

設定 MAC、ワイヤレスアクセスポイントの IPv4 および IPv6 アクセス制御リスト

目標

Access Control List (ACL) はセキュリティを向上するために使用されるネットワークのリストトラフィックフィルタおよび関連させた操作です。それは許可されていないユーザおよび特定のリソースにアクセスするために割り当て許可されたユーザをブロックします。ACL はまたはネットワークデバイスへの拒否されたアクセス権許可されるホストが含まれています。ACL は 2 つの方法の 1 つで定義することができます: による IPv4 アドレスまたは IPv6 アドレス。

この技術情報は方法で正常に ACL を作成しネットワーク セキュリティを向上するためにワイヤレスアクセスポイント (WAP) の IPv4、IPv6 および Media Access Control (MAC) ベースの ACL を設定するガイドします。

適当なデバイス

- WAP100 シリーズ
- WAP300 シリーズ
- WAP500 シリーズ

[Software Version]

- 1.0.6.2 - WAP121、WAP321
- 1.2.0.2 - WAP371、WAP551、WAP561
- 1.0.1.4 - WAP131、WAP351
- 1.0.0.16 - WAP150、WAP361

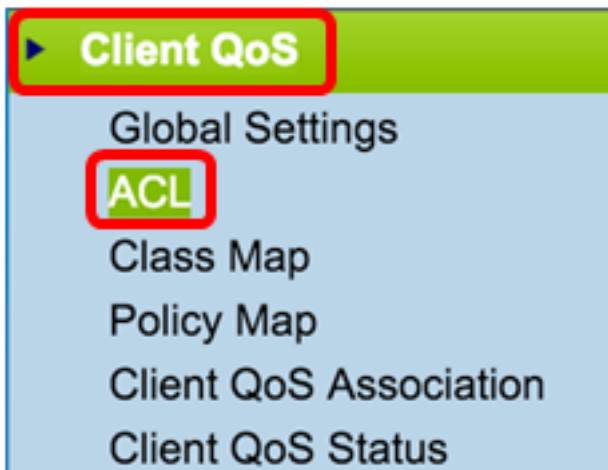
ACL の作成

注: この設定に使用するイメージは WAP150 からあります。

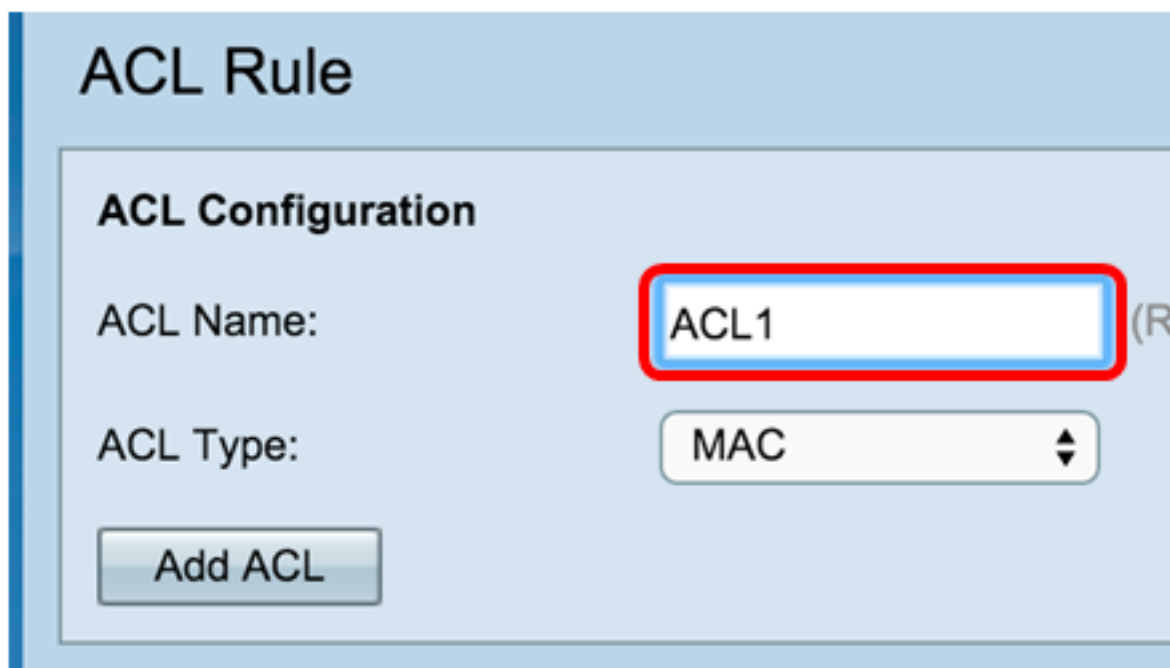
ステップ 1. アクセス ポイント Web ベース ユーティリティへのログインは ACL > ACL ルール 選択し。



