思科美洲台与ACL的第3层OOB

目录

简介

思科网络准入控制(美洲台)强制执行在寻找网络访问的所有设备的组织的网络安全策略。思科美洲台只允许兼容并且委托端点设备，例如PCs、服务器和PDA，在网络上。访问为固执的设备限制，限制从新兴安全威胁和风险的可能损害。思科美洲台给组织一个强大，基于任务的方法对防止未经授权的访问并且改进网络弹性。

思科美洲台解决方案提供以下商业效益：

- **安全策略标准**：保证终端依照安全策略;保护基础设施和员工生产力;巩固被管理的和不受管理资产;支持内部环境和访客访问;为策略专门制作您的风险级别。
- **保护现有投资**：是与第三方管理应用程序兼容;灵活部署选项最小化对基础设施升级的需要。
- **缓和从病毒、蠕虫病毒和未经授权的访问的风险**：控制和减少大规模基础设施中断;由动态和自动化的进行的移动，添加和更改减少运营费用，启用更高的IT效率;集成其他思科自防御网络组件提供全面的安全保护。

解决方案概述

此部分简要地引入第3层带外(OOB)使用访问控制表(ACL)方法实现思科网络准入控制(美洲台)体系结构。

解决方案描述

思科美洲台用于网络基础设施强制执行在寻找对网络资源的访问的所有设备的安全策略标准。在他们授权网络访问前，思科美洲台允许网络管理员验证和授权用户和评估和修正他们相关的机器。有您能使用完成此任务的几个配置方法，但是第3层带外(OOB)迅速地变为其中一美洲台的最普遍的部署方法学。此转移在大众化中根据几Dynamics，包括硬件资源的更加好的利用率。

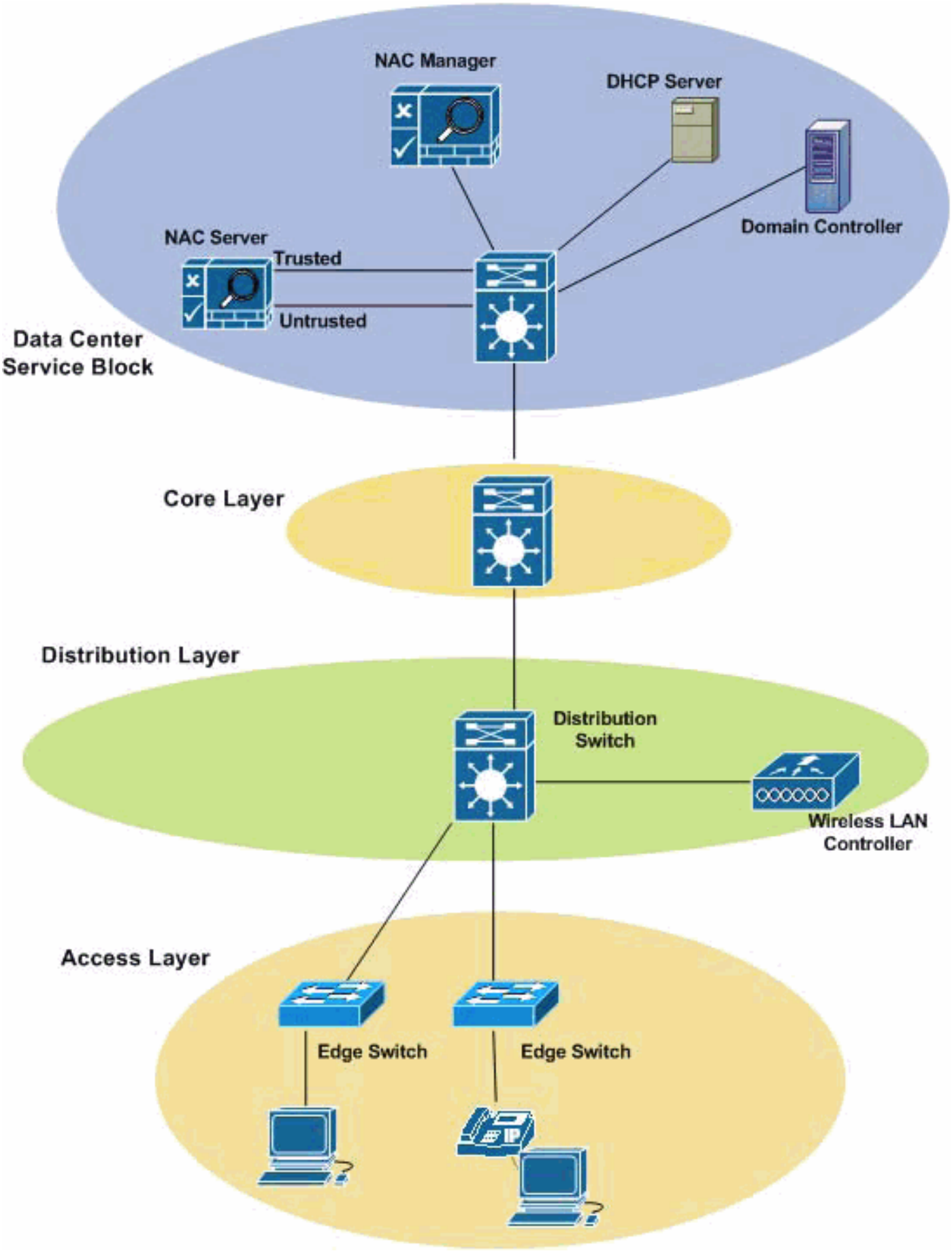
通过部署在第3层OOB方法的思科美洲台，单个Cisco NAC设备(思科美洲台管理器或思科美洲台服务器)能扩展适应更多用户。它也允许美洲台在中央查找的伊莱克斯而不是被分配在校园或组织间。因此，第3层OOB部署从大写和操作费用支架是有效两个。

