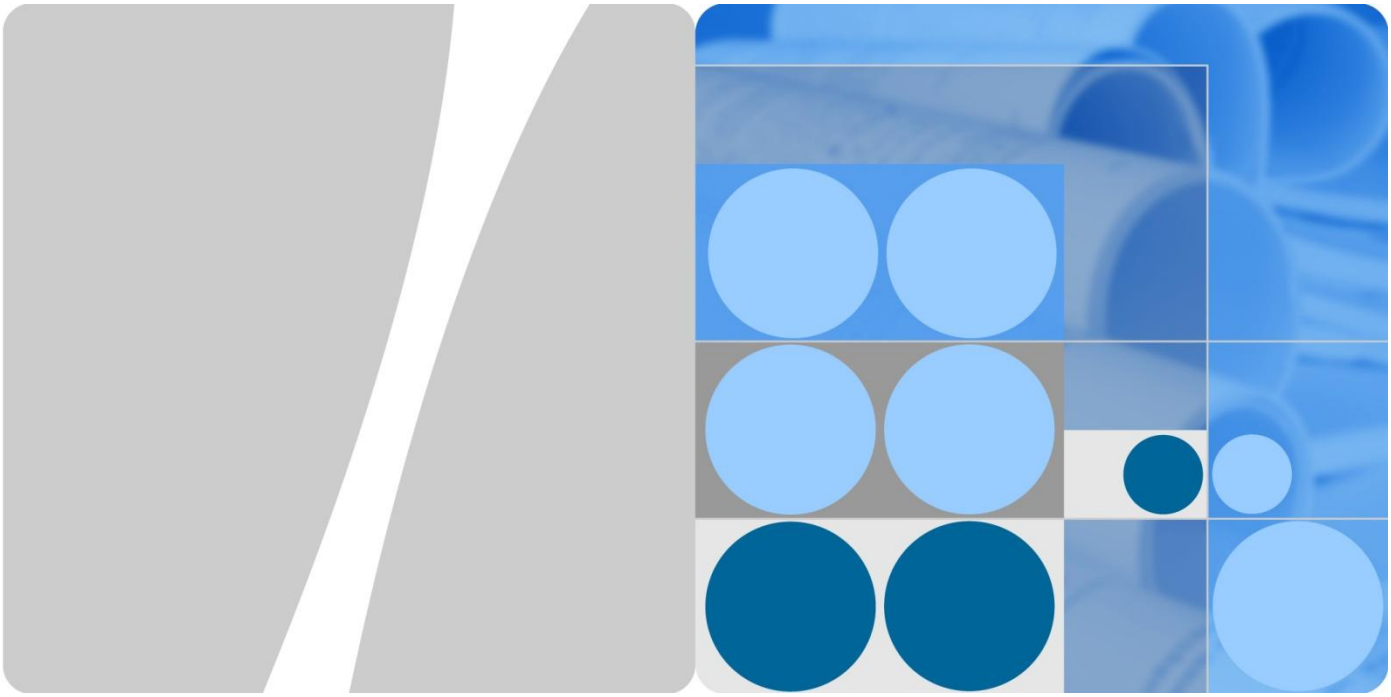


eSight
V300R001C10
终端资源特性技术白皮书

文档版本 01

发布日期 2013-12-10

华为技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： http://enterprise.huawei.com

前 言

概述

本文档通过对 eSight 终端资源的基本原理、典型场景处理流程等方面的描述，帮助用户了解终端资源的使用场景与使用方法。

读者对象

本文档（本指南）主要适用于以下工程师：

- 技术支持工程师
- 维护工程师

符号约定

在本文中可能出现下列标志，它们所代表的含义如下。

符号	说明
 危险	用于警示紧急的危险情形，若不避免，将会导致人员死亡或严重的人身伤害。
 警告	用于警示潜在的危险情形，若不避免，可能会导致人员死亡或严重的人身伤害。
 小心	用于警示潜在的危险情形，若不避免，可能会导致中度或轻微的人身伤害。
 注意	用于传递设备或环境安全警示信息，若不避免，可能会导致设备损坏、数据丢失、设备性能降低或其它不可预知的结果。 “注意”不涉及人身伤害。
 说明	用于突出重要/关键信息、最佳实践和小窍门等。 “说明”不是安全警示信息，不涉及人身、设备及环境伤害信息。

