

# Présentation des listes de contrôle d'accès téléchargeables dans les commutateurs Catalyst 1300

## Objectif

L'objectif de cet article est de vous fournir une vue d'ensemble de la fonctionnalité de liste de contrôle d'accès téléchargeable (DACL) dans les commutateurs Catalyst 1300.

## Périphériques pertinents | Version logicielle

- Gamme Catalyst 1300 |4.1.6.54

## Introduction

Les listes de contrôle d'accès dynamiques sont des listes attribuées à un port de commutateur en fonction d'une stratégie ou de critères tels que l'appartenance à un groupe de comptes d'utilisateurs, l'heure, etc. Il peut s'agir de listes de contrôle d'accès locales spécifiées par filter-ID ou de listes de contrôle d'accès téléchargeables (DACL).

Les listes de contrôle d'accès téléchargeables sont des listes dynamiques créées et téléchargées à partir du serveur Cisco ISE. Ils appliquent dynamiquement des règles de contrôle d'accès basées sur l'identité des utilisateurs et le type de périphérique. La liste de contrôle d'accès dynamique a l'avantage de vous permettre d'avoir un référentiel central pour les listes de contrôle d'accès. Vous n'avez donc pas besoin de les créer manuellement sur chaque commutateur. Lorsqu'un utilisateur se connecte à un commutateur, il n'a qu'à s'authentifier et le commutateur télécharge les listes de contrôle d'accès applicables à partir du serveur Cisco ISE.

## Table des matières

- [Considérations DACL](#)
- [Processus de téléchargement DACL](#)
- [Noms ACL téléchargeables](#)

