使用 VRF-Lite 进行数据流隔离的 NAC 第 3 层带外设计指南

目录

简介

注意： 本文档中的信息如有更改，恕不另行通知。如果可能，请确认所有建议。

本文档旨在介绍在第 3 层带外 (OOB) 部署中基于 VRF-Lite 的 NAC 实施，其中 NAC 服务器 (CAS) 是在实际 IP 网关（路由）模式下配置的。“第 3 层带外”已迅速成为一种最受欢迎的 NAC 部署方法。之所以变得受欢迎，主要基于几个动力因素。第一是可以更好地利用硬件资源。通过在第 3 层 OOB 方法中部署 NAC，可对单个 NAC 设备进行扩展以容纳更多用户。它还允许将 NAC 设备集中放置，而不是分布在整个园区或组织中。因此，从资本支出和运营费用这两个角度来看，第 3 层 OOB 部署都更具成本效益。在第 3 层 OOB 体系结构中部署 NAC 有两种广泛使用的方法。

1. 基于发现主机的方法 - 使用 NAC 代理中的固有功能到达 NAC 服务器 (CAS)。应用于接入交换机的 ACL 控制脏网络上的数据流实施。有关详细信息，请参阅使用 SWISS 协议连接到 NAC 服务器 (CAS)。
2. 基于 VRF 的方法 - 使用 VRF 将未经验证的数据流路由到 CAS。在 NAC 服务器 (CAS) 上配置的数据流策略用于脏网络上的实施。此方法有两个子方法。在第一个方法中，VRF 遍布在整个基础架构中，在这种情况下，所有第 3 层设备都参与标记交换。第二个方法使用 VRF-Lite 和 GRE 隧道通过不了解标记交换的第 3 层设备以隧道方式传输 VRF。第二个方法的好处是，核心基础架构所需的配置更改最少。

注意： 虽然第 3 层 OOB 是最常用的部署方法之一，但它不可能始终是每个环境的最佳解决方案。

还有一些其他选项可供选择，这些选项可能更适合于您的特定要求。有关这些其他 NAC 设计选项的详细信息，请参阅计划您的部署。

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

- 基本了解第 2 层和第 3 层基础架构操作和配置
- 基本了解 Cisco NAC 设备以及与其关联的各种实施方法之间的区别
- 所有 NAC 部署和设计都应基于明确的业务需求。这些是此测试设置的商业需求假定：用户必须在经过身份验证后才被授权访问整个网络。访问权限根据用户身份进行限制。这些权限映射到 Active Directory 中的组成员资格。包括访客组、承包商组和员工组。系统基于 AD 组成员资格将用户放到具有适合于每个组的网络访问权限的 VLAN 中。来宾用户流量继续从网络的其余隔离在验证以后。在用户被允许访问网络后，NAC 设备必须不再位于数据流路径中。这可防止 NAC 设备成为瓶颈并使得经过验证的用户可以充分利用网络的潜力。
- NAC 包含许多本文档中未介绍的功能。本指南旨在研究和记录基于 VRF-Lite 的第 3 层带外 NAC 部署所需的设计准则和配置。本指南不重点介绍状态评估或修正。关于NAC设备的更多信息和其全部的功能可以在www.cisco.com/go/nac (仅限注册用户)找到。

使用的组件

本文档不限于特定的软件和硬件版本。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

配置

基础架构配置

前言：

考虑基于 VRF-Lite 的第 3 层 OOB NAC 部署时，需要考虑几个重要的设计原理。此处列出了这些原理，并包括了有关其重要性的简短论述。

1. **数据流分类和工程** - 对于此类型的 NAC 设计，要了解并记住的主要概念是分类为“脏”的数据流 *必须* 流入 NAC 服务器 (CAS) 的不受信任端。在 NAC 实施的设计期间，请始终牢记此原理。此外，不应允许干净网络和脏网络相互直接通信。在使用 VRF 的第 3 层 OOB 设计中，NAC 服务器 (CAS) 充当确保在干净网络和脏网络之间进行隔离和安全通信的实施点或控制器。
2. **数据流隔离** - 必须确保选择适当的实施机制为源自未经验证和授权的主机的所有数据流提供数据流和路径隔离。此处使用 VRF-Lite 来实现完全的数据和控制层面隔离 (VRF)。
3. **集中实施** - 因为 VRF-Lite 方法遵循由路由功能创建的自然路径选择：拓扑更改、访问控制要求和/或地址更改不会导致需要在整个基础架构中处理 ACL。如果将 VRF-Lite 和 GRE 隧道结合使用，则可灵活地将脏数据流正好放在 NAC 服务器面前，而不需要配置多次跳跃。将

