Wireless LAN Per−User Rate Limiting Solution

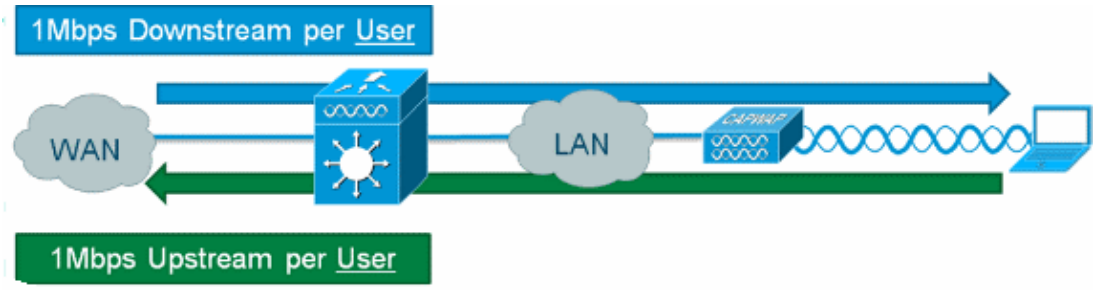
Document ID: 113435

Contents

Introduction
Prerequisites
Requirements
Components Used
Conventions
Catalyst 6500 Configuration
Microflow Policing Configuration
Adjusting the Bandwidth Policing Policy
Whitelisting Resources from Bandwidth Policing
IPv6 Microflow Policing

Appliance−based (2500, 4400, 5500) Controller Configuration
Module−based (WiSM, WiSM2) Controller Configuration
Solution Verification
Related Information

Introduction



Providing downstream per−user rate limiting for wireless users is possible on Cisco Wireless LAN controllers, but the addition of IOS Microflow policing to the solution allows for granular rate limiting in both the upstream and downstream directions. The motivation for implementing per−user rate limiting ranges from bandwidth hog protection is to implement tiered bandwidth models for customer network access, and in some cases, whitelist particular resources that are exempt from bandwidth policing as a requirement. In addition to throttling current generation IPv4 traffic, the solution is capable of per−user IPv6 rate limiting. This provides investment protection.

Prerequisites

Requirements

Microflow policing requires the use of a Supervisor 720 or later that runs a version of Cisco IOS® Software Release 12.2(14)SX or later.

Components Used

The information in this document is based on these software and hardware versions:

- Wireless LAN controllers
- Access Points (APs)
- Cisco Catalyst Supervisor 720 or later

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Catalyst 6500 Configuration

Microflow Policing Configuration

Complete these steps:

1. Utilizing Microflow policing first requires that an access control list (ACL) be created to identify traffic in order to apply a throttling policy.

   Note: This configuration example uses the 192.168.30.x/24 subnet for wireless clients.

   ```
   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. Create a class−map to match on the previous ACL.

   ```
   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. Creating a policy−map will link the previously created ACL and class−map to a distinct action to apply to the traffic. In this case the traffic is being throttled to 1Mbps in both directions. A source flow mask is used in the upstream direction (client to AP) and a destination flow mask is used in the downstream direction (AP to 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
   ```

For more information on configuring Microflow policing, refer to User−Based Rate Limiting in the Cisco Catalyst 6500.

Adjusting the Bandwidth Policing Policy

The policy statement within the policy−map is where the actual *Bandwidth* (configured in bits) and *Burst* size (configured in bytes) parameters are configured.

A good rule of thumb for the burst size is:

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

Example:

This line uses a rate of 1Mbps (bits):

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

This line uses a rate of 5Mbps (bits):

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

Whitelisting Resources from Bandwidth Policing

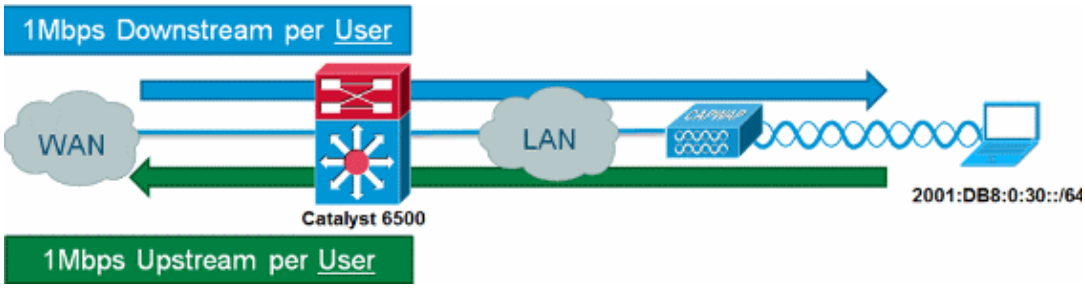
In some cases, certain network resources should be exempt from bandwidth policing such as a Windows Update server or posture remediation appliance. In addition to hosts, whitelisting can also be used to exempt whole subnets from bandwidth policing.

Example:

This example excludes the host 192.168.20.22 from any bandwidth limitation when communicating with the 192.168.30.0/24 network.