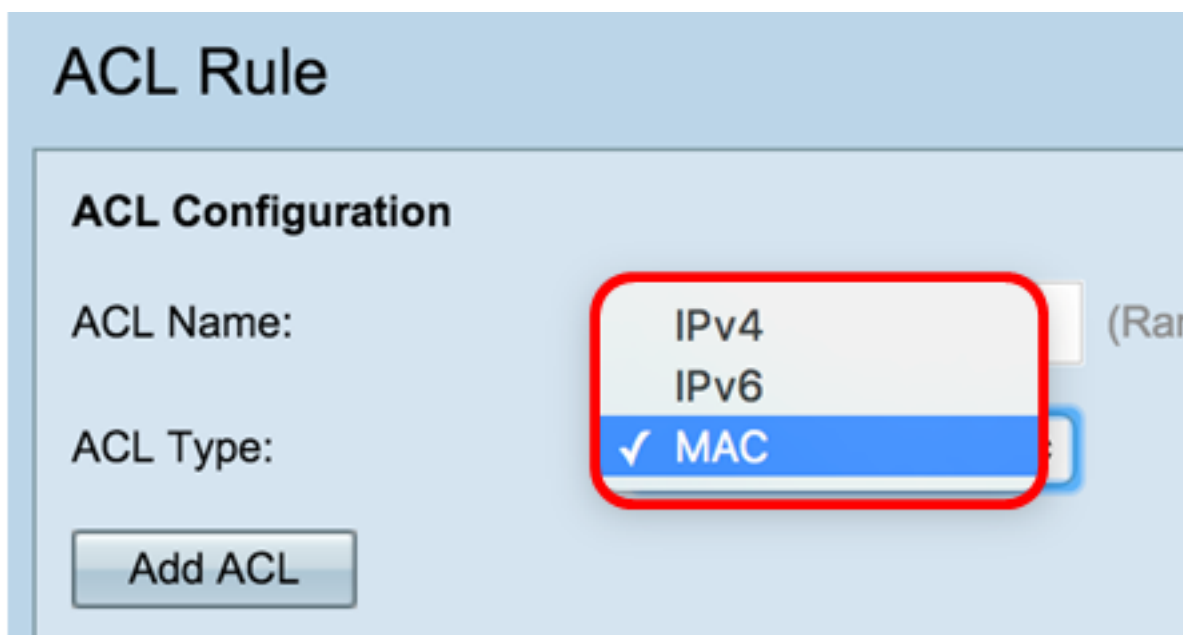
注: WAP121、WAP321、WAP371、WAP551 および WAP561 に関しては: アクセス ポイント Web ベース ユーティリティへのログインは QoS > ACL 『Client』 を選択し。