修改记录

修改记录累积了每次文档更新的说明。最新版本的文档包含以前所有文档版本的更新内容。

文档版本 01 (2013-12-10)

第一次正式发布。

目 录

1 执行摘要

eSight 终端资源提供对网络中接入终端的统一管理，通过分析设备 MAC 转发表、ARP 表数据来发现并管理所有接入终端。

重点功能包括终端接入记录、可疑终端日志、非法接入管理等几个部分。

2 简介

随着 IP 网络规模的不断扩大，网络中接入的终端设备也越来越多，对这些终端资源的管理将会面临如下挑战：

- 终端故障难以定位，缺乏高效的故障协查手段
- 终端安全风险难以防范，缺乏有效的安全控制手段和预警机制

eSight 终端资源能够展现多维度的终端信息，包括终端 MAC、终端 IP、接入设备端口、所属 VLAN 等，为用户提供有效的故障协查手段。同时支持识别端口下私接设备、IP 盗用、MAC 盗用这些网络中潜在的安全风险，并能够根据用户设定的白名单、交换机端口绑定规则、IP-MAC 绑定规则，检测接入终端的合法性，帮助用户构筑安全的终端接入环境。

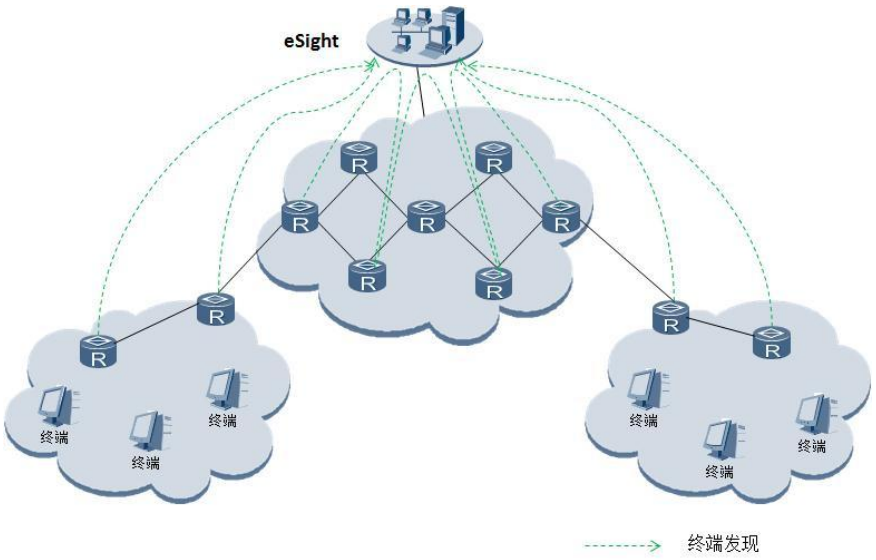
3 解决方案

3.1 解决方案整体介绍

eSight 终端资源通过分析设备 MAC 转发表、ARP 表数据来发现网络中的所有接入终端，并记录终端接入历史、识别可疑和非法终端，为网络维护者提供统一的终端资源的监控和管理手段。

详细的解决方案如下：

图3-1 终端资源解决方案



说明

终端发现作为所有终端数据的来源，是终端资源管理的基础，eSight 允许用户手工立即执行或者自动的周期执行终端发现。

步骤 1 eSight 终端资源可以根据白名单和接入绑定规则识别网络中的非法接入终端，维护人员可以把合法的 IP 地址和 MAC 地址范围录入到白名单中，可以配置 PORT-IP 或 PORT-MAC 规则以限制设备端口下准许接入的终端，可以配置 IP-MAC 规则以限制 IP 地址与 MAC 地址的对应关系。如果不配置白名单和接入绑定规则，则默认所有终端均合法。

