思科身份服务引擎的全局交换机配置

安全访问操作指南系列

作者：Fay Lee

日期：2012 年 8 月

目录

全局交换机配置

本文档说明如何执行全局交换机配置。在 Cisco TrustSec 2.1 系统中，交换机执行多种关键功能。它处理 Web 身份验证的 URL 重定向以及从状态代理（思科网络访问控制 [NAC] 设备代理）到 Cisco ISE 服务器的发现流量的重定向。交换机在网络入口同时提供第 2 层和第 3 层流量实施，其中，第 2 层实施有助于确保仅授权用户和设备才可以获得网络访问权限。

这些推荐配置经过编译，成为适用于所有部署的最佳实践。最佳实践的目标是使该配置在部署的不同阶段自始自终保持一致并选定不同的部署类型。借此可以使用软件工具（例如 Cisco Prime™ 基础设施）设置端口模板，以便于配置多个端口和在接入层进行故障排除工作。

思科最佳实践：建议使用网络配置管理解决方案（例如 Cisco Prime LAN 管理解决方案 [LMS]）管理整个企业范围的配置。但是，此方案已经超过 Cisco TrustSec 2.1 测试实验室的范围，因此文中将不再提及。相关内容将在未来版本中加以介绍。

交换机配置 – 全局设置

相较于之前的 NAC 解决方案需要设备捕捉网络流量并重定向至 Web 身份验证页面，新的解决方案是在第 2 层接入（边缘）设备执行 URL 重定向，这可以简化 Web 身份验证部署和状态代理发现流程，无疑是一项巨大的改进。

注：必备配置：本指南假定交换机已预先配置了基础配置。例如，最佳实践是使用网络时间协议 (NTP) 设置正确的日期和时间，但本指南中不会提及此设置。

最佳实践：始终确保交换机能够与客户端子网通信，有助于确保 HTTP 重定向功能正常运作。为安全地进行最佳实践，请使用接入等级来限制可以管理交换机的地址。本主题不在本文档说明范围之内。

在交换机上配置 HTTP 服务器

步骤 1 在交换机上设置 DNS 域名。

a. 在设备上定义 DNS 域名之前，思科 IOS® 软件不允许创建和安装证书或自生成密钥。输入以下命令：

```
C3750X(config)#ip domain-name domain_name
```

步骤 2 通过输入以下命令，生成要用于 HTTPS 的密钥：

```
C3750X(config)#crypto key generate rsa general-keys mod 2048
```

注：为避免在 Web 重定向期间可能发生的证书不匹配错误，我们建议您使用由受信任证书颁发机构颁发的证书而非本地证书。本主题不在本文档说明范围之内。

步骤 3 在交换机上启用 HTTP 服务器。

必须在交换机上启用 HTTP 服务器才能执行 HTTP/HTTPS 捕捉和重定向。输入以下命令：

```
C3750X(config)#ip http server
C3750X(config)#ip http secure-server
```

注：在执行步骤 2 生成密钥之前，请勿运行 **ip http secure-server** 命令。如果您没按照顺序执行命令，那么交换机会自动生成密钥长度较短的证书，此证书会导致重定向 HTTPS 流量时出现意外。

配置全局 AAA 命令

步骤 1 在接入交换机上启用身份验证、授权和记帐 (AAA)。

默认情况下会禁用思科交换机的 AAA“子系统”。启用 AAA 子系统之前，配置中所需的任何命令均不可用。输入以下命令：

```
C3750X(config)#aaa new-model
```

注：此命令启用 AAA 网络安全服务提供的任何服务（例如，本地登录身份验证和授权），从而定义并应用方法列表等等。有关更多详细信息，请参阅《思科 IOS 安全配置指南》。

步骤 2 创建 802.1X 的身份验证方法。

必须通过身份验证方法指示交换机哪组 RADIUS 服务器用于处理 802.1X 身份验证请求：

```
C3750X(config)#aaa authentication dot1x default group radius
```

步骤 3 创建 802.1X 的授权方法。

通过步骤 2 中创建的方法，可以由 RADIUS 服务器验证用户/设备身份（用户名/密码或证书）。但是，只有有效的凭证还不够，还必须获得授权。授权是指用于定义用户或设备是否真正获得网络访问权限的条件以及实际允许的访问级别。

```
C3750X(config)#aaa authorization network default group radius
```

