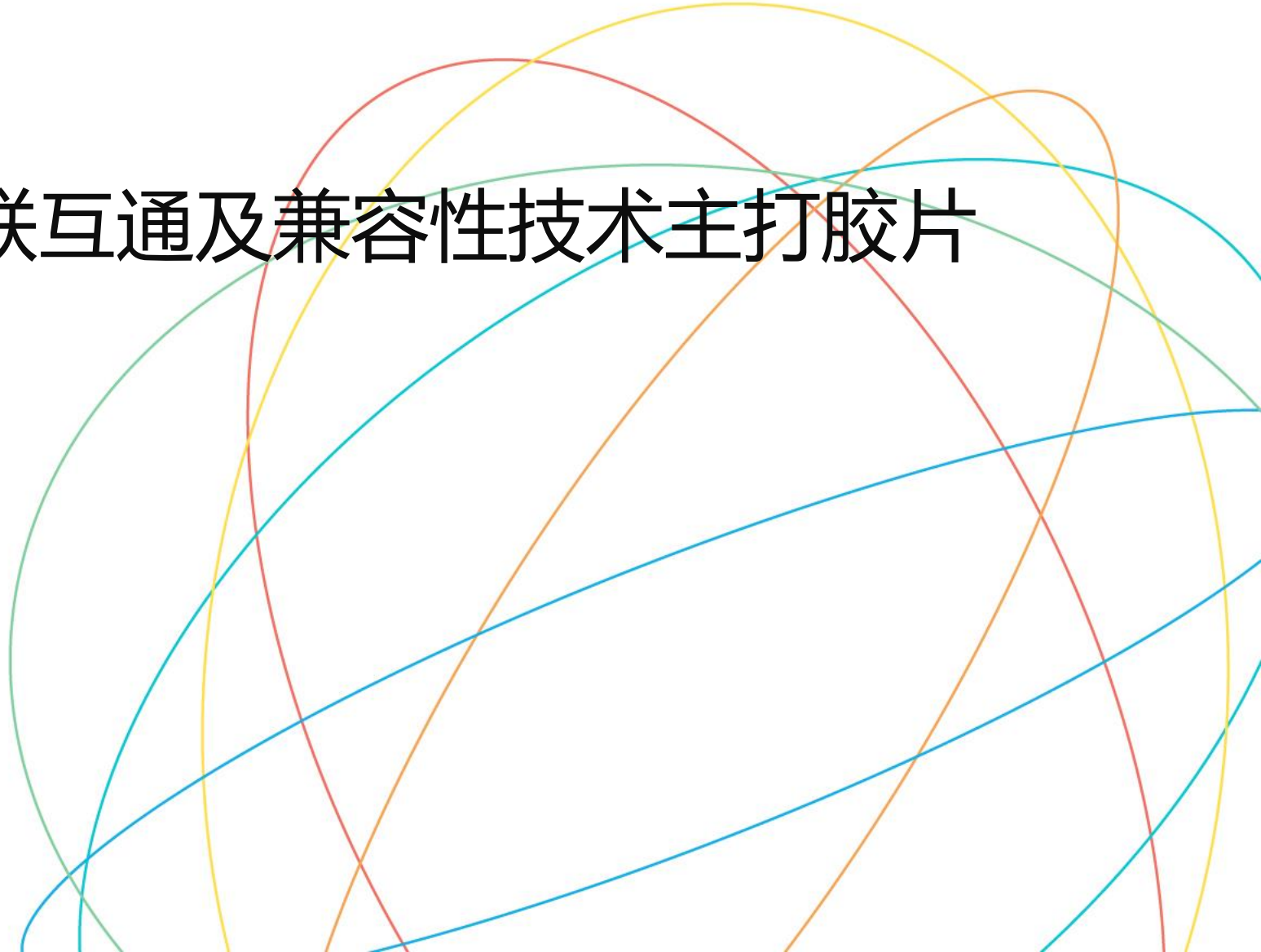
Day/ Month/ Year

园区网络搬迁 - 互联互通及兼容性技术主打胶片

敏捷园区解决方案部



背景介绍

客户案例1：世界500强某企业交换机RFI需求

背景及网络现状

- 电力与自动化技术的领导者,范围包括自动化，电机，机器人等领域；
- 营收超400亿美金，大约有15万名员工，分布在全球100+国家；
- 现在网络设备基本上由思科提供，价格贵且服务响应慢；
- 预计在2018年和2019年全球有**1500台交换机**需要更新；
- 客户出于TCO考虑，评估引入第二厂商，对华为开放机会。

技术诉求

- 支持与现网的思科**交换机，AP，CheckPoint防火墙**互联互通；
- 兼容现网的思科**IP Phone**；
- 支持**IoT**设备的认证接入及**设备识别**；
- 支持与现网的思科**ISE**认证系统集成；
- 支持第三方的**SIEM**系统集成；
- 支持**多因子**认证；
- 支持**SCOM管理套件**的网络监控

客户案例2: 欧洲知名制造企业新大楼网络POC需求

背景及网络现状

- 全球领先的电梯，自动扶梯、自动人行道及相关服务的供应商；
- 超过**60000**名员工遍布于全球100多个国家和地区；
- 与华为在**IoT**方案有深度合作，建立了良好的信任关系；
- 总部新建的管理大楼，对华为开放**LAN/WLAN**机会；
- 要求进行POC测试，保障兼容现网环境；

技术诉求

- 要求交换机支持与思科核心交换机**Nexus7000**互联互通；
- 支持包括Laptop，手机，**扫描枪**等各类移动设备的兼容；
- 支持与微软**NPS**认证系统集成；
- 支持与第三方网管系统**Solwarwinds**集成；
- 支持现网**短信网关**集成；

客户案例3: 亚太知名银行园区大楼网络更新需求

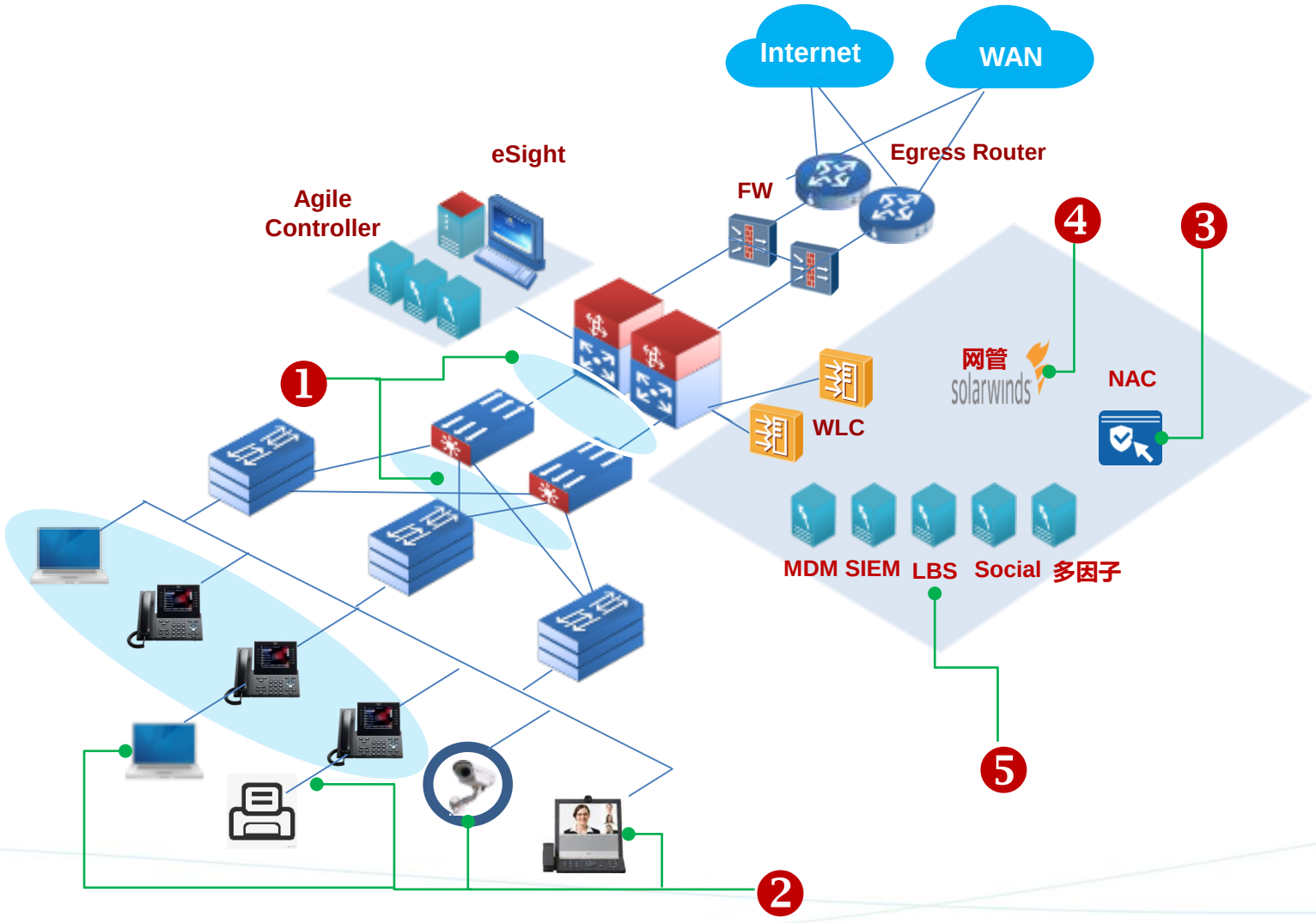
背景及网络现状

- 东南亚某岛国最大商业银行；
- 本国超过100家分行，在美国，英国，日本，印度，马来等国设立海外分行；
- 网络一直采用思科的设备，对思科的价格和服务存在不满；
- 总部大楼网络设备逐渐EOS, 开放其中一栋大楼的交换机POC机会给华为；
- 该大楼包含5000台电脑终端和4000台IP电话

主要诉求

- 简化网络管理；
- 控制器实现交换机和防火墙安全策略统一纳管；
- 支持与**ISE集成**
  - 实现Anyconnet，NACAgent的终端安全检查；
  - 采用EAP FAST协议替换EAP MD5对接ISE；
  - 实现基于MAB认证的终端仿冒检测能力

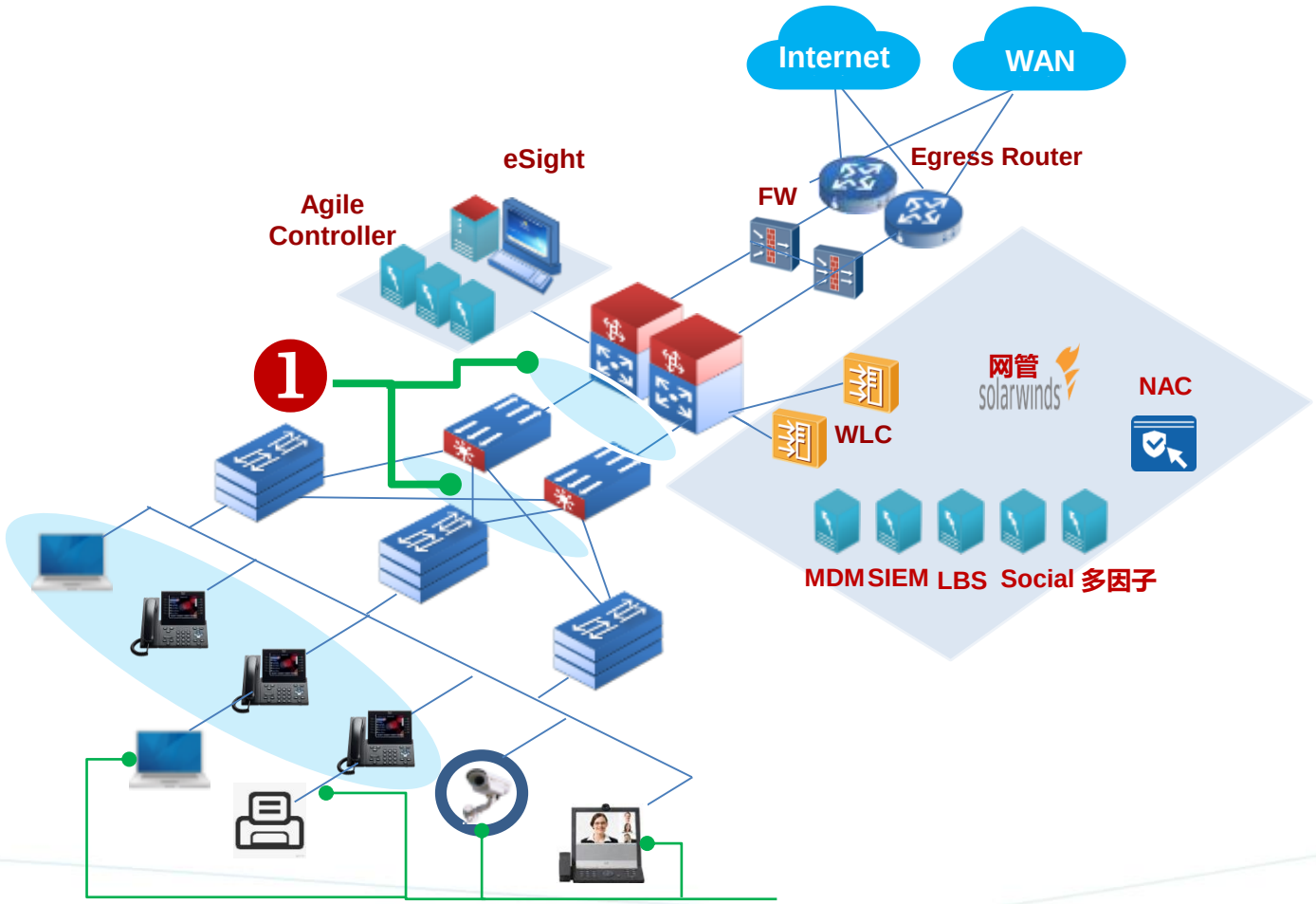
互联互通及兼容性主要问题概览



类型	子类型	示例
❶ 网络协议	二层协议	PVST
	路由协议	EIGRP
	HA协议	HSRP
❷ 终端设备	IT设备	IP Phone,
	OT设备	扫描枪，打印机等
❸ NAC系统	NAC+华为设备	ISE, ClearPass
	AC1.0+友商设备	友商设备:Cisco, HP等
	设备管理	TACACS+兼容性
❹ 网管系统	网络管理	Solarwinds
	日志管理	Kiwisyslog
❺ 增值系统	MDM服务器	AirWatch
	SIEM	Splunk
	定位	蓝牙Beacon
	社交账号	Facebook, Twitter等
	多因子	RSA

