# Creation and Configuration of IPv6 Based Class Map on the WAP121 and WAP321 Access Points

## Objective

The Client Quality of Service (QoS) feature contains Differentiated Services (DiffServ) support that allows you to classify and manage network traffic. The configuration of diffserv begins with the configuration of a class map, which classifies traffic with respect to the IP protocol and other criteria. The configuration of class map is essential so that important traffic can be separated into different classes and can be given higher priority. For typical internet applications like email and file transfer a slight degradation in service is acceptable, but for applications like voice call and video stream any degradation of service has undesirable effects.

This article explains how to create and configure an IPv6 Class Map on WAP121 and WAP321 Access Points.

## Applicable Devices

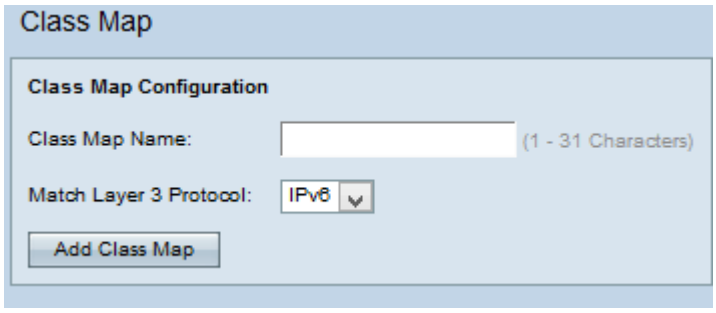
- WAP121
- WAP321

## Software Version

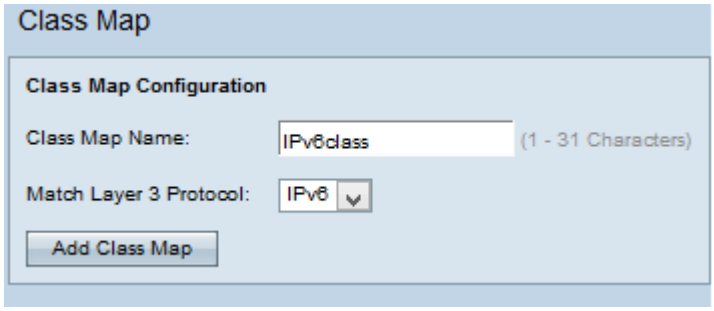
- v1.0.3.4

## Creation of IPv6 Class Map

Step 1. Log in to the Access Point Configuration Utility and choose **Client QoS > Class Map** . The *Class Map* page opens:




Step 2. Enter the name of the class map in the *Class Map Name* field.