步骤 4 创建 802.1X 的记账方法。

RADIUS 记账数据包非常有用，并且对于许多 ISE 功能是必需的。这些类型的数据包将有助于确保 RADIUS 服务器 (Cisco ISE) 了解交换机端口和终端的确切状态。如果没有记账数据包，Cisco ISE 将只能了解身份验证和授权通信情况。记账数据包提供有关授权会话的长度以及交换机制定的本地决策（例如 AuthFail VLAN 分配等）的信息。

```
C3750X(config)#aaa accounting dot1x default start-stop group radius
```

配置全局 RADIUS 命令

我们配置主动方法来检查 RADIUS 服务器的可用性。通过此操作，交换机将定期向 RADIUS 服务器 (Cisco ISE) 发送测试身份验证消息，并等待服务器的 RADIUS 响应。并非一定要得到成功消息，身份验证失败的消息也可以，因为这也足以证明服务器处于活动状态。

最佳实践：不可能将这些身份验证记录从 Cisco ISE 1.1(377) 中的日志记录服务器中过滤掉。过滤会使 Cisco ISE 控制面板上显示的身份验证成功和失败信息出现偏差，因此我们建议使用能够成功进行身份验证、但授权会拒绝访问的帐户。

步骤 1 在全局配置模式下，为 RADIUS 保持连接间隔添加用户名和密码。

此处创建的用户名将在后面的步骤中添加至 Cisco ISE 中的本地用户数据库中，我们在稍后定义 RADIUS 服务器的步骤中会用到此帐户。

```
C3750X(config)#username radius-test password password
```

步骤 2 将 Cisco ISE 服务器添加至 RADIUS 组。

在此步骤中，将使用以前创建的测试帐户把各个 Cisco ISE 策略服务节点 (PSN) 添加至交换机配置中，并对各个 PSN 重复此步骤。

```
C3750X(config)#radius-server host ise_ip_address auth-port 1812 acct-port 1813 test username
radius-test key shared_secret
```

注：除正常过程中发生的所有身份验证或授权以外，服务器还将每小时一次主动检查响应。

步骤 3 设置停机条件。

交换机已配置为主动检查 Cisco ISE 服务器来获取 RADIUS 响应。现在配置交换机上的计数器，以确定服务器是处于活动状态还是处于停机状态。默认设置为，等待 5 秒以获取来自 RADIUS 服务器的响应，并且进行 3 次测试尝试后将服务器标记为停机。如果 Cisco ISE 服务器在 15 秒内没有作出有效响应，系统会将其标记为停机。

```
C3750X(config)#radius-server dead-criteria time 5 tries 3
```

注：我们会在部署模式部分更加详细地讨论高畅通性。

步骤 4 启用授权变更 (CoA)。

之前，已经定义了 RADIUS 服务器（交换机会将 RADIUS 消息发送到该服务器）的 IP 地址。而我们还会在其他列表中定义可执行授权变更 (RFC 3576) 操作的服务器，此操作也是在全局配置模式下进行，如下所示：

```
C3750X(config)#aaa server radius dynamic-author
C3750X(config-locsvr-da-radius)#client ise_ip_address server-key shared_secret
```

步骤 5 将交换机配置为使用思科供应商特定属性。

此处我们将交换机配置为在身份验证请求和记账更新期间向 Cisco ISE PSN 发送任何已定义的供应商特定属性 (VSA)。

```
C3750X(config)#radius-server vsa send authentication
C3750X(config)#radius-server vsa send accounting
```

步骤 6 接下来，我们将启用供应商特定属性 (VSA)。

```
C3750X(config)#radius-server attribute 6 on-for-login-auth
C3750X(config)#radius-server attribute 8 include-in-access-req
C3750X(config)#radius-server attribute 25 access-request include
```

步骤 7 确保交换机始终从正确的接口发送流量。

交换机通常可能具有多个与其关联的 IP 地址。因此，最好始终强制所有管理通信均通过一个指定接口执行，此接口 IP 地址必须与 Cisco ISE 网络设备对象中定义的 IP 地址相匹配。

思科最佳实践：作为网络管理最佳实践，对于所有管理通信使用环回适配器，同时向内部路由协议通告该环回接口。

```
C3750X(config)#ip radius source-interface interface_name
C3750X(config)#snmp-server trap-source interface_name
C3750X(config)#snmp-server source-interface informs interface_name
```