此指南描述思科美洲台的一个基于ACL的实施在第3层OOB部署的。

解决方案体系结构

解决方案体系结构(请参阅图1)识别关键解决方案组件和集成点。

图 1：在典型的园区环境的Cisco NAC设备放置



以下部分描述组成典型的校园体系结构的接入层、分布层、核心层和数据中心业务集成点。

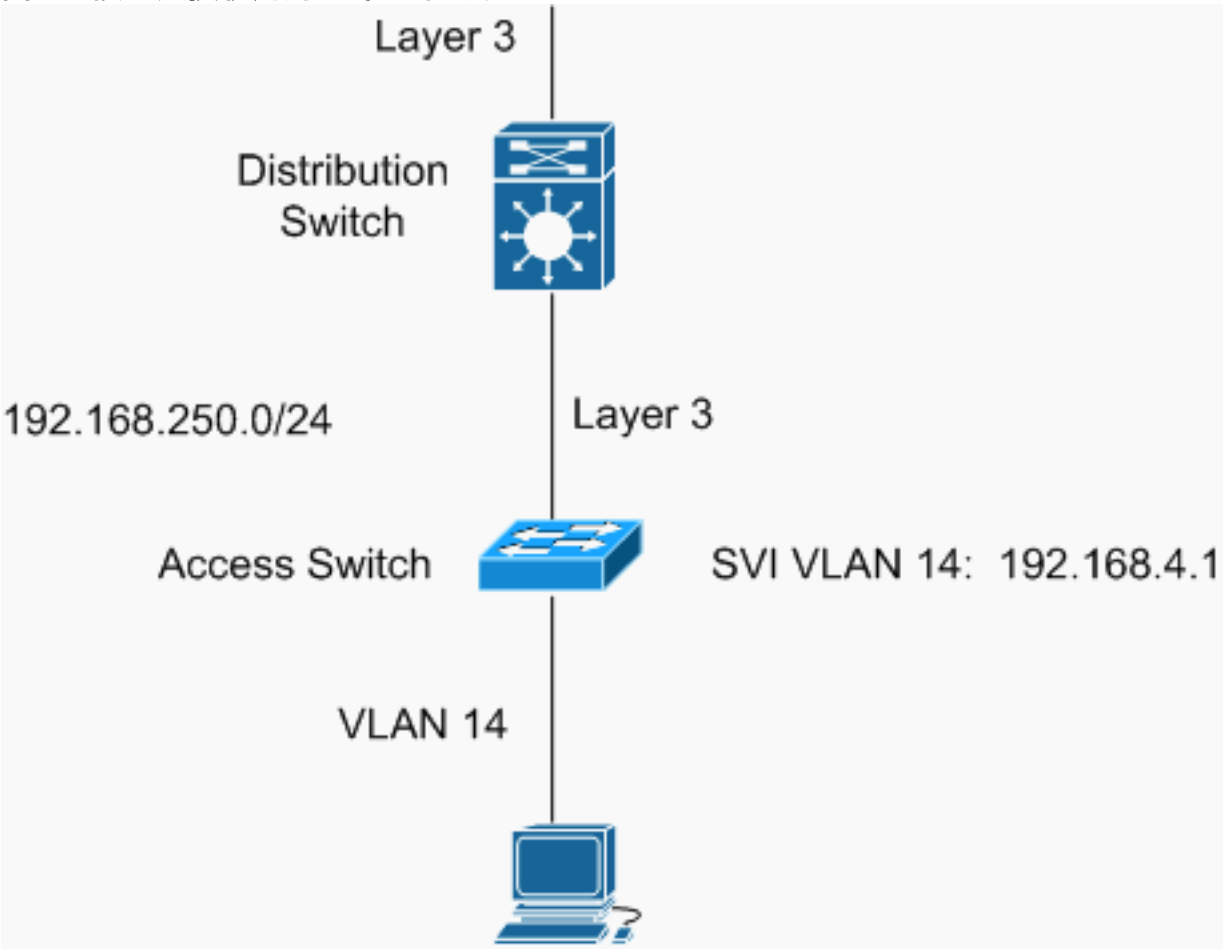
接入层

思科第3层OOB美洲台解决方案是可适用的对一个已路由访问园区网设计。在已路由接入模式，第3层交换虚拟接口(SVIs)在接入交换机配置和那里是在访问和分布式交换机之间的一第3层链路。

注意： 用语“接入交换机”和“边界交换机”在本文可互换使用。

如在图2中看到，第3层访问VLAN (例如， VLAN14)在边界交换机配置，第3层路由从交换机支持到上行分布式交换机或路由器，并且思科美洲台管理器管理接入交换机的端口。

图 2：接入交换机用对边缘的第3层



分布层

分布层对第3层路由负责。不同于Layer2解决方案，思科美洲台服务器不需要查找在分布层。反而，它在中央被放置在数据中心服务块。

核心层

核心层使用基于Cisco IOS的路由器。核心层为高速的路由保留，不用任何服务。服务在服务交换机可以安置在数据中心。

数据中心服务层

数据中心服务分层堆积用途基于Cisco IOS的路由器和交换机。思科美洲台管理器和思科美洲台服务器在中央查找在数据中心服务块。

解决方案组成部分

此部分描述Cisco NAC设备解决方案的组件。

思科美洲台管理器