步骤 2 选择设备，配置终端发现的范围，如果启用了终端自动发现，还可以设置自动发现的周期。

步骤 3 配置完成后，网管会根据相关参数，采集并分析设备的 MAC 转发表和 ARP 表数据，以发现网络中的接入终端。

步骤 4 维护人员可以通过查看终端接入记录、可疑终端日志、非法接入记录，监控所有的接入终端资源。

----结束

3.2 关键技术点介绍

3.2.1 终端数据发现原理

如图 3-2 所示，终端 A、B、C 接入到网络中，eSight 通过以下步骤发现终端：

步骤 1 网管采集所有设备的 MAC 转发表和 ARP 表数据。

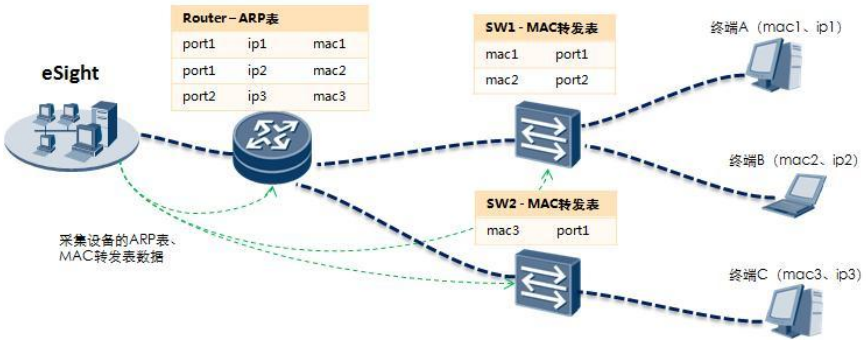
步骤 2 网管对采集到的数据进行分析，计算出终端的 MAC 地址、IP 地址、接入端口等信息。

步骤 3 网管对发现到的终端进行检测，识别出可疑终端和非法终端。

步骤 4 网管将多维度的终端数据呈现给维护人员。

----结束

图3-2 终端数据发现原理



3.3 功能约束

3.3.1 适用设备类型约束

设备	设备类型	设备版本
支持华为私有 MIB 读	ACU、AC66、AR150、AR200、	无

设备	设备类型	设备版本
取 MAC 转发表、公有 MIB 读取 ARP 表数据的华为设备	AR1200、AR150、AR2200、AR3200、AR500、ASG、CE5800、CE6800、ME5000、ME60、NE20、NE20E、NE40、NE40E、NE80、NE80E、NE5000E、NIP、S23、S27、S33、S37、S53、S57、S63、S67、S77、S93、S97、Eudemon1000E、Eudemon200E、Eudemon200E-X、Eudemon200S、Eudemon300、Eudemon8000E、FatAP、SIG、SRG、SPU、SVN、USG2100、USG2110、USG2200、USG3030、USG50、USG5300、USG5500、USG9100、USG9200、USG9300、USG9500、USR20、WS6600、WSG2110、WSG2200、WSG5100、WSG5300、WSG5500、WSG9300、WSG9500	
支持公有 MIB 读取 MAC 转发表和 ARP 表数据的设备	以上未包含的设备类型	

3.3.2 适用场景约束

设备	设备类型	场景约束
支持华为私有 MIB 读取 MAC 转发表、公有 MIB 读取 ARP 表数据的华为设备	ACU、AC66、AR150、AR200、AR1200、AR150、AR2200、AR3200、AR500、ASG、CE5800、CE6800、ME5000、ME60、NE20、NE20E、NE40、NE40E、NE80、NE80E、NE5000E、NIP、S23、S27、S33、S37、S53、S57、S63、S67、S77、S93、S97、Eudemon1000E、Eudemon200E、Eudemon200E-X、Eudemon200S、Eudemon300、Eudemon8000E、FatAP、SIG、SRG、SPU、SVN、USG2100、USG2110、USG2200、USG3030、USG50、USG5300、USG5500、	适用于有线接入的终端