将交换机配置为允许面向/来自 Cisco ISE 的分析

Cisco ISE 将使用简单网络管理协议 (SNMP) 查询交换机的某些属性，从而帮助识别连接至交换机的设备。我们会配置 SNMP 社区供 Cisco ISE 查询，并配置要发送至 Cisco ISE 的 SNMP 陷阱。

步骤 1 配置只读 SNMP 社区。

Cisco ISE 只需“只读”SNMP 命令，确保此社区字符串与 Cisco ISE 内网络设备对象中配置的社区字符串相匹配。

思科最佳实践：该最佳实践是使用接入类限制 SNMP 对交换机的访问的安全最佳实践。SNMP 配置不属于 Cisco TrustSec 2.1 的测试范围，因此本文档中不会进行介绍。

```
C3750X(config)#snmp-server community community_string RO
```

步骤 2 配置交换机来发送陷阱消息。

现在，我们将启用 SNMP 陷阱发送，其中包含对 MAC 地址表的更改。每当在地址表中插入、删除或移动新地址时，都会向 Cisco ISE 发送包括设备 MAC 地址和接口标识符的陷阱。

```
C3750X(config)#snmp-server enable traps mac-notification change move threshold
```

步骤 3 将 Cisco ISE 添加为 SNMP 陷阱接收器。

在此，将服务器添加陷阱接收器，用于接收已配置的 MAC 通知：

```
C3750X(config)#snmp-server host ise_ip_address version 2c community_string mac-notification
```

步骤 4 为受信任端口配置动态主机配置协议 (DHCP) 监听。

DHCP 监听对于 Cisco TrustSec 2.1 不是必需的做法，但却是最佳实践。它不仅通过拒绝欺诈 DHCP 服务器实现更好的可用性，而且还为诸如动态地址解析协议 (ARP) 检测等其他安全工具准备交换机。DHCP 监听还有助于为 Cisco TrustSec 技术后续版本中引入的功能准备交换机。

配置 DHCP 监听之前，请确保对您信任的 DHCP 服务器位置进行备注。配置 DHCP 监听时，交换机会拒绝来自任何未配置为“trusted”的端口的 DHCP 服务器应答。输入上行链路接口的接口配置模式，并将其配置为信任端口。

注：仅当上行链路端口是交换机端口或中继端口而不是第 3 层接口时，才需要执行此步骤。这一事实说明，本节结尾处的示例配置中不使用 **ip dhcp snooping trust** 命令的原因。

```
C3750X(config)#interface interface_name
C3750X(config-if)#ip dhcp snooping trust
```

步骤 5 启用 DHCP 监听。

系统在全局配置模式下启用 DHCP 监听。启用 DHCP 监听后，必须配置与之配合使用的 VLAN，如下所示：

```
C3750X(config)#ip dhcp snooping
C3750X(config)#ip dhcp snooping vlan vlan_id_or_vlan_range
```

配置本地访问控制列表

交换机上的某些功能需要使用本地配置的访问控制列表 (ACL)，例如 URL 重定向。您创建的某些 ACL 可以立即使用，而某些则要到部署的稍后阶段才能使用。本部分的目标是同时为所有可能的部署模式准备好交换机，并限制重复的交换机配置所带来的运营成本。

步骤 1 添加以下要在监控模式下交换机端口上使用的 ACL：

```
C3750X(config)#ip access-list ext ACL-ALLOW
C3750X(config-ext-nacl)#permit ip any any
```

步骤 2 添加以下要在低影响和封闭模式下交换机端口上使用的 ACL：

```
C3750X(config)#ip access-list ext ACL-DEFAULT
C3750X(config-ext-nacl)#remark DHCP
C3750X(config-ext-nacl)#permit udp any eq bootpc any eq bootps
C3750X(config-ext-nacl)#remark DNS
C3750X(config-ext-nacl)#permit udp any any eq domain
C3750X(config-ext-nacl)#remark Ping
C3750X(config-ext-nacl)#permit icmp any any
C3750X(config-ext-nacl)#remark PXE / TFTP
C3750X(config-ext-nacl)#permit udp any any eq tftp
C3750X(config-ext-nacl)#remark Drop all the rest
C3750X(config-ext-nacl)#deny ip any any log
```