思科美洲台管理器是集中所有思科美洲台服务器、用户和策略配置和监视在Cisco NAC设备部署的管理服务器和数据库。对于OOB美洲台部署，管理器提供OOB管理添加和控制开关在管理器的域和配置交换机端口。

思科美洲台服务器

思科美洲台服务器是在不信任(管理的)网络和委托(内部)网络之间的实施点。服务器强制执行修正定义在思科美洲台管理器，并且终端与服务器联络在验证时。在此设计，没有放置服务器逻辑上或物理的“线型”分离不信任和可靠网络。此概念是较详细地寻址的以后在“带外(OOB)模式”部分。

思科美洲台代理程序

思科美洲台代理程序是思科美洲台解决方案的一个可选组件。当代理程序为您的思科美洲台部署时启用，代理程序保证访问您的网络满足系统状态需求您的计算机指定。思科美洲台代理程序只读，易用，在用户机器驻留的斯莫尔覆盖区程序。当用户尝试访问网络时，代理程序检查客户端系统您需要的软件，并且帮助用户获取所有缺少更新或软件。

带外(OOB)模式

在Cisco NAC设备OOB部署，思科美洲台服务器与终端主机仅联络在认证过程中，摆评估和修正姿势。在被确认后，终端主机不用服务器通信。在OOB模式，思科美洲台管理器使用简单网络管理协议(SNMP)对控制开关和set vlan分配端口。当Cisco NAC管理器和服务器为OOB时设置，管理器能控制支持的交换机交换机端口。对于支持的交换机列表，请去对：

http://www.cisco.com/en/US/docs/security/nac/appliance/support_guide/switch_spt.html#wp40017
。