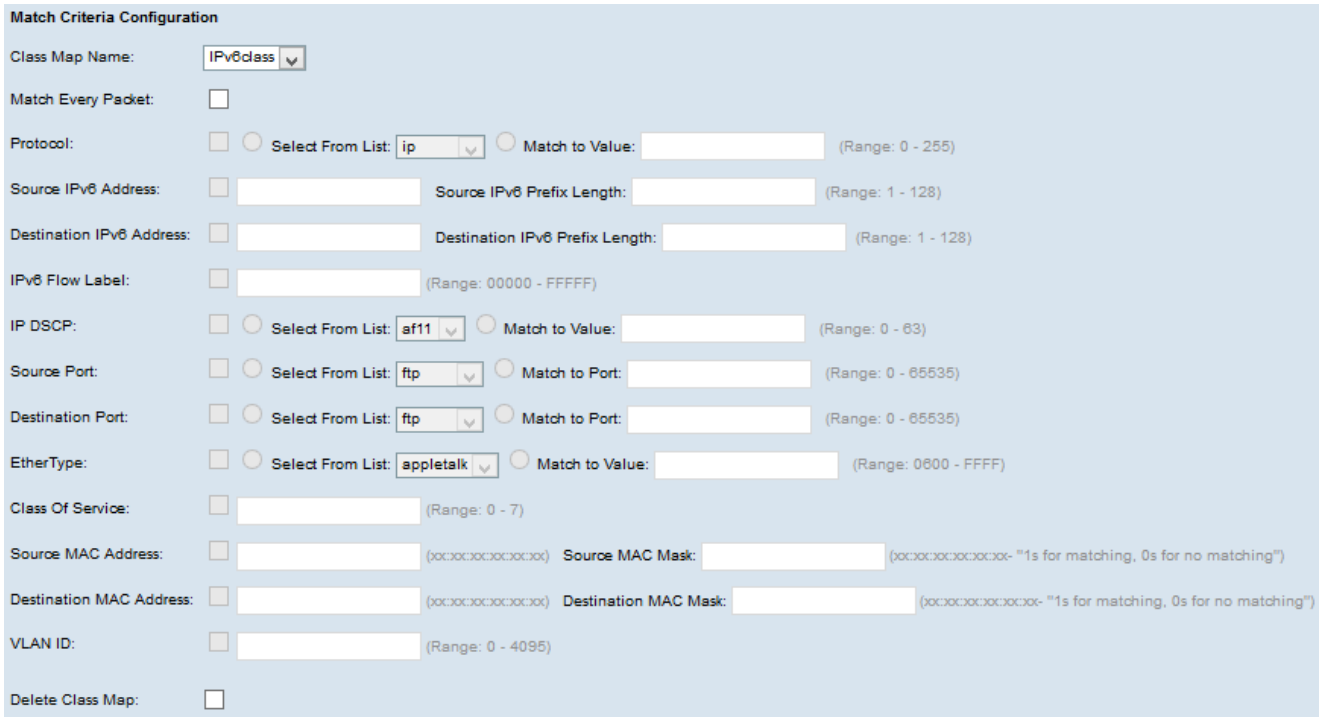

Step 3. Choose **IPv6** protocol from the *Match Layer 3 Protocol* drop-down list to apply the class map only to the IPv6 traffic on the WAP device.

**Note:** For information on IPv4 class maps, refer to the article *Creation and Configuration of IPv4 Based Class Map on WAP121 and WAP321 Access Points*.

Step 4. Click **Add Class Map** to add a new class map.

## Configuration of IPv6 Class Map

Follow the steps given below to configure the parameters in the *Match Criteria Configuration* area.

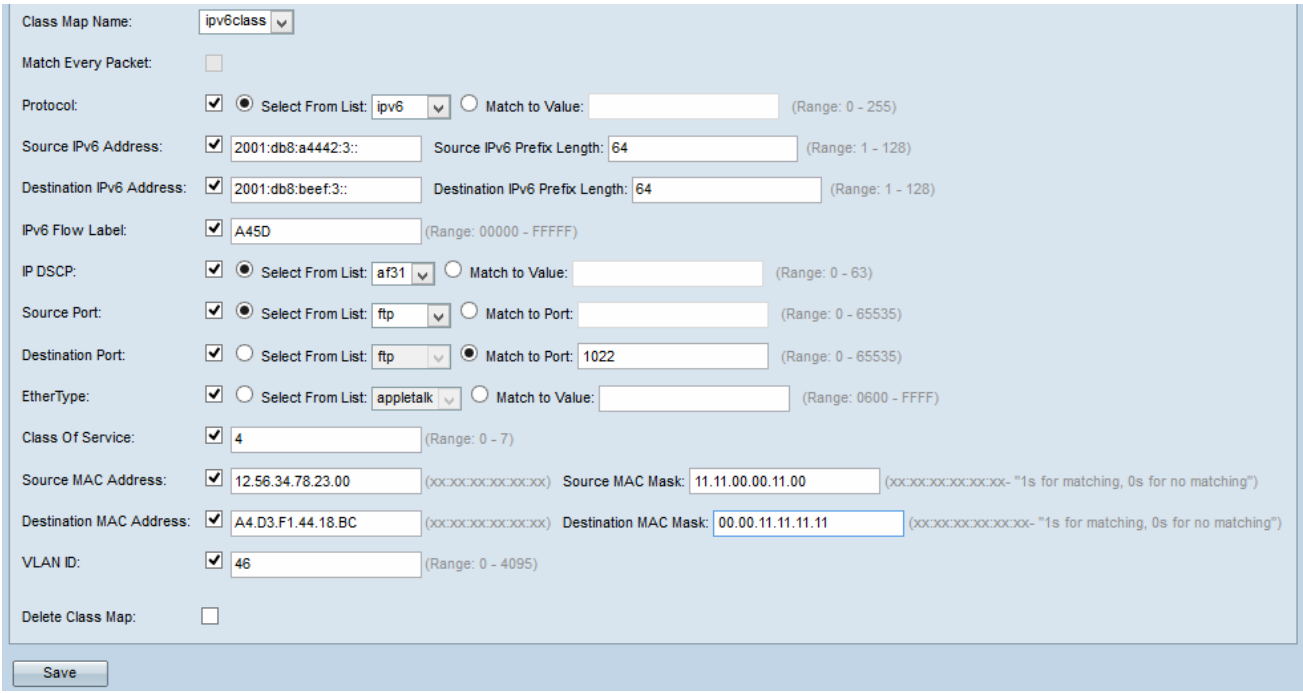



Step 1. Choose the class map from the *Class Map Name* drop-down list for which configuration must be done.

**Note:** All of the following steps are optional. Check boxes that are checked will be enabled. Uncheck the box if you do not want to apply a specific rule.

Step 2. Check the **Match Every Packet** check box for all the IP packets to match the class map for every frame or packet regardless of the content of the frame or packet; otherwise, uncheck the **Match Every Packet** check box.