VRF-Lite 和 GRE 结合使用只需对边缘第 3 层设备进行配置。这极大地减少了提供路径隔离要求所必须涉及的设备数。

4. **困难** - 实施和长期维护的困难。在确定您可能用于网络中的 NAC 第 3 层 OOB 的方法时，必须考虑简化实施和降低长期运营成本，并考虑实施该技术的复杂性，特别是在动态环境中。

注意： NAC 设备不会注意数据流是如何提供给它的。换句话说，对于数据流是通过 GRE 隧道到达，还是通过基于策略的路由配置进行了重定向，还是进行了 VRF 路由等等，设备自身没有偏好。

注意： 为了获得可能的最佳最终用户经验，请记住使用最终用户的浏览器信任的证书。对于生产环境，不建议在 NAC 服务器上使用自生成的证书。

注意： 请始终使用 NAC 服务器的不受信任接口的 IP 地址生成 NAC 服务器的证书。

下面是一个使用 VRF 的设备虚拟化图。此方法提供用于路径隔离的控制层面和数据层面。

拓扑

此图表是用于撰写本文的拓扑的表示形式。内部网络通过全局路由表路由，并且没有 VRF 与之关联。脏 VRF 仅包含 Dirty_VLAN 和关联的中转网络，这些中转网络是强制所有源自 DIRTY_VLAN 的数据流经 NAC 设备的脏端所必需的。访客 VRF 包含 GUEST_VLAN 和关联的中转网络，这些中转网络是在防火墙的单独子接口上终止源自 GUEST_VLAN 的所有数据所必需的。这三个虚拟网络中的每一个都在同一个物理基础架构上实施并分别提供完全的数据流和路径隔离。

流程

此部分显示在安装和不安装代理的情况下获得网络访问权限所需的基本流程。这些流程实质上是宏分析，并且仅包含功能决策步骤。它们不包括发生的每个选项或步骤，也不包括基于终点评估标准的授权决策。

配置

配置信息详细说明了使用 VRF-Lite/GRE 配置网络以进行路径隔离所必需的步骤，以及将 NAC 设备作为第 3 层 OOB 实际 IP 网关插入网络所必需的配置。

注意： VRF-lite 是一个允许您支持两个或多个虚拟网络的功能。VRF-lite 也允许在虚拟网络之间重叠 IP 地址。但是，不建议对 NAC 实施使用 IP 地址重叠，因为虽然基础架构自身支持重叠地址，但它可能导致故障排除变得复杂并导致不正确的报告。

VRF-lite 使用输入接口区分不同虚拟网络的路由，并通过将一个或多个第 3 层接口与每个 VRF 关联来构建虚拟数据包转发表。VRF 中的接口可以是物理接口，如以太网端口；也可以是逻辑接口，如子接口、隧道接口或 VLAN SVI。请注意，在任何时候第 3 层接口都不能属于多个 VRF。

VRF-Lite 的重要考虑事项

- VRF-Lite 只对在其中定义它的交换机本地有意义，并且 VRF 成员资格由输入接口确定。不执行任何数据包报头或有效负载处理。
- 使用 VRF-lite 的交换机由多个安全域共享，并且所有安全域都有它们自己的唯一路由表。
- VRF-Lite 可让多个安全域在网络设备之间共享同一物理链路。具有多个 VLAN 或 GRE 隧道的中继端口提供数据流隔离功能，该功能将来自各个不同安全域的数据包分开。
- 所有安全域都必须具有它们自己的 VLAN。

- VRF-lite 并不支持所有 MPLS-VRF 功能：标签交换、LDP 邻接或标记的数据包。
- 第 3 层 TCAM 资源在所有 VRF 之间共享。要确保任何一个 VRF 都具有足够的 CAM 空间，请使用 **maximum routes** 命令。
- 使用 VRF-Lite 的 Catalyst 交换机可以支持一个全局网络，并最多可以支持 64 个 VRF。支持的路由总数受 TCAM 的大小限制。
- 大多数路由协议（BGP、OSPF、EIGRP、RIP 和静态路由）都可以在运行 VRF-Lite 的设备之间使用。
- 除非需要在 VRF 之间泄漏路由，否则不需要将 BGP 和 VRF-Lite 一起运行。
- VRF-Lite 不影响数据包交换速率。
- 多播和 VRF-Lite 不能同时配置在同一个第 3 层接口上。
- 当您配置 OSPF 作为网络设备之间的路由协议时，应使用 router ospf 下的 **capability vrf-lite** 子命令。

定义 VRF

在此设计示例中，要求为未经身份验证的脏用户和访客提供路径隔离。允许所有其他数据流使用内部网络。这需要定义两个 VRF。下面是配置：

```
!
ip vrf DIRTY
!--- Names the VRF and places you into VRF Configuration
Mode description DIRTY_VRF_FOR_NAC !--- Gives the VRF a
user friendly description field for documentation rd
10:1 !--- Creates a VRF table by specifying a route
distinguisher. !--- Enter either an AS number and an
arbitrary number (xxx:y) or an !--- IP address and
arbitrary number (A.B.C.D:y). ! ip vrf GUESTS
description GUESTS_VRF_FOR_VISITORS rd 30:1 !
```

