entrée à partir du contrôleur.

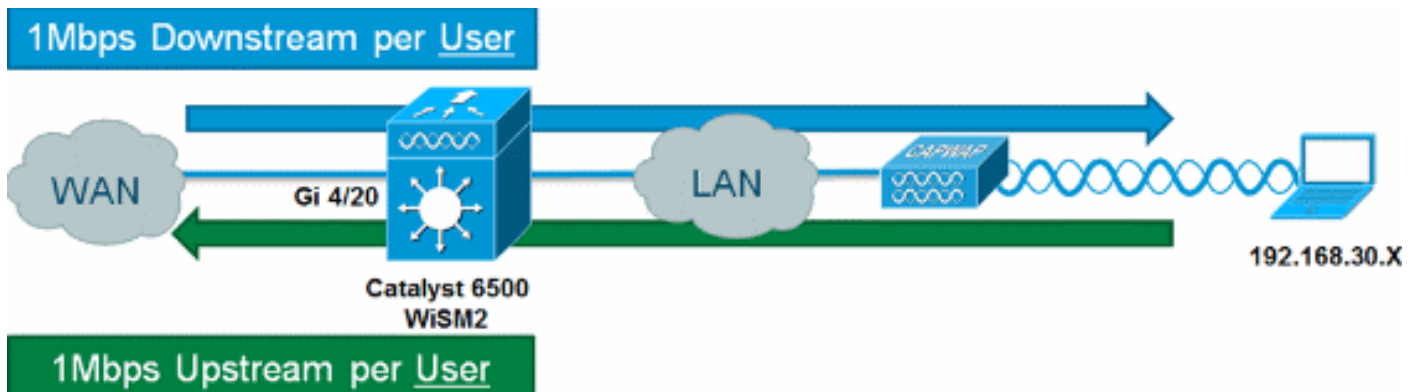
```
interface GigabitEthernet4/13
description WLC
switchport
switchport trunk allowed vlan 30
switchport mode trunk
service-policy input police-wireless-upstream
end
```

2. Appliquez le `stratégie-radio-en aval` sur les ports de la liaison ascendante

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

(WiSM, WiSM2) configuration basée sur module de contrôleur

Afin d'accroître Microflow maintenant l'ordre sur le Catalyst 6500 avec le service sans fil Module2 (WiSM2), la configuration doit être ajustée pour utiliser le Qualité de service (QoS) basé sur VLAN. Ceci signifie que le Microflow maintenant l'ordre la stratégie n'est pas appliqué directement à l'interface du port (par exemple, Gi1/0/1), mais est appliqué sur l'interface VLAN.



Procédez comme suit :

1. Configurez le WiSM pour QoS basé sur VLAN :`wism service-vlan 800`

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

2. Appliquez le `stratégie-radio-en amont` sur le client VLAN SVI :`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. Appliquez le `stratégie-radio-en aval` sur les ports de la liaison ascendante