网络协议

网络协议互联互通



类型	友商私有协议	功能
二层协议	PAgP	二层链路聚合
	CDP	邻居发现协议
	VTP	在 VTP 域内同步 VLAN信息
	DTP	两台交换机的直连二层端口协商
	PVST PVST+	二层网络破环协议
	UDLD	链路单通检测
三层路由协议	EIGRP	思科私有路由协议
网关冗余协议	HSRP, GLBP	网关冗余协议

PAgP： 华为LACP与思科PAgP协议

协议说明

功能	思科协议	华为协议
以太网链路聚合简称链路聚合，通过将多条物理链路捆绑成为一条逻辑链路，从而增加链路带宽并提高可靠性	端口聚集协议(PAgP) Port Aggregation Protocol	链路聚合控制协议LACP Link Aggregation Control Protocol

功能对比

华为和思科在实现原理上没有区别，仅缺省配置和命令行有所差别

对接替换方案

方案1：

华为S系列交换机和思科交换机采用手工模式链路聚合对接替换

配置步骤：

1、配置思科交换机手工模式链路聚合：

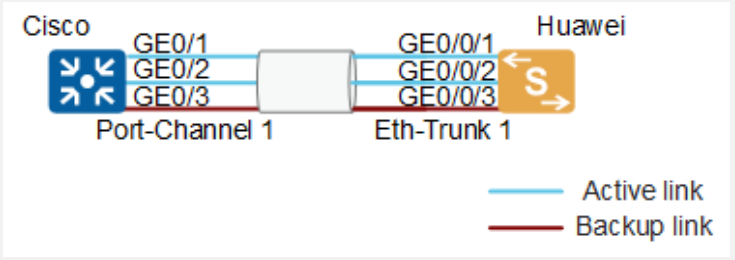
a. 创建Port-Channel接口并加入成员接口，配置链路聚合方式。
b. 配置负载分担方式。

2、配置华为S系列交换机手工模式链路聚合：

a. 创建Eth-Trunk接口并加入成员接口。
b. 配置负载分担方式。

方案2：

华为S系列交换价和思科交换机采用LACP模式链路聚合对接替换



配置步骤：

1、配置思科交换机PAgP模式链路聚合：

a. 创建Port-Channel接口并加入成员接口，配置链路聚合方式。
b. 配置负载分担方式。
c.

2、配置华为S系列交换机LACP模式链路聚合：

a. 创建Eth-Trunk接口并加入成员接口，配置Eth-Trunk为LACP模式。
b. 配置负载分担方式。
c. 配置系统优先级，确定主动端。
d. 配置接口优先级，确定活动链路接口，优先级高的接口将被选作活动接口。

VTP： 华为VTP与思科VCMP协议

协议说明

功能	思科协议	华为协议
在二层网络中传播VLAN配置信息，自动地在整个二层网络中保证VLAN配置信息一致。其中Server角色用于维护该域内所有VLAN信息，并同步出去	思科私有： VLAN中继协议VTP（VLAN Trunking Protocol）	华为私有：VLAN集中管理协议VCMP（VLAN Central Management Protocol）

功能对比

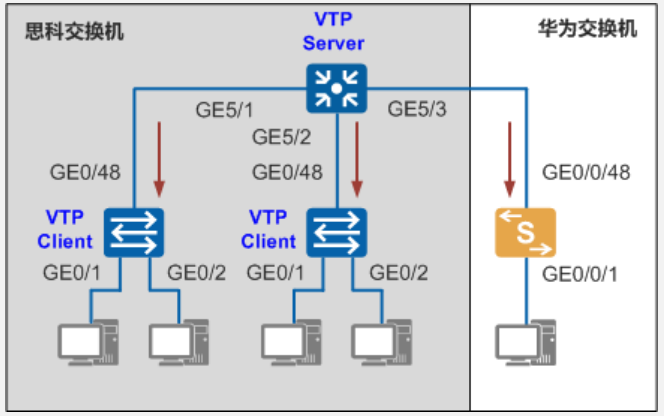
思科VTP域内可以有多个Server，且任意设备均可以作为Server，Server间互相同步。
华为VCMP域由一台设备统一控制整网的配置，域内不允许出现多台Server。

对接替换方案

VTP和VCMP都是私有协议，两者不能直接对接。但在整个组网中，在华为和思科直接相连的交换机上分别做一些配置，可以实现互通，从而支持混合组网。

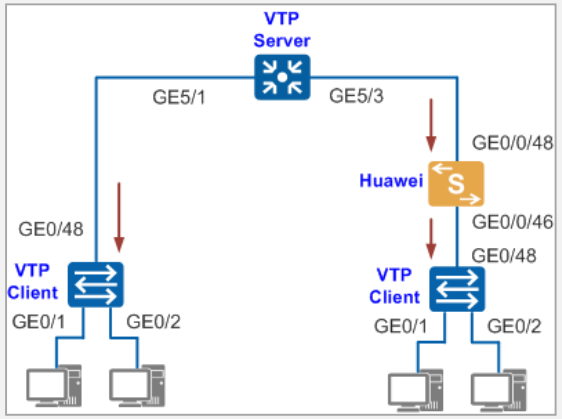
场景1：C-H模型混合组网

- 华为交换机上手动配置VLAN



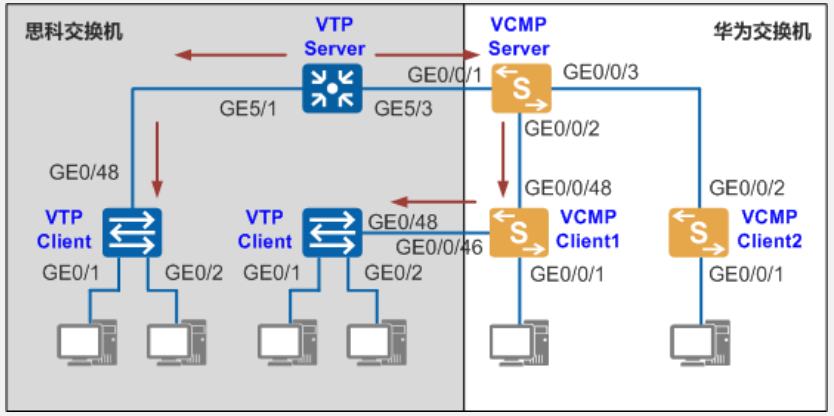
场景2：C-H-C模型混合组网

- 华为交换机上手动配置VLAN
- 并配置二层协议透传功能，透传VTP报文



场景3：C-H-H-C模型混合组网

- 华为交换机对思科VTP协议报文透明传输。
- 华为组网中使用VCMP协议同步VLAN配置。组网内部接口使用LNP协商链路类型，减少配置和维护的工作量



DTP： 华为LNP与思科DTP协议

协议说明

功能	思科协议	华为协议
动态协商以太网接口的链路类型为Access或者Trunk	动态中继协议DTP(Dynamic Trunking Protocol)	链路类型协商协议LNP(Link-type Negotiation Protocol)

功能对比

功能项描述	思科协议	华为协议
开启/关闭全局端口链路类型自协商	不支持	支持，默认开启
开启/关闭端口的链路类型自协商	支持，默认情况请参考思科手册	支持，默认开启
动态协商链路类型	支持	支持
动态协商链路类型后，根据协商结果下发接口下的VLAN信息	支持	支持
显示端口链路类型协商信息	支持	支持
主备倒换后动态链路协商状态自恢复	支持	支持

对接替换方案

- 华为交换机和思科交换机相连时，不能使用动态协议协商接口类型，需要把两台交换机的接口类型都手动配置为Trunk

对接限制

- 接口的封装方式必须使用IEEE 802.1Q标准协议

PVST+：生成树协议兼容性

协议说明

功能	思科协议	华为协议
生成树协议，用于局域网中消除环路	PVST（Per VLAN Spanning Tree）（私有） PVST+（Per VLAN Spanning Tree Plus）（私有） Rapid-PVST+（Rapid PVST+）（私有） MST（Multiple Spanning Tree）（标准）	STP（Spanning Tree Protocol）（标准） RSTP（Rapid Spanning Tree Protocol）（标准） MSTP（Multiple Spanning Tree Protocol）（标准） VBST（VLAN-Based Spanning Tree）（私有）

功能对比

- 功能无本质差别。差别主要体现在报文处理方式、命令格式、路径开销算法和MSTP域摘要。
- PVST+可与标准的STP协议互通。
- 思科的MST属于标准MSTP，但用于生成MSTP摘要信息的密钥各厂家不同。

对接替换方案

方案1：华为S系列交换机透传PVST报文，思科交换机自己协商破环

成树收敛速度变慢，且容易产生临时环路

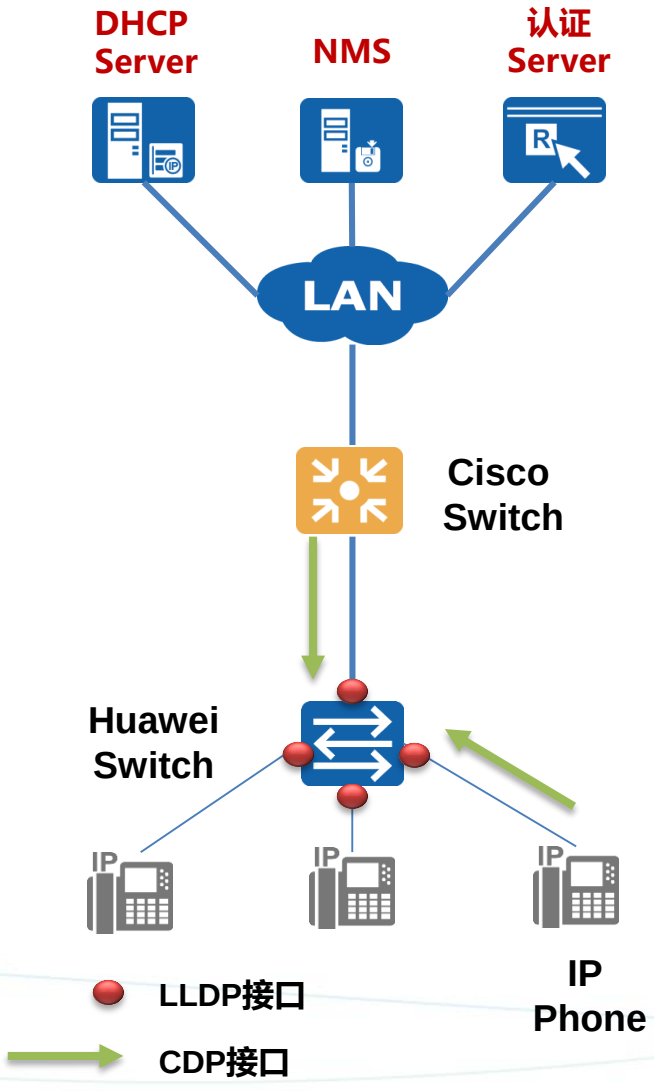
方案2：华为S系列交换机通过VBST与思科交换机PVST/PVST+/Rapid PVST+对接

华为S系列交换机VBST与思科交换机PVST/PVST+/Rapid PVST+互通时，就如同华为S系列交换机VBST跟自身互通一样

方案3：更改思科交换机PVST为MST同华为S系列交换机MSTP对接

华为S系列交换机MSTP同思科交换机MST互通，除了当域摘要信息格式不一致时，要使能摘要侦听功能。其他原理同思科交换机一致

CDP协议



配置LLDP兼容CDP协议

1. 使能SwitchA的全局LLDP功能

   [Huawei Switch] **lldp enable**

2. 接口上配置LLDP兼容CDP协议的功能

   [Huawei Switch] **lldp compliance cdp receive**

配置LLDP可配置Voice VLAN功能与支持CDP协议的语音设备互通

1. 配置接口的LLDP可配置Voice VLAN功能

   [Huawei Switch] **lldp tlv-enable med-tlv network-policy voice-vlan vlan vlan-id [cos cvalue | dscp dvalue]***

