

Soluzione di limitazione della velocità per utente LAN wireless

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[Configurazione Catalyst 6500](#)

[Configurazione criteri di microflusso](#)

[Regolazione dei criteri di controllo della larghezza di banda](#)

[Eliminazione di risorse dal controllo della larghezza di banda](#)

[Policy di microflusso IPv6](#)

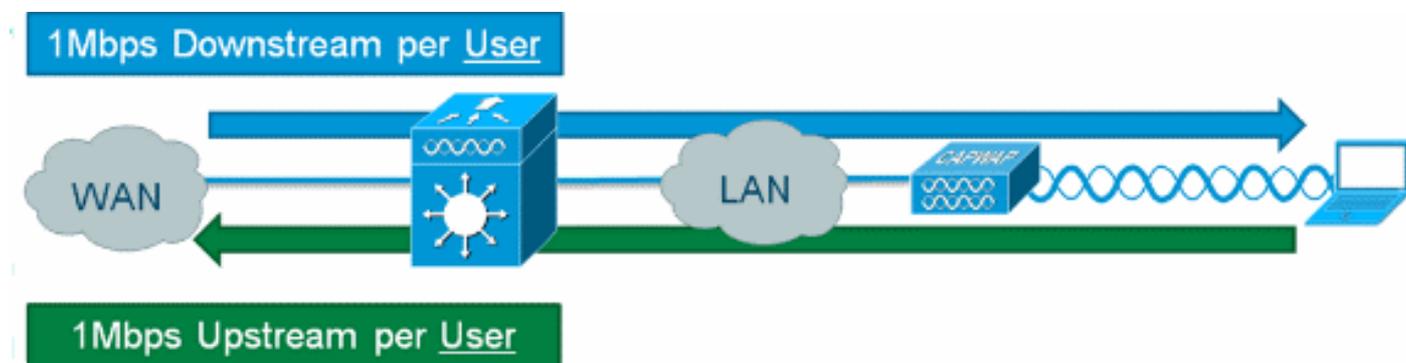
[Configurazione controller basato su appliance \(2500, 4400, 5500\)](#)

[Configurazione controller basato su modulo \(WiSM, WiSM2\)](#)

[Verifica della soluzione](#)

[Informazioni correlate](#)

Introduzione



Sui controller LAN wireless Cisco è possibile fornire agli utenti una limitazione della velocità downstream per singolo utente, ma l'aggiunta del controllo di microflusso IOS alla soluzione consente una limitazione della velocità granulare sia in upstream che in downstream. La motivazione per l'implementazione di una serie di misure di limitazione della velocità di trasmissione per utente, dalla protezione "hog" della larghezza di banda, è l'implementazione di modelli di larghezza di banda su più livelli per l'accesso alla rete dei clienti e, in alcuni casi, la creazione di una lista bianca di particolari risorse che sono esenti dal controllo della larghezza di banda come requisito. Oltre a limitare il traffico IPv4 della generazione corrente, la soluzione è in grado di limitare la velocità IPv6 per utente. Ciò garantisce la protezione dell'investimento.

Prerequisiti

Requisiti

Per le policy di microflusso è necessario utilizzare un Supervisor 720 o versioni successive con software Cisco IOS® versione 12.2(14)SX o successive.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Controller LAN wireless
- Access Point (AP)
- Cisco Catalyst Supervisor 720 o successivo

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento [Cisco sulle convenzioni nei suggerimenti tecnici](#).

Configurazione Catalyst 6500

Configurazione criteri di microflusso

Attenersi alla seguente procedura:

1. L'utilizzo del criterio Microflow richiede la creazione di un elenco di controllo di accesso (ACL) per identificare il traffico e applicare un criterio di limitazione. **Nota:** in questo esempio di configurazione viene utilizzata la subnet 192.168.30.x/24 per i client wireless.

```
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. Creare una mappa di classe che corrisponda all'ACL precedente.