将 VLAN 或接口与 VRF 关联

在第 3 层交换机或路由器上定义 VRF 后，参与 VRF-Lite 配置的接口必须与它们所属的 VRF 关联。如前文所述，物理接口和虚拟接口都可与 VRF 关联。所包括的是与 VRF 关联的物理接口、交换虚拟接口、子接口和隧道接口的示例。

```
!
interface FastEthernet0/1
ip vrf forwarding GUESTS
!!Associates the interface with the appropriate VRF
defined in Step 1!!
ip address 192.168.39.1 255.255.255.252
!
interface FastEthernet3/1.10
encapsulation dot1Q 10
ip vrf forwarding DIRTY
ip address 192.168.10.1 255.255.255.252
!
interface Vlan100
ip vrf forwarding DIRTY
ip address 192.168.100.1 255.255.255.0
!
interface Tunnel0
ip vrf forwarding GUESTS
ip address 192.168.38.2 255.255.255.252
tunnel source Loopback0
```

```
tunnel destination 192.168.254.1
!
```

在两个设备之间扩展 VRF

在基础架构的两个片段之间扩展 VRF 有几种可接受的方法。您应根据以下标准选择方法：

1. 平台的功能 - 关于平台功能，支持第 3 层功能的所有当前 Cisco 企业交换和路由平台都支持 VRF-Lite。这包括但不限于 Catalyst 6500、4500、3750 和 3560 平台。
2. 运行相应 Cisco IOS 的任何路由平台，这包括但不限于 7600、3800、2800、1800 和 800 系列 ISR。
3. 基础架构的相关片段之间的第 3 层跳数 - 确定第 3 层跳数对于保持部署尽可能简单非常关键。例如，如果在托管 CAS 设备和客户端的基础架构之间有五个第 3 层跳，这可能导致额外的管理开销。

使用不正确的解决方案：

1. 第 2 层中继将导致一个并非最佳的第 2 层拓扑。
2. 第 3 层子接口将导致许多要配置的附加接口。因此，这可能导致额外的管理开销和潜在的 IP 编址问题。这在图表中进行了说明。如果假设基础架构中没有冗余，则所显示的每个网络层都有一个输入物理接口和一个输出物理接口。子接口数的计算方法则为 (2 * 网络中的层数 * (VRF 数))。在本示例中，有两个 VRF，因此公式为 ((2*5)*2)，即 20 个子接口。一旦添加冗余，此数字将多出两倍。将其与 GRE 扩展进行比较，要得到相同的最终结果，GRE 扩展只需要四个接口。这清楚地阐明了 GRE 是如何显著降低配置影响的。

第 2 层中继

在未部署第 3 层机柜或网络设备不支持 GRE 或子接口的情况下，首选第 2 层中继。应该注意的是，Catalyst 3560、3750 和 4500 平台不支持子接口。Catalyst 3560 和 3750 也不支持 GRE。Catalyst 4500 在软件中支持 GRE，Catalyst 6500 在硬件中支持 GRE。

在第 3 层机柜模型（您在其中将不支持子接口或 GRE 的平台连接到支持子接口或 GRE 的平台）中，最好只在一端使用第 2 层中继，在另一端使用子接口。这使您可以保持第 3 层机柜体系结构的所有优点，并且仍可以克服某些平台上无 GRE 或子接口支持的限制。仅在链路的一端配置第 2 层中继的一个主要优点是，不会将生成树重新引入第 3 层环境。请参见以下示例，其中 3750 接入交换机（无 GRE 或子接口支持）连接到支持 GRE 或子接口的 6500 分布层交换机。

3750 相关配置：

在此配置中，请注意，在快速以太网 1/0/1 上，本地 VLAN 的默认设置是 VLAN 1。此配置未进行更改。但是，您也注意到，VLAN 1 不被允许在链路上进行中继。允许的 VLAN 仅限于已标记的 VLAN。由于在此第 3 层拓扑中不需要进行中继协商，也没有在交换机之间流动的 VTP 数据流，因此未封装的数据流也不需要经过此链路。此配置可改善体系结构的安全状况，因为它不会造成无益的第 2 层安全漏洞。

```
!
ip vrf DIRTY
description DIRTY_VRF_FOR_NAC
rd 10:1
!
ip vrf GUESTS
description GUESTS_VRF_FOR_VISITORS
rd 30:1
```

```
!
!
interface FastEthernet1/0/1
description CONNECTION_TO_DISTRIBUTION_6504
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 10,20,30
switchport mode trunk
speed 100
duplex full
!
!
interface Vlan10
description DIRTY_VRF_TRANSIT
ip vrf forwarding DIRTY
ip address 192.168.10.2 255.255.255.252
!
interface Vlan20
description CLEAN_TRANSIT
ip address 192.168.20.2 255.255.255.252
!
interface Vlan30
description GUESTS_VRF_TRANSIT
ip vrf forwarding GUESTS
ip address 192.168.30.2 255.255.255.252
!
```