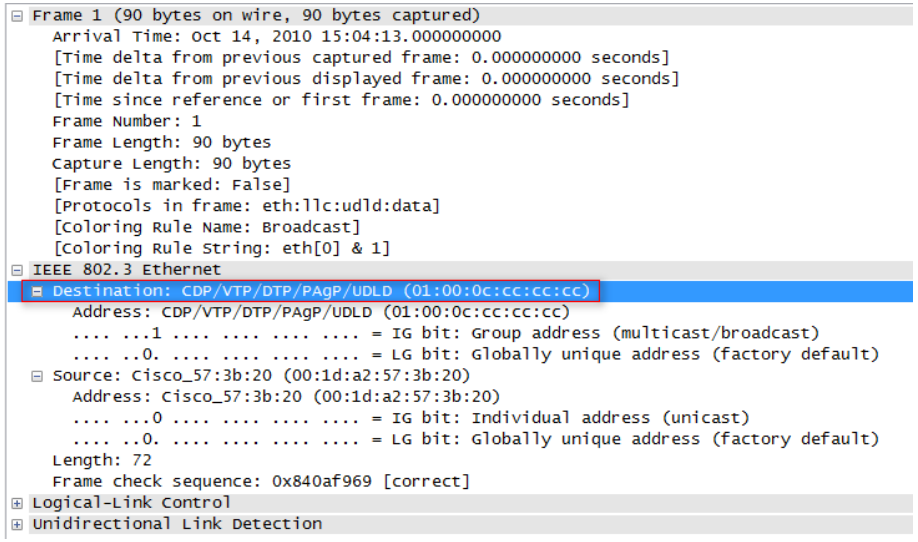
2. 使能接口与支持CDP协议的语音设备互通前的信息交互功能

   [Huawei Switch] **lldp compliance cdp txrx**

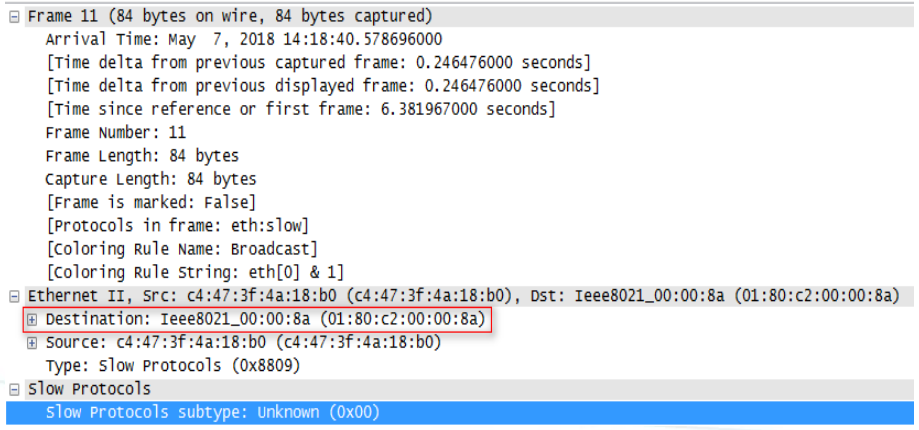
注意事项

配置这些命令的接口兼容是单向的，即华为设备端能够兼容思科CDP设备，但反之，思科设备端无法显示连接华为设备的信息

UDLD协议



UDLD Protocol Packet Format



DLDP Protocol Packet Format

对接分析

UDLD （UniDirectional Link Detection 单向链路检测）：是个Cisco私有的二层协议，用于监听利用光纤或双绞线连接的以太链路的物理配置，当出现单向链路时，UDLD可以检测出这一状况，关闭相应接口并发送警告信息。UDLD需要链路两端设备都支持才能正常运行。

华为**DLDP**可实现类似功能，两者实现基本原理类似，但是协议报文格式不同，所以DLDP和UDLD两者不可以对接

可选方案

1. 整网替换，所有使用UDLD的思科交换机全部替换为支持DLDP的华为S系列交换机。
2. 使用**LACP**协议替代**UDLD**，华为和思科互连端口均配置**LACP**。
3. 使用**802.3ah ETH-OAM**协议替代**UDLD**，华为和思科均配置**ETH-OAM**

HSRP： 华为VRRP与思科HSRP协议

协议说明

功能	思科协议	华为协议
多台路由器组成一个“热备份组”，组成虚拟的路由器，提升网络冗余性	热备份路由协议HSRP（Hot Standby Router Protocol） （私有）	虚拟冗余路由协议VRRP（Virtual Redundancy Router Protocol） （标准）

功能对比

- 协议基本原理和功能相似，但报文、运行机制、封装方式和命令均不同。思科交换机也支持VRRP协议。

对接替换方案

- HSRP报文的目的MAC与VRRP完全不同，两种协议无法对接。因此，华为S系列交换机替换思科设备时，只能选择使用VRRP协议替换HSRP协议

■ 方案1：割接前将Cisco设备HSRP整改为VRRP

a.将HSRP备设备三层接口shutdown

b.将HSRP备设备配置整改为VRRP主设备，保持三层接口down；

c.将HSRP主设备三层接口shutdown，打开主设备的三层接口，完成业务切换；

d.将HSRP主设备整改为VRRP备设备，打开三层接口，HSRP切换VRRP完成；

e.将VRRP备设备的业务割接至华为VRRP备设备；

f. 将VRRP主设备的业务割接至华为VRRP主设备。

■ 方案2：直接将HSRP下行主备链路同时割接至华为VRRP主备设备

a.保证华为设备有网络侧路由，使业务平台割接至华为设备后业务损失降到最低；

b.将HSRP备设备下行接口shutdown，将物理线缆割接是VRRP主设备；

c.将HSRP主设备下行接口shutdown，打开VRRP主设备端口，业务完成切换；

d.将原互连HSRP主设备的物理线缆割接至VRRP备设备，打开VRRP备设备端口，割接完成。

EIGRP：华为OSPF与思科EIGRP兼容性

	OSPF	EIGRP
协议标准	IETF 标准协议，协议设计完美成熟，绝大部分厂商支持，组网不受厂商选择限制	Cisco 私有协议，不能与其它厂商联合组网；协议实现在根据使用经验不断优化。
部署范围	IETF 推荐的 IGP，世界上使用最广泛的路由协议	仅有少数网络使用，而且部署越来越少
核心算法	SPF 算法收敛快，无环路	采用分布式的 DUAL 算法，中间状态不可预测，可能陷入 SIA 状态，查询可能扩散到全网
网络拓扑支持	支持层次性网络拓扑，具有很好的可管理性和扩展性	不支持层次性网络

OSPF与EIGRP协议对比

EIGRP无法直接与OSPF对接，从 EIGRP 切换到 OSPF 有多种切换方案，最常见的两种切方案

全网切换方案

1. 所谓“全网切换”是指把全网所有路由设备上的 EIGRP 协议一次性的切换为 OSPF 协议，切换后全网为纯净的OSPF 网络
2. 适用于网络规模不大，业务流量模型清晰的网络

渐进切换方案

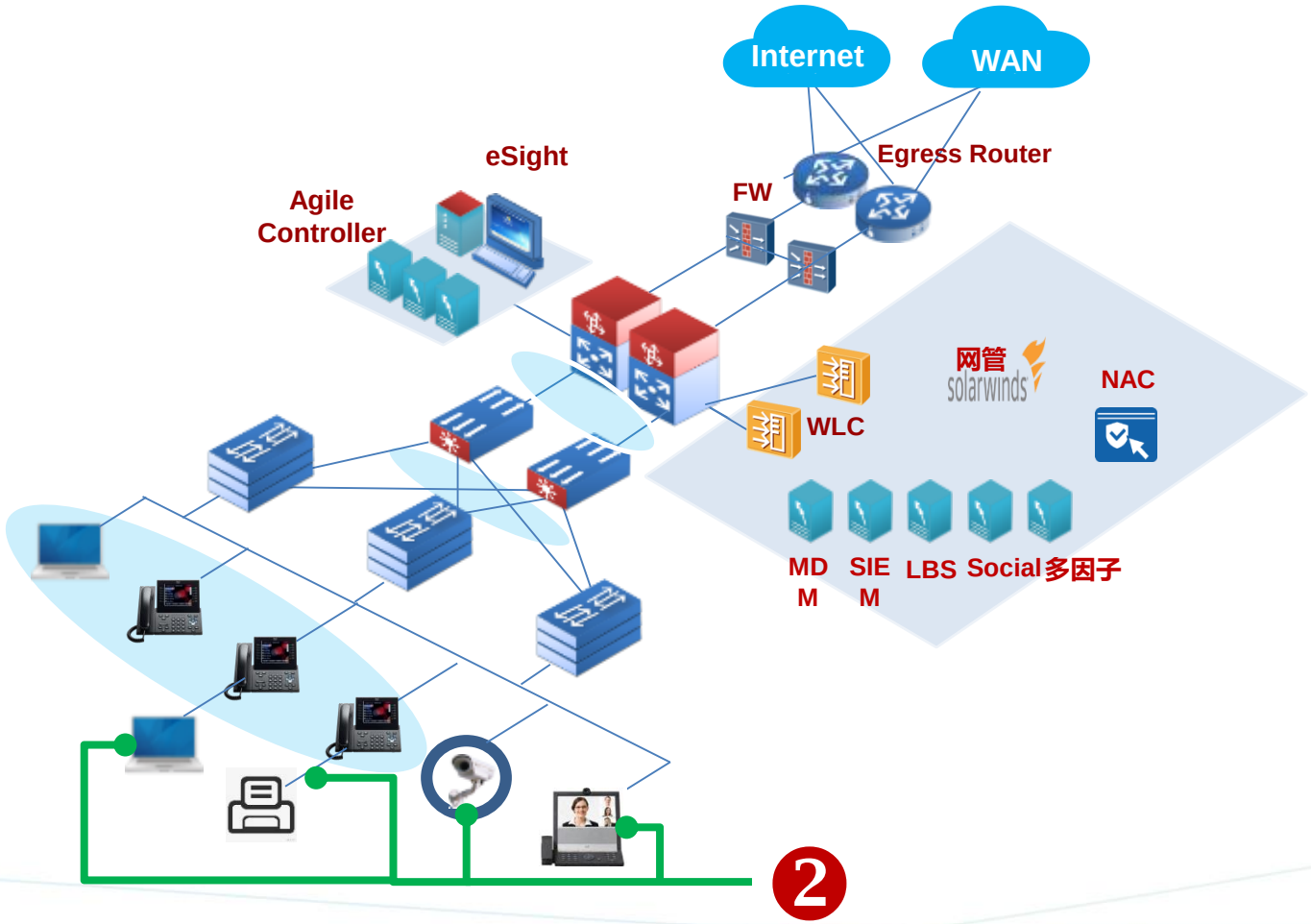
1. 是指当网络规模较大时，首先先将边缘网络的 EIGRP 切换到OSPF（存在多个分支时，多个分支可以逐步进行切换），最后当所有边缘网络的 EIGRP 都切换为 OSPF 后，再将骨干网络的 EIGRP 切换到 OSPF，最终达到全网切换的目的。
2. 适合用于网络拓扑复杂，业务流量模型复杂的网络。切换可以分步骤进行

网络协议互联互通方案概览

思科私有	华为协议	协议对接方案	协议替换方案
PAgP	**LACP**	不支持	采用 LACP 模式链路聚合对接
CDP	**LLDP**	单向互通，LLDP可兼容CDP	将思科交换机从CDP改为LLDP实现同华为交换机LLDP的协商对接
VTP	**VCMP**	VTP 是 Cisco 的私有协议, 华为交换机不可与 VTP 直接互通,可采用其他方式完成混合组网。	华为和思科直接相连的交换机上分别做一些配置，实现混合组网。如C-H, C-H-C, C-H-H-C.
DTP	**LNP**	DTP 是 Cisco 私有协议，华为设备不可与 DTP 互通。但可采用其他方式完成混合组网。	需要把对端思科交换机的端口配置为非协商类型，两台交换机的接口类型都手动配置为Trunk，同时指定思科交换机报文的封装方式IEEE 802.1Q封装模式
PVST/PVST+	**VBST**	支持，华为交换机通过配置VBST同思科交换机PVST报文协商破环	NA
PVST/PVST+	**MST**	不支持	将思科交换机从PVST改为MST实现同华为S系列交换机MSTP的协商对接
UDLD	**DLDP**	不支持	1. 全部替换为华为设备。 2. Alternative Solution: LACP 3. 802.3ah OAM Link Fault Trigger Interface Down
HSRP, GLBP	**VRRP**	不支持	只能选择VRRP协议替换HSRP协议
EIGRP	**OSPF**	不支持	1. EIGRP 切换到 OSPF 2. 通过路由重分布

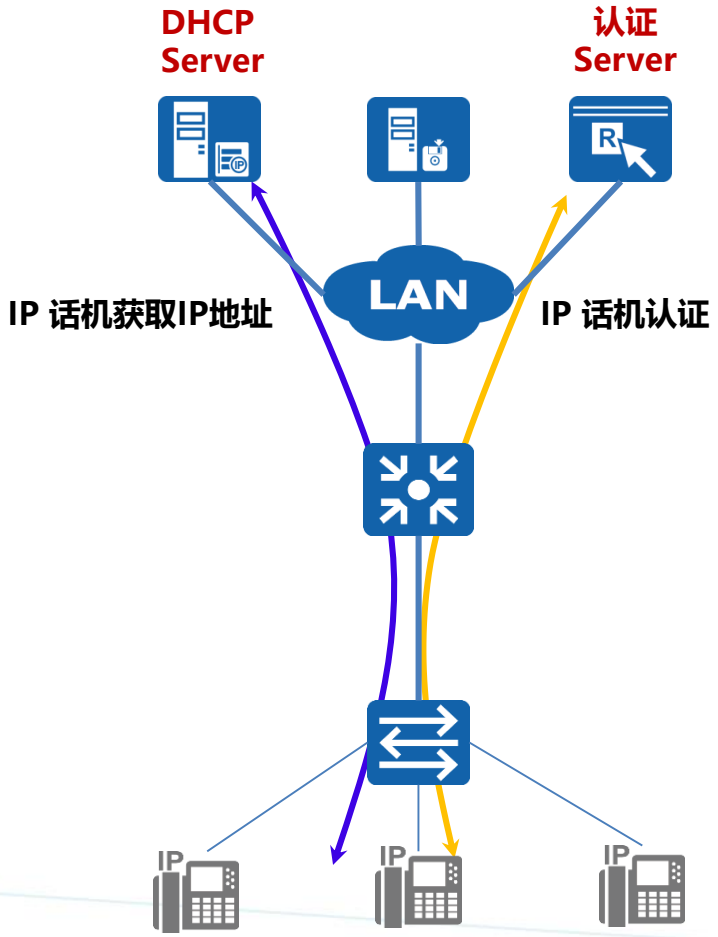
终端设备

终端设备兼容性



- IP Phone兼容性
- POE终端
- 无线终端接入

IP话机对接



IP话机对接概述

IP话机需要通过和交换机对接实现语音流量的传输，在IP网络中就会同时存在语音流量和数据流量。所以IP话机和交换机对接的关键就是在语音流量和数据流量同时接入时，如何协商Voice LAN, 保证语音流量的优先传输，以保证通话质量。