步骤 3 添加以下要用于对 Web 身份验证进行 URL 重定向的 ACL：

```
C3750X(config)#ip access-list ext ACL-WEBAUTH-REDIRECT
C3750X(config-ext-nacl)#remark explicitly deny DNS from being redirected to address a bug
C3750X(config-ext-nacl)#deny udp any any eq 53
C3750X(config-ext-nacl)#remark redirect all applicable traffic to the ISE Server
C3750X(config-ext-nacl)#permit tcp any any eq 80
C3750X(config-ext-nacl)#permit tcp any any eq 443
C3750X(config-ext-nacl)#remark all other traffic will be implicitly denied from the redirection
```

步骤 4 添加以下要用于状况代理 URL 重定向的 ACL：

```
C3750X(config)#ip access-list ext ACL-AGENT-REDIRECT
C3750X(config-ext-nacl)#remark explicitly deny DNS from being redirected to address a bug
C3750X(config-ext-nacl)#deny udp any any eq 53
C3750X(config-ext-nacl)#remark redirect HTTP traffic only
C3750X(config-ext-nacl)#permit tcp any any eq 80
C3750X(config-ext-nacl)#remark all other traffic will be implicitly denied from the redirection
```

配置全局 802.1X 命令

步骤 1 在交换机上全局启用 802.1X。

在交换机上全局启用 802.1X 实际上不会在任何交换机端口上启用身份验证。此时会对身份验证进行配置，但直到配置监控模式才会启用身份验证。

```
C3750X(config)#dot1x system-auth-control
```

步骤 2 使可下载的 ACL 发挥作用。

可下载访问控制列表 (dACL) 是 Cisco TrustSec 部署中十分常见的实施机制。为使 dACL 在交换机上正常运作，必须全局启用 IP 设备跟踪，如下所示：

```
C3750X(config)#ip device tracking
```

注：在某些不常见情况下，Windows 7 和设备不会响应 ARP，此时要求使用命令 **ip device tracking use SVI**。

步骤 3 在交换机上启用系统日志。

许多事件都会在思科 IOS® 软件上生成系统日志。某些系统日志消息可以发送至思科 ISE，用于排除故障。要帮助确保思科 ISE 能够编译来自交换机的合适系统日志消息，请使用以下命令：

注：日志应发送至起监控作用的思科 ISE 节点。

```
C3750X(config)#logging monitor informational
C3750X(config)#logging origin-id ip
C3750X(config)#logging source-interface <interface_id>
C3750X(config)#logging host <ISE_MNT_PERSONA_IP_Address_x> transport udp port 20514
```

在交换机上设置标准日志记录功能，以支持对思科 ISE 功能进行故障排除/录制。实施策略模块 (EPM) 是思科 IOS 软件的一部分，负责实现诸如 Web 身份验证和可下载 ACL 等功能：

启用 EPM 日志记录会生成与可下载 ACL 授权相关的系统日志，当此类日志发送至思科 ISE 时，部分日志可以在思科 ISE 中进行关联。

注：对于概念验证或试点项目来说，启用系统日志是理想之选。对于大规模建立的部署来说，如果担心流量问题，可以禁用系统日志记录。

```
C3750X(config)#epm logging
```

实际上，思科 ISE 仅收集和使用以下 NAD 系统日志消息：

- AP-6-AUTH_PROXY_AUDIT_START
- AP-6-AUTH_PROXY_AUDIT_STOP
- AP-1-AUTH_PROXY_DOS_ATTACK
- AP-1-AUTH_PROXY_RETRIES_EXCEEDED
- AP-1-AUTH_PROXY_FALLBACK_REQ
- AP-1-AUTH_PROXY_AAA_DOWN
- AUTHMGR-5-MACMOVE
- AUTHMGR-5-MACREPLACE
- MKA-5-SESSION_START
- MKA-5-SESSION_STOP
- MKA-5-SESSION_REAUTH
- MKA-5-SESSION_UNSECURED
- MKA-5-SESSION_SECURED
- MKA-5-KEEPALIVE_TIMEOUT
- DOT1X-5-SUCCESS / FAIL
- MAB-5-SUCCESS / FAIL
- AUTHMGR-5-START / SUCCESS / FAIL
- AUTHMGR-SP-5-VLANASSIGN / VLANASSIGNERR
- EPM-6-POLICY_REQ
- EPM-6-POLICY_APP_SUCCESS / FAILURE
- EPM-6-IPEVENT:
- DOT1X_SWITCH-5-ERR_VLAN_NOT_FOUND
- RADIUS-4-RADIUS_DEAD