设备	设备类型	场景约束
	USG9100、USG9200、USG9300、USG9500、USR20、WS6600、WSG2110、WSG2200、WSG5100、WSG5300、WSG5500、WSG9300、WSG9500、USG2100、USG2110、USG2200、USG3030、USG50、USG5300、USG5500、USG9100、USG9200、USG9300、USG9500、USR20、WS6600	
支持公有 MIB 读取 MAC 转发表和 ARP 表数据的设备	以上未包含的设备类型	

3.3.3 技术约束

设备	设备类型	技术约束
支持华为私有 MIB 读取 MAC 转发表、公有 MIB 读取 ARP 表数据的华为设备	ACU、AC66、AR150、AR200、AR1200、AR150、AR2200、AR3200、AR500、ASG、CE5800、CE6800、ME5000、ME60、NE20、NE20E、NE40、NE40E、NE80、NE80E、NE5000E、NIP、S23、S27、S33、S37、S53、S57、S63、S67、S77、S93、S97、Eudemon1000E、Eudemon200E、Eudemon200E-X、Eudemon200S、Eudemon300、Eudemon8000E、FatAP、SIG、SRG、SPU、SVN、USG2100、USG2110、USG2200、USG3030、USG50、USG5300、USG5500、USG9100、USG9200、USG9300、USG9500、USR20、WS6600、WSG2110、WSG2200、WSG5100、WSG5300、WSG5500、WSG9300、WSG9500	支持获取此类设备下接入终端的 VLAN 信息。 不在发现范围中的设备，会被作为终端发现到网管。
支持公有 MIB 读取 MAC 转发表和 ARP	以上未包含的设备类型	支持获取 Cisco 设备下接入终端的 VLAN 信

设备	设备类型	技术约束
表数据的设备		息。 不在发现范围中的设备，会被作为终端发现到网管。

3.4 典型场景应用

终端资源管理目前可以支持白名单和接入绑定规则两种非法终端检测手段，还支持端口多 MAC 地址、重复 IP 地址、重复 MAC 地址维度的可疑终端识别。

3.4.1 终端故障协查

在终端应用出现问题时，往往涉及网络侧的排查，此时需要先找到终端连接的交换机设备。维护人员可以进入终端接入记录，通过搜索终端的 IP 或 MAC 地址，快速定位终端资源位置。

图3-3 典型应用-终端定位

对于搜索到的终端记录，可以通过查看历史记录了解该终端的上下线历史，如图 3-4 所示。

图3-4 典型应用-回溯终端接入历史

在**终端接入记录**页面，单击接入设备名称的链接，可以进入设备管理器页面。支持Telnet、Ping、Trace 设备，查看关键的性能指标和告警：

图3-5 典型应用-查看设备状态和关键指标

3.4.2 非法接入监视

维护人员希望管控网络中的终端安全，有非法终端接入时能够及时发现并预警。首先需要把合法的 IP 地址和 MAC 地址范围录入到白名单中，配置 PORT-IP 或 PORT-MAC 规则以限制设备端口下准许接入的终端，配置 IP-MAC 规则以限制 IP 地址与 MAC 地址的对应关系。