```
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
```

IPv6 Microflow Policing



Complete these steps:

1. Add another access list on the Catalyst 6500 to identify IPv6 traffic to be throttled.

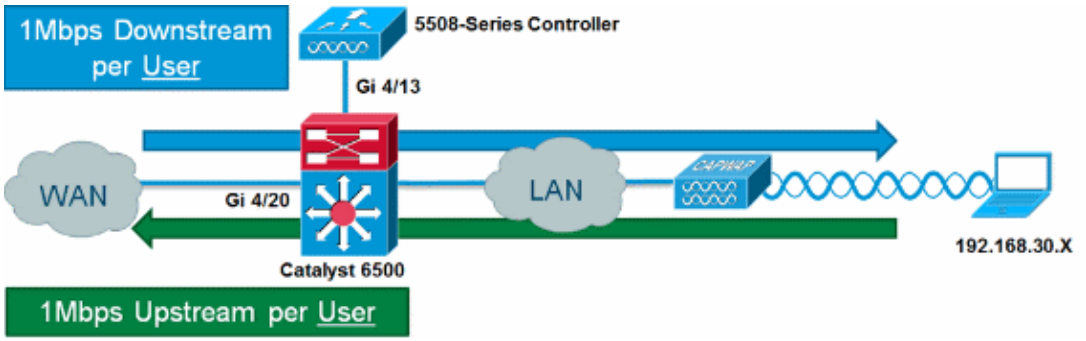
```
ipv6 access-list aclv6-wireless-downstream
permit ipv6 any 2001:DB8:0:30::/64
!
ipv6 access-list aclv6-wireless-upstream
permit ipv6 2001:DB8:0:30::/64 any
```

2. Modify the class-map to include the 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
```

Appliance−based (2500, 4400, 5500) Controller Configuration

In order to provide Microflow policing with an appliance−based controller, such as the 5508 series, the configuration is simplistic. The controller interface is configured similar to any other VLAN, while the Catalyst 6500 service policy is applied to the controller interface.



Complete these steps:

1. Apply `police−wireless−upstream` on the incoming port from the controller.

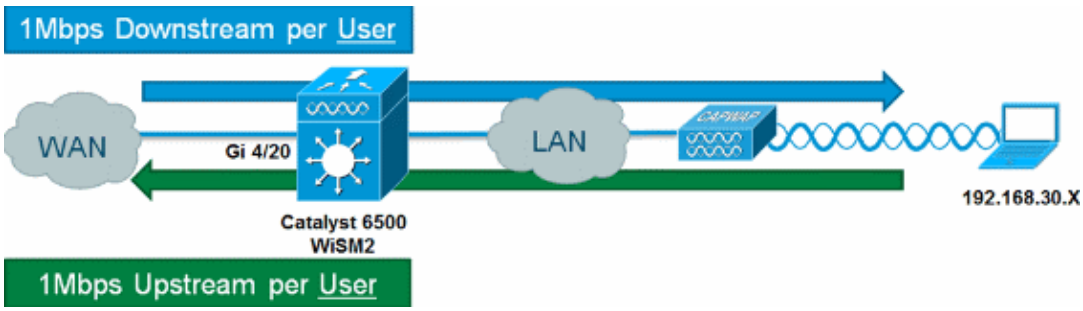
```
interface GigabitEthernet4/13
description WLC
switchport
switchport trunk allowed vlan 30
switchport mode trunk
service−policy input police−wireless−upstream
end
```

2. Apply `policy−wireless−downstream` on the uplink LAN/WAN ports.

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

Module−based (WiSM, WiSM2) Controller Configuration

In order to leverage Microflow policing on the Catalyst 6500 with the Wireless Service Module2 (WiSM2), the configuration must be adjusted to use VLAN−based Quality of Service (QoS). This means that the Microflow policing policy is not applied directly to the port interface (for example, Gi1/0/1), but is applied on the VLAN interface.



