思科身份服务引擎封闭模式

安全访问操作指南系列

日期：2012 年 8 月

作者：Adrianne Wang

目录

封闭模式

封闭模式概述

封闭模式是 802.1X 的一种较为传统的部署模式。在准备妥当的网络中，封闭模式提供对交换机级别（第 2 层）网络访问的全面控制。此类部署仅推荐用于具有 802.1X 部署背景并已将所有相关细节都考虑在内的环境。请将此模式视为一种“需谨慎部署”的模式。

思科建议分阶段部署 TrustSec 和 802.1X。初始阶段首先部署监控模式，最终状态则是低影响模式或封闭模式。本文档重点介绍封闭模式部署。

图 1 封闭模式默认 802.1X 端口行为

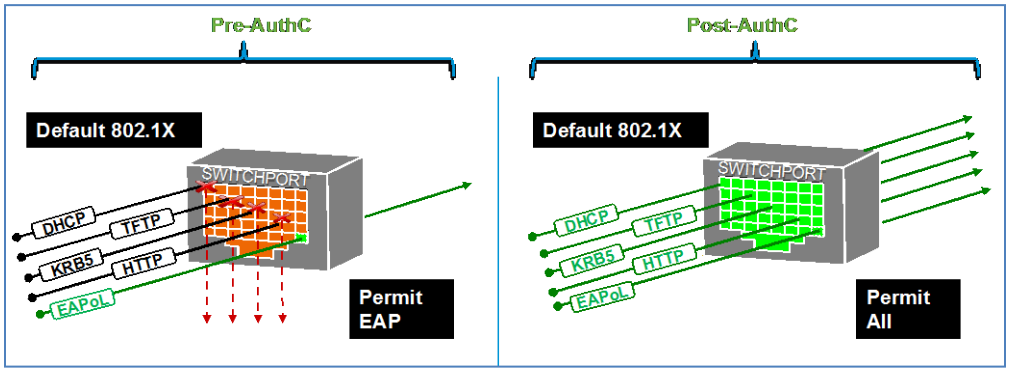

图 1. 封闭模式默认 802.1X 端口行为

在封闭模式下，在身份验证成功以前，交换机端口将不允许除局域网扩展认证协议 (EAPoL) 之外的任何流量通过。此模式没有预身份验证访问的概念，这意味着在身份验证过程中将不允许任何访问，例如动态主机配置协议 (DHCP)、HTTP 和域名系统 (DNS)。封闭模式对基于 VLAN 的实施很有用，因为客户端在其成功通过身份验证之前，不会获得 IP 地址。

对于成功完成 802.1X 身份验证的用户和设备，这通常不会造成问题，因为这种情况下身份验证通常很快。对于无法执行 802.1X 的设备，网络访问可能会出现严重延迟。由于交换机配置为首先尝试最安全的身份验证方法，因此不支持 802.1X 的设备必须等待身份验证计时结束并且交换机端口回退至 MAC 身份验证绕行 (MAB) 和/或作为辅助身份验证方法的 Web 身份验证。正如《通用交换机配置操作指南》中所建议的一样，一种方法是将 802.1X tx 计时器从 30 秒改为 10 秒，这将缩短不支持 802.1X 的设备访问网络之前的总等待时间，使之从 90 秒降至 30 秒。更改此计时器的一个常见原因是为了允许设备在其 DHCP 计时器到期之前接收 IP 地址。图 4 展示的是 802.1X 超时身份验证流程。