```
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 creazione di una mappa dei criteri collegherà l'ACL e la mappa delle classi creati in precedenza a un'azione distinta da applicare al traffico. In questo caso, il traffico viene limitato a 1 Mbps in entrambe le direzioni. Una maschera di flusso di origine viene utilizzata nella direzione a monte (dal client al punto di accesso), mentre una maschera di flusso di destinazione viene utilizzata nella direzione a valle (dal punto di accesso al 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
```

Per ulteriori informazioni sulla configurazione delle policy di microflusso, consultare il documento sulla [limitazione della velocità basata sull'utente in Cisco Catalyst 6500](#).

Regolazione dei criteri di controllo della larghezza di banda

L'istruzione di criterio all'interno della mappa dei criteri è la posizione in cui vengono configurati i parametri *Bandwidth* effettivo (configurato in bit) e *Burst size* (configurato in byte).

Una buona regola pratica per le dimensioni della frammentazione è:

$Burst = (Bandwidth / 8) * 1.5$

Esempio:

Questa linea utilizza una velocità di 1 Mbps (bit):

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

Questa linea utilizza una velocità di 5 Mbps (bit):

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

Eliminazione di risorse dal controllo della larghezza di banda

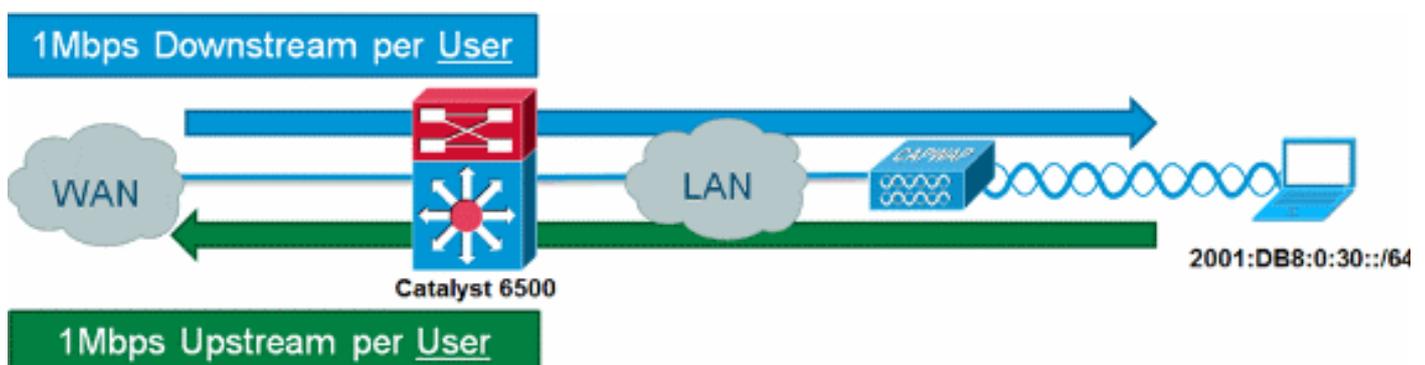
In alcuni casi, è consigliabile esentare alcune risorse di rete dal controllo della larghezza di banda, ad esempio un server Windows Update o un accessorio di monitoraggio e aggiornamento della postura. Oltre agli host, la tecnologia whitelisting può essere utilizzata per escludere intere subnet dal controllo della larghezza di banda.

Esempio:

192.168.30.0/24 Nell'esempio, se si comunica con la rete 192.168.20.22, l'host 192.168.20.22 viene escluso da qualsiasi limitazione della larghezza di banda.

```
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
```

Policy di microflusso IPv6



Attendersi alla seguente procedura:

1. Aggiungere un altro elenco degli accessi allo switch Catalyst 6500 per identificare il traffico

IPv6 da limitare.

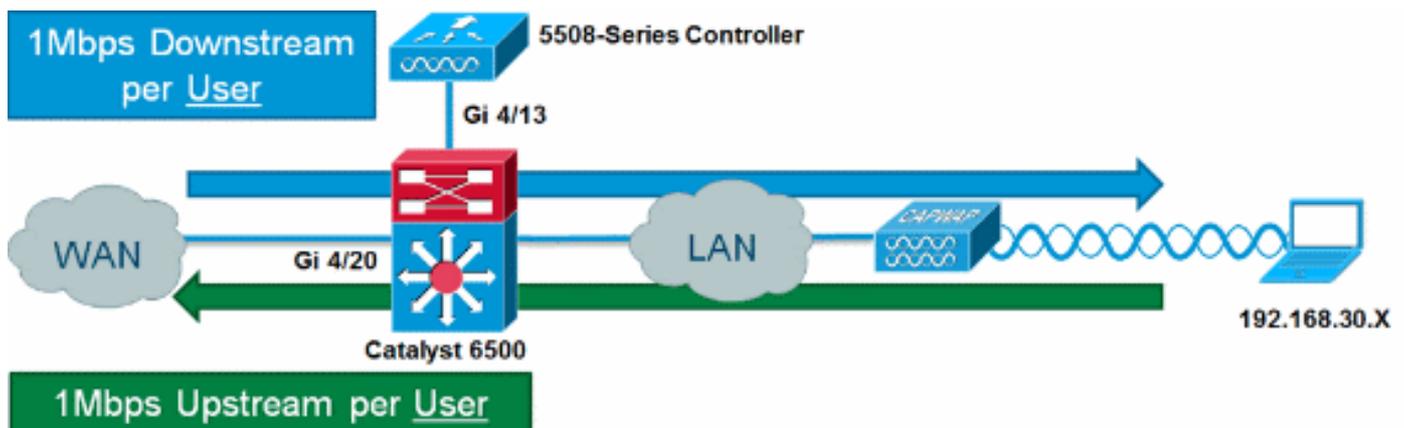
```
ipv6 access-list aclv6-wireless-downstream
permit ipv6 any 2001:DB8:0:30::/64
!
ipv6 access-list aclv6-wireless-upstream
permit ipv6 2001:DB8:0:30::/64 any
```

2. Modificare la mappa delle classi in modo da includere l'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
```

