

Creation and Configuration of a Rule for IPv4 Based Access Control List (ACL) on the WAP121 and WAP321 Access Points

Objective

An Access Control List (ACL) is a list of network traffic filters and correlated actions used to improve security. An ACL contains the hosts that are allowed or denied access to the network device. The QoS feature contains Differentiated Services (DiffServ) support that allows traffic to be classified into streams and given certain QoS treatment in accordance with defined per-hop behaviors.

This article explains how to create and configure IPv4 based ACL on WAP121 and WAP321 Access Points (WAP).

Applicable Devices

- WAP121
- WAP321

Software Version

- v1.0.3.4

IPv4 Based ACL Configuration

IP ACLs classify traffic for Layers 3 in the IP stack. Each ACL is a set of up to 10 rules applied to traffic sent from a wireless client or to be received by a wireless client. Each rule specifies whether the contents of a given field should be used to permit or deny access to the network. Rules can be based on various criteria and may apply to one or more fields within a packet, such as the source or destination IP address, the source or destination port, or the protocol carried in the packet.

Creation of IPv4 ACL

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

The screenshot shows a software interface for managing Access Control Lists (ACLs). The main title is "ACL". Below it, under "ACL Configuration", there are two main settings: "ACL Name:" and "ACL Type:". The "ACL Name:" field is a text input box with the placeholder "(Range: 1-31 Characters)". The "ACL Type:" field is a dropdown menu currently set to "IPv4". At the bottom left of the configuration area is a button labeled "Add ACL".

Step 2. Enter the name of the ACL in the *ACL Name* field.

ACL

ACL Configuration

ACL Name: ExampleAllowSMTP

ACL Type: IPv4

Add ACL

Step 3. Choose the **IPv4** type for the ACL from the *ACL Type* drop-down list.

ACL

ACL Configuration

ACL Name: ExampleAllowSTMP (Range: 1-31 Characters)

ACL Type:

IPv4

IPv6

MAC

Add ACL

Step 4. Click **Add ACL** to create a new IPv4 ACL.

ACL

ACL Configuration

ACL Name: ExampleAllowSTMP (Range: 1-31 Characters)

ACL Type: IPv4

Add ACL

Configuration of a Rule for IPv4 ACL

Step 1. Choose the ACL from the *ACL Name-ACL Type* drop-down list for which rules have to be configured.

ACL Rule Configuration

ACL Name - ACL Type: ExampleAllowSMTP - IPv4

Rule: New Rule

Action: Deny

Match Every Packet:

Step 2. If a new rule has to be configured for the chosen ACL, choose **New Rule** from the *Rule* drop-down list; otherwise, choose one of the present rules from the *Rule* drop-down list.

ACL Rule Configuration

ACL Name - ACL Type: ExampleAllowSMTP - IPv4

Rule: **New Rule** 

Action: Deny

Match Every Packet:

Note: A maximum of 10 rules can be created for a single ACL.

Step 3. Choose the action for the ACL rule from the Action drop-down list.

ACL

ACL Configuration

ACL Name: ExampleAllowSMTP (Range: 1-31 Characters)

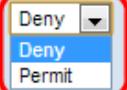
ACL Type: IPv4

Add ACL

ACL Rule Configuration

ACL Name - ACL Type: User1 - IPv4

Rule: **New Rule**

Action: 

Match Every Packet:

Protocol: Select From List: ip Match to Value: (Range: 0-255)

Source IP Address: (xxx.xxx.xxx.xxx) Wild Card Mask:

The available options are described as follows:

- Deny — Blocks all traffic that meets the rule criteria to enter or exit the WAP device.
- Permit — Allows all traffic that meets the rule criteria to enter or exit the WAP device.

Step 4. Check the *Match Every Packet* checkbox to match the rule for every frame or packet regardless of its contents. If you want to configure a specific match criteria, then uncheck the *Match Every Packet* checkbox.