6500 相关配置：

请注意，在此配置中使用了 dot1q 封装并且标记了 VLAN 10、20 和 30 的帧。在选择要使用的 VLAN 标记时，您不能使用在交换机上的 VLAN 数据库中已经本地定义的 VLAN 编号。

```
!
ip vrf DIRTY
description DIRTY_VRF_FOR_NAC
rd 10:1
!
ip vrf GUESTS
description GUESTS_VRF_FOR_VISITORS
rd 30:1
!
interface FastEthernet3/1
description CONNECTION_TO_3750_ACCESS
no ip address
speed 100
duplex full
!
!
interface FastEthernet3/1.10
description DIRTY_VRF_TRANSIT
encapsulation dot1Q 10
ip vrf forwarding DIRTY
ip address 192.168.10.1 255.255.255.252
!
interface FastEthernet3/1.20
description CLEAN_TRANSIT
encapsulation dot1Q 20
ip address 192.168.20.1 255.255.255.252
!
interface FastEthernet3/1.30
description GUESTS_VRF_TRANSIT
encapsulation dot1Q 30
ip vrf forwarding GUESTS
```

```
ip address 192.168.30.1 255.255.255.252
!
```

第 3 层子接口

当您只需要在网络中的一个第 3 层跳上扩展 VRF 时，第 3 层子接口是理想的选择。可以选择 GRE 或子接口，具体可根据与每个配置符合的程度。以下是第 3 层子接口的示例配置：

```
!
interface FastEthernet3/1
description CONNECTION_TO_3750_ACCESS
no ip address
speed 100
duplex full
!
!
interface FastEthernet3/1.10
description DIRTY_VRF_TRANSIT
encapsulation dot1Q 10
ip vrf forwarding DIRTY
ip address 192.168.10.1 255.255.255.252
!
```

GRE 隧道

GRE 隧道是当需要访问 VRF 的客户端之间存在多个第 3 层跳时用来扩展 VRF-Lite VRF 的首选方法。这种类型的设计更常用于远程客户端希望访问位于中心的 NAC 服务器的远程分支机构 NAC。例如，在一个典型的核心层、分布层、接入层网络模型中，客户端不直接连接到分布层或核心层。因此，不需要在分布层和核心层设备上增加 VRF 定义的复杂性。可以使用 GRE 来仅仅传输需要隔离到网络中与 NAC 服务器连接的点的数据流。以下是 GRE 隧道接口的示例。

```
!
interface Tunnel0
ip vrf forwarding GUESTS
ip address 192.168.38.2 255.255.255.252
tunnel source Loopback0
tunnel destination 192.168.254.1
!
```

为 VRF 配置路由

如本文档前面部分所讨论，VRF-Lite 支持 BGP、OSPF 和 EIGRP。在此配置示例中，选择了 EIGRP，因为它是 Cisco 通常建议在需要快速收敛的园区网络中实施的路由协议。

应注意，OSPF 与 VRF-Lite 一起使用和 BGP 与 VRF-Lite 一起使用效果一样好。

还应注意，如果设计要求应在 VRF 之间泄漏数据流，则需要 BGP。

以下是使用 EIGRP 的 VRF 的路由配置示例。

```
!
!--- As with any configuration this is base routing
protocol !--- configuration which handles the routing
for the Global Routing Table. router eigrp 1 network
192.168.20.0 0.0.0.3 network 192.168.21.0 network
192.168.22.0 network 192.168.28.0 0.0.0.3 network
```

```
192.168.29.0 0.0.0.3 network 192.168.254.1 0.0.0.0 no
auto-summary ! !--- An Address Family must be defined
for each VRF !--- that is to be routing through the
routing protocol. !--- Routing Protocol options such as
auto-summarization, !--- autonomous system number,
router id, and so forth are all !--- configured under
the address family. Note that EIGRP does not !---
neighbor without the autonomous system specified under
!--- the address family. Also note, that this autonomous
system !--- number should be unique for each VRF and
should not be !--- the same as the Global AS number. !
address-family ipv4 vrf GUESTS network 192.168.30.0
0.0.0.3 network 192.168.38.0 0.0.0.3 no auto-summary
autonomous-system 30 exit-address-family ! address-
family ipv4 vrf DIRTY network 192.168.10.0 0.0.0.3
network 192.168.11.0 no auto-summary autonomous-system
10 exit-address-family !
```