Configurazione controller basato su appliance (2500, 4400, 5500)

Per fornire il controllo Microflow con un controller basato su accessorio, come la serie 5508, la configurazione è semplicistica. L'interfaccia del controller è configurata in modo simile a tutte le altre VLAN, mentre i criteri del servizio Catalyst 6500 vengono applicati all'interfaccia del controller.



Attenersi alla seguente procedura:

1. Applicare `Police-wireless-upstream` sulla porta in ingresso del controller.

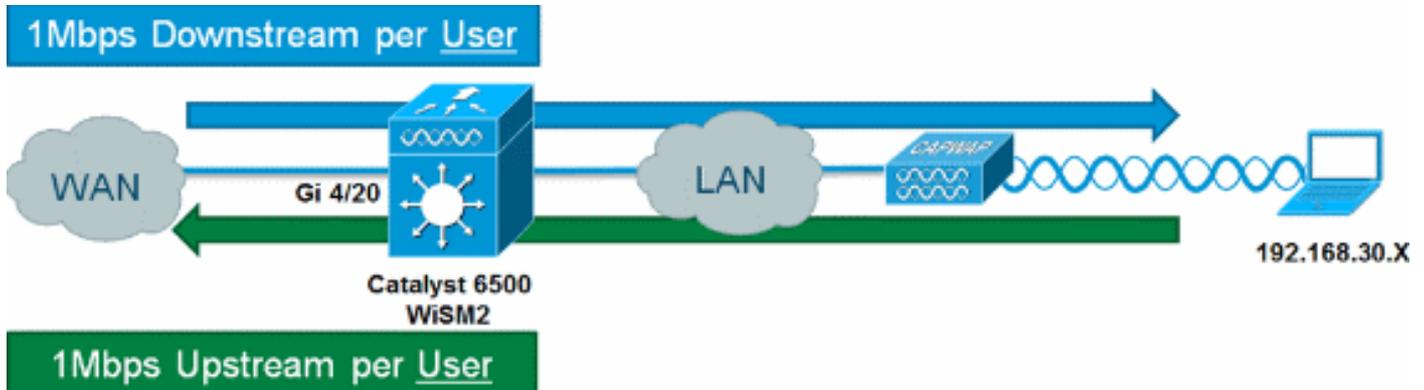
```
interface GigabitEthernet4/13
description WLC
switchport
switchport trunk allowed vlan 30
switchport mode trunk
service-policy input police-wireless-upstream
end
```

2. Applicare `policy-wireless-downstream` sulle porte LAN/WAN uplink.

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

Configurazione controller basato su modulo (WiSM, WiSM2)

Per usare le policy di microflusso su Catalyst 6500 con Wireless Service Module2 (WiSM2), la configurazione deve essere modificata in modo da usare la QoS (Quality of Service) basata su VLAN. Ciò significa che il criterio di controllo del microflusso non viene applicato direttamente all'interfaccia della porta (ad esempio, Gi1/0/1), bensì all'interfaccia VLAN.



Attenersi alla seguente procedura:

1. Configurare WiSM per QoS basato su VLAN:

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

2. Applicare policy-wireless-upstream sulla VLAN client 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. Applicare policy-wireless-downstream sulle porte LAN/WAN uplink.