图3-6 典型应用-创建白名单

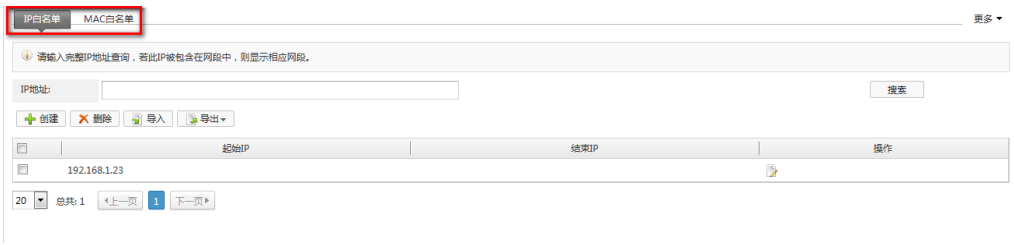
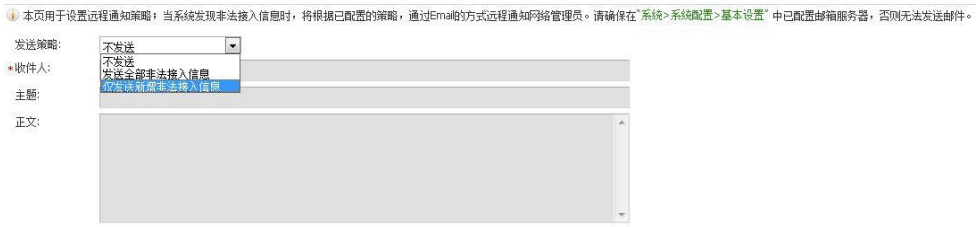


图3-7 典型应用-创建接入绑定规则

通过设置远程通知规则，发现非法接入后可以 Email 通知用户：

图3-8 典型应用-远程通知



在非法接入管理中记录了所有非法终端的接入历史，帮助进一步的跟踪和回溯。对于合法终端，维护人员可以快速将其添加到白名单和接入绑定规则中，或者确认其处理状态：

图3-9 典型应用-非法接入管理

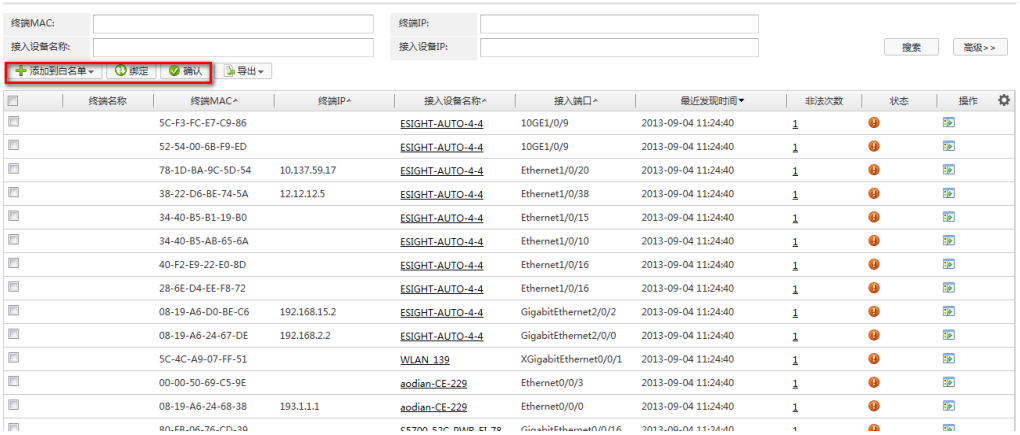


图3-10 典型应用-非法接入日志

4 推广

- 海量终端统一管理。

  终端资源管理通过分析设备 MAC 转发表和 ARP 表数据，实现异构网络中接入终端的快速发现，使企业网用户可以直观了解终端在线趋势，跟踪终端的位置变化和上下线历史。

- 快速故障协查。

  终端资源管理能够展现多维度的终端信息，包括终端 MAC、终端 IP、接入设备端口、所属 VLAN 等，帮助企业网用户快速定位终端接入位置，查看接入设备的运行状态、性能指标、告警等关键数据，有效支撑故障协查和故障分责的运维需要。

- 终端安全管控。

  终端资源管理支持根据用户配置的白名单和接入绑定规则，快速发现网络中接入的非法终端并及时预警。还支持识别端口下私接设备、IP 盗用、MAC 盗用这些网络中潜在的安全风险。

5 结论

终端资源能够统一管理网络中的所有接入终端，帮助网络维护人员快速定位终端的接入位置，回溯终端接入历史，并有效防范终端安全风险。

6 缩略语表

英文缩写	英文全称	中文全称
ARP	Address Resolution Protocol	地址解析协议
SNMP	Simple Network Management Protocol	简单网络管理协议