

Catalyst 1300交换机中的可下载ACL概述

目标

本文的目的是让您概括了解Catalyst 1300交换机中的可下载ACL(DACL)功能。

适用设备 | 软件版本

- Catalyst 1300 系列 | 4.1.6.54

简介

动态ACL是根据策略或条件（如用户帐户组成员资格、时间等）分配给交换机端口的ACL。它们可以通过filter-ID指定的本地ACL或可下载ACL(DACL)。

可下载ACL是从思科ISE服务器创建和下载的动态ACL。它们根据用户身份和设备类型动态应用访问控制规则。DACL的优点是允许您为ACL设置一个中央存储库，因此您无需在每台交换机上手动创建它们。当用户连接到交换机时，他们只需进行身份验证，交换机将从思科ISE服务器下载适用的ACL。

目录

- [DACL注意事项](#)
- [DACL下载过程](#)
- [可下载的ACL名称](#)

DACL注意事项

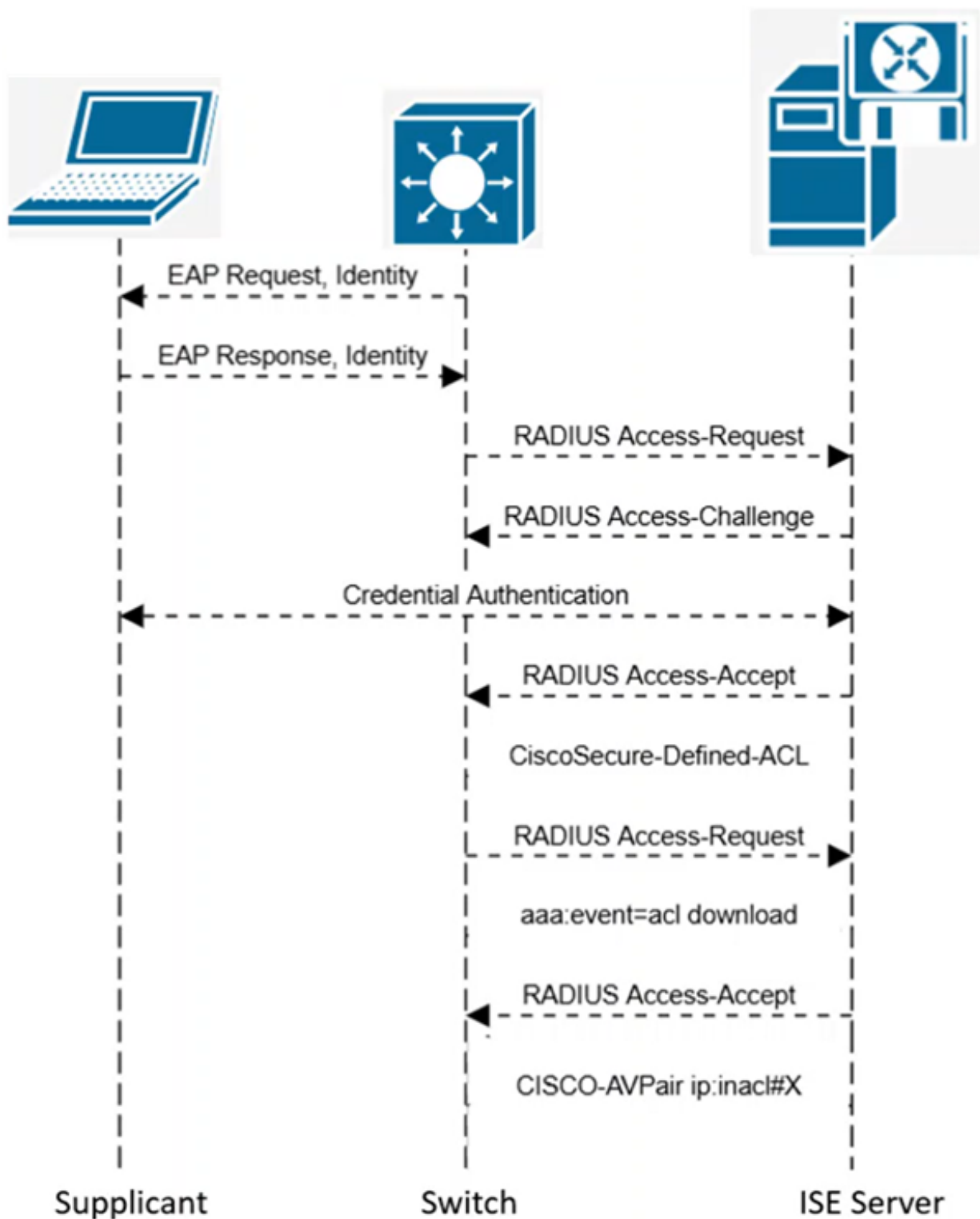
在Catalyst 1300交换机上使用DACL时，需要记住几个注意事项。

- 此功能专用于Catalyst 1300交换机；catalyst 1200交换机不支持此功能。
- 应用了策略映射的接口不支持动态ACL。
 - 交换机不会为ACL规则发送访问请求。
 - 请求方将被设置为Authenticated而不是Authorized状态。
- 动态ACL与IP源保护和（接口级别）安全套件相关配置互斥
- 将动态ACL与堆叠交换机配合使用时，需要考虑以下几点。
 - 如果主用设备发生故障转移，新的主用交换机不会将DACL存储在其本地内存中，并且需要重新下载所有DACL。

- 应用于作为客户端系统身份验证一部分分配的接口的所有规则将被删除。
- 如果使用MAB (MAC身份验证绕行) , 则必须将MAC身份验证类型设置为RADIUS (而不是默认EAP方法) 。
- ACL名称长度
 - DACL:64个字符
 - 静态 : 32个字符
- 动态ACL都是扩展ACL。
- DACL使用的TCAM资源比您预期的多。
- 可下载的ACL会在没有端口使用该ACL时自动删除。