在全局路由表和脏 VRF 之间路由数据流

它取决于 NAC 的部署要求：是否有必要将数据流从不受信任的网络端或脏网络端传输到受信任的网络端或干净网络端。例如，修正服务可能存在于 NAC 设备的受信任端。在 Active Directory 单一登录部署中，必须将一部分数据流传送到 Active Directory 以允许交互登录、Kerberos 票证交换等。无论如何，如果有任何数据需要在全局路由表和脏 VRF 之间传送，全局路由表都必须知道如何到达脏 VRF，并且脏 VRF 必须知道如何到达全局路由表。这通常由此方法处理。

脏 VRF 默认为 NAC 设备的不受信任接口或脏接口。全局路由表中仅 具有到被认为是脏 VLAN 的子网的静态路由。

考虑下图。

NAC 设备的不受信任端或脏端上的第 1 个第 3 层跳将一个指向 NAC 设备的默认路由重分配到路由进程中。NAC 设备的受信任端或干净端上的第 1 个第 3 层跳将为属于 VLAN 100 的子网重分配一个默认路由，本例中为 192.168.100.0/24。

注意： NAC 设备相反端上的第一个第 3 层跳可能位于同一个物理设备上但位于不同的 VRF 中。在下一个示例中，NAC 服务器的不受信任端或脏端位于 VRF 中，而 NAC 设备的受信任端或干净端保留在全局路由表中。

此配置如下所示：

```
!
router eigrp 1
 redistribute static
 network 192.168.20.0 0.0.0.3
 network 192.168.21.0
 network 192.168.22.0
 network 192.168.28.0 0.0.0.3
 network 192.168.29.0 0.0.0.3
 network 192.168.254.1 0.0.0.0
 no auto-summary
 !
 address-family ipv4 vrf GUESTS
  network 192.168.30.0 0.0.0.3
  network 192.168.38.0 0.0.0.3
  no auto-summary
  autonomous-system 30
 exit-address-family
```

```
 !
 address-family ipv4 vrf DIRTY
  redistribute static
  network 192.168.10.0 0.0.0.3
  network 192.168.11.0
  no default-information out
  no auto-summary
  autonomous-system 10
 exit-address-family
!
ip classless
ip route 192.168.100.0 255.255.255.0 192.168.21.10
ip route vrf DIRTY 0.0.0.0 0.0.0.0 192.168.11.2
!
!!
```

第 3 层 OOB 的 NAC 配置

CAS 设置

切记“简介”部分中的第一条原理：一个成功 NAC 设计的诀窍是始终记得分类为“脏”的数据流*必须* 流入 NAC 服务器 (CAS) 的不受信任端。

在第一个屏幕截图中，请注意 NAC 服务器网络设置。您将注意到，服务器是作为带外实际 IP 网关部署的。请注意，NAC 服务器的默认路由指向受信任端。

需要为服务器的不受信任端上存在的每个脏 VLAN 配置静态路由。请参见第二个屏幕截图。

验证

查找正在登录到网络的用户 NAC-Employee 的已记录过程。Cisco 已从接入交换机、工作站捕获活动，并显示分布层交换机的路由表中的信息。

使用本部分可确认配置能否正常运行。

命令输出解释程序（仅限注册用户）(OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输出的分析。

第 1 阶段 - 您尚未连接到网络，并且接入交换机上的交换机端口已关闭。

```
! – Catalyst 3750 Access Switch
!--- Note: Client mahcine is off the network at this
point. ! 3750-Access#show int status | i Fa1/0/13
Fa1/0/13 CLIENT_CONNECTION notconnect 100 auto auto
10/100BaseTX ! ! 3750-Access#!Notice it is in the
"notconnect" state. !
```

第 2 阶段 - Windows 客户端插入到网络，并且交换机上的初始 VLAN 是 VLAN 100（脏 VLAN）。如您在此屏幕截图中所看到的一样，已为主机分配了一个 IP 地址。

```
! – Catalyst 3750 Access Switch
!--- Note: Client just connected to the network. 2w5d:
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan100,
changed state to up 2w5d: %LINK-3-UPDOWN: Interface
FastEthernet1/0/13, changed state to up 2w5d:
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet1/0/13, changed state to up ! ! 3750-
Access#show int status | i Fa1/0/13 Fa1/0/13
CLIENT_CONNECTION connected 100 a-full a-100
10/100BaseTX !
```

第 3 阶段 - 在几秒钟内，NAC 代理将开始其登录进程。在本示例中，已配置 Active Directory 单一登录，因此不会提示您输入用户名和口令。相反，您会看到一个说明已发生单一登录的弹出式窗口。