下几个图表显示思科美洲台管理器如何使用OOB控制用户如何获得对网络的访问。顺序如下：

1. PC物理的连接到在网络的一交换机(请参见图3)。
2. 交换机发送MAC地址使用SNMP对思科美洲台管理器(请参见图3)。
3. 思科美洲台管理器验证PC “是否被确认”。如果PC没有被确认，思科美洲台管理器提示交换机分配PC的交换机端口对验证VLAN (请参见图4)。继续步骤4至步骤6。如果PC被确认，请进入步骤5。
4. PC与思科美洲台服务器联络并且通过验证、状态评估和修正(请参见图4)。
5. 思科美洲台服务器通知思科美洲台管理器PC “被确认” (请参见图5)。
6. PC连接对网络作为可信的设备。

图 3：OOB SNMP通信(1 3)

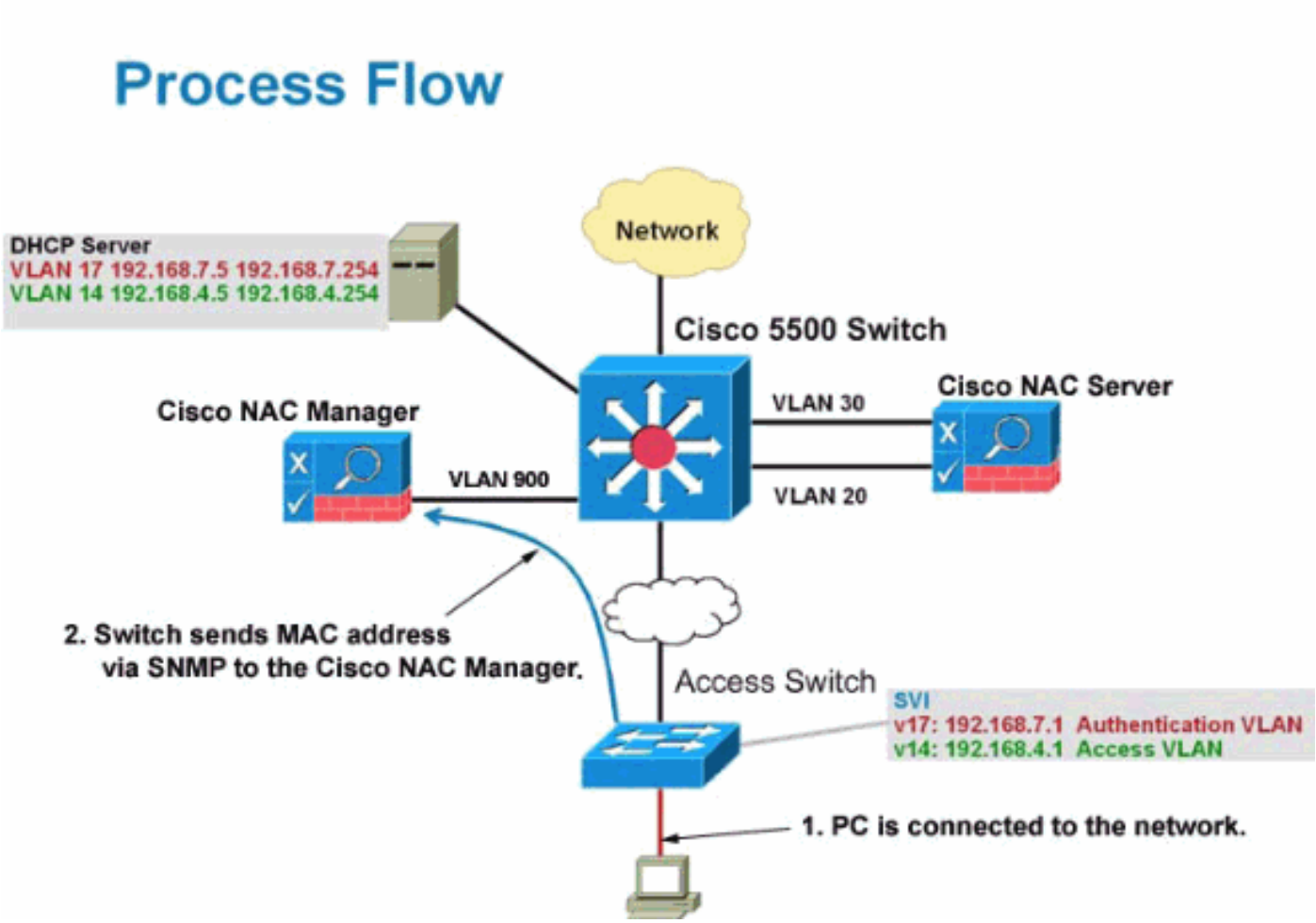


图 4：OOB SNMP通信(2 3)

