

Creatie en configuratie van MAC-gebaseerde toegangscontrolelijst (ACL's) op WAP121 en WAP321 access points

Doel

Een toegangscontrolelijst (ACL) is een verzameling vergunningen en ontkenningvoorwaarden, genaamd regels, die beveiliging bieden en onbevoegde gebruikers blokkeren en geautoriseerde gebruikers toegang geven tot specifieke bronnen. ACL kan om het even welke ongerechtvaardigde pogingen blokkeren om netwerkmiddelen te bereiken. MAC ACL is Layer 2 ACL. Het netwerkapparaat inspecteert het kader en controleert de ACL-regels tegen de inhoud van het kader zoals het bron- en doeladres van MAC. Als een van de regels overeenkomt met de inhoud, wordt een vergunning afgegeven of ontkende actie ondernomen op het frame.

Dit artikel legt uit hoe u MAC ACL op WAP121 en WAP321 access points (WAP) kunt maken en configureren.

Toepasselijke apparaten

- WAP121
- WAP321

Softwareversie

- v1.0.3.4

Creatie van op MAC gebaseerde ACL

Stap 1. Meld u aan bij het Access Point Configuration-hulpprogramma en kies **client-QoS > ACL**. De *ACL*-pagina wordt geopend:

ACL

ACL Configuration

ACL Name: (Range: 1-31 Characters)

ACL Type:

ACL Rule Configuration

ACL Name - ACL Type:

Rule:

Action:

Match Every Packet:

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

Source IPv6 Address: Source IPv6 Prefix Length: (Range: 1 - 128)

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

Destination IPv6 Address: Destination IPv6 Prefix Length: (Range: 1 - 128)

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

IPv6 Flow Label: (Range: 00000 - FFFFF)

IPv6 DSCP: Select From List: Match to Value: (Range: 0 - 63)

Delete ACL:

Creatie van een op MAC gebaseerde ACL

ACL Configuration

ACL Name: (Range: 1-31 Characters)

ACL Type:

Stap 1. Voer de naam van de ACL in het veld *ACL-naam in*.

Stap 2. Kies **MAC** voor het ACL-type in de vervolgkeuzelijst *ACL-type*.

Stap 3. Klik op **Add ACL** om een nieuwe MAC-ACL te maken.

Configuratie van een regel voor op MAC gebaseerde ACL

ACL Rule Configuration

ACL Name - ACL Type:

Rule:

Action:

Match Every Packet:

EtherType: Select From List Match to Value: (Range: 0600 - FFFF)

Class Of Service: (Range: 0 - 7)

Source MAC Address: (xxxxxxxxxxxx) Source MAC Mask: (xxxxxxxxxxxx- "0s for matching, 1s for no matching")

Destination MAC Address: (xxxxxxxxxxxx) Destination MAC Mask: (xxxxxxxxxxxx- "0s for matching, 1s for no matching")

VLAN ID: (Range: 0 - 4095)

Delete ACL:

Stap 1. Kies de gewenste *ACL-naam* - vervolgkeuzelijst *ACL-type*.

Stap 2. Als een nieuwe regel voor de geselecteerde ACL moet worden ingesteld, kiest u **Nieuwe regel** in de vervolgkeuzelijst *Regel*. anders kiest u een van de huidige regels uit de vervolgkeuzelijst *Regel*.

Opmerking: Er kunnen maximaal 10 regels worden gemaakt voor één ACL.

Stap 3. Kies de actie voor de ACL-regel in de vervolgkeuzelijst *Action*.

- Ontken - blokkeert al het verkeer dat aan de standaardcriteria voldoet om het WAP-apparaat in te voeren of te verlaten.
- Toestaan van — Hiermee kan al het verkeer dat aan de criteria voldoet om het WAP-apparaat in te voeren of te verlaten.

Opmerking: De stappen 4 tot 11 zijn optioneel. Filters die zijn ingeschakeld. Schakel het vakje voor het filter uit als u wilt dat deze niet op deze specifieke regel wordt toegepast.

Stap 4. Controleer de optie **Overeenkomsten met elk pakket** om de regel voor elk frame of pakket **aan** te passen ongeacht de inhoud ervan. Schakel het vakje **Match Elk pakket** uit om een van de extra overeenkomende criteria te configureren.

Timesaver: Als **elke verpakking** is afgesteld, sla dan over naar [Stap 12](#).

Stap 5. Controleer het aankruisvakje **EtherType** om de overeenkomende criteria te vergelijken met de waarde in de kop van een Ethernet-kader. Als het vakje **EtherType** is ingeschakeld, klikt u op een van deze knoppen.

- Selecteer vanuit Lijst - Kies een protocol in de vervolgkeuzelijst. De vervolgkeuzelijst is opgevuld, arp, ipv4, ipv6, ipx, netbios, ppo.
- Overeenkomend met waarde — voor de identicator van het aangepaste protocol. Voer de identificatiecode in die varieert van 0600 tot FFFF.

Stap 6. Controleer het aankruisvakje **voor serviceklasse** om 802.1p gebruikersprioriteit in te voeren om dit te vergelijken met een Ethernet-kader. Geef de prioriteit op die in het veld *Serviceklasse* van 0 tot 7 varieert.

Stap 7. Controleer het aanvinkvakje **Bron-MAC** om het bron-MAC-adres te vergelijken tegen

een Ethernet-frame en voer het bron-MAC-adres in het veld *Bron-MAC-adres in*.

Stap 8. Voer het bron-MAC-adresmasker in in het veld *Bron-MAC-masker* dat specificeert welke bits in de bron-MAC om te vergelijken met een Ethernet-kader. Als het MAC-masker een bit gebruikt, wordt het adres geaccepteerd en als het 1 bit gebruikt, wordt het adres genegeerd.

Stap 9. Controleer het aanvinkvakje **MAC-adres van de bestemming** om het MAC-adres van de bestemming te vergelijken met een Ethernet-frame en voer het MAC-adres van de bestemming in het veld *MAC-adres van de bestemming in*.

Stap 10. Voer het doelmasker van MAC in in het veld *MAC-masker* van de *doellocatie* dat specificeert welke bits in de MAC-indeling moeten worden vergeleken met een Ethernet-kader. Als het MAC-masker een 0 bit gebruikt, wordt het adres geaccepteerd en als het een 1 bit gebruikt, wordt het adres genegeerd.

Stap 1. Controleer het vakje **VLAN-ID** om de VLAN-id te vergelijken met een Ethernet-kader. Voer de VLAN-id in die van 0 tot 4095 in het veld *VLAN-ID* varieert.

Opmerking: Raadpleeg het artikel *Configuratie van beheer en niet-gelabelde VLAN-id's op WAP121 en WAP321* voor informatie over het maken van een nieuw VLAN.

[Stap 12](#). Klik op **Opslaan** om de instellingen op te slaan.

Stap 13. (Optioneel) Om de ingesteld ACL te verwijderen, controleert u het vakje **ACL verwijderen** en vervolgens klikt u op **Opslaan**.