完成身份验证和状态评估后，将显示一条成功消息，交换机端口已从脏 VLAN 移到员工 VLAN，并且 NAC 代理会刷新 PC 的 IP 地址。

```
! – Catalyst 3750 Access Switch
2w5d: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Vlan100, changed state to down
2w5d: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Vlan200, changed state to up
!
!--- Note: As you can tell from the previous messages,
!--- the switchport was just moved from VLAN 100 to VLAN
200. ! 3750-Access#show int status | i Fa1/0/13 Fa1/0/13
CLIENT_CONNECTION connected 200 a-full a-100
10/100BaseTX ! !
```

此屏幕截图显示最终 IP 地址，该地址位于员工 VLAN (VLAN 200) 中。

此屏幕截图显示 NAC-Employee 用户的设备，如“认证设备”列表中所列。Role 已指定为 *EMPLOYEES*，VLAN 是 200。

此屏幕截图显示 NAC 管理器上的联机用户列表。

这是 NAC 管理器事件日志，其中显示了带外用户的成功登录。

在此部分中，将检查全局路由表和脏 VRF 的路由表。在第一个屏幕截图中，请注意 **show ip route** 命令。这表明显示的是全局路由的路由表。

```
6504-DISTRIBUTION#show ip route Codes: C - connected, S
- static, R - RIP, M - mobile, B - BGP D - EIGRP, EX -
EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF
NSSA external type 1, N2 - OSPF NSSA external type 2 E1
- OSPF external type 1, E2 - OSPF external type 2 i -
IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-
IS level-2 ia - IS-IS inter area, * - candidate default,
U - per-user static route o - ODR, P - periodic
downloaded static route Gateway of last resort is
192.168.28.2 to network 0.0.0.0 192.168.29.0/30 is
subnetted, 1 subnets D 192.168.29.0 [90/30720] via
192.168.28.2, 2w5d, FastEthernet3/48 192.168.28.0/30 is
subnetted, 1 subnets C 192.168.28.0 is directly
connected, FastEthernet3/48 D EX 192.168.31.0/24
[170/30976] via 192.168.28.2, 2w5d, FastEthernet3/48 D
EX 192.168.30.0/24 [170/30976] via 192.168.28.2, 2w5d,
FastEthernet3/48 D 192.168.200.0/24 [90/28416] via
192.168.20.2, 6d19h, FastEthernet3/1.20 D EX
192.168.38.0/24 [170/30976] via 192.168.28.2, 2w5d,
FastEthernet3/48 C 192.168.21.0/24 is directly
connected, Vlan21 D EX 192.168.39.0/24 [170/30976] via
192.168.28.2, 2w5d, FastEthernet3/48 192.168.20.0/30 is
```

```
subnetted, 1 subnets C 192.168.20.0 is directly
connected, FastEthernet3/1.20 D EX 192.168.36.0/24
[170/30976] via 192.168.28.2, 2w5d, FastEthernet3/48 C
192.168.22.0/24 is directly connected, Vlan22 D EX
192.168.37.0/24 [170/30976] via 192.168.28.2, 2w5d,
FastEthernet3/48 D EX 192.168.34.0/24 [170/30976] via
192.168.28.2, 2w5d, FastEthernet3/48 192.168.254.0/32 is
subnetted, 3 subnets D 192.168.254.2 [90/156160] via
192.168.20.2, 2w5d, FastEthernet3/1.20 D 192.168.254.3
[90/156160] via 192.168.28.2, 2w5d, FastEthernet3/48 C
192.168.254.1 is directly connected, Loopback0 D EX
192.168.35.0/24 [170/30976] via 192.168.28.2, 2w5d,
FastEthernet3/48 D EX 192.168.32.0/24 [170/30976] via
192.168.28.2, 2w5d, FastEthernet3/48 S 192.168.100.0/24
[1/0] via 192.168.21.10 D EX 192.168.33.0/24 [170/30976]
via 192.168.28.2, 2w5d, FastEthernet3/48 D*EX 0.0.0.0/0
[170/30976] via 192.168.28.2, 2w5d, FastEthernet3/48
```

注意： 192.168.100.0/24 网络（脏网络）在路由表中作为静态路由，其下一跳为 NAC 服务器的受信任接口。

请注意 **show ip route vrf DIRTY** 命令。这表明显示的只是脏虚拟网络的路由表。

```
6504-DISTRIBUTION#show ip route vrf DIRTY Routing Table:
DIRTY Codes: C - connected, S - static, R - RIP, M -
mobile, B - BGP D - EIGRP, EX - EIGRP external, O -
OSPF, IA - OSPF inter area N1 - OSPF NSSA external type
1, N2 - OSPF NSSA external type 2 E1 - OSPF external
type 1, E2 - OSPF external type 2 i - IS-IS, su - IS-IS
summary, L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-
IS inter area, * - candidate default, U - per-user
static route o - ODR, P - periodic downloaded static
route Gateway of last resort is 192.168.11.2 to network
0.0.0.0 192.168.10.0/30 is subnetted, 1 subnets C
192.168.10.0 is directly connected, FastEthernet3/1.10 C
192.168.11.0/24 is directly connected, Vlan11 D
192.168.100.0/24 [90/28416] via 192.168.10.2, 01:03:19,
FastEthernet3/1.10 S* 0.0.0.0/0 [1/0] via 192.168.11.2
```