IP话机对接方式

根据话机本身能力，有以下不同的对接方式

- LLDP
- LLDP_MED
- HDP
- VOICE-VLAN INCLUDE_UNTAG
- PVID=VOICE-VLAN
- MAC-VLAN
- 流策略
- DHCP
- NAC认证+VOICE VLAN

IP 话机对接方式

- **LLDP**

  交换机上启用LLDP和Voice VLAN功能实现IP话机接入，通过LLDP协议为设备分配Voice VLAN

- **LLDP-MED**

  IP话机支持**LLDP**协议，并且支持通过network-policy TLV字段获取Voice VLAN，可以在交换机上配置命令lldp tlv-enable med-tlv network-policy voice-vlan为语音设备分配Voice VLAN

- **CDP**

  IP话机支持CDP协议获取Voice VLAN，可以使用交换机提供的HDP（Huawei Discovery Protocol）方式为话机分配Voice VLAN

- **VOICE-VLAN INCLUDE_UNTAG**

  IP 话机发送的是Untagged或者Tag0报文，通过识别语音报文的**OUI**地址，为语音报文添加Voice VLAN ID

- **PVID=VOICE VLAN**

  IP 话机发送的是Untagged或者Tag0报文，通过接口的PVID为语音报文打上VLAN ID

- **DHCP**

  通过DHCP协议为IP话机分配Voice VLAN

- **MAC VLAN**

  IP话机不支持LLDP和DHCP协议，通过MAC VLAN方式实现IP话机接入

- **流策略**

  IP话机不支持LLDP和DHCP协议,可以通过以下流策略方式实现IP话机接入,

  - **ACL方式**: 在接口下配置port add-tag acl命令
  - **基于ACL的简化流策略**方式: 在接口下配置traffic-remark inbound ACL 命令

- **NAC认证+VOICE VLAN**

  通过NAC认证，下发Voice VLAN

IP话机对接支持概览

厂商	型号	POE	是否标准PD	LLDP	CDP	VOICE-VLAN INCLUDE_UNTAG	PVID=VOICE VLAN	MAC-VLAN	流策略	NAC	DHCP
Cisco	39/69/78/79/88/89/99/SPA30/SPA50/SPA51/SPA52/SPA94/SPA96 series	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	**N**
Avaya	12/16/46/96 series	**Y**	**Y**	**Y**	**N**	**Y**	**Y**	**Y**	**Y**	**Y**	**N**
Polycom	300/400/600 series	**Y**	**Y**	**Y**	**N**	**Y**	**Y**	**Y**	**Y**	**Y**	**N**
MITEL	5212/5340	**Y**	**Y**	**Y**	**N**	**Y**	**Y**	**Y**	**Y**	**Y**	**N**

详细对接款型与对接情况请参考如下链接：
http://3ms.huawei.com/mm/docMaintain/mmMaintain.do?method=showMMDetail&f_id=EDC180810553915269

有线终端设备PoE对接能力

PoE供电标准

PoE供电标准包括IEEE 802.3bt、IEEE 802.3at和IEEE 802.3af。不同供电标准的供电技术的特性参数之间有差异

POE原理简介

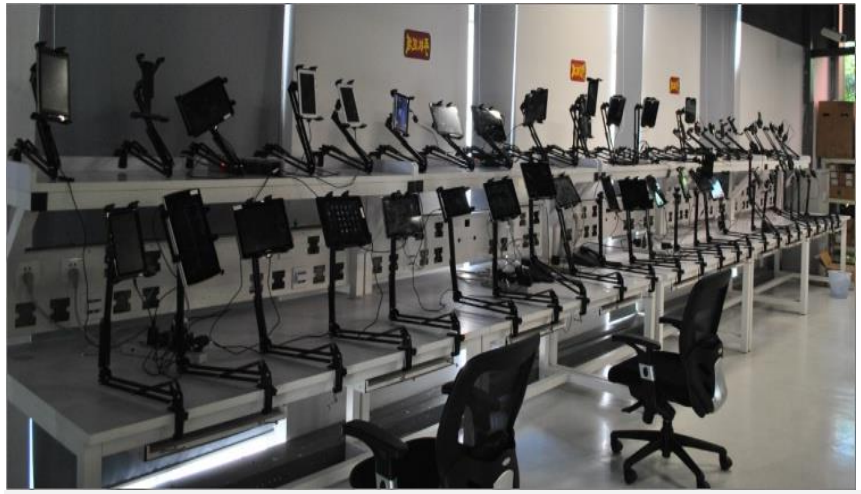
PoE供电系统包括：

- **PSE**（Power-Sourcing Equipment）：指通过以太网给受电设备供电的PoE设备，提供检测、分析、智能功率管理等功能。
- **PD**（Powered Device）：如无线AP（Access Point）、摄像头等受电设备。按照是否符合IEEE标准，PD分为**标准PD**和**非标准PD**。
- **PoE电源**：PoE电源为整个PoE系统供电，PSE下接的PD数量受制于PoE电源的功率。

终端类型	厂商	型号(示例)	POE	标准PD
IP话机	Cisco	39/69/78/79/88/89/99	Y	Y
	Avaya	12/16/46/96 series	Y	Y
	Polycom	300/400/600 series	Y	Y
	MITEL	5212/5340	Y	Y
摄像头	Dahua	DH-SDZ2030U-N	Y	Y
	HIKVISION	DS-2CD4126FWD-IZ	Y	Y
	Huawei	IPC6525-Z30	Y	Y
AP	Cisco	1602I/3702I/2602I/1131/3602I/1702	Y	Y
	Aruba	205/325 series	Y	Y
	Rucks	R510/R610/R710	Y	Y
	Meraki	MR34	Y	Y
	Mikro	Tik	Y	N

详细对接款型与对接情况请参考如下链接：
http://3ms.huawei.com/mm/docMaintain/mmMaintain.do?method=showMMDetail&f_id=EDC180810553915269

无线终端兼容性测试环境及工具



WLAN产品终端兼容性实验室

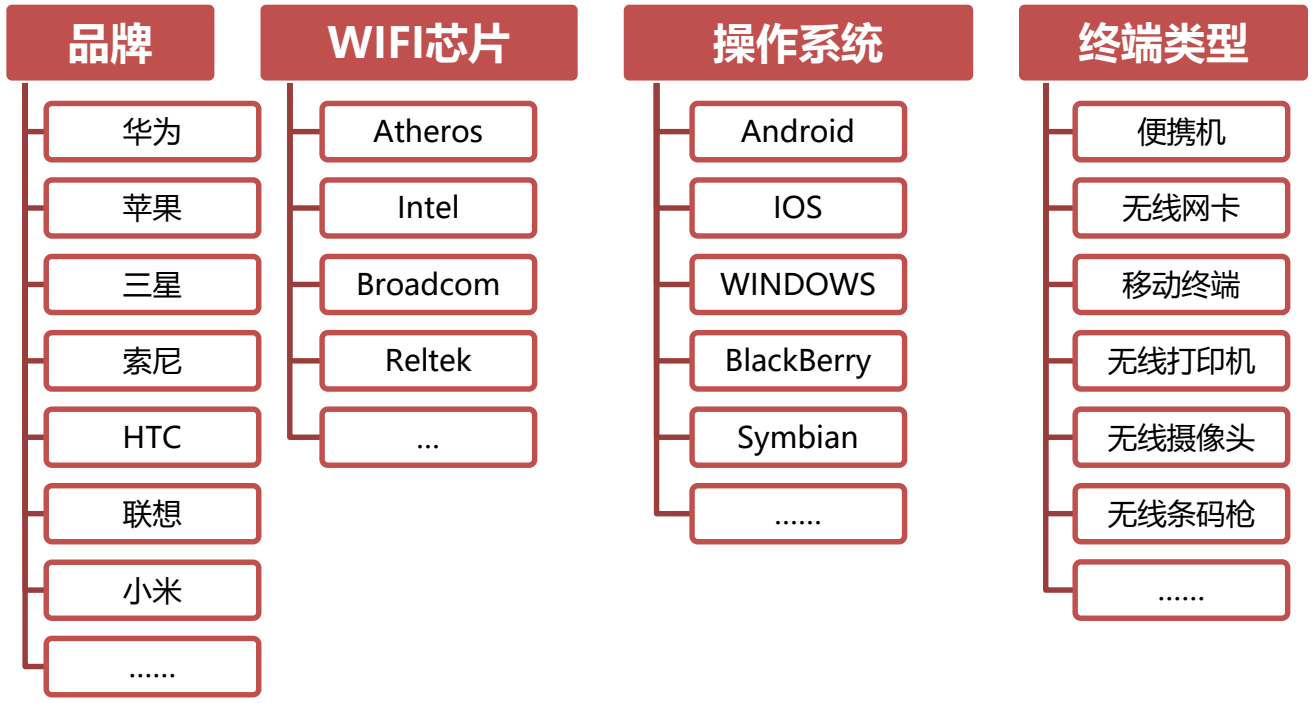
1. 目前验证过的WIFI终端数量200+
2. 手机等消费终端覆盖TOP 10品牌
3. WI-FI芯片覆盖全部芯片供应商
4. 操作系统覆盖主流系列及版本
5. 覆盖平板电脑/手机/笔记本/行业终端等

Wi-Fi Manager

是测试团队自主研发的WLAN终端控制工具。其主要功能

1. 支持监控在线设备；
2. 支持终端漫游监控、主动漫游、自动漫游；
3. 支持PC端远程控制，可多终端并行测试；
4. 支持智能终端反复自动关联、去关联；
5. 支持信号监控功能，守候特定SSID；
6. 支持查看终端Logcat信息功能；
7. 支持iperf、FTP、Ping等测试工具；
8. 支持自动化测试接口；

无线终端兼容性测试方法



从多个维度选择无线终端，充分考虑终端的全面性和代表性，且定期评估市场新增终端，及时纳入测试范围

无线终端测试用例更新

WLAN终端兼容性测试方案定期刷新，测试用例有以下三个来源

1. 借鉴业界终端兼容性测试中的测试项目。
2. 从产品规格入手，分析识别出我司WLAN产品与终端兼容性相关功能点。
3. 通过每周例行的网上问题分析，总结终端兼容性故障模式。

无线终端兼容性结果示例

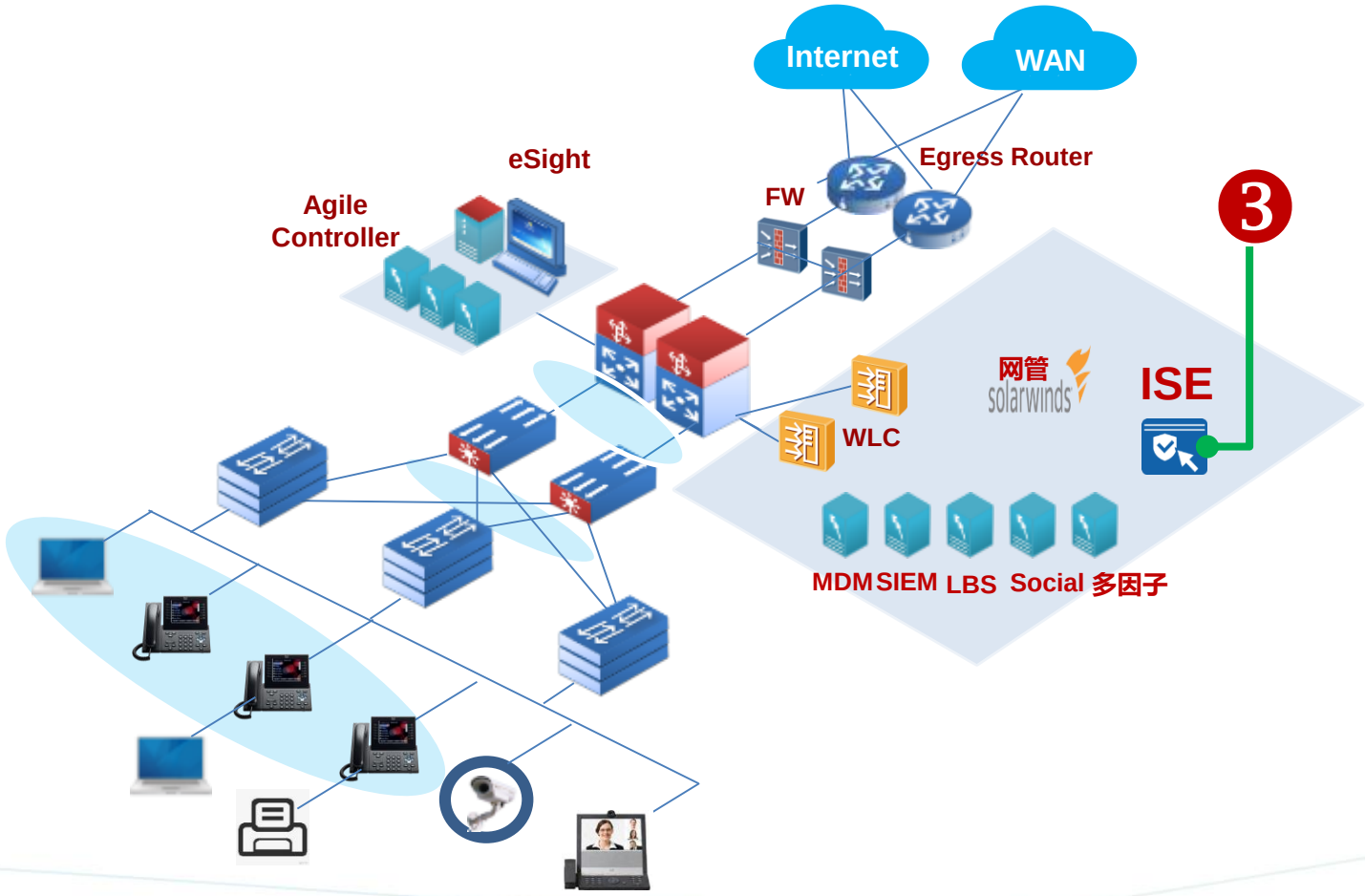
终端类型	厂商	型号(示例)	WEP					WPA/WPA2	
			Open	PSK(64)	PSK(128)	MAC	Portal	PSK	802.1X
Wi-Fi Phone	Cisco	8821	Y	Y	-	Y	Y	Y	Y
	FlyingVoice	IP622W	Y	Y	-	Y	-	Y	-
Laptop	Dell	Inspiron N4110	Y	Y	-	Y	Y	Y	Y
	HP	HP 2540p	Y	Y	-	Y	Y	Y	Y
	Apple	Mac Book-Air	Y	Y	-	Y	Y	Y	Y
Tablet	Samsung	TabGT-P7300	Y	Y	-	Y	Y	Y	Y
	Sony	SGPT212	Y	Y	-	Y	Y	Y	Y
Mobile Phone	Apple	iPhone X	Y	Y	-	Y	Y	Y	Y
	Samsung	S9	Y	Y	-	Y	Y	Y	Y
Printer	Canon	Canon iC MF628CW	Y	Y	-	Y	-	Y	-
Netcard	LINKSYS	LINKSYS NG-AC	Y	Y	-	Y	Y	Y	Y