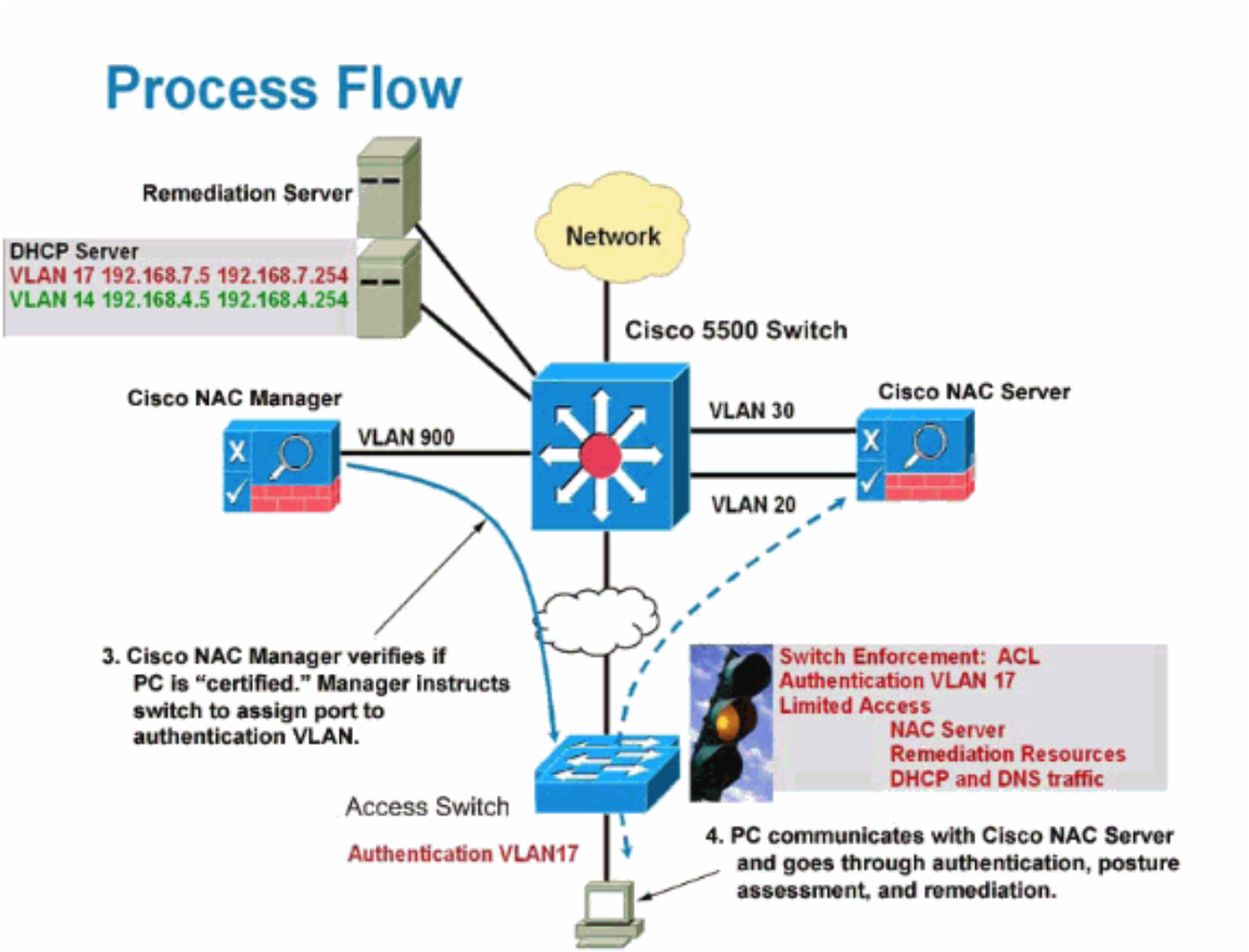