注意： 请注意，只有在脏 VRF 路由表中，才能从 3750 接入交换机通过 EIGRP 在分布层中获知脏接入 VLAN (192.168.100.0/24)。此路由在全局表中不存在。

附录 A：交换机配置

接入交换机运行配置

```
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 3750-Access
!
!
no aaa new-model
clock timezone EST -5
clock summer-time EST recurring
switch 1 provision ws-c3750-24ts
ip subnet-zero
ip routing
```

```
!
ip vrf DIRTY
 description DIRTY_VRF_FOR_NAC
 rd 10:1
!
ip vrf GUESTS
 description GUESTS_VRF_FOR_VISITORS
 rd 30:1
!
!
!
crypto pki trustpoint TP-self-signed-819048320
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-819048320
 revocation-check none
 rsakeypair TP-self-signed-819048320
!
!
crypto ca certificate chain TP-self-signed-819048320
 certificate self-signed 01
!
!
no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
!
interface Loopback0
 ip address 192.168.254.2 255.255.255.255
!

!
interface FastEthernet1/0/1
 description CONNECTION_TO_DISTRIBUTION_6504
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 10,20,30
 switchport mode trunk
 speed 100
 duplex full
!
interface range FastEthernet1/0/2 - 24
 description CLIENT_CONNECTION
 switchport access vlan 100
 switchport mode access
 spanning-tree portfast
 spanning-tree bpduguard enable
!
!- SNIP -
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan10
 description DIRTY_VRF_TRANSMIT
 ip vrf forwarding DIRTY
 ip address 192.168.10.2 255.255.255.252
!
interface Vlan20
 description CLEAN_TRANSIT
 ip address 192.168.20.2 255.255.255.252
!
```

```
interface Vlan30
 description GUESTS_TRANSIT
 ip vrf forwarding GUESTS
 ip address 192.168.30.2 255.255.255.252
!
interface Vlan100
 description DIRTY_VLAN
 ip vrf forwarding DIRTY
 ip address 192.168.100.1 255.255.255.0
 ip helper-address 192.168.22.11
!
interface Vlan200
 description EMPLOYEES_VLAN
 ip address 192.168.200.1 255.255.255.0
 ip helper-address 192.168.22.11
!
interface Vlan210
 description CONTRACTORS_VLAN
 ip address 192.168.210.1 255.255.255.0
 ip helper-address 192.168.22.11
!

!
interface Vlan300
 description GUESTS
 ip vrf forwarding GUESTS
 ip address 192.168.31.1 255.255.255.0
!
router eigrp 1
 network 192.168.20.0 0.0.0.3
 network 192.168.200.0
 network 192.168.254.2 0.0.0.0
 no auto-summary
 !
 address-family ipv4 vrf GUESTS
 network 192.168.30.0 0.0.0.3
 network 192.168.31.0
 no auto-summary
 autonomous-system 30
 exit-address-family
 !
 address-family ipv4 vrf DIRTY
 network 192.168.10.0 0.0.0.3
 network 192.168.100.0
 no auto-summary
 autonomous-system 10
 exit-address-family
!
router bgp 1
 no synchronization
 bgp log-neighbor-changes
 neighbor 192.168.254.3 remote-as 1
 neighbor 192.168.254.3 update-source Loopback0
 no auto-summary
!
ip classless
ip route 192.0.2.1 255.255.255.255 Null0
ip http server
ip http secure-server
!
!
snmp-server community NIC-NAC-PADDYWHACK RW
snmp-server user NIC-NAC-PADDYWHACK NIC-NAC-PADDYWHACK
v1
```

```
snmp-server user NIC-NAC-PADDYWHACK NIC-NAC-PADDYWHACK
v2c
snmp-server trap-source Loopback0
snmp-server host 192.168.22.5 version 2c NIC-NAC-
PADDYWHACK
!
!- SNIP
!
ntp clock-period 36028450
ntp source Loopback0
ntp server 192.168.254.1 version 2 prefer
end
```