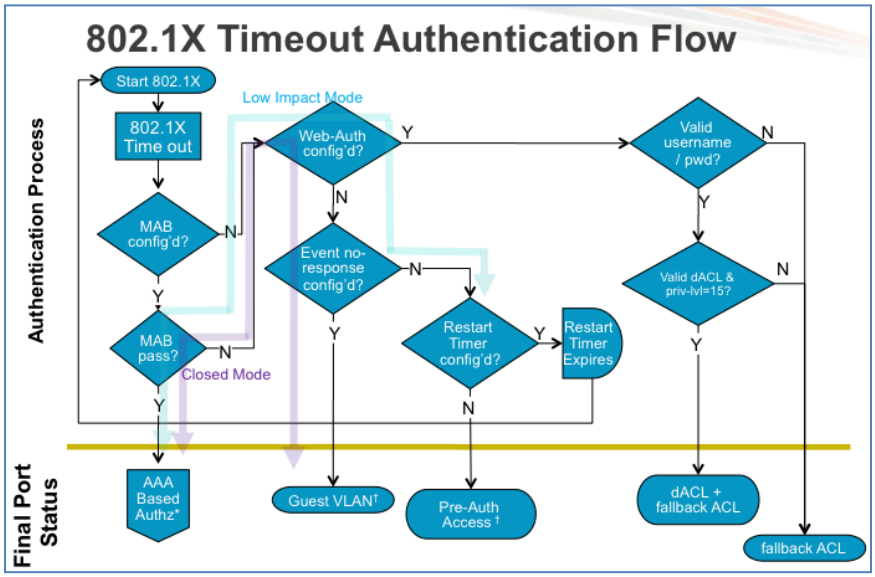

图 2. 超时身份验证流程

为了添加更精细的访问控制，封闭模式使用动态 VLAN 分配来将不同类用户隔离至不同的广播域。通过将来自不同类用户的流量隔离至单独的 VLAN，封闭模式为虚拟化网络服务奠定了基础。无法进行身份验证或身份验证失败的设备仍保留身份验证之前的相同访问级别：即没有网络访问权限，因为拒绝访问不及提供有限访问权限或访客访问权限那么可取。部署建议为配置辅助身份验证机制，例如采用思科身份服务引擎 (ISE) 的集中 Web 身份验证 (CWA)。

注：默认情况下，无线连接遵循与封闭模式相同的逻辑；但是建议在进行身份验证后添加对无线连接使用无线访问控制列表 (wACL) 或动态 VLAN (dVLAN) 的身份验证和实施模式逻辑，而不是允许所有流量。

封闭模式使用案例

采用有线和无线网络的封闭模式部署在身份验证成功之后为用户提供完整的网络访问权限，并将 VLAN 分配给已经过身份验证的用户。对于无线连接，身份验证失败会导致无法访问网络（这就是无线网络本质上的运行方式），但是，在有线连接中身份验证失败则会导致使用下一个身份验证方法。因此，有线环境中的非 802.1X 身份验证会尝试对交互用户使用 MAB 和 WebAuth (CWA)。以下是封闭模式的更多使用案例。

- 通过身份验证之前禁止访问
- 对不支持 802.1X 的公司资产提供快速访问
- 在接入边缘对流量进行逻辑隔离

部署注意事项

采用 VLAN 分配部署封闭模式可能会对网络架构产生重大影响。了解这些潜在影响对于成功部署此模式来说至关重要。因此，部署封闭模式必须进行战略规划并注意各种事项。以下流程概述的是一些帮助您在部署之前进行规划的做法。

VLAN 注意事项

动态 VLAN 分配要求每个用户可能会连接和进行身份验证的接入交换机都支持每个动态 VLAN。此要求有多种影响。例如，假设您要向三个用户组分配唯一 VLAN：工程、财务和 HR。在这种情况下，每个接入交换机都必须按名称定义这三个 VLAN（VLAN 的编号不必一样）。您可以通过用户分配功能将多个 VLAN 映射至一个 VLAN 组名。这可能对于大园区 LAN 很有用，因为它允许交换机在不同的 VLAN 上实现同一组内的用户负载平衡，从而降低任何单个 VLAN 的广播域大小。顾名思义，用户分配功能原本就是为这种使用案例而开发的。

如果交换机尝试将一个不存在的 VLAN 应用于某个端口，则授权会失败并且用户将无法获得访问权限（即使他们提供了有效的凭证而且通过了身份验证）。

使用所需的最小数量的 VLAN

从 IP 寻址的角度来看，单个接入交换机支持多个 VLAN 意义重大。优秀的园区设计原则要求每个 VLAN 一个子网，任何 VLAN 均不得跨越多台交换机。您的 IP 寻址方案应支持一台交换机多个子网，而且这种支持不会加剧园区分配程序块的控制层和数据层的负担。

实际上，您分配的 VLAN 越少，您的解决方案的可管理性和可扩展性就越高。事实上，有些客户已发现，经过分析后，使用非常少的 VLAN 即可满足其安全策略要求（例如，员工、访客/故障和语音）。

MAB 配置注意事项

如果您选择更改身份验证顺序，在 802.1X 之前执行 MAB，则要注意的是，这将意味着每个设备（即便是那些支持 802.1X 的设备）都将接受 MAB。这可能会显著增加您的网络控制层的流量。