- 当没有端口使用动态或可下载ACL时, 为动态ACL创建的默认ACL将自动删除。

DACL下载过程

- 作为标准802.1x身份验证启动。
- 客户端通过身份验证后
 - ISE服务器通过思科供应商AVPair - ACS发送RADIUS Access-Accept: CiscoSecure-Defined-ACL = <ACL Name>
 - 交换机通过思科供应商AVPair - aaa:event=acl-download发送RADIUS访问请求
 - ISE服务器发送RADIUS Access-Accept with Cisco Vendor AVPair-ip:inac1#<Number of the ACE entry> = ACE



可下载的ACL名称

在交换机上下载并分配给DACL的名称与您在ISE上创建的DACL的名称不同。

例如，如果名为Marketing_ACL的DACL在ISE中创建，下载时可能会显示为#ACSACL#-IP-Marketing_ACL-57f6b0d4。

- ISE服务器上的格式：<name> — 例如：Marketing_ACL
- 下载到C1300交换机的格式
 - #ACSACL#-IP-<name>-<number>
 - 例如：#ACSACL#-IP-Marketing_ACL-57f6b0d4
- 名称段
 - #ACSACL# - ISE添加的前缀
 - IP — 表示ACL的类型(IP ACL)
 - <name> — 在ISE上创建的ACL的名称
 - <number> — 版本号，以ASCII十六进制表示
- 名称长度必须小于或等于64个字符
- 封装在Cisco-AVPair中：ACS:CiscoSecure-Defined-ACL= <下载名称>

结论

现在您已了解Catalyst 1300交换机中的可下载ACL，请查看[Catalyst 1300交换机中的可下载ACL](#)文章，了解配置它的步骤。

有关详细信息，请参阅[Catalyst 1300管理指南](#)和[Cisco Catalyst 1300系列支持页](#)。

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。