定期在3MS和公司官网对外发布WLAN产品终端兼容性测试报告

http://3ms.huawei.com/mm/docMaintain/mmMaintain.do?method=showMMDetail&f_id=1697980

NAC系统

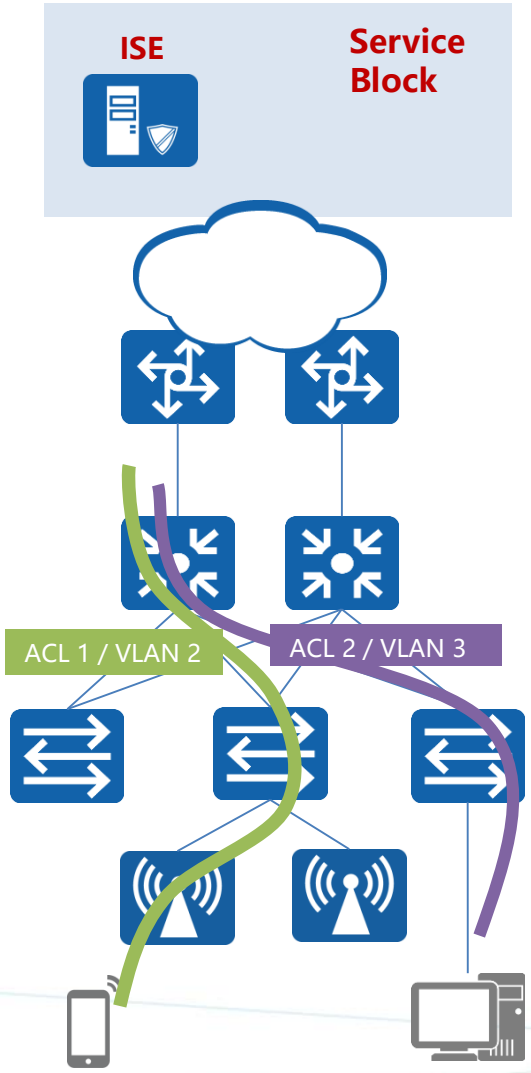
NAC系统对接



NAC(ISE)兼容性

1. 策略授权及CoA
2. 802.1X认证
3. MAB认证
4. Web认证
5. 终端安全(Posture)
6. 终端识别(Profiling)

ISE对接 – 授权



典型场景

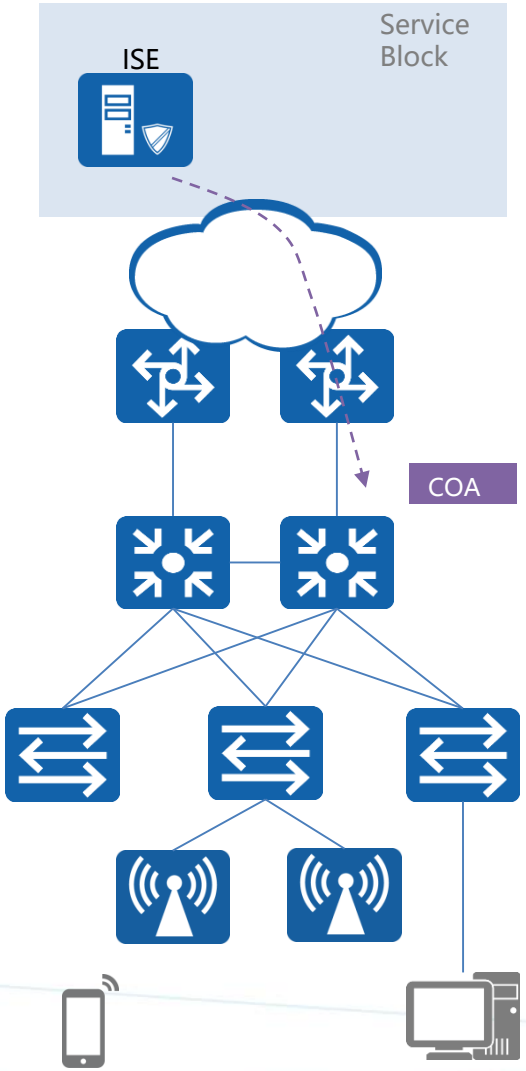
用于区分不同的用户属性进行网络隔离或者差异化权限控制

对接能力

主要通过Radius授权完成，部分授权方式需要通过在ISE中导入华为的**私有属性**完成对接。

授权方式	LSW对接支持情况	WLAN对接支持情况	备注
VLAN	Y	Y	Portal认证不支持动态VLAN授权
ACL	Y	Y	
DACL	Y	N	通过在ISE中导入华为私有属性完成对接 HW-Data-Filter
CAR	Y	Y	通过在ISE中导入华为私有属性完成对接 上行CAR：HW-Input-Committed-Information-Rate 下行CAR：HW-Output-Committed-Information-Rate
URL Redirect	Y	Y	通过在ISE中导入华为私有属性完成对接 HW-Portal-URL HW-Redirect-ACL
UCL Group	Y	Y	通过在ISE中导入华为私有属性完成对接 HW-Data-Filter
MACSec Policy	N	N	

ISE对接 – CoA



典型场景

配合ISE完成WEB CWA认证、设备注册、设备安全检查、BYOD等业务。

对接能力

ISE主动发起，通知接入设备对用户授权进行变更，通过Radius协议交互

CoA	LSW对接支持情况	WLAN对接支持情况	备注
Bounce Host Port	Y	NA	交换机V2R12版本新增支持
Disable Host Port	Y	NA	交换机V2R12版本新增支持
Session Reauthenticate	Y	Y	
Session Terminate	Y	Y	

ISE策略授权及CoA　兼容性配置（添加华为私有属性字典）

1. 在ISE属性字典需要新建华为厂商，华为的Vendor ID 是**2011**
2. 添加右表所示的华为私有Radius属性
3. 其中属性字段类型和ID必须跟华为定义的一致，参考华为产品手册。

华为私有属性	用途
HW-Data-Filter	用于下发动态ACL，类似思科DACL
HW-Ext-Specific	通过该属性可以实现重认证、Port Shutdown和 Port Bounce类型CoA动作
HW-Input-Committed-Information-Rate	上行限速
HW-Output-Committed-Information-Rate	下行限速
HW-Portal-URL	重定向URL，配合重定向ACL实现终端安全检查及CWA Portal等功能
HW-Redirect-ACL	重定向ACL，ACL内容需在设备上配置，配合重定向URL实现终端安全检查及CWA Portal等功能
HW-VoiceVLAN	配合标准动态VLAN属性一起可以为语音用户下发动态Voice VLAN
HW-Exec-Privilege	华为设备通过该属性授权管理用户优先级（0~15）

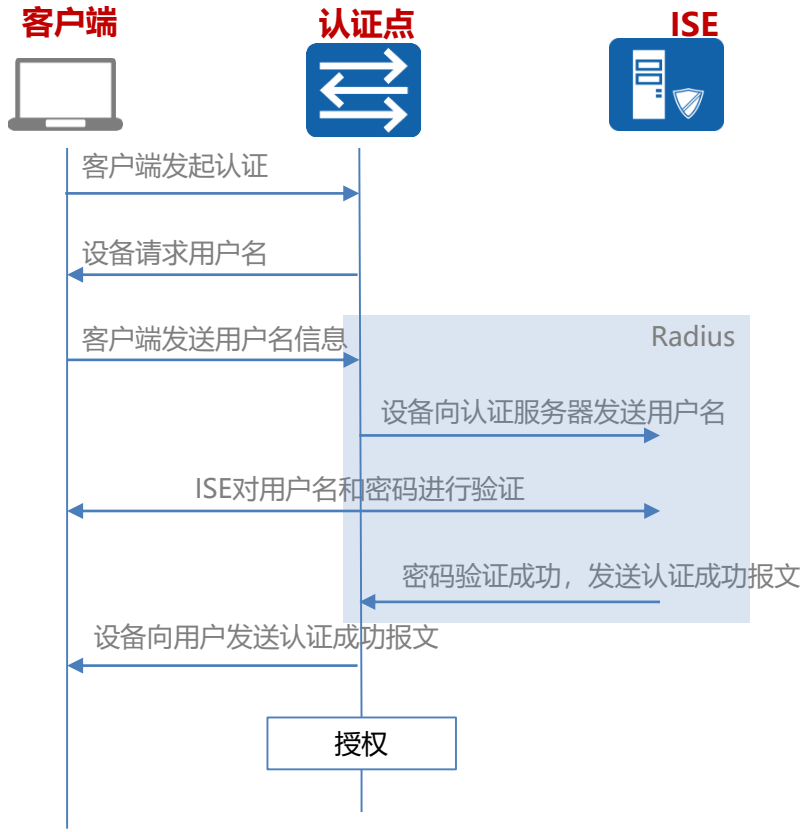
ISE策略授权及CoA　兼容性配置（自定义网络设备模板）

网络设备模板(Network Device Profile)

1. **网络设备模板(Network Device Profile)**定义了一个厂商所支持的各种功能范围，影响着后面几乎每一步的配置内容（例如添加设备及创建授权结果时都需要选择网络设备模板）。
2. **ISE1.x**版本中没有**设备模板**的概念，如果第三方设备与思科存在实现差异的话，就会造成无法对接的现象，包括但不仅限于：
   - CoA
   - Client Provisioning and Posture Check
   - CWA Portal
   - BYOD
3. ISE**2.x**支持用户创建并自定义网络设备模板，在兼容第三方设备上做出的比较大的改进；

模板配置内容	注意事项
创建设备模板	Radius字典选择之前创建的华为私有Radius属性字典
Authentication	定义Radius Flow Type，ISE根据收到的Radius请求消息中Radius属性值来来判断认证请求类型，如有线802.1X, 无线802.1X, 有线MAB, 无线MAB等
Permission	定义下发动态VLAN及ACL使用的Radius属性，华为采用业界标准方式 **VLAN**: IETF 802.1X Attributes **ACL**: Radius Filter-ID
CoA	华为使用的CoA目的端口是**3799，** 思科使用的是**1700.** ISE从2.0开始才支持设备模板，之前的版本CoA目的端口固定采用1700，无法与华为设备对接
Redirect	关于Redirect URL格式的定义，主要用于终端安全检查和Web认证等场合，通过华为的私有Radius属性**HW-Portal-URL**下发

ISE对接 - 用户接入认证（802.1X）



图：EAP中继方式业务流程

典型场景

主要用于解决企业员工的网络准入控制。安全性相对其他认证方式，如MAC、Protal等更高。

对接能力

对接主要通过认证点设备和ISE间的Radius协议完成；

认证方式	LSW对接支持情况	WLAN对接支持情况	备注
PAP/CHAP	Y	Y	
EAP-MD5	Y	Y	
EAP-PEAP	Y	Y	
EAP-TLS	Y	Y	
EAP-LEAP	N	N	LEAP属于思科私有认证属性，这个认证方式存在安全漏洞，因此应对策略可以考虑引导使用其他EAP认证替代
EAP-FAST	Y	Y	

ISE对接 – 802.1X配置示例

思科ISE端配置

1. **配置认证允许的协议。**通常情况下802.1x认证使用EAP-MD5，PEAP-MSCHAPv2，EAP-TLS及EAP-FAST协议

2. **配置授权结果模板。**配置给设备授权下发的属性，例如动态VLAN、ACL和限速

3. **创建802.1x的认证（Authentication）策略.**
   - 可以选择多个条件，条件之间可使用AND或者OR；
   - 认证用户源，可以使用本地创建的用户，也可以使用AD域用户或者证书用户

4. **创建802.1x的授权策略。**
   - 可针对不同用户组进行分类授权
   - 可以选择多个条件，条件之间可使用AND或者OR
   - 选择先前创建的授权结果模板对认证用户做授权

华为设备端配置样例

- **配置Radius Server模板**

```
radius-server template ISE
 radius-server shared-key cipher xxx
 radius-server authentication 192.89.12.248 1812 weight 80
 radius-server accounting 192.89.12.248 1813 weight 80
 undo radius-server user-name domain-included
 calling-station-id mac-format hyphen-split mode2
```