Complete these steps:

1. Configure the WiSM for VLAN−based QoS:

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

2. Apply `policy−wireless−upstream` on 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
```

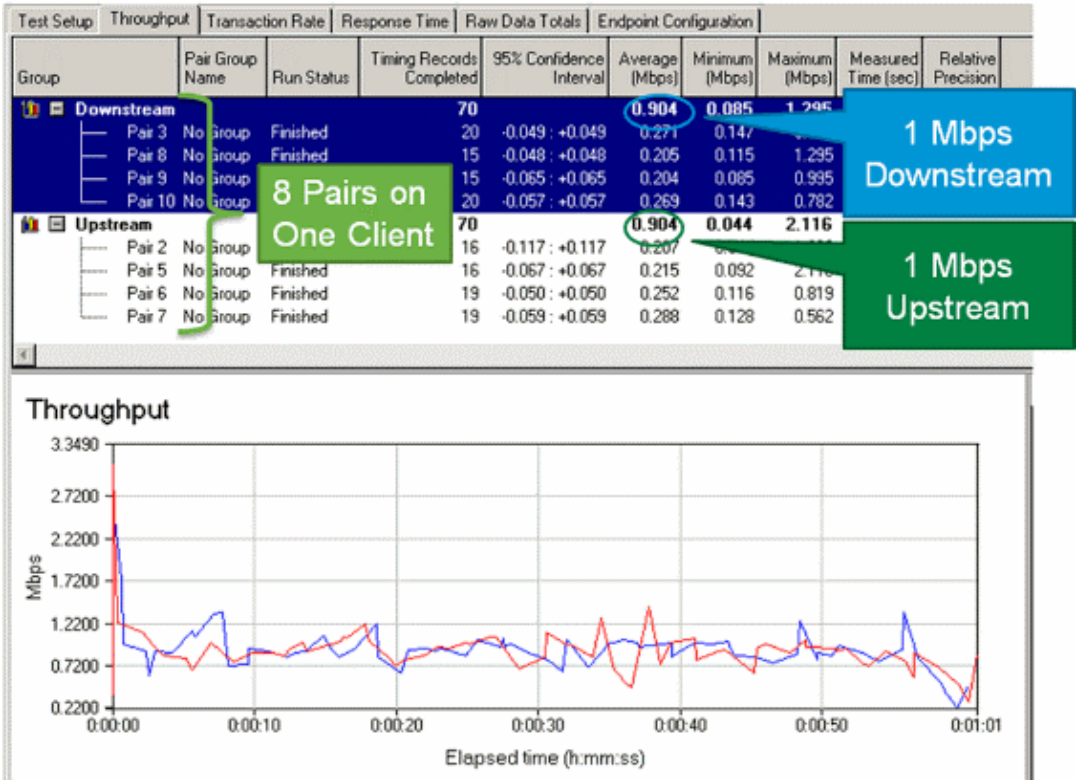
3. Apply `policy−wireless−downstream` on the uplink LAN/WAN ports.

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

Solution Verification

One of the main requirements of per−user rate limiting is the ability to limit all flows coming from and destined to a particular user. In order to verify that the Microflow policing solution meets this requirement, IxChariot is used to simulate four simultaneous download sessions and four simultaneous upload sessions for a particular user. This can represent someone launching a FTP session, browsing the web and watching a video stream while sending an email with a large attachment, etc.

In this test IxChariot is configured with the Throughput.scr script using TCP traffic in order to measure the speed of the link using throttled traffic. The Microflow policing solution is able to throttle all streams down to a total of 1Mbps downstream and 1Mbps upstream for the user. In addition, all of the streams use roughly 25% of available bandwidth (for example, 250kbps per stream x 4 = 1Mbps).



Note: Because the Microflow policing action occurs at Layer 3, the end result for TCP traffic throughput can be less than the configured rate because of protocol overhead.

Related Information

- **Technical Support & Documentation − Cisco Systems**

Updated: Feb 13, 2012 Document ID: 113435