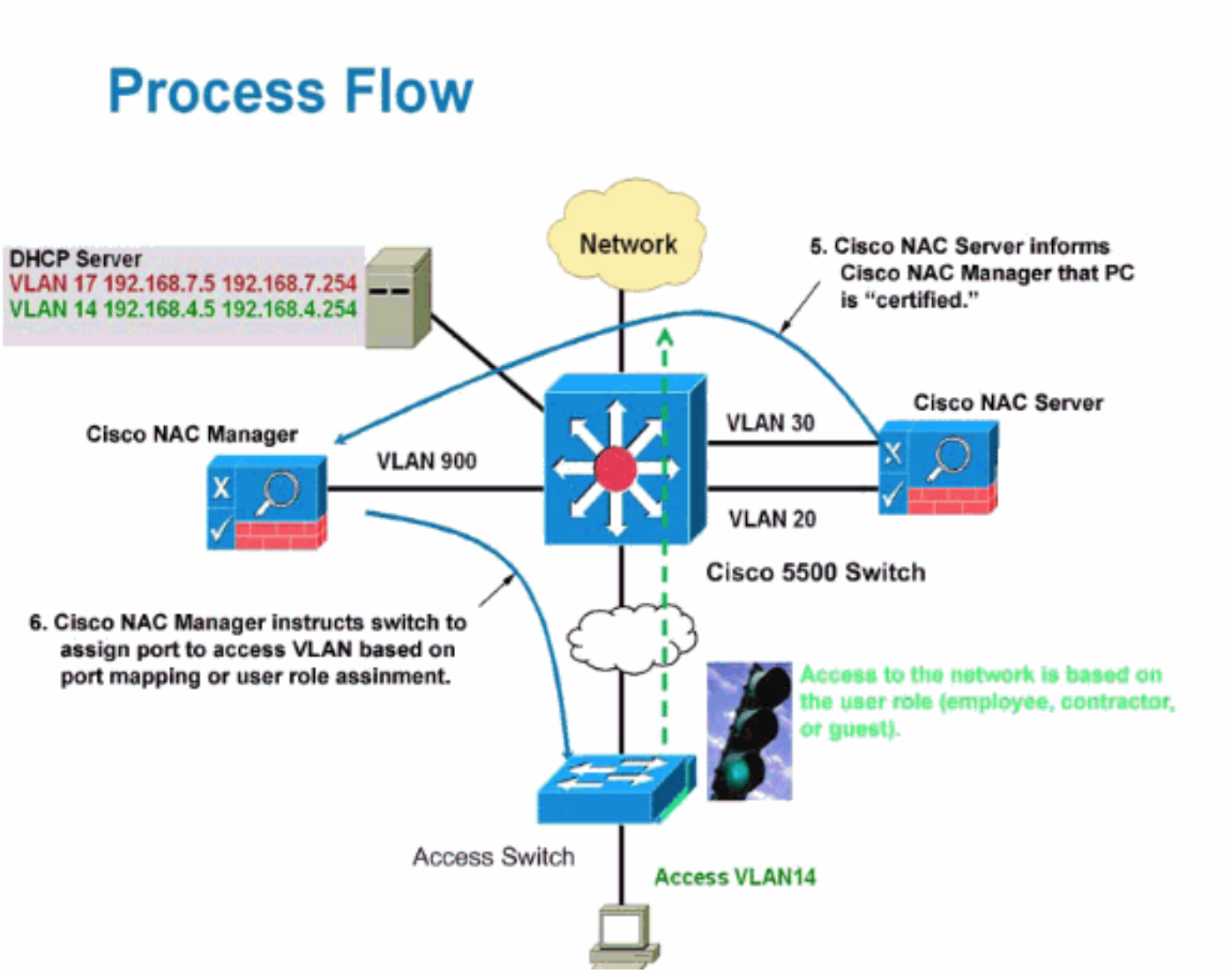