- **配置授权服务器参数**

```
radius-server authorization calling-station-id decode-mac-format ascii hyphen-split common
radius-server authorization 192.89.12.248 shared-key cipher xxx
```

- **配置AAA参数**

```
 aaa
  authentication-scheme ise
  authentication-mode radius
accounting-scheme ise
  accounting-mode radius
  accounting start-fail online
domain default
  authentication-scheme ise
  accounting-scheme ise
  radius-server ISE
```

- **配置接入及认证模板**

```
authentication-profile name dot1x
 dot1x-access-profile dot1x
dot1x-access-profile name dot1x
```

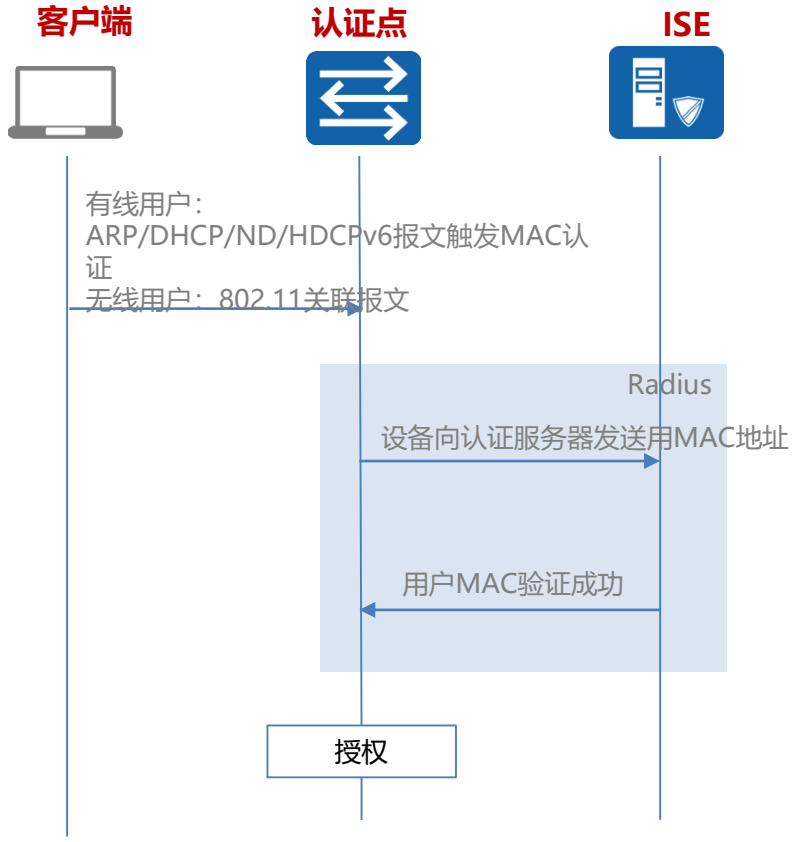
- **配置用户接入端口**

```
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
 authentication-profile dot1x
```

- **配置授权VLAN或ACL（可选，根据实际需要）**

```
vlan 200
acl number 3000
 rule 5 deny ip destination 100.1.1.10 0
 rule 10 pemit ip
```

ISE对接 - 用户接入认证（MAC）



图：MAC认证流程

典型场景

主要用于解决没有1x客户端的哑终端，如打印机、摄像头等设备的网络准入控制。MAC认证不需要专用的客户端，也不需要终端用户介入

对接能力

对接主要通过认证点设备和ISE间的Radius协议完成；Radius属性Service-Type为10对于ISE对应MAC认证。

认证方式	LSW对接支持情况	WLAN对接支持情况	备注
MAC	Y	Y	
MAB（Mac By Pass）	Y	Y	MAC旁路认证

ISE对接 – MAB配置示例

思科ISE端配置

1. **添加终端MAC，有两种方式添加**
   - 在**Endpoint**中手动添加终端的**MAC**
   - 自动添加终端的**MAC**地址
2. **配置认证允许的协议。** MAB认证使用Host Lookup，认证协议支持PAP和CHAP（**V2R12**后支持）两种
3. **配置授权结果模板。**配置给设备授权下发的属性，例如动态VLAN、ACL和限速
4. **创建802.1x的认证（Authentication）策略.**
   - 可以选择多个条件，条件之间可使用AND或者OR；
   - 选择认证用户源，使用本地终端MAC账号；如果使用自动方式添加MAC账号的话用户不存在的下一步动作需要选择‘**Continue**’
5. **创建802.1x的授权策略。**
   - 可针对不同用户组进行分类授权
   - 可以选择多个条件，条件之间可使用AND或者OR
   - 选择先前创建的授权结果模板对认证用户做授权

华为设备端配置样例

- **配置Radius Server模板**

```
radius-server template ISE
 radius-server shared-key cipher xxx
 radius-server authentication 192.89.12.248 1812 weight 80
 radius-server accounting 192.89.12.248 1813 weight 80
 undo radius-server user-name domain-included
 calling-station-id mac-format hyphen-split mode2
 radius-attribute set Service-Type 10 auth-type mac
calling-station-id mac-format hyphen-split mode2
```

- **配置授权服务器参数**

```
radius-server authorization calling-station-id decode-mac-format ascii hyphen-split common
radius-server authorization 192.89.12.248 shared-key cipher xxx
```

- **配置AAA参数**

```
aaa
 authentication-scheme ise
 authentication-mode radius
accounting-scheme ise
 accounting-mode radius
 accounting start-fail online
domain default
 authentication-scheme ise
 accounting-scheme ise
 radius-server ISE
```

- **配置接入及认证模板**

```
authentication-profile name dot1x
 mac-access-profile mab
mac-access-profile name mab
 mac-authen username macaddress format with-hyphen normal uppercase
```

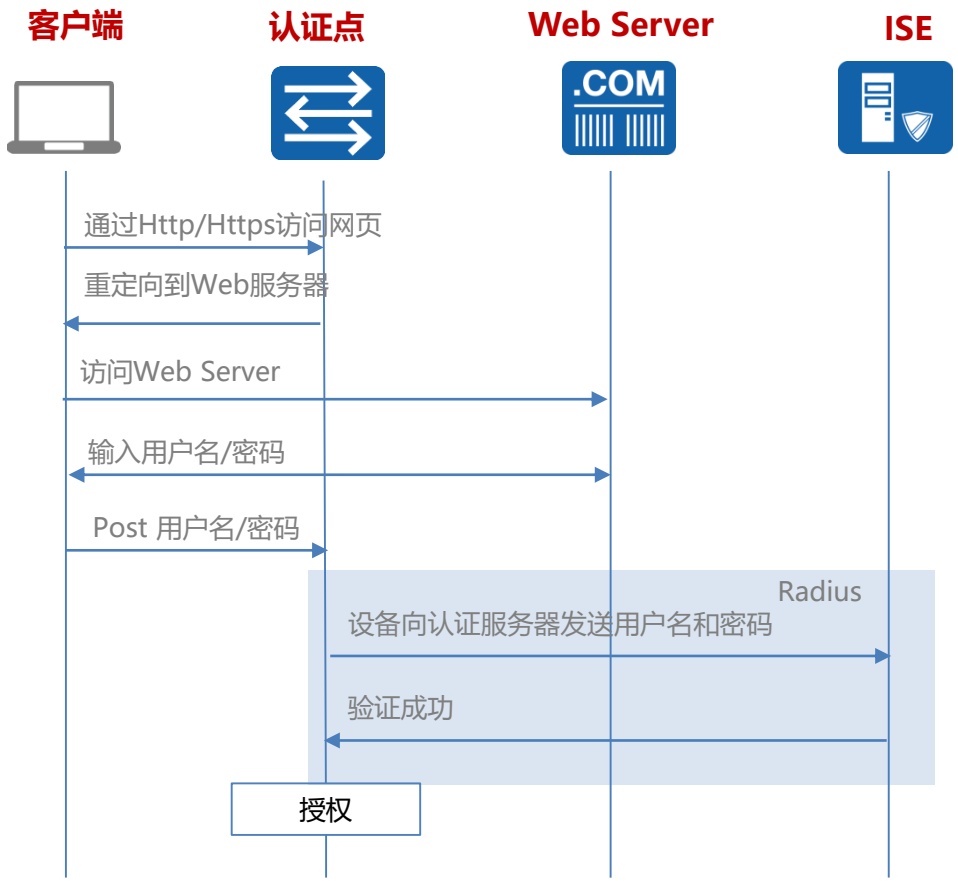
- **配置用户接入端口**

```
interface GigabitEthernet0/0/1
 voice-vlan 200 enable
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
 port hybrid tagged vlan 200
 lldp tlv-enable med-tlv network-policy voice-vlan vlan 200
 lldp compliance cdp txrx
 authentication-profile mab
```

- **配置授权VLAN或ACL（可选，根据实际需要）**

```
vlan 200
acl number 3000
 rule 5 deny ip destination 100.1.1.10 0
 rule 10 pemit ip
```

ISE对接 - 用户接入认证（WEB）



图：WEB认证流程

典型场景

主要应用在企业园区场景下给访客、供应商等提供INTERNET访问权限，或者商业/公共WIFI场景下给用户提供网络访问权限；WEB认证不需要专门的客户端

对接能力

认证点和ISE间采用Radius协议对接；

认证方式	LSW对接支持情况	WLAN对接支持情况	备注
Web	Y	Y	需要在ISE导入华为私有属性

ISE对接– Web认证配置示例

思科ISE端配置

1. **创建认证（Authentication）策略.**
   - 匹配条件选择**MAC**认证，数据源中用户不存在选项的下一步动作选择 ‘**Continue**’
2. **配置授权结果模板，要配置两个**
   - 访客第一次接入授权重定向URL和ACL
   - 访客注册认证后授权正常的用户权限
3. **创建802.1x的授权策略，同样需要配置两条分别对应上一步创建的授权结果。**
   - 第一条策略使用访客在portal页面的注册或者登入信息作为匹配条件，授权结果放通网络权限
   - 第二条授权策略使用MAB认证作为匹配条件，授权结果中下发重定向ACL及URL
   - 已注册用户的授权策略优先级更高，所以顺序靠前
   - **ISE**校验访客用户名密码成功后发送**CoA**通知用户进行重认证，用户此时的MAC账号和先前注册的访客账号已经绑定，匹配第一条授权策略，放通用户的网络访问权限。

华为设备端配置样例

- **配置Radius Server模板**

```
radius-server template ISE
 radius-server shared-key cipher xxx
 radius-server authentication 192.89.12.248 1812 weight 80
 radius-server accounting 192.89.12.248 1813 weight 80
 undo radius-server user-name domain-included
 calling-station-id mac-format hyphen-split mode2
 radius-attribute set Service-Type 10 auth-type mac
```

- **配置授权服务器参数**

```
radius-server authorization calling-station-id decode-mac-format ascii hyphen-split common split radius-server authorization 192.89.12.248 shared-key cipher xxx
```

- **配置AAA参数**

```
aaa
 authentication-scheme ise
 authentication-mode radius
accounting-scheme ise
 accounting-mode radius
 accounting start-fail online
domain default
 authentication-scheme ise
 accounting-scheme ise
 radius-server ISE
```

- **配置接入及认证模板**

```
authentication-profile name dot1x
 mac-access-profile mab
mac-access-profile name mab
 mac-authen username macaddress format with-hyphen normal uppercase
```

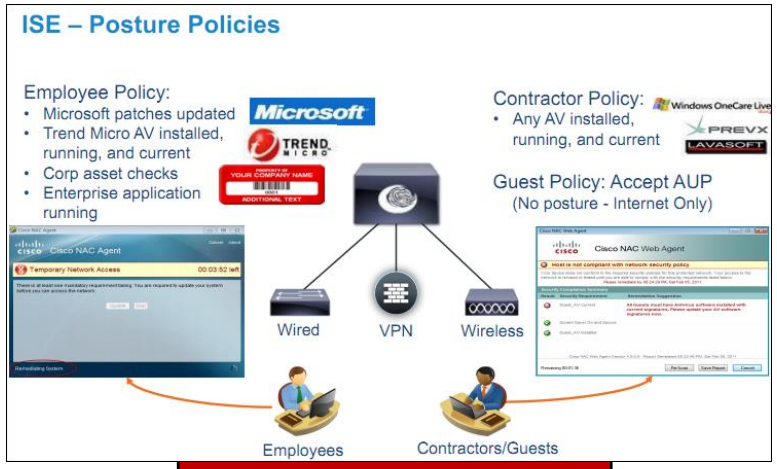
- **配置重定向ACL（Deny表示不重定向，匹配permit规则流量被重定向）**

```
acl number 3002    ///ACL id与授权结果中HW-Redirect-ACL值相同
 rule 1 deny udp destination-port eq dns
 rule 2 deny udp source-port eq dns     放通DNS流量
 rule 3 deny udp destination-port eq bootps
 rule 4 deny udp destination-port eq bootpc
 rule 5 deny udp source-port eq bootpc
 rule 6 deny udp source-port eq bootps  放通DHCP流量
 rule 7 deny ip destination 192.89.11.79 0  放通目的地址为ISE服务器的流量
 rule 8 permit ip
```