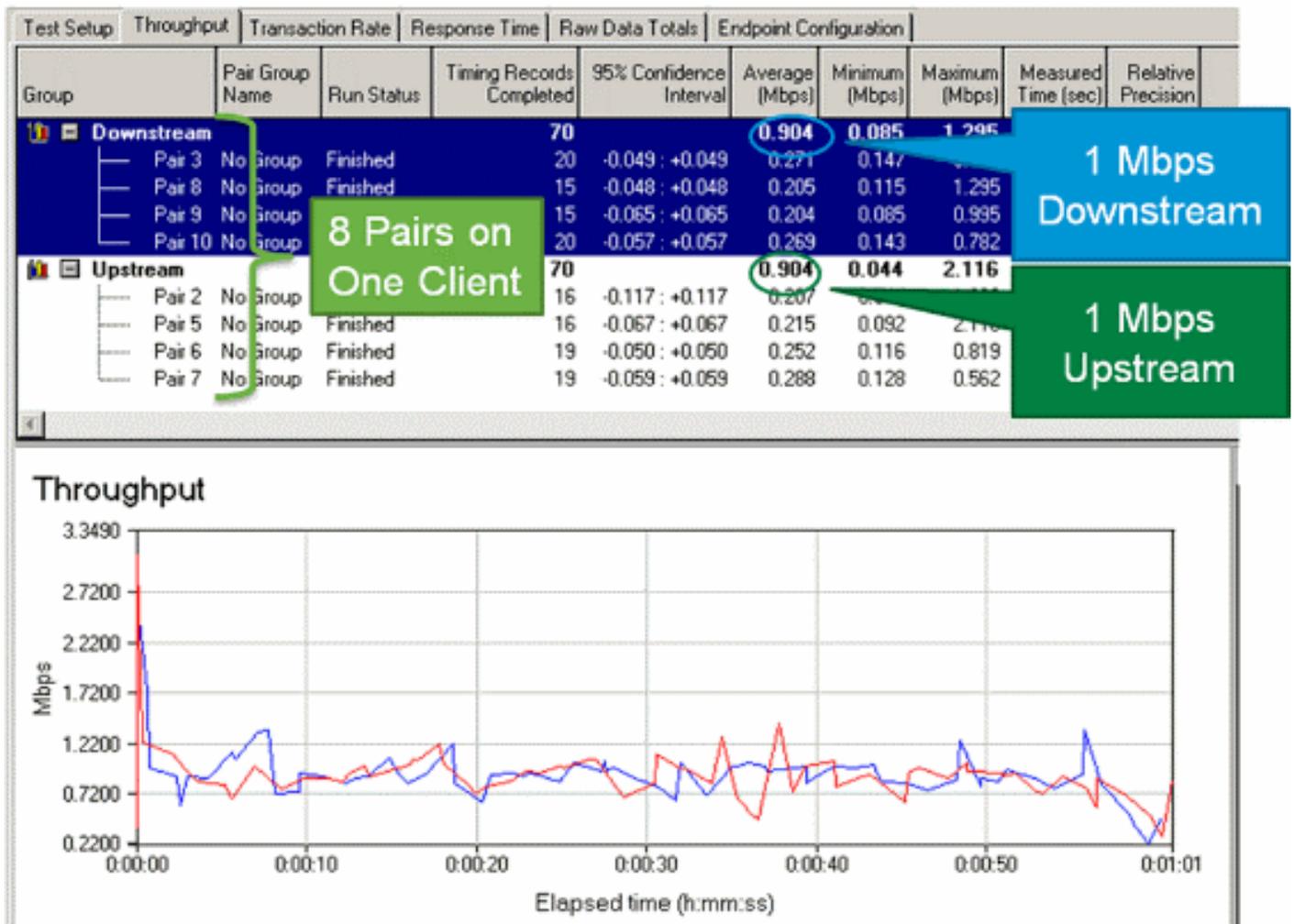
```
interface GigabitEthernet4/20  
description WAN  
switchport  
switchport access vlan 20  
switchport mode access  
service-policy input police-wireless-downstream  
end
```

Verifica della soluzione

Uno dei principali requisiti della limitazione della velocità per utente è la capacità di limitare tutti i flussi in arrivo e in arrivo verso un particolare utente. Per verificare che la soluzione di controllo Microflow soddisfi questo requisito, IxChariot viene utilizzato per simulare quattro sessioni di download simultanee e quattro sessioni di caricamento simultanee per un particolare utente. Può indicare l'avvio di una sessione FTP, l'esplorazione del Web e la visualizzazione di un flusso video durante l'invio di un'e-mail con un allegato di grandi dimensioni, ecc.

In questo test IxChariot è configurato con lo script "Throughput.scr" utilizzando il traffico TCP per misurare la velocità del collegamento utilizzando il traffico limitato. La soluzione di controllo Microflow è in grado di ridurre tutti i flussi fino a un totale di 1Mbps downstream e 1Mbps upstream per l'utente. Inoltre, tutti i flussi utilizzano all'incirca il 25% della larghezza di banda disponibile (ad

esempio, 250 kbps per flusso x 4 = 1 Mbps).



Nota: poiché l'azione di controllo Microflow si verifica al layer 3, il risultato finale per il throughput del traffico TCP può essere inferiore alla velocità configurata a causa del sovraccarico del protocollo.

Informazioni correlate

- [Documentazione e supporto tecnico – Cisco Systems](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).