全局配置示例

```
hostname C3750X
username radius-test password 0 Cisco123
!
aaa new-model
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting dot1x default start-stop group radius
!
aaa server radius dynamic-author
 client 10.1.100.3 server-key Cisco123
!
ip dhcp snooping vlan 10-13
ip dhcp snooping
ip domain-name cts.local
ip device tracking
!
dot1x system-auth-control
!
ip http server
ip http secure-server
!
ip access-list extended ACL-AGENT-REDIRECT
 remark explicitly prevent DNS from being redirected to address a bug
 deny udp any any eq domain
 remark redirect HTTP traffic only
 permit tcp any any eq www
 remark all other traffic will be implicitly denied from the redirection
ip access-list extended ACL-ALLOW
 permit ip any any
ip access-list extended ACL-DEFAULT
 remark DHCP
 permit udp any eq bootpc any eq bootps
 remark DNS
 permit udp any any eq domain
 ping <
 permit icmp any any
 remark PXE / TFTP
 permit udp any any eq tftp
 remark Drop all the rest
 deny ip any any log
ip access-list extended ACL-WEBAUTH-REDIRECT
 remark explicitly prevent DNS from being redirected to accommodate certain switches
 deny udp any any eq domain
 remark redirect all applicable traffic to the ISE Server
 permit tcp any any eq www
 permit tcp any any eq 443
 remark all other traffic will be implicitly denied from the redirection
!
ip radius source-interface Loopback0
snmp-server community Cisco123 RO
snmp-server trap-source Loopback0
snmp-server source-interface informs Loopback0
snmp-server enable traps mac-notification change move threshold
snmp-server host 10.1.100.3 version 2c Cisco123 mac-notification
radius-server attribute 6 on-for-login-auth
radius-server attribute 8 include-in-access-req
radius-server attribute 25 access-request include
radius-server dead-criteria time 5 tries 3
radius-server host 10.1.100.3 auth-port 1812 acct-port 1813 test username radius-test key Cisco123
radius-server vsa send accounting
radius-server vsa send authentication
logging monitor informational
epm logging
logging origin-id ip
logging source-interface Loopback0
logging host 10.1.100.3 transport udp port 20514
```

交换机：通用交换机端口配置

在上一节中，我们定义了接入层交换机全局配置设置的通用命令，包括 RADIUS、SNMP、分析和 AAA 方法。

本节重点介绍如何构建一个端点配置，从而无论使用哪种交换机类型或部署模式，均可以在整个思科 TrustSec 部署中使用该端点配置。

注：如果您使用的是诸如 Cisco Prime LAN 管理解决方案 (LMS) 4.1 等批量配置工具，则可能需要确保在以下任何命令之前运行此命令。

设置基本交换机端口配置

在配置交换机端口上的任何身份验证设置之前，必须确保将交换机端口配置为第 2 层端口，而不是第 3 层端口。要实现此配置，我们要运行一个只有一个单词的简单命令，此后，我们运行的其他命令均会生效。

步骤 1 输入交换机端口范围的接口配置模式：

```
C3750X(config)#interface range first_interface - last_interface
```

步骤 2 确保端口是第 2 层交换机端口。

```
C3750X(config-if-range)#switchport
```

步骤 3 使用主机宏为第 2 层边缘配置端口。

主机宏会自动为您运行三条命令。它会将端口配置为接入端口（非中继）、禁用隧道组，以及将生成树配置为处于快速端口模式。

```
C3750X(config-if-range)#switchport host
! - Switch Output:
switchport mode will be set to access
spanning-tree portfast will be enabled
channel group will be disabled
```

身份验证设置 – 灵活身份验证和高畅通性

802.1X 的默认行为是如果身份验证失败则拒绝访问网络。许多客户部署均不希望采用这种行为，因为它既不允许访客访问，也不允许员工修复其计算机系统和获取完整网络访问权限。处理 802.1X 身份验证失败的下一个阶段是提供“Auth-Fail VLAN”，使身份验证失败的设备/用户能够获得授权，可访问提供有限资源的 VLAN。