ACL Rule Configuration

ACL Name - ACL Type:	sample - IPv4
Rule:	New Rule
Action:	Deny
Match Every Packet: <input checked="" type="checkbox"/>	
Protocol:	<input type="radio"/> Select From List: ip <input type="radio"/> Match to Value: <input type="text"/>
Source IP Address:	<input type="radio"/> <input type="text"/> (xxx.xxx.xxx.xxx) Wild Card Mask: <input type="text"/>
Source Port:	<input type="radio"/> Select From List: <input type="text"/> <input type="radio"/> Match to Port: <input type="text"/>
Destination IP Address:	<input type="radio"/> <input type="text"/> (xxx.xxx.xxx.xxx) Wild Card Mask: <input type="text"/>
Destination Port:	<input type="radio"/> Select From List: <input type="text"/> <input type="radio"/> Match to Port: <input type="text"/>
Service Type	
IP DSCP:	<input type="radio"/> Select From List: <input type="text"/> <input type="radio"/> Match to Value: <input type="text"/>
IP Precedence:	<input type="radio"/> <input type="text"/> (Range: 0 - 7)
IP TOS Bits:	<input type="radio"/> <input type="text"/> (Range: 00 - FF) IP TOS Mask: <input type="text"/>
Delete ACL:	<input type="checkbox"/>
Save	

Timesaver: If you check *Match Every Packet* checkbox then skip to [Step 13](#).

Step 5. (Optional) Check the *Protocol* checkbox for the L3 or L4 protocol match condition based on the value of the IP Protocol field in IPv4 packets. If the *Protocol* checkbox is checked, click one of these radio buttons.

ACL Rule Configuration

ACL Name - ACL Type:	User1 - IPv4
Rule:	New Rule
Action:	Deny
Match Every Packet: <input type="checkbox"/>	
Protocol:	<input checked="" type="checkbox"/> <input type="radio"/> Select From List: ip <input type="radio"/> Match to Value: <input type="text"/>
Source IP Address:	<input type="radio"/> <input type="text"/> (xxx.xxx.xxx.xxx) Wild Card Mask: <input type="text"/>
Source Port:	<input type="radio"/> Select From List: <input type="text"/> <input type="radio"/> Match to Port: <input type="text"/>
Destination IP Address:	<input type="radio"/> <input type="text"/> (xxx.xxx.xxx.xxx) Wild Card Mask: <input type="text"/>
Destination Port:	<input type="radio"/> Select From List: <input type="text"/> <input type="radio"/> Match to Port: <input type="text"/>
Service Type	
IP DSCP:	<input type="radio"/> Select From List: <input type="text"/> <input type="radio"/> Match to Value: <input type="text"/>

The options are described as follows:

- Select From List — Choose a protocol from the *Select From List* drop-down list. The drop-down list has ip, icmp, igmp, tcp, udp protocols.
- Match to Value — For protocol not presented in the list. Enter a standard IANA-assigned protocol ID ranging from 0 to 255.

Step 6. (Optional) Check the *Source IP Address* checkbox to include an IP address of the source in the match condition. Enter the IP address and *Wild Card Mask* of the source in the respective fields. The wild card mask lets you specify to which host of the source IP address this access list is applied.

ACL Rule Configuration

ACL Name - ACL Type:	User1 - IPv4
Rule:	New Rule
Action:	Deny
Match Every Packet:	<input type="checkbox"/>
Protocol:	<input checked="" type="radio"/> Select From List: ip <input type="button" value="▼"/> <input type="radio"/> Match to Value: 0 (Range: 0 - 255)
Source IP Address:	<input checked="" type="checkbox"/> 192.168.10.0 (xxx.xxx.xxx.xxx) Wild Card Mask: 0.0.0.255 (xxx.xxx.xxx.xxx)
Source Port:	<input type="checkbox"/> Select From List: <input type="button" value="▼"/> <input type="radio"/> Match to Port: <input type="text"/> (Range: 0 - 65535)
Destination IP Address:	<input type="checkbox"/> <input type="text"/> (xxx.xxx.xxx.xxx) Wild Card Mask: <input type="text"/> (xxx.xxx.xxx.xxx)
Destination Port:	<input type="checkbox"/> Select From List: <input type="button" value="▼"/> <input type="radio"/> Match to Port: <input type="text"/> (Range: 0 - 65535)
Service Type	
IP DSCP:	<input type="checkbox"/> Select From List: <input type="button" value="▼"/> <input type="radio"/> Match to Value: <input type="text"/> (Range: 0 - 63)
IP Precedence:	<input type="checkbox"/> <input type="text"/> (Range: 0 - 7)
IP TOS Bits:	<input type="checkbox"/> <input type="text"/> (Range: 00 - FF) IP TOS Mask: <input type="text"/> (Range: 00 - FF)
Delete ACL:	<input type="checkbox"/>
<input type="button" value="Save"/>	

Step 7. (Optional) 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.