图 5：OOB SNMP通信(3 3)



设计注意事项

当您考虑一第3层OOB美洲台部署时，您应该查看几设计注意事项。在以下小节是列出的讨论的这些考虑事项，并且简要论述他们的重要包括。

终端分类

几个要素造成终端分类，包括设备类型和用户角色。设备类型和用户角色影响终端角色。

可能的设备类型

- 公司设备
- 非公司设备
- 非个人计算机设备

可能的用户角色

- 员工
- 承包商
- 访客

最初，所有终端分配到未经鉴定的VLAN。对其他角色的访问在标识以后允许，并且状态进程完成。

终端角色

必须最初确定终端的每种类型角色。一典型的校园部署包括几个角色，例如员工，访客和承包商和其他终端，例如打印机、无线接入点和IP摄像头。角色被映射到边界交换机VLAN。

注意： 未经鉴定的角色最初映射所有用户对首次验证的未经鉴定的VLAN。

角色隔离

当您实现思科美洲台解决方案时，隔离终端角色是重要的。选择一种适当的执行机制为起源所有的流量提供流量和路径隔离从未经鉴定和未授权的主机主机。在第3层OOB环境，第3层边界交换机(使用ACL)作为保证在之间的隔离“的实施点清洗”和“未经鉴定的”网络。

通信流

当终端连接到一美洲台托管型交换机，美洲台进程开始。作为“未经鉴定”分类的流量由在未经鉴定的VLAN应用的ACL限制。终端允许通信到思科美洲台服务器的“不信任”接口通过状态评估和修正进程继续(有是讨论以后在从Cisco.com的“更新策略在思科美洲台管理器执行状态评估和修正的几个方法”。部分)。在验证以后，终端移动向委托VLAN。

思科美洲台服务器模式

思科美洲台服务器在虚拟网关(网桥)模式或雷亚尔德蒙特罗伊IP网关(路由)模式可以部署。

虚拟网关(网桥)模式

典型地使用虚拟网关(网桥)模式，当思科美洲台服务器是Layer2在终端附近时。在此模式，服务器在网络流量的路由决策作为网桥和没有涉及。

注意： 虚拟网关(网桥)模式为第3层OOB ACL设计不是可适用的。

雷亚尔德蒙特罗伊IP网关(路由)模式

当思科美洲台服务器是远离终端时的多跳雷亚尔德蒙特罗伊IP网关(路由)模式是可适用的。当您使用服务器作为雷亚尔德蒙特罗伊IP网关时，请指定其两个接口的IP地址：委托侧的一个IP地址(提供从思科美洲台管理器的管理)和不信任侧的一个IP地址。双地址应该在不同的子网。不信任的接口IP地址使用通信与在不信任子网的终端。一第3层OOB部署使用ACL要求终端与认证和授权目的不信任的接口联络。由于雷亚尔德蒙特罗伊IP模式使用一个有效IP地址不信任的接口，在雷亚尔德蒙特罗伊IP网关模式必须配置思科美洲台服务器作用。

可扩展性

一个标准的思科美洲台服务器能管理5000并发最终用户。第3层OOB ACL设计适用与服务不大于5000个用户的站点。如果有多个站点，您能有另外的服务器每个站点。如果需要服务超过5000个用户的有一单站点，您能使用外部负载均衡技术(例如，应用程序控制引擎(ACE)负载平衡器)扩展超过单站点的5000个用户。

注意： ACE负载平衡器讨论是超出本文的范围之外。

发现号主机

发现号主机是思科美洲台代理程序用于的完全合格的域名(FQDN)或不信任的接口IP地址发现思科美洲台服务器查找的多跳离开在网络。代理程序通过发送UDP数据包开始发现过程对已知发现号主机地址。发现信息包必须到达美洲台服务器不信任的接口收到答复。一旦第3层OOB部署，服务器不在数据流路径在验证VLAN的。所以，必须配置发现号主机设置是思科美洲台服务器的不信任的接口的IP地址，以便代理程序能发送发现信息包直接地到服务器。

用户体验(用思科美洲台代理程序)

一般，公司网络管理员在发出那些机器前安装在客户端机器的思科美洲台代理程序给用户。发现号主机IP地址或可解决名称在思科美洲台代理程序触发将发送的发现信息包对美洲台服务器的不信任的接口，通过美洲台进程自动地指导客户端机器。

用户体验(没有思科美洲台代理程序)

没有思科美洲台代理程序(很可能访客、承包商和非公司资产)的终端可能不通过美洲台进程自动地继续。手工和被指导的方法存在协助没有代理程序的终端。欲知详情，请参阅“对思科美洲台服务器通信的终端”部分。

注意： 可能最好的终端用户经验，由最终用户的浏览器委托的使用证书。使用在思科美洲台服务器的自生的证书没有为生产环境推荐。

思科美洲台进程流

此部分说明美洲台OOB解决方案的基本流程流程。方案是描述的都有和没有在客户端机器安装的思科美洲台代理程序。此部分显示思科美洲台管理器如何控制交换机端口使用SNMP作为控制介质。这些流程实质上是宏分析，并且仅包含功能决策步骤。进程流不包括发生的每个选项也不跨步和不包括根据终端评估标准的审定决定。