此步骤是正确定向中的一步，但仍缺乏所需的可行性，在必须对所有打印机和其他非身份验证设备使用 MAC 身份验证绕行的环境中尤其如此。如果使用 802.1X 的默认行为，对于没有请求方的打印机和其他设备，管理员所采用的端口配置方式必须与计划进行身份验证的端口的配置方式不同。

因此，思科创建了灵活身份验证 (Flex-Auth)。Flex-Auth 允许网络管理员在交换机端口上设置身份验证顺序和优先级，从而使端口能够依次尝试使用 802.1X、MAC 身份验证绕行和 Web 身份验证。提供所有这些功能的同时，还能够在所有接入端口上保持完全相同的配置，因此能够为客户提供比传统 802.1X 部署更简单的运行模式。

如前所述，在交换机端口上执行身份验证有多种方法：802.1X (dot1x)、MAC 身份验证绕行 (MAB) 和基于 Web 的身份验证 (Web-Auth)。如果采用 802.1X 身份验证，则交换机会在链路状态变更为“up”之后定期发送身份请求 (EAP-Identity-Request)（请参阅“身份验证设置 - 定时器”一节，了解建议的定时器更改方式）。此外，终端请求方还应该定期将基于 LAN 的 EAP 启动（EAPoL 启动）消息发送至交换机端口，从而加快身份验证速度。如果设备无法进行身份验证，则只需等待 dot1x 超时，随后系统将执行 MAC 身份验证绕行 (MAB)。假如设备 MAC 地址位于正确的数据库中，则会获得网络访问授权（图 3）。

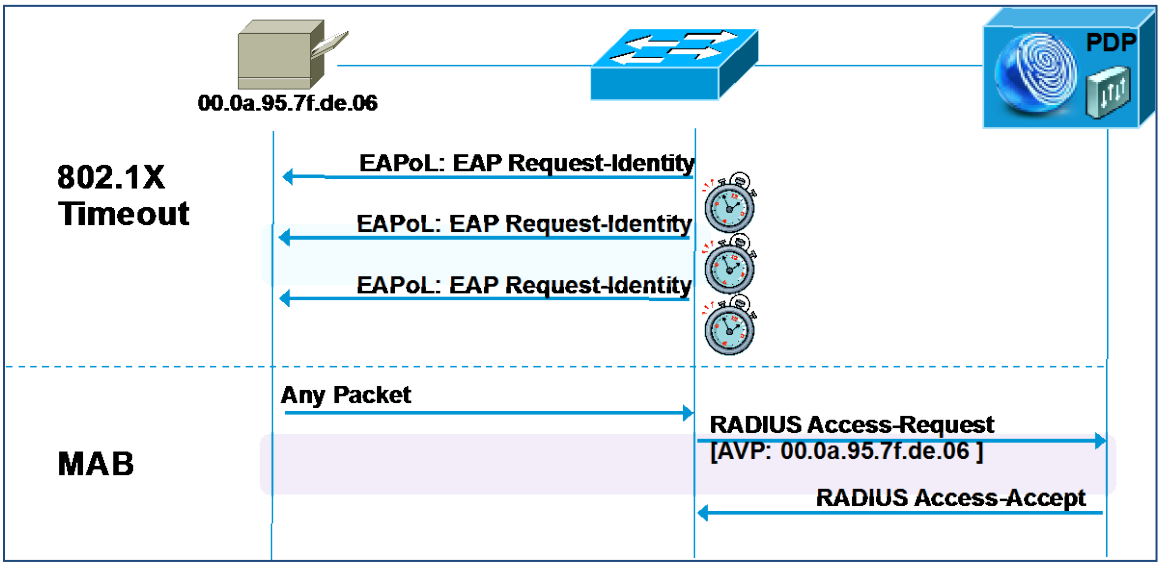

图 1. 灵活身份验证

以下步骤引导您完成 Flex-Auth 的配置，执行身份验证高可用性的可配置操作。

步骤 4 在交换机端口上配置身份验证方法的优先级。

最佳实践是始终首选较强的身份验证方法 (dot1x)。dot1x 方法也是所有思科交换机的默认设置。

```
C3750X(config-if-range)#authentication priority dot1x mab
```