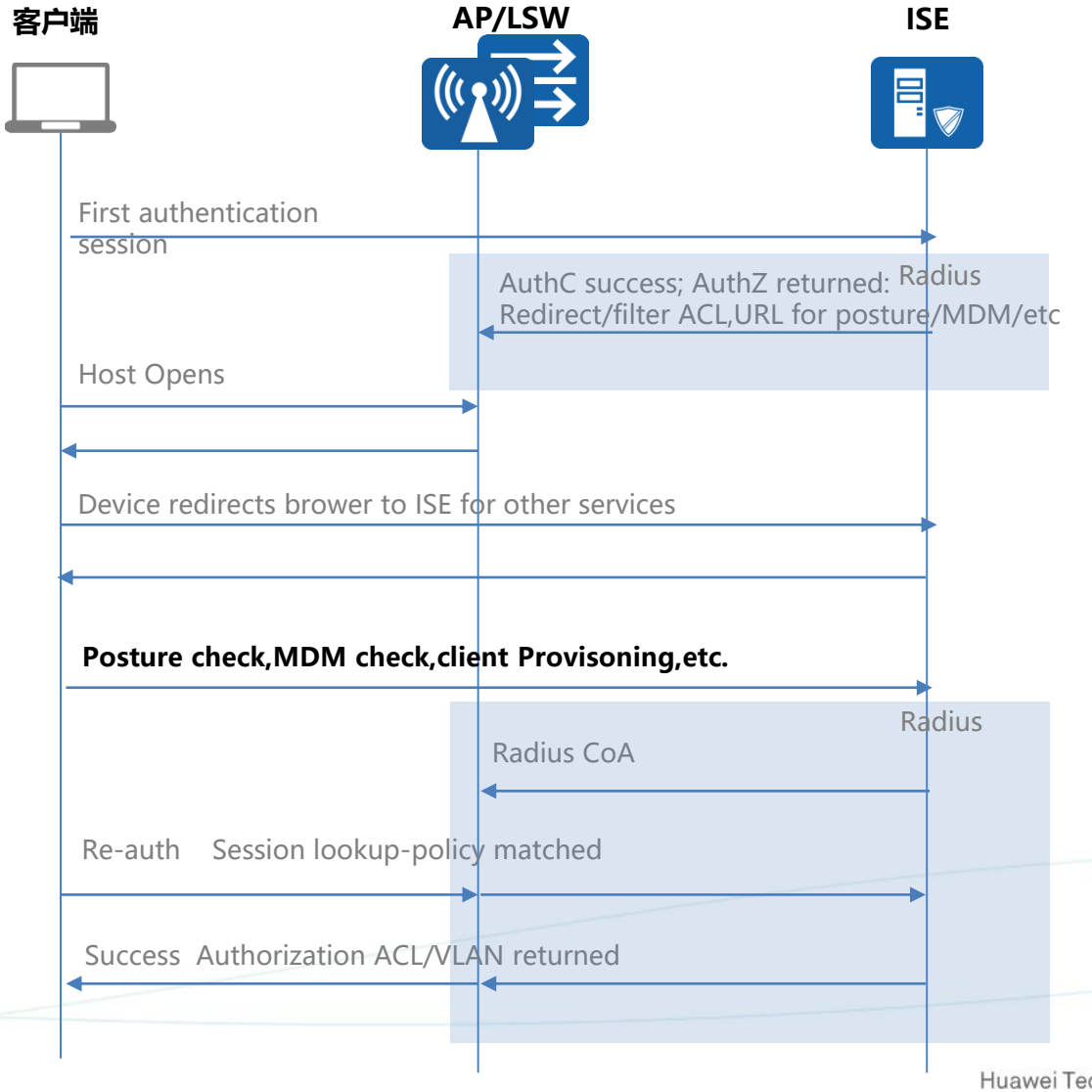
- **配置用户接入端口**

```
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
 authentication-profile mab
```

ISE对接 – 终端安全（Posture）



安全检查项目
操作系统补丁检查
进程检查
注册表检查
文件检查
应用程序检查
防病毒软件安装检查
防病毒版本/更新日期检查
防间谍软件安装检查
防间谍软件版本/更新日期检查
Windows更新运行检查
Windows更新配置检查
WSUS遵从性设置



ISE对接– 终端安全检查（Posture）示例

思科ISE端配置

1. **上传Anyconnect部署包至ISE (**包括Anyconnect安装包及compliance组件包)，**创建客户端推送策略.**
2. **配置安全检查条件及修复策略**
3. **配置授权结果。**
   - 为Unknown，Non-Compliant及Compliant终端安全状态创建授权结果； Unknown和Non-Compliant的授权结果可以使用同一个，即下发重定向ACL和重定向URL（到ISE的CPP URL）
4. **终端安全检查的重定向授权结果包括如下属性：**
   - **重定向ACL（必选）**：通过HW-Redirect-ACL属性下发，ACL内容需要在设备上配置，ACL中匹配permit rule的流量会被重定向到ISE的Posture URL
   - **重定向URL（必选）：**通过**Cisco-av-pair**属性（实际通过HW-Portal-URL）下发
   - **动态ACL（可选）**：可以通过标准Filter-id或者华为私有HW-Data-Filter属性下发，目的是控制用户还未通过安全检查时的网络权限
5. **为终端状态为unknown、Non-Compliant及**Compliant的接入请求创建授权策略；
   - 授权策略中session：PostureStatus是必选的匹配条件

华为设备端配置样例

- **配置Radius Server模板**

```
radius-server template ISE
 radius-server shared-key cipher xxx
 radius-server authentication 192.89.12.248 1812 weight 80
 radius-server accounting 192.89.12.248 1813 weight 80
 undo radius-server user-name domain-included
 calling-station-id mac-format hyphen-split mode2
 radius-attribute set Service-Type 10 auth-type mac
```

- **配置授权服务器参数**

```
radius-server authorization calling-station-id decode-mac-format ascii hyphen-split commonsplit radius-server authorization 192.89.12.248 shared-key cipher xxx
```

- **配置AAA参数**

```
 aaa
  authentication-scheme ise
  authentication-mode radius
accounting-scheme ise
  accounting-mode radius
  accounting start-fail online
domain default
  authentication-scheme ise
  accounting-scheme ise
  radius-server ISE
```

- **配置接入及认证模板**

```
authentication-profile name test
 dot1x-access-profile dot1x
 mac-access-profile mab
 authentication dot1x-mac-bypass
dot1x-access-profile name dot1x
mac-access-profile name mab
 mac-authen username macaddress format with-hyphen normal uppercase
```

- **配置用户接入端口**

```
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
 authentication-profile test
```

- **配置重定向ACL（Deny表示不重定向，匹配permit规则流量被重定向**

```
acl number 3002    ///ACL id与授权结果中HW-Redirect-ACL值相同
 rule 1 deny udp destination-port eq dns
 rule 2 deny udp source-port eq dns     放通DNS流量
 rule 3 deny udp destination-port eq bootps
 rule 4 deny udp destination-port eq bootpc
 rule 5 deny udp source-port eq bootpc
 rule 6 deny udp source-port eq bootps  放通DHCP流量
 rule 7 deny ip destination 192.89.11.79 0  放通目的地址为ISE服务器的流量
 rule 8 permit ip
```

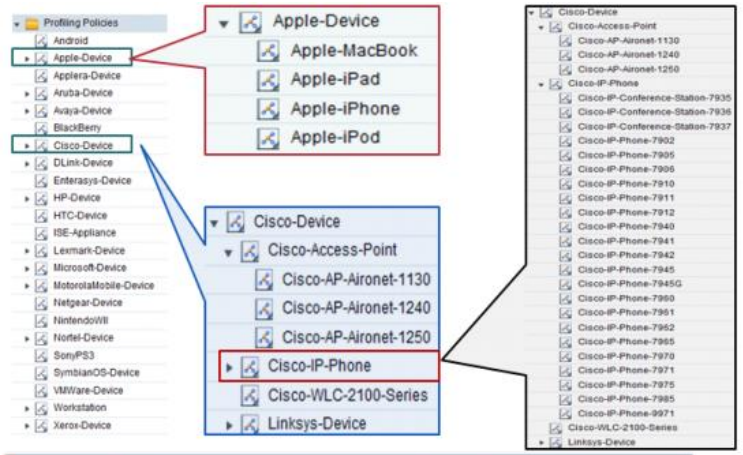
ISE对接 – 终端安全（Posture）

对接能力

监控接入企业园区的设备有无按照企业规定安装防病毒软件/最新系统补丁/手机未Root等。

终端安全检查项	LSW	WLAN	终端安全检查项	LSW	WLAN
Client Provisioning (Desktop Posture)-AnyConnect	Y	Y	Posture assessment （Misc） File data Services Applications / Processes Registry Keys Patch Management Personal FW USB Check	Y	Y
Client Provisioning (Desktop Posture)-NACConnect	Y	Y	Authenticate based on Posture status(Unkown/Compliant/Not Compliant)	Y	Y
Client Provisioning (Desktop Posture)-WebConnect	Y	Y	Quarantine(dVLAN/dACLs)	Y	Y
Posture assessment on Windows OS platforms: Microsoft Windows 7, 8, or 10 (32-bit or 64-bit)	Y	Y	Remediate Microsoft SCCM Launch App Scripts	Y	Y
Posture assessment on MAC OS platforms: Mac OS X 10.7, 10.8, 10.9, or 10.11	Y	Y	Authorize(VLAN/dACLs/URL Redirect)	Y	Y
Posture assessment （Microsoft Updates） Service Packs Hotfixes OS/Browser versions	Y	Y			
Posture assessment （Antivirus/ Antispyware） AV/AS	Y	Y			

ISE对接 – 终端识别Profiling



Probe	Data Provided
RADIUS	OUI, MAC Address
DHCP	DHCP attributes, hostname
DNS	FQDN, hostname
HTTP	User-Agent
NMAP	OS fingerprint
NETFLOW	TCP/UDP ports used
SNMP	MIB strings

终端识别场景及流程

1. 用户终端第一次上线时（此时终端未识别）匹配MAB公共的授权策略;
2. ISE上配置终端识别策略，通过MAC OUI、DHCP镜像或SNMP方式匹配到策略后识别出终端类型，并将终端MAC加入对应的Endpoint Group;
3. ISE识别出终端类型后对当前在线用户下发重认证或者Port Bounce CoA（在终端识别策略中定义）触发用户重新认证上线，此时会通过Endpoint Group条件匹配到更精细的授权策略，实现不同类型终端分类权限控制
4. 利用报文Probe（DHCP、Radius等）、MIB等收集终端信息，根据其中的有效字段判定属于哪种终端类型。数据越多识别的类型越精确。

授权方式	LSW对接支持情况	WLAN对接支持情况	备注
CDP/LLDP	N	N	思科交换机支持CDP和LLDP方式识别终端用户，并通过私有属性封装LLDP和CDP属性后上传Radius服务器，华为交换机不支持 CDP终端识别，也不支持通过私有属性上传
SNMP	N	N	ISE支持通过SNMP的方式读取接入设备上的MIB信息用来判断终端类型，华为交换机不支持
MAC	Y	Y	
DHCP	Y	Y	
HTTP	Y	Y	
Radius	Y	Y	
NMAP	Y	Y	
SPAN	Y	Y	
AD	Y	Y	

ISE对接– 终端识别(Profiling)示例

思科ISE端配置

1. **配置终端识别条件（以MAC OUI识别为例）。**

2. **创建终端识别策略。**
   - 一般在识别后，会自动创建一个跟策略同名的EndPoint Group 组。
   - 识别出终端类型后对当前在线用户下发重认证或者Port Bounce CoA（在终端识别策略中定义）触发用户重新认证上线，此时会通过Endpoint Group条件匹配到更精细的授权策略，实现不同类型终端分类权限控制

3. **创建认证及授权策略.**
   - 识别后终端的授权策略，通过EndPoint Group 匹配
   - 授权策略中，公共的授权策略位置应在精细化的授权策略下面；

华为设备端配置样例

- **配置Radius Server模板**

```
radius-server template ISE
 radius-server shared-key cipher xxx
 radius-server authentication 192.89.12.248 1812 weight 80
 radius-server accounting 192.89.12.248 1813 weight 80
 undo radius-server user-name domain-included
 calling-station-id mac-format hyphen-split mode2
 radius-attribute set Service-Type 10 auth-type mac
```

- **配置授权服务器参数**

```
radius-server authorization calling-station-id decode-mac-format ascii hyphen-split common split radius-server authorization 192.89.12.248 shared-key cipher xxx
```

- **配置AAA参数**

```
 aaa
  authentication-scheme ise
  authentication-mode radius
accounting-scheme ise
  accounting-mode radius
  accounting start-fail online
domain default
  authentication-scheme ise
  accounting-scheme ise
  radius-server ISE
```

- **配置接入及认证模板**

```
authentication-profile name test
 mac-access-profile mab
mac-access-profile name mab
 mac-authen username macaddress format with-hyphen normal uppercase
```