**Timesaver:** If Match Every Packet is checked, skip to Step 16.




Step 3. Check the **Protocol** check box for protocol match condition. If the Protocol check box is checked, click one of these radio buttons.

- Select From List — Choose the desired protocol from the Select From List drop-down list. The available options are IP, ICMP, IPv6, ICMP, ICMPv6, IGMP, TCP and UDP.

- Match to Value — For a protocol not presented in the list. Enter a standard IANA-assigned protocol ID ranges from 0 to 255.

Step 4. Check the **Source IPv6 Address** check box to include an IP address of the source in the match condition. If the Source IPv6 Address check box is checked, enter the source IP address in the *Source IPv6 Address* field and the source prefix length in the *Source IPv6 Prefix Length* field.

Step 5. Check the **Destination IPv6 Address** check box to include an IP address of the destination in the match condition. If the Destination IPv6 Address check box is checked, enter the destination IP address in the *Destination IPv6 Address* field and the destination prefix length in the *Destination IPv6 Prefix Length* field.

Step 6. Check the **IPv6 Flow label** check box to include the IPv6 flow label in the match condition. Enter the number which ranges from 00000 to FFFFF in the *IPv6 Flow Label* field. The IPv6 flow label is present in the IPv6 header and is used to label IPv6 packets that require special handling by the source.

Step 7. Check the **IP DSCP** check box to include the IP DSCP values in the match condition. If IP DSCP check box is checked, click one of these radio buttons.

- Select From List — Choose the IP DSCP value from the *Select From List* drop-down list.

- Match to Value — Enter the DSCP value in the *Match to Value* field which ranges from 0 to 63.

Step 8. Check the **Source Port** check box to include a source port in the match condition. If the Source Port check box is checked, click one of these radio buttons.

- Select From List — Choose the source port from the *Select From List* drop-down list.

• Match to Port — For source port not presented in the list. Enter the port number which ranges 0 to 65535. The range includes three different types of ports.

– 0 to 1023 — Well known ports. These ports are used widely in many types of network services.

– 1024 to 49151 — Registered ports. These ports are used for specific services and can be obtained only by request to the Internet Assigned Numbers Authority (IANA).

– 49152 to 65535 — Dynamic and/or Private ports. These ports are used for temporary purpose only.

Step 9. Check the **Destination Port** check box to include a destination port in the match condition. If the Destination Port check box is checked, click one of these radio buttons.

• Select From List — Choose the destination port from the *Select From List* drop-down list.

• Match to Port — For destination port not presented in the list. Enter the port number which ranges from 0 to 65535 in the *Match to Port* field. The range includes three different types of ports.

– 0 to 1023 — Well Known Ports. These ports are used widely in many types of network services.

– 1024 to 49151 — Registered Ports. These ports are used for specific services and can be obtained only by request to the Internet Assigned Numbers Authority (IANA).

– 49152 to 65535 — Dynamic and/or Private Ports. These ports are used for temporary purpose only.

Step 10. Check the **EtherType** check box to compare the match criteria against the EtherType value in the header of an Ethernet frame. If EtherType check box is checked, click one of these radio buttons.

• Select From List — Choose a protocol from the drop-down list. The available options are appletalk, arp, IPv4, IPv6, IPx, netbios and pppoe.

• Match to Value — For the custom protocol identifier. Enter the identifier which ranges from 0600 to FFFF.

Step 11. Check the **Class of Service** check box to compare the 802.1p user priority against an Ethernet frame. Enter the priority which ranges from 0 to 7 in the *Class of Service* field.

• 0 — Best Effort.

• 1 — Background.

• 2 — Spare.

• 3 — Excellent Effort.

• 4 — Controlled Load.

• 5 — Video.

• 6 — Voice.

- 7 — Network Control.

Step 12. Check the **Source MAC Address** check box to compare source MAC address against an Ethernet frame. If it is checked, enter the source MAC address in the *Source MAC Address* field and the source MAC mask in the *Source MAC Mask* field.

**Note:** Source MAC mask specifies which bits in the source MAC address are to be compared against an Ethernet frame.

Step 13. Check the **Destination MAC Address** check box to compare destination MAC address against an Ethernet frame. If it is checked, enter the destination MAC address in the *Destination MAC Address* field and the destination MAC mask in the *Destination MAC Mask* field.

**Note:** Destination MAC mask specifies which bits in the destination MAC address are to be compared against an Ethernet frame.

Step 14. Check the **VLAN ID** check box for the VLAN ID to be matched with IP packets. Enter the VLAN ID which ranges from 0 to 4095 in the VLAN ID field.

Step 15. To delete the class map, check the **Delete Class Map** check box.

Step 16. Click **Save**.