步骤 5 配置交换机端口上身份验证方法的顺序。

在某些部署方法中，MAC 身份验证绕行 (MAB) 应发生在 802.1X 身份验证之前。对于这些极端情况，思科交换机确实允许网络管理员设置用户可定义的身份验证顺序。但是，最佳实践是保持先 dot1x 后 MAB 的顺序。

```
C3750X(config-if-range)#authentication order dot1x mab
```

注：Web 身份验证也是身份验证顺序命令的一个选项。此处配置的 Web-Auth 是指本地 Web 身份验证。最佳实践是使用中央 Web 身份验证。有关 Web 身份验证的详细信息，请参阅“Web 身份验证”。

步骤 6 将端口配置为使用 Flex-Auth，如下所示：

```
C3750X(config-if-range)#authentication event fail action next-method
```

步骤 7 将端口配置为在 RADIUS 服务器关闭时使用本地 VLAN。

在“Configure the Global RADIUS Commands”程序中，我们已将 RADIUS 服务器条目配置为使用测试帐户，该帐户会在思科 ISE 停止响应 RADIUS 请求后主动向交换机发送警报。现在，我们将交换机端口配置为在发现服务器处于“停机”状态后对端口进行本地授权，并在服务器再次启动时重新初始化身份验证。

```
C3750X(config-if-range)#authentication event server dead action reinitialize vlan vlan-id
```

引入此功能的目的在于解决单个端口上存在多个身份验证主机时发生的以下问题：一部分身份验证主机已进行身份验证，而 RADIUS 服务器可运行；而其他主机（新主机）尝试在 RADIUS 服务器关闭时进行身份验证。

引入这一新功能之前，所有通过身份验证的主机（RADIUS 服务器运行时）均能获取完整的网络访问权限，而其他主机（新主机）则无法获取网络访问权限。通过这一新的命令行界面 (CLI) 功能，当新主机尝试访问网络并且 RADIUS 服务器关闭时，该端口会立即重新初始化，并且所有主机（在此端口中）都均会获得相同的 VLAN。

步骤 8 将端口配置为在 RADIUS 服务器关闭时允许在网络上使用电话。

电话是在身份验证成功后通过配置 RADIUS 服务器以将属性 **device-traffic-class=voice** 向下传递到网络来放置在语音域上，从而无法运行。但是，当 RADIUS 服务器不可用时，电话将无法访问语音。这项新功能称为临界语音 VLAN。通过此新功能，当端口处于临界身份验证模式下并且来自主机的流量都带有语音 VLAN 标记时，设备（电话）会放入到端口的已配置语音 VLAN 中。电话通过思科发现协议 (CDP)、链路层发现协议 (LLDP) 或 DHCP 获取语音 VLAN 标识。以下是用于启用此功能的命令：

```
C3750X(config-if-range)#authentication event server dead action authorize voice
```

步骤 9 设置端口的主机模式。

启用 802.1X 的端口的默认行为是每个端口只授权一个 MAC 地址。我们还提供其他选项，最值得注意的是多域身份验证 (MDA) 和多重身份验证 (Multi-Auth) 模式。在所有思科 TrustSec 部署的初期，最佳实践是使用多重身份验证模式来确保部署 802.1X 的过程中不会出现拒绝服务。

```
注：由于 802.1X 在本地处理端口安全功能，因此在 TrustSec 部署中不推荐这一功能。
```

Multi-Auth 模式对于每个交换机端口的 MAC 地址数几乎没有限制，并且要求每个 MAC 地址均使用经过身份验证的会话。当部署到达身份验证的最后阶段或进入实施阶段，则建议使用多域模式。对于每个端口，多域身份验证将在数据域中支持一个 MAC 地址，在语音域中支持一个 MAC 地址。

```
C3750X(config-if-range)#authentication host-mode multi-auth
```

步骤 10 配置违例操作。

如果发生身份验证违例（例如 MAC 地址数超过端口上支持的最大数量），则默认会将端口置于错误禁用状态。虽然此行为看似正常且安全，但却可能带来意外的拒绝服务，在部署初期尤为如此。因此，我们会将该操作设置为受限制。使用这种运行模式，第一台通过身份验证的设备可以继续其授权操作，而其他设备则会被拒绝。

```
C3750X(config-if-range)#authentication violation restrict
```