分布层交换机运行配置

```
!– SNIP -
!
hostname 6504-DISTRIBUTION
!
boot-start-marker
boot system disk0:s72033-advipservicesk9_wan-mz.122-
33.SXH2a.bin
boot-end-marker
!
!
no aaa new-model
clock timezone EST -5
clock summer-time EST recurring
!
!- SNIP -
!
ip vrf DIRTY
 description DIRTY_VRF_FOR_NAC
 rd 10:1
!
ip vrf GUESTS
 description GUESTS_VRF_FOR_VISITORS
 rd 30:1
!
ipv6 mfib hardware-switching replication-mode ingress
vtp domain cmpd
vtp mode transparent
no mls acl tcam share-global
mls netflow interface
no mls flow ip
no mls flow ipv6
mls cef error action freeze
!
!
redundancy
 keepalive-enable
 mode sso
 main-cpu
  auto-sync running-config
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
diagnostic cns publish cisco.cns.device.diag_results
diagnostic cns subscribe cisco.cns.device.diag_commands
!
vlan internal allocation policy ascending
vlan access-log ratelimit 2000
```

```
!
!
!

!
vlan 11
 name CAS_DIRTY
!
vlan 21
 name CAS_CLEAN
!
vlan 22
 name SERVER_VLAN
!
interface Tunnel0
 ip vrf forwarding GUESTS
 ip address 192.168.38.1 255.255.255.252
 tunnel source Loopback0
 tunnel destination 192.168.254.3
!
interface Loopback0
 ip address 192.168.254.1 255.255.255.255
!
!- SNIP -
!
interface FastEthernet3/1
 description CONNECTION_TO_3750_ACCESS
 no ip address
 speed 100
 duplex full
!
interface FastEthernet3/1.10
 description DIRTY_VRF_TRANSIT
 encapsulation dot1Q 10
 ip vrf forwarding DIRTY
 ip address 192.168.10.1 255.255.255.252
 ip verify unicast source reachable-via rx allow-default
!
interface FastEthernet3/1.20
 description CLEAN_TRANSIT
 encapsulation dot1Q 20
 ip address 192.168.20.1 255.255.255.252
!
interface FastEthernet3/1.30
 description GUESTS_TRANSIT
 encapsulation dot1Q 30
 ip vrf forwarding GUESTS
 ip address 192.168.30.1 255.255.255.252
!
!
!
!

!
interface FastEthernet3/2
 description CAS1_DIRTY
 switchport
 switchport access vlan 11
 switchport mode access
 speed 100
 duplex full
 spanning-tree portfast
 spanning-tree bpduguard enable
!
```

```
interface FastEthernet3/3
 description CAS2_DIRTY
 switchport
 switchport access vlan 11
 switchport mode access
 speed 100
 duplex full
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet3/4
 description CAS1_CLEAN
 switchport
 switchport access vlan 21
 switchport mode access
 speed 100
 duplex full
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet3/5
 description CAS2_CLEAN
 switchport
 switchport access vlan 21
 switchport mode access
 speed 100
 duplex full
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet3/6
 description CAM
 switchport
 switchport access vlan 22
 switchport mode access
 speed 100
 duplex full
 spanning-tree portfast
 spanning-tree bpduguard enable
!
!
!- SNIP -
!
!

!
interface FastEthernet3/48
 description CONNECTION_TO_THE_WORLD
 ip address 192.168.28.1 255.255.255.252
 speed 100
 duplex full
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan11
 description NAC_DIRTY
 ip vrf forwarding DIRTY
 ip address 192.168.11.1 255.255.255.0
!
interface Vlan21
 description NAC_CLEAN
 ip address 192.168.21.1 255.255.255.0
```

```
!
interface Vlan22
 description SERVER_VLAN
 ip address 192.168.22.1 255.255.255.0
!
router eigrp 1
 redistribute static
 network 192.168.20.0 0.0.0.3
 network 192.168.21.0
 network 192.168.22.0
 network 192.168.28.0 0.0.0.3
 network 192.168.29.0 0.0.0.3
 network 192.168.254.1 0.0.0.0
 no auto-summary
 !
 address-family ipv4 vrf GUESTS
  network 192.168.30.0 0.0.0.3
  network 192.168.38.0 0.0.0.3
  no auto-summary
  autonomous-system 30
 exit-address-family
 !
 address-family ipv4 vrf DIRTY
  redistribute static
  network 192.168.10.0 0.0.0.3
  network 192.168.11.0
  no default-information out
  no auto-summary
  autonomous-system 10
 exit-address-family
!
!
!
!
!

!
router bgp 1
 no synchronization
 bgp log-neighbor-changes
 neighbor 192.168.254.3 remote-as 1
 neighbor 192.168.254.3 update-source Loopback0
 no auto-summary
!
ip classless
ip route 192.0.2.1 255.255.255.255 Null0
ip route 192.168.100.0 255.255.255.0 192.168.21.10
ip route vrf DIRTY 0.0.0.0 0.0.0.0 192.168.11.2
!
!
!- SNIP -
!
ntp source Loopback0
ntp master 2
!
end
```

故障排除

目前没有针对此配置的故障排除信息。

相关信息

- 技术支持和文档 - Cisco Systems