根据失败的身份验证方法类型授予有限访问权限

如果未通过 802.1X 身份验证的设备需要某个级别的访问权限（例如，为了允许证书已过期的员工下载新证书），可以将解决方案配置为根据失败的身份验证方法类型授予有限访问权限。如果 802.1X 失败，可以将交换机配置为向用于此用途的专用 VLAN（即 Auth-Fail VLAN）打开端口。

处理无法执行 802.1X 和 MAB 失败的设备

您的网络上可能会有无法执行 802.1X 而且无法通过 MAB 的设备（例如，无正确配置的请求方而且需要具有某种形式的网络访问权限的承包商）。对于无法通过 MAB 的未知 MAC 地址，默认策略为 WebAuth (CWA)。如果设备已经过分析而且与任何已定义的授权策略匹配，则应用此策略，否则，此设备将限制为 WebAuth 模式。

实施封闭模式

确保所有身份存储库数据库保持最新和在线

在过渡到封闭模式之前，您应确保所有终端均可进行身份验证。所有身份存储库数据库都应保持最新和在线。

注：从低影响模式到封闭模式，用户可以选择 dACL 或 dVLAN 来实施授权策略。封闭模式的关键是了解封闭模式的运行方式并选择符合要求的部署方法。因此，本节不会提供具体的 ISE 配置。但是，会提供所需的交换机配置。

配置交换机

封闭模式表示默认的 802.1X 行为。在此模式下，交换机端口在从身份验证、授权和记帐 (AAA) 服务器获得授权结果之前不会允许除局域网扩展认证协议 (EAPoL) 之外的任何流量。这通常是部署的理想最终状态，因为它提供了非常强的安全性。像低影响模式一样，封闭模式还可以使用 TrustSec 部署中的所有可用实施机制（包括 dVLAN、可下载的 ACL [dACL]、安全组访问 [SGA] 等），但是封闭模式可能会对 IT 部署的运行模式产生某些影响。

步骤 1 请验证在接入交换机上是按名称定义所有可分配的 VLAN，并且每个 VLAN 均有预期的连接性。如有必要，使用用户分配功能来映射现有 VLAN 名称。

步骤 2 请验证已将交换机配置为接受来自 Cisco ISE 的授权说明

步骤 3 从交换机删除所有入口端口 ACL，如下所示：

```
C3750X(config-if-range)# no ip access-group ACL-DEFAULT in
```

注：此部署情景不需要 ACL。

步骤 4 在所有端口上禁用开放式身份验证功能。

```
C3750X(config-if-range)# no authentication open
```

注：如果需要，请将身份验证顺序配置为在 802.1X 之前执行 MAB，并修改身份验证优先级，从而使 802.1X 可以抢先进行成功的 MAB 身份验证。

步骤 5 除非您出于具体情况，需要在单个端口上支持多个数据设备，（对于非 IP 电话服务部署）请为单主机模式配置所有访问端口，或（对于 IP 电话服务部署）请为多域主机模式配置所有访问端口。

附录 A：参考

Cisco TrustSec 系统：

- http://www.cisco.com/go/trustsec
- http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns744/landing_DesignZone_TrustSec.html

设备配置指南：

- 思科身份服务引擎用户指南：
  http://www.cisco.com/en/US/products/ps11640/products_user_guide_list.html

有关思科 IOS 软件、思科 IOS XE 软件和思科 NX-OS 软件版本的更多信息，请参阅以下 URL：

- 对于 Cisco Catalyst 2900 系列交换机：
  http://www.cisco.com/en/US/products/ps6406/products_installation_and_configuration_guides_list.html
- 对于 Cisco Catalyst 3000 系列交换机：
  http://www.cisco.com/en/US/products/ps7077/products_installation_and_configuration_guides_list.html
- 对于 Cisco Catalyst 3000-X 系列交换机：
  http://www.cisco.com/en/US/products/ps10745/products_installation_and_configuration_guides_list.html
- 对于 Cisco Catalyst 4500 系列交换机：
  http://www.cisco.com/en/US/products/hw/switches/ps4324/products_installation_and_configuration_guides_list.html
- 对于 Cisco Catalyst 6500 系列交换机：
  http://www.cisco.com/en/US/products/hw/switches/ps708/products_installation_and_configuration_guides_list.html
- 对于 Cisco ASR 1000 系列路由器：
  http://www.cisco.com/en/US/products/ps9343/products_installation_and_configuration_guides_list.html

对于思科无线 LAN 控制器：

- http://www.cisco.com/en/US/docs/wireless/controller/7.2/configuration/guide/cg.html