呼び出します。ACL構成 ページが開いたら、ACL Name フィールドで ACL 名前を入力して下さい。



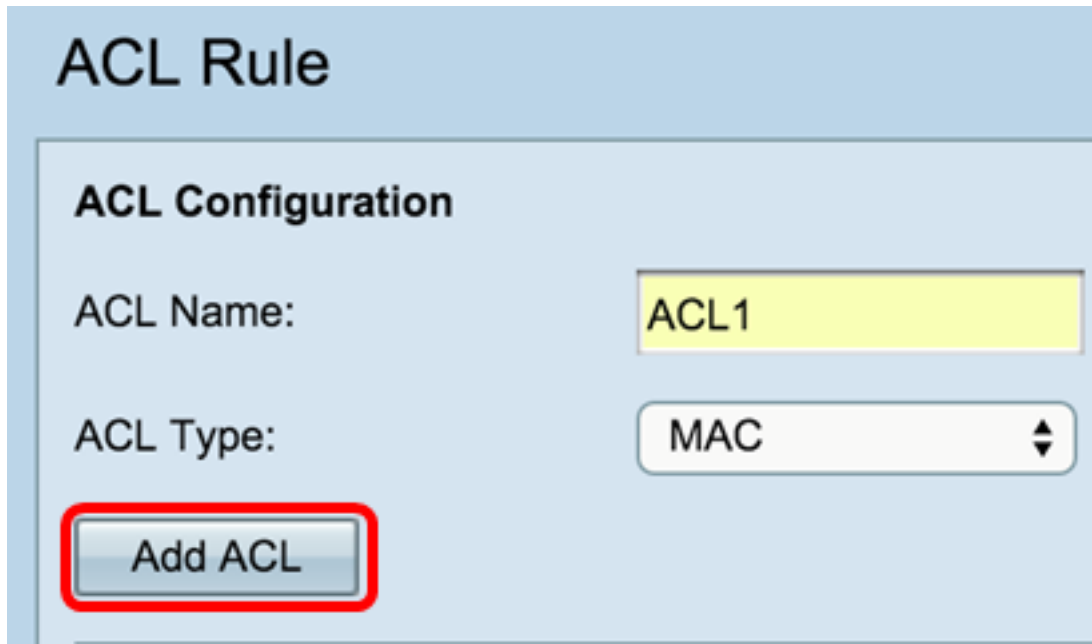
ステップ 3. ACL 型ドロップダウン リストから ACL 型を選択して下さい。



- IPv4 — 32ビット (4 バイト) アドレス。

- IPv6 — IPv4 へのサクセサは 128 ビット (8 バイト) アドレスで、構成されています。
- mac — MAC アドレスはネットワーク インターフェイスに割り当てられる固有のアドレスです。

ステップ 4. Add ACL ボタンをクリックして下さい。



ACL Rule

ACL Configuration

ACL Name: ACL1

ACL Type: MAC

Add ACL

MAC を選択した場合、[MAC ベースの ACL を設定するためにスキップして下さい](#)。

IPv4 を選択した場合、[IPv4-based ACL を設定するためにスキップして下さい](#)。

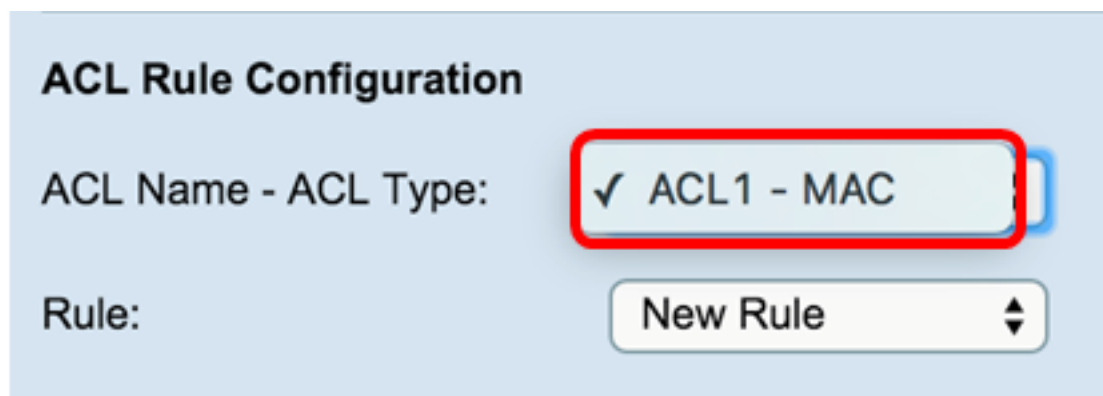
IPv6 を選択した場合、[IPv6-based ACL を設定するためにスキップして下さい](#)。