ACL Rule Configuration

ACL Name - ACL Type: User1 - IPv4

Rule: New Rule

Action: Deny

Match Every Packet:

Protocol: Select From List: ip Match to Value: (Range:

Source IP Address: 192.168.10.0 (xxx.xxx.xxx.xxx) Wild Card Mask: 0.0.0.255

Source Port: Select From List: ftp Match to Port: (Range:

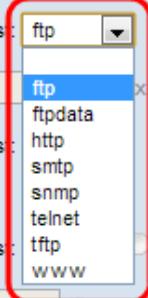
Destination IP Address: (xxx.xxx.xxx.xxx) Wild Card Mask:

Destination Port: Select From List: Match to Port: (Range:

Service Type

IP DSCP: Select From List: Match to Value: (Range:

IP Precedence: (Range: 0 - 7)



- **Select From List** — Choose a source port from the *Select From List* drop-down list. The drop-down list has ftp, ftpdata, http, smtp, snmp, telnet, tftp, www ports.

ACL Rule Configuration

ACL Name - ACL Type: User1 - IPv4

Rule: New Rule

Action: Deny

Match Every Packet:

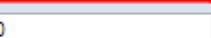
Protocol: Select From List: ip Match to Value: (Range:

Source IP Address: 192.168.10.0 (xxx.xxx.xxx.xxx) Wild Card Mask: 0.0.0.255

Source Port: Select From List: Match to Port: 80 (Range:

Destination IP Address: (xxx.xxx.xxx.xxx) Wild Card Mask:

Destination Port: Select From List: Match to Port: (Range:



- **Match to Port** — For source port not presented in the list. Enter the port number which ranges 0 to 65535.

Step 8. (Optional) Check the *Destination IP Address* checkbox to include the IP address of the destination in the match condition. Enter the IP address and *Wild Card Mask* of the destination in their respective fields. The wild card mask lets you specify to which host of the destination IP address this access list is applied.

Action: Deny

Match Every Packet:

Protocol: Select From List: ip Match to Value: (Range: 0 - 255)

Source IP Address: 192.168.10.0 (xxx.xxxx.xxxx.xxxx) Wild Card Mask: 0.0.0.255 (xxx.xxxx.xxxx.xxxx)

Source Port: Select From List: ftp Match to Port: (Range: 0 - 65535)

Destination IP Address: 192.168.20.0 (xxx.xxxx.xxxx.xxxx) Wild Card Mask: 0.0.0.255 (xxx.xxxx.xxxx.xxxx)

Destination Port: Select From List: Match to Port: (Range: 0 - 65535)

Service Type

IP DSCP: Select From List: Match to Value: (Range: 0 - 63)

IP Precedence: (Range: 0 - 7)

IP TOS Bits: (Range: 00 - FF) IP TOS Mask: (Range: 00 - FF)

Delete ACL:

Save

Step 9. (Optional) 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.

Action: Deny

Match Every Packet:

Protocol: Select From List: ip Match to Value: (Range: 0 - 255)

Source IP Address: 192.168.10.0 (xxx.xxxx.xxxx.xxxx) Wild Card Mask: 0.0.0.255 (xxx.xxxx.xxxx.xxxx)

Source Port: Select From List: ftp Match to Port: (Range: 0 - 65535)

Destination IP Address: 192.168.20.0 (xxx.xxxx.xxxx.xxxx) Wild Card Mask: 0.0.0.255 (xxx.xxxx.xxxx.xxxx)

Destination Port: Select From List: Match to Port: (Range: 0 - 65535)

Service Type

IP DSCP: Select From List: Match to Value: (Range: 0 - 63)

IP Precedence: (Range: 0 - 7)

IP TOS Bits: (Range: 00 - FF) IP TOS Mask: (Range: 00 - FF)

Delete ACL:

Save

- **Select From List** — Choose a destination port from the *Select From List* drop-down list. The drop-down list has ftp, ftpdata, http, smtp, snmp, telnet, tftp, www ports.