身份验证设置 – 开放式身份验证和其他步骤

默认情况下 802.1X 采用二进制。身份验证成功意味着已授权用户访问网络，不成功的身份验证意味着用户无权访问网络。此范例无法为现代企业提供很好的帮助，大多数组织需要利用预执行环境 (PXE) 进行工作站成像，或者可能具有某些必须通过 DHCP 进行启动且么有任何方法来运行请求方的瘦客户端。

此外，802.1X 的早期采用者在整个公司范围内部署身份验证时也造成了影响。例如，请求方配置错误，未知设备由于缺少请求方而无法进行身份验证，以及因许多其他原因对所有设备都有影响。参见下图 1。

为帮助部署，思科创建了开放式身份验证模式。采用开放式身份验证，所有流量均可通过交换机端口，即使端口未获得授权也可以。此功能允许在整个企业内对身份验证进行配置，而不会拒绝对任何设备的访问。

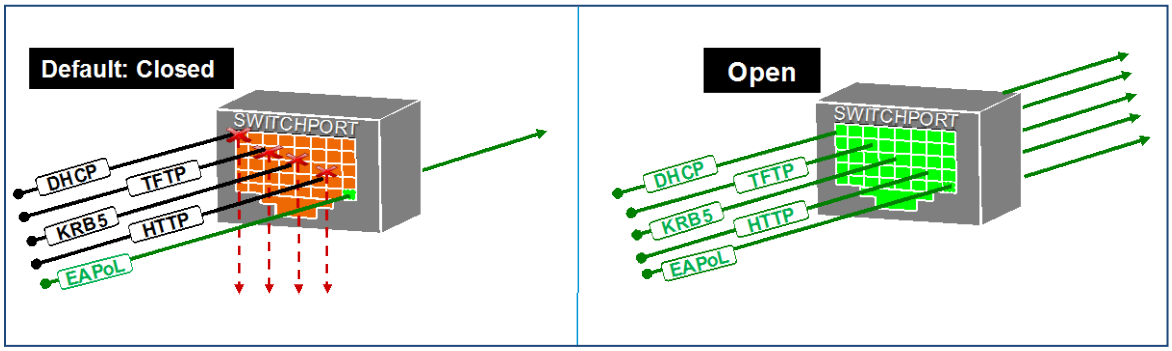

图 2. 默认身份验证模式（封闭式）与开放式身份验证模式

步骤 1 将端口设置为开放式身份验证。

```
C3750X(config-if-range)#authentication open
```

步骤 2 在端口上启用 MAC 身份验证绕行。

```
C3750X(config-if-range)#mab
```

步骤 3 支持端口执行 IEEE 802.1X 身份验证。

```
C3750X(config-if-range)#dot1x pae authenticator
```

身份验证设置 – 定时器

很多定时器可以在部署中根据需要进行修改。除非遇到调整定时器可纠正意外行为这种特定情况，否则我们建议将除 802.1X 传送定时器（传送时间）以外的所有定时器都保留默认值。

传送时间定时器的默认值为 30 秒。将此值保留为 30 秒意味着默认等待 90 秒（3 x 传送时间）后，交换机端口会开始采用下一方法进行身份验证，对非身份验证设备启用 MAB 流程。

思科最佳实践：根据多种配置，最佳实践的建议是将 tx-period 值设置为 10 秒，从而为 MAB 设备提供最佳时间。将该值设置为 10 秒以内可能会导致端口过快采用 MAC 身份验证绕行。

步骤 1 配置传送时间定时器。

```
C3750X(config-if-range)#dot1x timeout tx-period 10
```

在端口上应用初始 ACL 并启用身份验证

此步骤将为监控模式准备端口：在端口上应用默认 ACL 而不拒绝任何流量。

步骤 1 应用初始 ACL (ACL-ALLOW)。

```
C3750X(config-if-range)#ip access-group ACL-ALLOW in
```

步骤 2 开启身份验证。

```
C3750X(config-if-range)#authentication port-control auto
```

注：需要此命令才能启用身份验证（802.1X、MAB、Web-Auth）。如果没有此命令，则所有流程看似在运行，但不会向 RADIUS 服务器发送任何身份验证。

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

对于思科无线局域网控制器：
http://www.cisco.com/en/US/docs/wireless/controller/7.2/configuration/guide/cg.html