今正常に ACL を作成する必要があります。

設定 MAC ベースの ACL

ステップ 1. ACL 名前から ACL を-ルールを追加することを望む ACL 型ドロップダウン リスト選択して下さい。

注: 下記のイメージでは ACL1 MAC は一例として選択されました。



ACL Rule Configuration

ACL Name - ACL Type: ✓ ACL1 - MAC

Rule: New Rule

呼び出します。新しいルールが選択された ACL のために設定されなければならない場合ルール ドロップダウン リストからのルールを『New』を選択して下さい。さもなければ、ルール ドロップダウン リストからの現在のルールの 1 つを選択して下さい。

注: 最大 10 のルールは単一 ACL のために作成することができます。

ACL Rule Configuration

ACL Name - ACL Type:

Rule:

ステップ 3:処理 ドロップダウン リストから ACLルールのための操作を選択して下さい。

注: この例では、Deny ステートメントは作成されます。

Action:

Match Every Packet:

- 拒否—すべてのトラフィックをブロックします WAP に出入りするためにルールの基準を満たす。 暗示が明示的に許可されない各 ACL の終わりに拒否すべてのルールあるので、トラフィックは廃棄されます。
- permit —すべてのトラフィックを割り当てます WAP に出入りするためにルールの基準を満たす。 トラフィックは条件を満たさない廃棄されます。

注: ステップ 4 に 11 はオプションです。 チェックされるフィルタは有効になります。 それにこの特定のルールに適用してほしくないことフィルタのためのチェックボックスのチェックを外して下さい。

ステップ 4 各パケット チェックボックス 一致する コンテンツに関係なく各フレームのためのルールがパケットを一致するためにチェックして下さい。 の追加満たされた基準設定するためにボックスのチェックを外して下さい。

ヒント : 一致する場合各パケットは既にチェックされましたり、[ステップ 12](#) にスキップしています。

Action:

Match Every Packet:

ステップ 5 EtherType エリアで、イーサネットフレームのヘッダの値に対して満たされた条件を比較するために Radio ボタンを選択して下さい。 これらのオプションの 1 つを選択するか、または選択できません:

- から list—選択しますドロップダウン リストからプロトコルを選択して下さい。 リストに次のオプションがあります: AppleTalk、arp、IPv4、IPv6、IPX、NetBIOS、pppoe。
- 評価するべき一致—カスタム プロトコル 識別子に関しては、0600 から FFFF まで及び識別子を入力して下さい。

Protocol:

Any

Select From List:

Match to Value:

icmp

0 (Range)

ステップ 6 Class of Service (CoS) エリアで、802.1p ユーザ優先順位をイーサネットフレームに対して比較するために入力するように Radio ボタンを選択して下さい。またはユーザが定義する優先順位を選択できます。0 からユーザが定義するフィールドの 7 まで及び優先順位を入力して下さい。

Class Of Service:

Any

User Defined

6

ステップ 7 発信元MAC エリアで、イーサネットフレームに対して送信元MACアドレスを比較するために Radio ボタンを選択して下さい。選択しか、またはユーザが定義する選択し、提供されるフィールドで送信元MACアドレスを入力できます。

Source MAC:

Any

User Defined

Source MAC Address: 04:FE:36:A5:670B

Source MAC Mask:

ステップ 8.発信元MAC Mask フィールドで送信元MACアドレス マスクを入力して下さい規定 する イーサネットフレームに対して比較すべき発信元MAC のビット。

注: MAC マスクが 0 ビットを使用する場合、アドレスは、1 ビットを使用すれば、アドレス無視されます受け入れられ。

Source MAC:

Any

User Defined

Source MAC Address: 04:FE:36:A5:670B

Source MAC Mask: 00:00:00:00:00:00

ステップ 9 : 送信先MAC エリアで、イーサネットフレームに対して宛先MAC アドレスを比較するために Radio ボタンを選択して下さい。選択し、ユーザが定義する提供されるフィールドで入力します宛先MAC アドレスを Anyor を選択できます。

Destination MAC:

Any

User Defined

Destination MAC Address: F2:CA:46:11:EA:09

Destination MAC Mask:

ステップ 10.送信先MAC Mask フィールドで宛先MAC アドレス マスクを入力して下さい規定 する イーサネットフレームに対して比較すべき送信先MAC のビット。

注: MAC マスクが 0 ビットを使用する場合、アドレスは、1 ビットを使用すれば、アドレス無視されます受け入れられ。

Destination MAC: Any
 User Defined
Destination MAC Address: F2:CA:46:11:EA:09
Destination MAC Mask: 00:00:00:00:00:00

ステップ 11: VLAN ID エリアで、イーサネットフレームに対して VLAN ID を比較するために Radio ボタンを選択して下さい。0 から提供されるフィールドの 4095 まで及ぶ VLAN ID を入力して下さい。

VLAN ID: Any
 User Defined 52 (Range: 0 - 4095)

ステップ 12: [Save] をクリックします。

VLAN ID: Any
 User Defined
Delete ACL:

Save

ステップ 13: (オプションの) 設定された ACL を削除するために、削除 ACL チェックボックスをチェックし、次に『SAVE』をクリックして下さい。

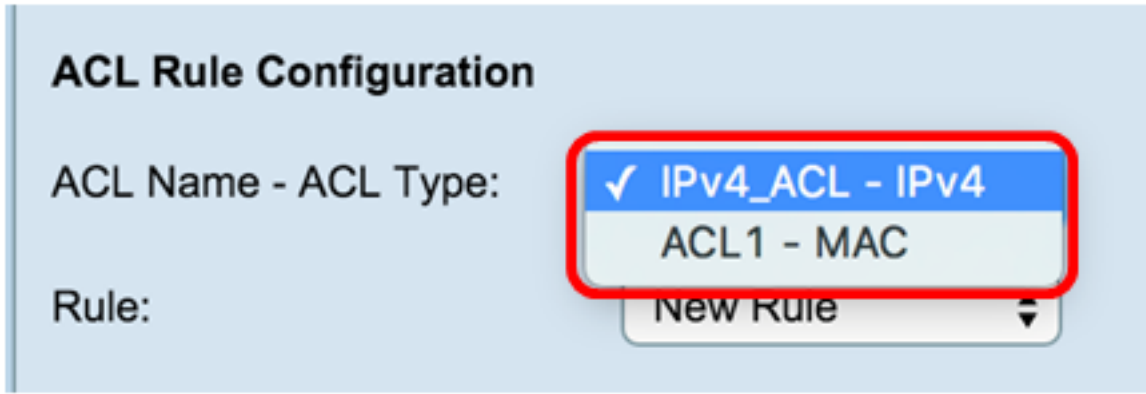
今うまく WAP の MAC ACL を設定する必要があります。

設定 IPv4-based ACL

1 ACL :

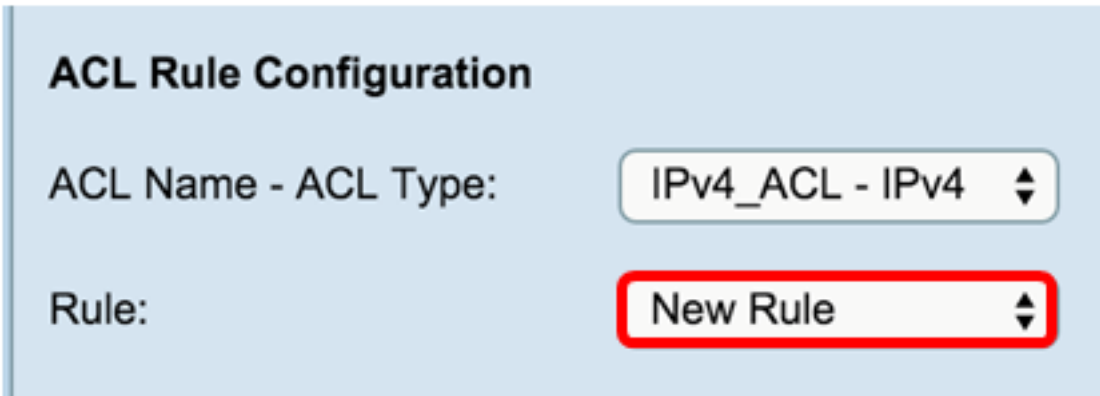
ACL - ACL TypeChoose ACL

: IPv4_ACL-IPv4



ACL New 1

: 10 ACL



3. ACL

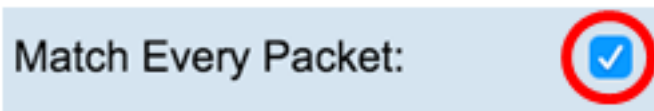
:

- — WAP ACL
- permit — WAP



: 4 9

4



[11.](#)

5 Radio

- list — 1 :

— ip —
— icmp — Send A

- IGMP — IPv4
- TCP — 2
- UDP —

- — 0 255 IANA ID

Protocol:

Any
 Select From List:
 Match to Value:

icmp (Range: 0 - 255)

6 IP IP Radio IP

- IP — IP
- — IP 255.255.255.255 0.0.0.0 IP

: 0.0.0.0 192.168.10.0/24 0.0.0.255 24

Source IP:

Any
 User Defined
 Source IP Address: 192.168.1.100 (xxx.xxx.xxx.xxx)
 Wild Card Mask: 0.0.0.255 (xxx.xxx.xxx.xxx)

7 Radio Anyto :

- list — :

- FTP — FTP TCP 1
- FTP — 20 D
- HTTP — HTTP World wide web -
- Simple Mail Transfer ProtocolSMTP — SMTP
- SNMP — SNMP IP
- telnet — A
- TFTP — TFTP FTP
- World Wide Web WWW — WWW HTTP

- port — 0 To Port 65535 3

- 0 1023 —
- 1024 49151 —
- 49152 65535 —/

- — 160 — 0xFFFF 0 1

Source Port:

Any
 Select From List:
 Match to Port:
 Mask:

www (Range: 0 - 65535)

8 IP IP Radio IP

- IP — IP
 - — IP 255.255.255.255 0.0.0.0 IP
- : 0.0.0.0 192.168.10.0/24 0.0.0.255 24

Destination IP:

Any
 User Defined

Destination IP Address: 192.168.1.110 (xxx.xxx.xxx.xxx)

Wild Card Mask: 0.0.0.255 (xxx.xxx.xxx.xxx -

9 Radio :

- list —

- FTP — TCP 1 A
- FTP — 20 D
- HTTP — World wide web -
- SMTP —
- snmp — IP
- telnet — A
- tftp — FTP
- WWW — HTTP

- port — 0 To Port 65535 3 :

- 0 1023 —
- 1024 49151 —
- 49152 65535 —/

- — 160-0xFFFF 0 1

Destination Port:

Any
 Select From List:

Match to Port: (Range: 0 - 65535)

Mask: (Range: 0 ~ 0xFFFF)

www

10 Radio :

- IP DSCP list — Differentiated Services Code Point DSCPAS Class of ServiceCoS CS Expedited Forwarding EF
- IP DSCP — DSCP 0 63
- ip precedence — IP 0 7. IP
- IP TOS — IP TOS
- IP TOS IP 8 IP TOS 00 ff 2 16 3 IP 6 IP DSCP
- IP TOS — IP TOS IP TOS IP TOS
- IP TOS 00 FF 2 16 IP TOS IP TOS IP TOS 7 7 5 1 IP TOS 0 IP TOS 00 IP TOS

Service Type

Any
 IP DSCP Select From List

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

IP Precedence: (Range: 0 - 7)

IP TOS Bits: (Range: 00 - FF)

IP TOS Mask: (Range: 00 - FF)

11. SAVE

VLAN ID: Any
 User Defined

Delete ACL:

Save

IPv4-based ACL

設定 IPv6-based ACL

1 ACL :

ACL - ACL type — ACL

: IPv6_ACL — Pv6

ACL Rule Configuration

ACL Name - ACL Type: **IPv6_ACL - IPv6**

Rule: **New Rule**

ACL New 1

: 10 ACL

ACL Rule Configuration

ACL Name - ACL Type: IPv6_ACL - IPv6

Rule: **New Rule**

3. ACL

- — WAP ACL
- permit — WAP

Action: Deny Permit

Match Every Packet:

: 4 11

4

Match Every Packet:

[12.](#)

5 Radio 1 :

- list — 1 :

— ip —

— icmp — Send A

— IGMP — IPv4

— TCP — 2

— UDP —

- — 0 255 IANA ID

Protocol: Any Select From List: Match to Value:

ipv6 (Range: 0)

6 IPv6 IP Radio IPv6 IPv6

- IPv6 address — IPv6
- IPv6 — IPv6

Source IPv6: Any User Defined

Source IPv6 Address: fd2d:43a5:25fe:9fef:ffff

Source IPv6 Prefix Length: 64 (Range: 0-128)

Source Port: Any

7 Radio :

- list — :

— FTP — TCP 1 A

— FTP — 20 D

— HTTP — World wide web —

— SMTP —

— snmp — IP

— telnet — A

— tftp — FTP

— WWW — HTTP

- port — 0 To Port 65535 3 :

— 0 1023 —

— 1024 49151 —

— 49152 65535 —/

- — 160 à 0xFFFF 0 1

Source Port:

Any
 Select From List: (Range:)
 Match to Port: (Range:)
 Mask: (Range:)

8 IPv6 IP Radio IPv6 IPv6

- IPv6 address — IPv6
- IPv6 — IPv6

Destination IPv6:

Any
 User Defined
 Destination IPv6 Address:
 Destination IPv6 Prefix Length: (Range:)

9 Radio :

- list — FTPFTP HTTPSNMPSMTPTFTPTelnetWWW
- port — 0 To Port 65535 3 :

— 0 1023 —

— 1024 49151 —

— 49152 65535 —/

- — 160-0xFFFF 0 1

Destination Port:

Any
 Select From List: (Ra
 Match to Port: (Ra
 Mask: (Ra

10 IPv6 IPv6 Radio IPv6 20 0-0xffff

IPv6 Flow Label:

Any
 User Defined: (

11 IPv6 DSCP IP DSCP Radio :

- list — 1 : DSCP Assured Forwarding AFClass of ServiceCoS CS Expedited Forwarding EF
- — 0 63 DSCP

IPv6 DSCP:

Any
 Select From List: ▼
 Match to Value: (Range: 0 - 63)

Delete ACL:

IPv6 DSCP: Any
 Select From List:
 Match to Value:

Delete ACL:

Save

13 ACL ACL ACL ACL ACL

IPv6-based ACL