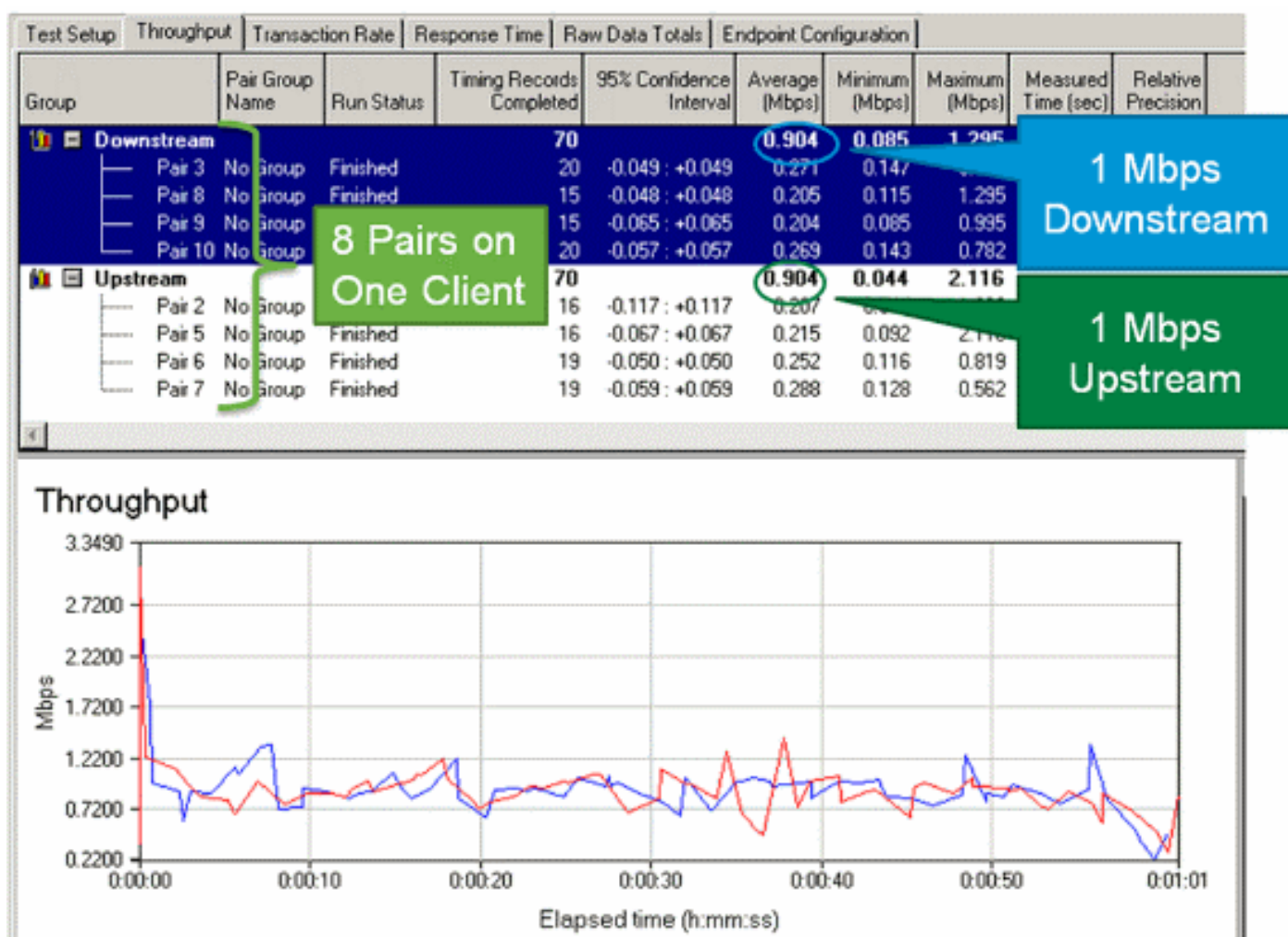
```
LAN/WAN.interface GigabitEthernet4/20
description WAN
switchport
switchport access vlan 20
switchport mode access
service-policy input police-wireless-downstream
```

end

Vérification de solution

Une des conditions requises principales de la limitation de débit de par-utilisateur est la capacité de limiter tous les écoulements provenant et destinés à un utilisateur particulier. Afin de vérifier que la solution de régulation de Microflow répond à cette exigence, IxChariot est utilisé pour simuler quatre sessions simultanées de téléchargement et quatre sessions simultanées de téléchargement pour un utilisateur particulier. Ceci peut représenter quelqu'un qui lance une session de FTP, qui parcourt le Web et qui observe un flux vidéo tout en envoyant un email avec un grand attachement, etc.

Dans ce test IxChariot est configuré avec le script « Throughput.scr » utilisant le trafic TCP afin de mesurer la vitesse du lien utilisant le trafic étranglé. La solution de régulation de Microflow peut étrangler tous les flots vers le bas à un total d'en aval 1Mbps et en amont 1Mbps pour l'utilisateur. En outre, tous les flots utilisent approximativement 25% de la bande passante disponible (par exemple, 250kbps par flot X 4 = 1Mbps).



Remarque: Puisque l'action de réglementation de Microflow se produit à la couche 3, le résultat final pour le débit de trafic TCP peut être moins que le débit configuré en raison de temps système de protocole.

Informations connexes

- [Support et documentation techniques - Cisco Systems](#)

Ce document était-il utile ? [Oui aucun](#)

Merci de votre feedback.

[Ouvrez une valise de support](#) (exige un [contrat de service Cisco](#).)

Cisco relatif prennent en charge des discussions de la Communauté

[Cisco prennent en charge la Communauté](#) est un forum pour que vous posiez et pour répondez à des questions, des suggestions de partage, et collabore avec vos pairs.

Référez-vous au [Conventions relatives aux conseils techniques Cisco](#) pour les informations sur des conventions utilisées dans ce document.

Mis à jour : FÉV 13, 2012

ID de document : 113435