

La création et la configuration du MAC ont basé la liste de contrôle d'accès (ACL) sur les Points d'accès WAP121 et WAP321

Objectif

Une liste de contrôle d'accès (ACL) est une collection d'autorisation et refuse des conditions, appelées les règles, qui fournissent la Sécurité et bloquent des utilisateurs non autorisés et permettent aux utilisateurs autorisés pour accéder aux ressources spécifiques. L'ACL peut bloquer toutes les tentatives injustifiées d'atteindre des ressources de réseau. L'ACL de MAC est un ACL de la couche 2. Le périphérique de réseau examine la trame et vérifie les règles d'ACL contre le contenu de la trame telle que la source et l'adresse MAC de destination. Si les règles l'un des appartient le contenu, une autorisation ou refusent l'action est prise sur la trame.

Cet article explique comment créer et configurer l'ACL de MAC sur les Points d'accès WAP121 et WAP321 (WAP).

Périphériques applicables

- WAP121
- WAP321

Version de logiciel

- v1.0.3.4

Création d'ACL basée sur de MAC

Étape 1. Ouvrez une session à l'utilitaire de configuration de Point d'accès et choisissez le client QoS > ACL. La page d'ACL s'ouvre :

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:

Création d'un ACL basée sur de MAC

ACL Configuration

ACL Name: (Range: 1-31 Characters)

ACL Type:

Étape 1. Écrivez le nom de l'ACL dans la zone d'identification d'ACL.

Étape 2. Choisissez le **MAC** pour le type d'ACL de la liste déroulante de *type d'ACL*.

Étape 3. Cliquez sur Add l'ACL pour créer un nouvel ACL de MAC.

Configuration d'une règle pour l'ACL basée sur de MAC

Étape 1. Choisissez l'ACL désiré du *nom d'ACL* - liste déroulante de *type d'ACL*.

Étape 2. Si une nouvelle règle doit être configurée pour l'ACL sélectionné, choisissez la **nouvelle règle de la** liste déroulante de *règle* ; autrement, choisissez une des règles actuelles de la liste déroulante de *règle*.

Remarque: Un maximum de 10 règles peut être créé pour un ACL simple.

Étape 3. Choisissez l'action pour la règle d'ACL de la liste déroulante d'*action*.

- Refusez — Bloque tout le trafic qui répond aux critères de règle pour écrire ou quitter le périphérique WAP.
- Autorisation — Permet tout le trafic qui répond aux critères de règle pour écrire ou quitter le périphérique WAP.

Remarque: Étapes 4 11 sont facultatives. Des filtres qui sont vérifiés sont activés. Décochez la case pour le filtre si vous ne voulez pas qu'il s'applique à cette règle spécifique.

Étape 4. Cochez la **correspondance chaque** case de **paquet** pour apparier la règle de chaque trame ou paquet indépendamment de son contenu. Décochez la **correspondance chaque** case de **paquet** pour configurer le critère de correspondance supplémentaire l'un des.

Timesaver : Si la **correspondance chaque paquet** est vérifiée alors ignorez à l'[étape 12](#).

Étape 5. Cochez la case d'**EtherType** pour comparer le critère de correspondance contre la valeur dans l'en-tête d'une trame Ethernet. Si la case d'**EtherType** est cochée, cliquez sur une de ces cases d'option.

- Choisissez parmi la liste — Choisissez un protocole de la liste déroulante. La liste déroulante a l'AppleTalk, ARP, ipv4, IPv6, IPX, Netbios, PPPoE.
- Correspondance à évaluer — Pour l'identificateur de protocole fait sur commande. Entrez dans l'identifiant qui s'étend de 0600 à FFFF.

Étape 6. Cochez la case de **classe de service** pour écrire la priorité utilisateur 802.1p pour comparer contre une trame Ethernet. Écrivez la priorité qui s'étend de 0 à 7 dans le domaine de *classe de service*.

Étape 7. Cochez la case d'**adresse MAC source** pour comparer l'adresse MAC source contre une trame Ethernet et pour introduire l'adresse MAC source dans la zone adresse d'*adresse MAC source*.

Étape 8. Écrivez le masque d'adresse MAC source dans le domaine de *masque de MAC de source* qui spécifie qui des bits dans le MAC de source à comparer contre une trame Ethernet. Si le masque de MAC utilise des 0 bits, alors l'adresse est reçue, et si elle utilise 1 bit, alors l'adresse est ignorée.

Étape 9. Cochez la case d'**adresse MAC de destination** pour comparer l'adresse MAC de destination contre une trame Ethernet et pour écrire l'adresse MAC de destination dans le domaine d'*adresse MAC de destination*.

Étape 10. Écrivez le masque d'adresse MAC de destination dans le domaine de *masque de MAC de destination* qui spécifie qui des bits dans le MAC de destination à comparer contre une trame Ethernet. Si le masque de MAC utilise des 0 bits, alors l'adresse est reçue, et si elle utilise un 1 bit, alors l'adresse est ignorée.

Étape 11. Cochez la case d'**ID DE VLAN** pour comparer l>ID DE VLAN contre une trame Ethernet. Écrivez l>ID DE VLAN qui s'étend de 0 à 4095 dans le domaine d'*ID DE VLAN*.

Remarque: Pour les informations sur la façon dont créer un nouveau VLAN, référez-vous la *configuration d'article des id de Gestion et de VLAN non balisé sur WAP121 et WAP321*.

[Étape 12](#). **Sauvegarde de clic** pour sauvegarder les configurations.

Étape 13. (Facultatif) pour supprimer l'ACL configuré, cochez la case d'**ACL d'effacement** et puis cliquez sur la **sauvegarde**.