Action:	<input type="button" value="Deny ▾"/>
Match Every Packet:	<input type="checkbox"/>
Protocol:	<input checked="" type="checkbox"/> <input checked="" type="radio"/> Select From List: <input type="button" value="ip ▾"/> <input type="radio"/> Match to Value: <input type="text"/> (Range: 0 - 65535)
Source IP Address:	<input checked="" type="checkbox"/> <input checked="" type="radio"/> Select From List: <input type="text" value="192.168.10.0"/> (xxx.xxx.xxx.xxx) Wild Card Mask: <input type="text" value="0.0.0.255"/>
Source Port:	<input checked="" type="checkbox"/> <input checked="" type="radio"/> Select From List: <input type="button" value="ftp ▾"/> <input type="radio"/> Match to Port: <input type="text"/> (Range: 0 - 65535)
Destination IP Address:	<input checked="" type="checkbox"/> <input checked="" type="radio"/> Select From List: <input type="text" value="192.168.20.0"/> (xxx.xxx.xxx.xxx) Wild Card Mask: <input type="text" value="0.0.0.255"/>
Destination Port:	<input checked="" type="checkbox"/> <input type="radio"/> Select From List: <input type="button" value="80 ▾"/> <input checked="" type="radio"/> Match to Port: <input type="text" value="80"/> (Range: 0 - 65535)
Service Type	
IP DSCP:	<input type="checkbox"/> <input type="radio"/> Select From List: <input type="button" value="0 - 63 ▾"/> <input type="radio"/> Match to Value: <input type="text"/> (Range: 0 - 63)
IP Precedence:	<input type="checkbox"/> <input type="text"/> (Range: 0 - 7)
IP TOS Bits:	<input type="checkbox"/> <input type="text"/> (Range: 00 - FF) IP TOS Mask: <input type="text"/> (Range: 00 - FF)
Delete ACL:	<input type="checkbox"/>
<input type="button" value="Save"/>	

- 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.

Note: Only one of the services can be selected from the *Service Type* area and can be added for the match condition.

Step 10. (Optional) Check the *IP DSCP* checkbox to match the packets based on IP DSCP values. If the *IP DSCP* checkbox is checked, click one of these radio buttons. DSCP is used to specify the traffic priorities over the IP header of the frame. This categorizes all packets for the associated traffic stream with the IP DSCP value that you select from the list. For further details on DSCP, please refer [here](#).

ACL Rule Configuration

ACL Name - ACL Type: User1 - IPv4

Rule: New Rule

Action: Deny

Match Every Packet:

Protocol: Select From List: af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, cs0, cs1, cs2, cs3, cs4, cs5, cs6

Source IP Address: 192.168.10.0

Source Port: Select From List: af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, cs0, cs1, cs2, cs3, cs4, cs5, cs6

Destination IP Address: 192.168.20.0

Destination Port: Select From List: af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, cs0, cs1, cs2, cs3, cs4, cs5, cs6

Service Type

IP DSCP: Select From List: af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, cs0, cs1, cs2, cs3, cs4, cs5, cs6

IP Precedence: (Range: 0 - 7)

IP TOS Bits: (Range: 00 - FF) IP TOS Mask: (Range: 00 - FF)

Delete ACL:

Save

- **Select From List** — Choose a IP DSCP value from the *Select From List* drop-down list. The drop-down list has DSCP Assured Forwarding (AS), Class of Service (CS) or Expedited Forwarding (EF) values.
- **Match to Value** — To customize DSCP values. Enter the DSCP value which ranges from 0 to 63 in the Match to Value field.

Step 11. (Optional) Check the *IP Precedence* checkbox to include a IP Precedence value in the match condition. If IP Precedence check box is checked, enter an IP precedence value which ranges from 0 to 7. For further details on IP Precedence, please refer [here](#).

Service Type

IP DSCP: Select From List: af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, cs0, cs1, cs2, cs3, cs4, cs5, cs6

IP Precedence: 5 (Range: 0 - 7)

IP TOS Bits: DF (Range: 00 - FF) IP TOS Mask: DE

Delete ACL:

Save

Step 12. (Optional) Check the *IP TOS Bits* checkbox to use the packet's Type of Service bits in the IP header as match criteria. If the IP TOS Bits check box is checked, enter the IP TOS bits which ranges from 00-FF and IP TOS mask which ranges from 00-FF in the respective fields.

Service Type

IP DSCP: Select From List: Match to Value: 24 (Range: 0 - 255)

IP Precedence: 5 (Range: 0 - 7)

IP TOS Bits: DF (Range: 00 - FF) IP TOS Mask: DE

Delete ACL:

Save

[Step 13.](#) (Optional) If you want to delete the configured ACL then, check the *Delete ACL* checkbox.

Service Type

IP DSCP: Select From List: Match to Value: 24 (Range: 0 - 255)

IP Precedence: 5 (Range: 0 - 7)

IP TOS Bits: DF (Range: 00 - FF) IP TOS Mask: DE

Delete ACL:

Save

Step 14. Click **Save** to save the settings.