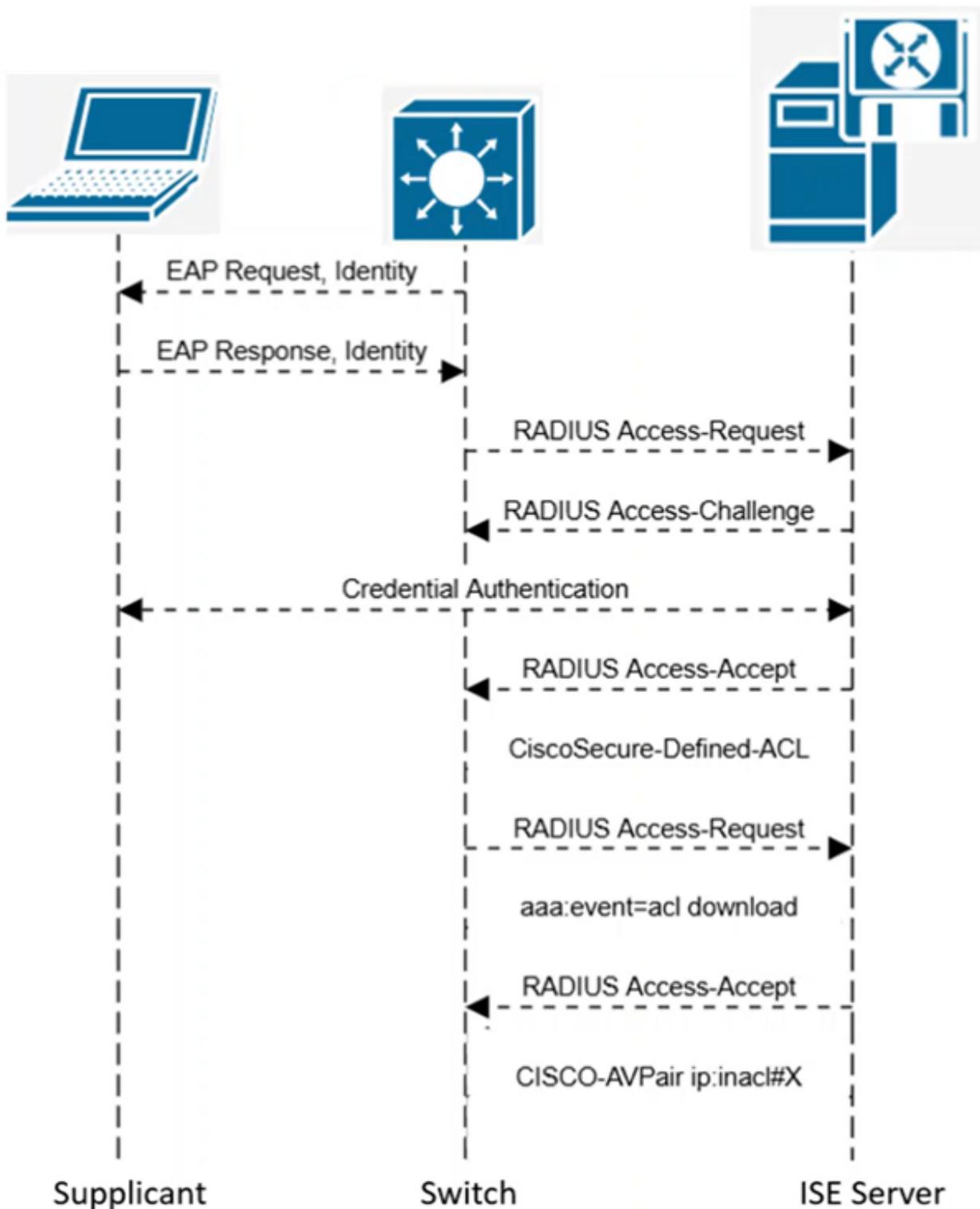
## Considérations DACL

Lors de l'utilisation de la liste de contrôle d'accès sur les commutateurs Catalyst 1300, il convient de garder à l'esprit quelques considérations.

- Cette fonction est réservée aux commutateurs Catalyst 1300 ; il n'est pas pris en charge sur les commutateurs Catalyst 1200.
- Les listes de contrôle d'accès dynamiques ne sont pas prises en charge sur les interfaces avec une carte de stratégie appliquée.
  - Le commutateur n'envoie pas de demande d'accès pour les règles ACL.
  - Le demandeur sera défini sur Authentifié mais pas sur Autorisé.
- Les listes de contrôle d'accès dynamiques s'excluent mutuellement avec la protection de source IP et la configuration liée à la suite de sécurité (niveau interface)
- Lors de l'utilisation de listes de contrôle d'accès dynamiques avec des commutateurs empilés, certains points doivent être pris en compte.
  - Si l'unité active bascule, les listes de contrôle d'accès ne sont pas stockées dans la mémoire locale du nouveau commutateur actif et toutes les listes de contrôle d'accès doivent être téléchargées à nouveau.
  - Toutes les règles appliquées aux interfaces qui ont été attribuées dans le cadre de l'authentification du système client seront supprimées.
- Il est nécessaire de définir le type d'authentification MAC sur RADIUS (au lieu de la méthode EAP par défaut) si vous utilisez MAB (MAC Authentication Bypass).
- Longueur du nom ACL
  - DACL : 64 caractères
  - Statique : 32 caractères
- Les ACL dynamiques sont toutes des ACL étendues.
- Les DACL utilisent plus de ressources TCAM que vous ne le pensez.
- Les listes de contrôle d'accès téléchargeables sont automatiquement supprimées lorsqu'aucun port ne les utilise.
- La liste de contrôle d'accès par défaut créée pour les listes dynamiques est automatiquement supprimée lorsqu'aucun port n'utilise de liste dynamique ou téléchargeable.

## Processus de téléchargement DACL

- Démarre en tant qu'authentification 802.1x standard.
- Une fois le client authentifié
  - Le serveur ISE envoie un message d'acceptation d'accès RADIUS avec Cisco Vendor AVPair - ACS : CiscoSecure-Defined-ACL = <Nom ACL>
  - Le commutateur envoie une requête d'accès RADIUS au fournisseur Cisco AVPair - aaa:event=acl-download
  - Le serveur ISE envoie un message d'acceptation d'accès RADIUS au fournisseur Cisco AVPair-ip:inacl#<Numéro de l'entrée ACE> = ACE



## Noms ACL téléchargeables

Le nom qui est téléchargé et attribué à la DACL sur le commutateur n'est pas le même que la DACL que vous créez sur ISE.

Par exemple, si une liste de contrôle d'accès nommée Marketing\_ACL est créée dans

ISE, lorsqu'elle est téléchargée, elle peut apparaître sous la forme #ACSACL#-IP-Marketing\_ACL-57f6b0d4.

- Format sur le serveur ISE : <name> - ex : ACL\_Marketing
- Format téléchargé sur le commutateur C1300
  - #ACSACL#-IP-<nom>-<numéro>
  - ex : #ACSACL#-IP-Marketing\_ACL-57f6b0d4
- Nom des segments
  - #ACSACL# - Préfixe ajouté par ISE
  - IP : indique le type de liste de contrôle d'accès (IP ACL)
  - <name> : nom de la liste de contrôle d'accès créée sur ISE
  - <number> - numéro de version au format hexadécimal ASCII
- La longueur du nom doit être inférieure ou égale à 64 caractères
- Encapsulé dans Cisco-AVPair : ACS:CiscoSecure-Defined-ACL= <Nom téléchargé>

## Conclusion

Maintenant que vous savez tout sur les ACL téléchargeables dans le commutateur Catalyst 1300, consultez l'article [ACL téléchargeable dans les commutateurs Catalyst 1300](#) pour les étapes pour le configurer.

Pour plus d'informations, consultez le [Guide d'administration de Catalyst 1300](#) et la [page de support de la gamme Cisco Catalyst 1300](#).

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.