参考在Figure7显示的进程流流程图关于在图显示的盘旋的步骤6.上。

图 6：第3层带外美洲台解决方案的美洲台进程流

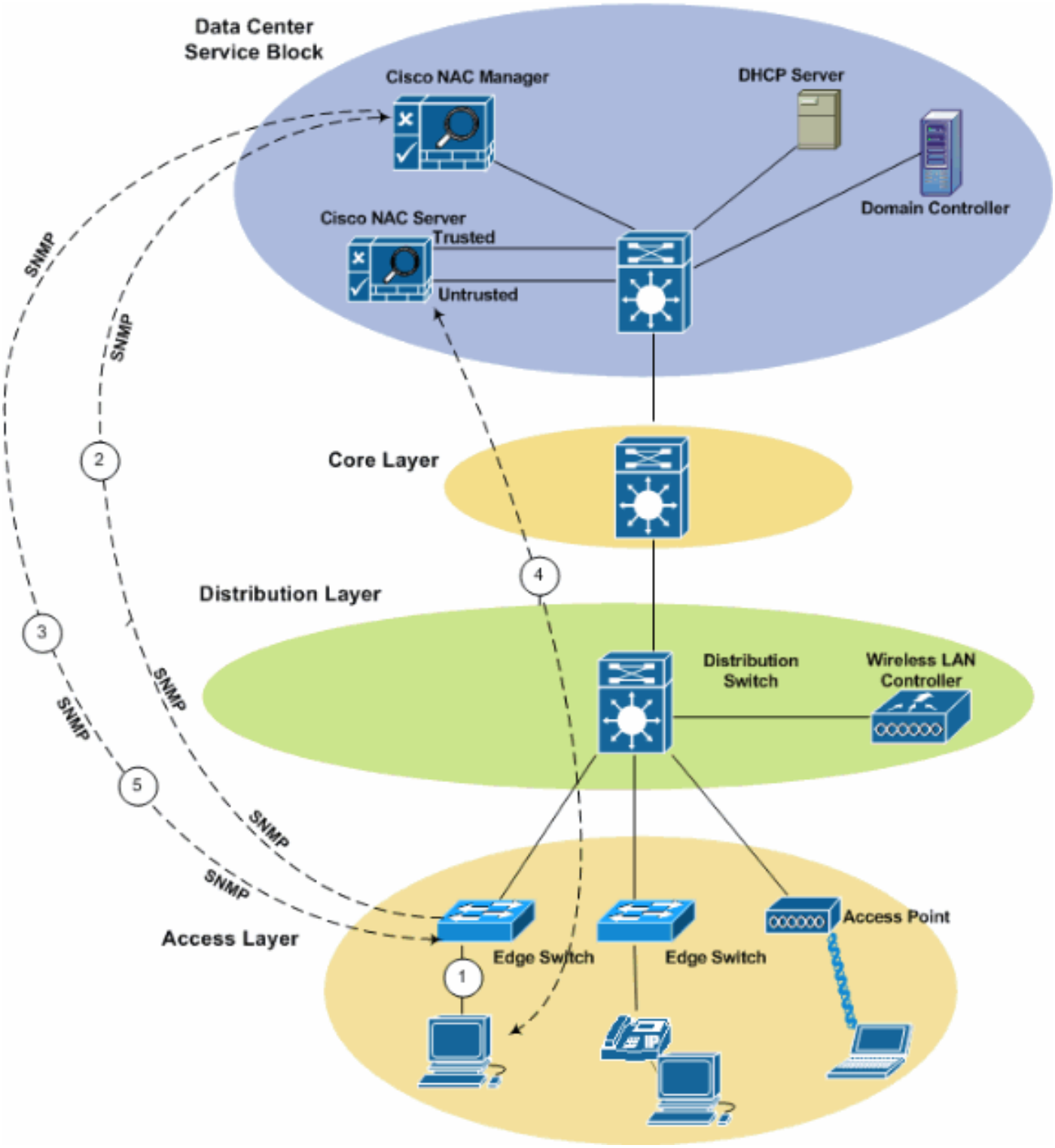

Data Center
Service Block
Cisco NAC Manager
DHCP Server
Domain Controller
Cisco NAC Server
Trusted
Untrusted
SNMP
SNMP
SNMP
SNMP
SNMP
SNMP
2
3
4
5
Core Layer
Distribution Layer
Distribution
Switch
Wireless LAN
Controller
Access Layer
Edge Switch
Edge Switch
Access Point
1
IP

图 7：进程流流程图