- **配置用户接入端口**

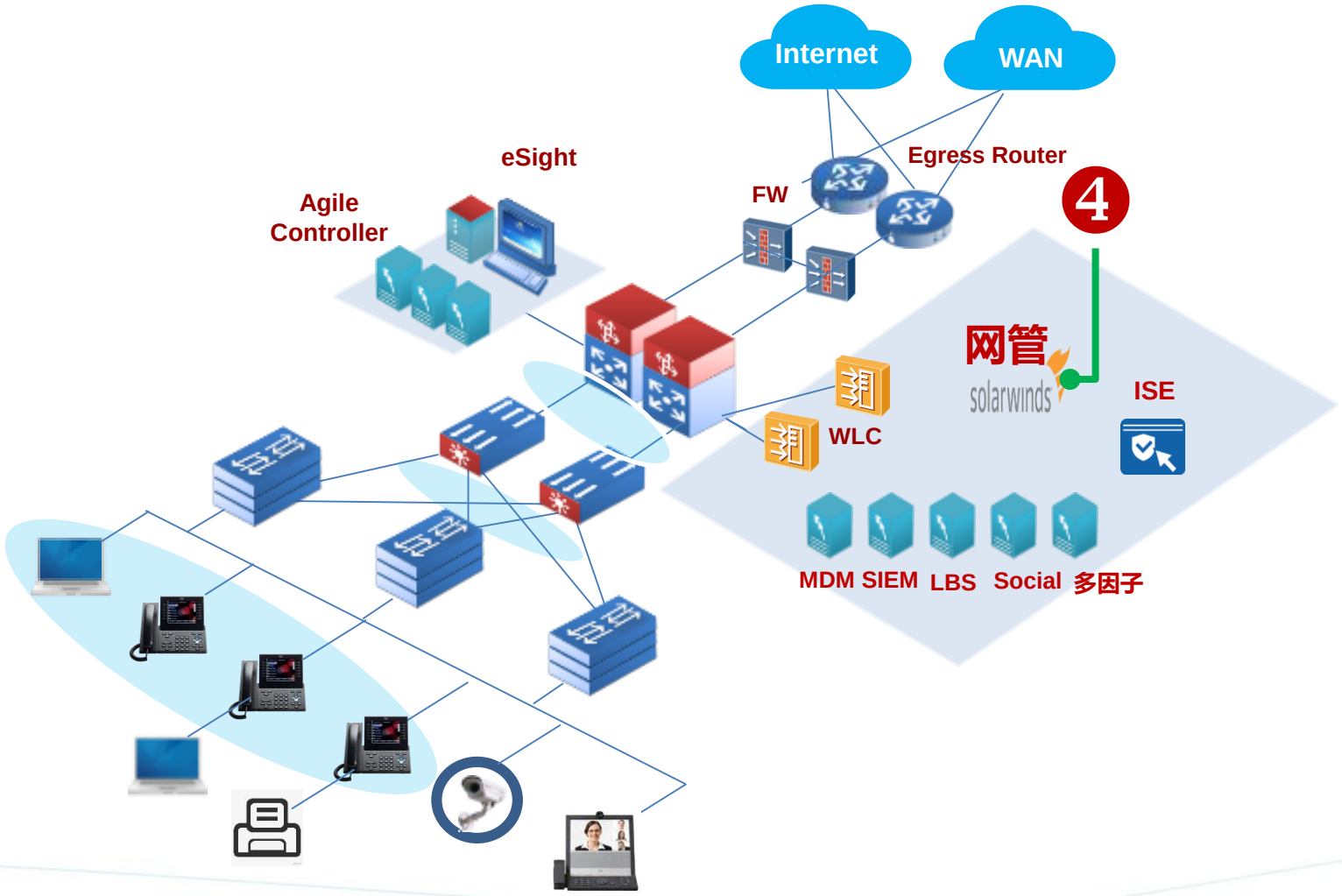
```
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
 authentication-profile mab
```

ISE整体兼容性结果

特性	兼容性	备注
802.1x	Compatible	
MAC Authentication	Compatible	
Web Authentication	Compatible	No URL-Rdirect with session information
Authorization	Compatible	
Profiling Probes	Limitations	仅支持Radius、DHCP等探针，对于cisco私有的MIB以及CDP等其他探针不支持；
RADIUS Change of Authorization	Limitations	支持标准的COA属性，但是对于私有的属性并不支持；
Posture Assessment	Limitations	

网络管理

第三方网管兼容性



1. 网管对接原理
2. Solarwinds兼容性
3. CA网管兼容性

网管对接

网管对接概述

- 目前网管使用最为广泛的管理协议还是SNMP（Simple Network Management Protocol）
- 华为设备完整支持SNMP，包括SNMPv1, SNMPv2c, SNMPv3
- 网管通过**SNMP**协议调用**MIB**对设备进行管理
- 华为设备**支持包括ENTITY-MIB、 IF-MIB 、 RFC1213-MIB**等50多个标准MIB，完全可以被其他同样支持这些标准MIB的第三方网管统一管理
- **标准MIB**一般只能完成设备管理、告警采集和部分业务的管理，要全面管理第三方设备还需要适配厂商的私有MIB
- 目前经过验证测试的第三方网管包括**Solarwinds**和**CA Technology**

第三方网管之Solarwinds

solarwinds

一家专门提供IT基础设施管理系统的公司

网管可对多厂家组网进行集中管理

数十
厂家网络管理

- 华为
- 思科
- HP
- Juniper
- Dell
- Extreme
- …

强大的
网络管理功能

- 性能
- 流量
- 配置
- 终端
- 链路
- 拓扑

应用场景

场景1：友商存量园区网络，搬迁部分友商设备后，形成多厂家混合组网。

需求：对多厂家混合组网进行集中网络管理。

场景2：新建网络，由专业的管理服务供应商托管。

需求：管理服务供应商维护多套网络，各厂家混合组网，要进行集中网络管理。

华为设备与SolarWinds网管的对接验证，相对系统完整， 包括了设备发现、Poller管理、设备状态查询、无线信号状态查询、网络配置管理、流量监控、报表管理、告警时间管理等

Solarwinds 与华为园区网络设备对接能力

协议：

SNMP、ICMP、TELNET/SSH(CLI)、syslog、netstream

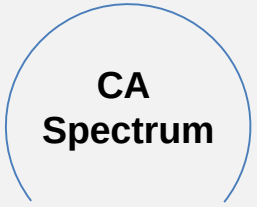
产品：

交换机、WLAN AC和AP

分类	功能点	测试结果
基础功能	添加设备	√
	设备管理	√
	查看设备告警、日志、trap	√
NPM	端口管理	√
	AC管理(目的是管理AP和用户)	√
	自定义监控	√
LEM	设备对接	√
	日志显示	√
	日志解析	√
NTA	设备对接	√
	数据监控	√
NCM	配置管理	√
	配置变更历史记录	√

第三方网管之CA Technology

CA专门生产和开发企业用的管理软件
CA的Spectrum和Performance软件提供网络管理、配置、性能等功能



网络故障管理

网络性能监控

应用场景

场景1：友商存量园区网络，搬迁部分友商设备后，形成多厂家混合组网。

需求：对多厂家混合组网进行集中网络管理。

场景2：新建网络，由专业的管理服务供应商托管。

需求：管理服务供应商维护多套网络，各厂家混合组网，要进行集中网络管理。

华为设备与CA对接成熟度与SolarWinds相似

CA Spectrum和CA Performance与华为园区网络设备对接能力

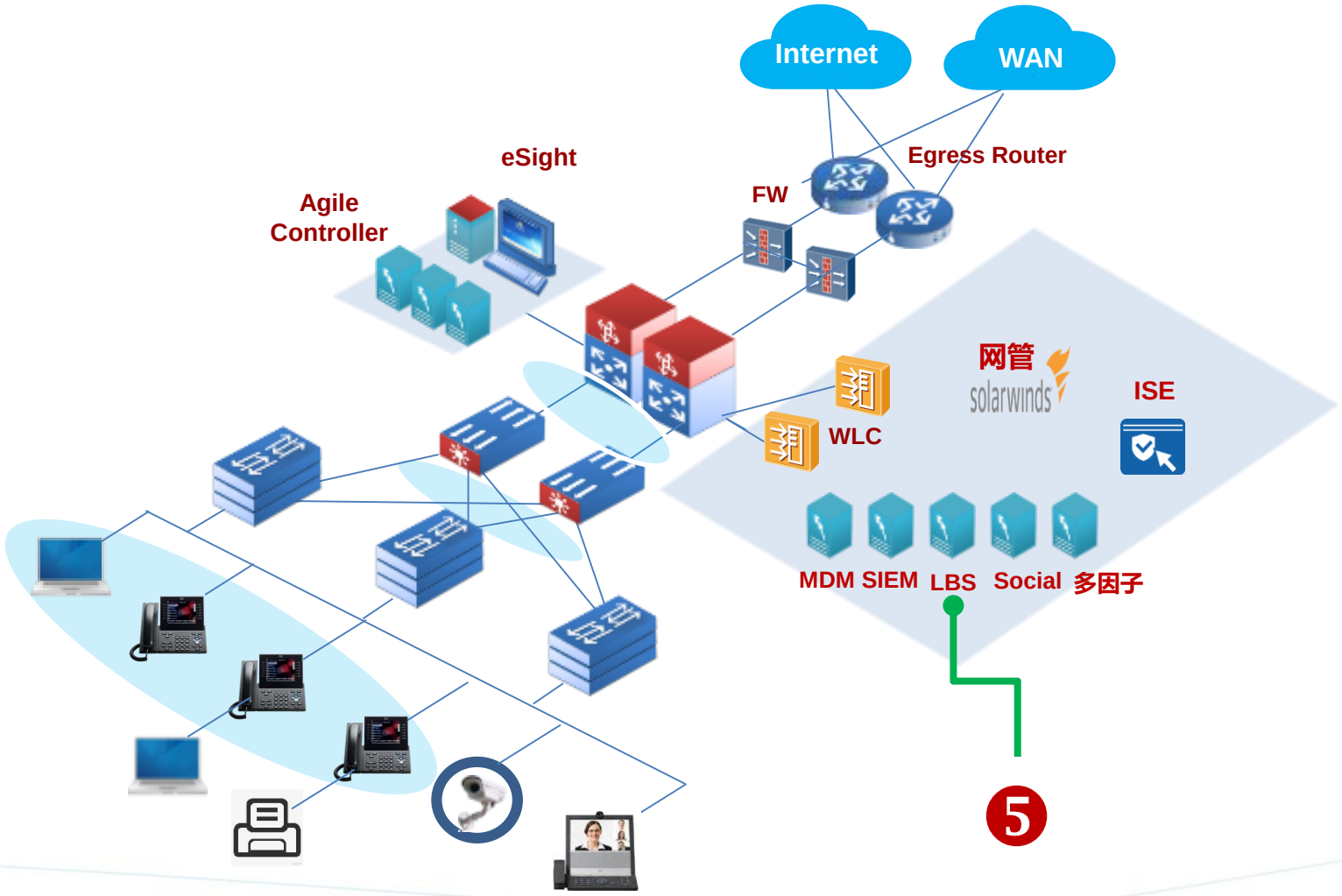
协议： SNMP、ICMP、TELNET/SSH(CLI)、Syslog、Netstream

产品： WLAN AC和AP

	功能点	测试结果
CA Spectrum	设备发现	√
	查看网络设备配置	√
	对之前不支持的设备自认证	√
	管理警报并分析原因	√
	展示维护模式	√
	基于策略的告警通知	√
	报警，资产和可用性报告	√
CA Performance	多租户	√
	性能测试	√
	对之前不支持的设备自认证	√
	设备组计分趋势图	√
	性能告警，报告和仪表盘	√
	动态分组	√

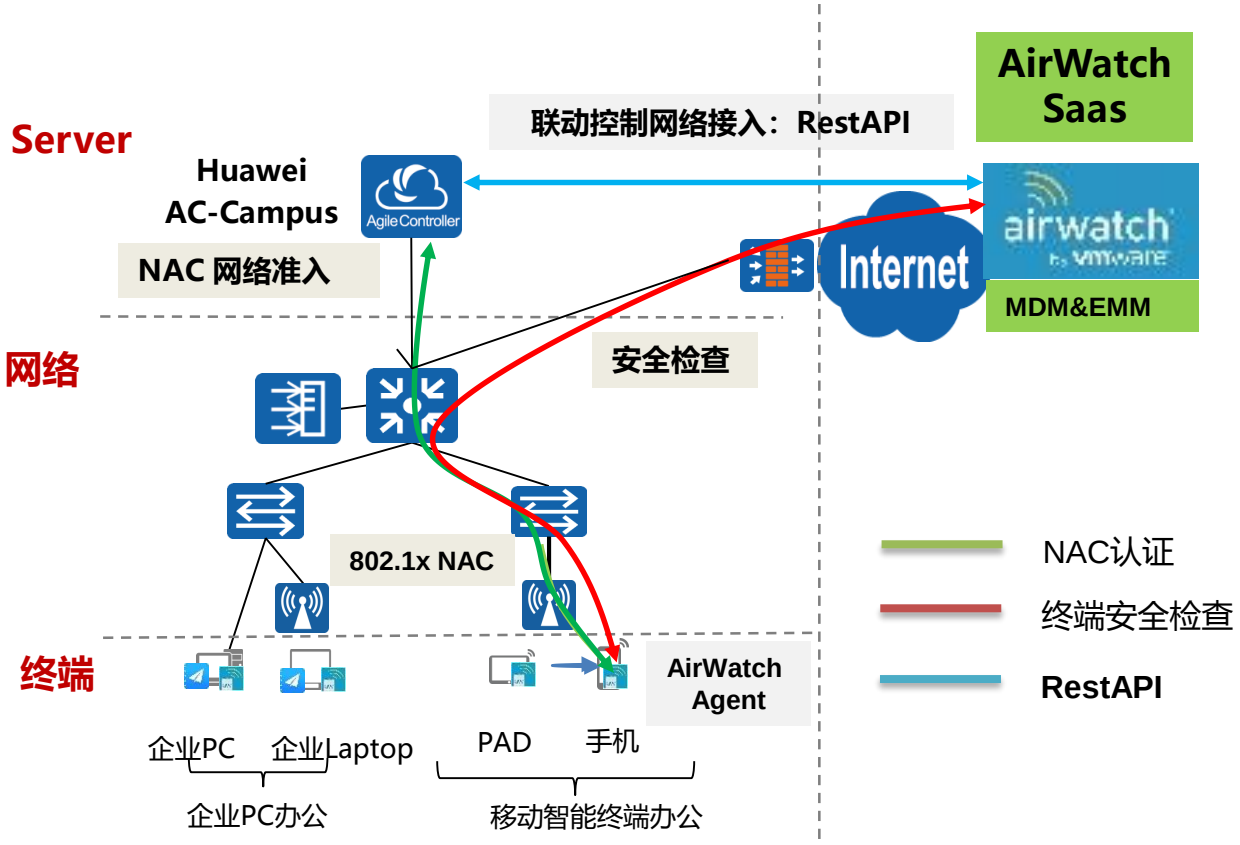
增值系统

第三方增值系统集成



1. MDM集成
2. SIEM集成
3. LBS系统集成
4. 社交账号集成
5. 多因子认证系统集成

AirWatch MDM服务对接方式



AC-Campus与Airwatch MDM集成方式

终端

- 智能终端上部署Airwatch Agent

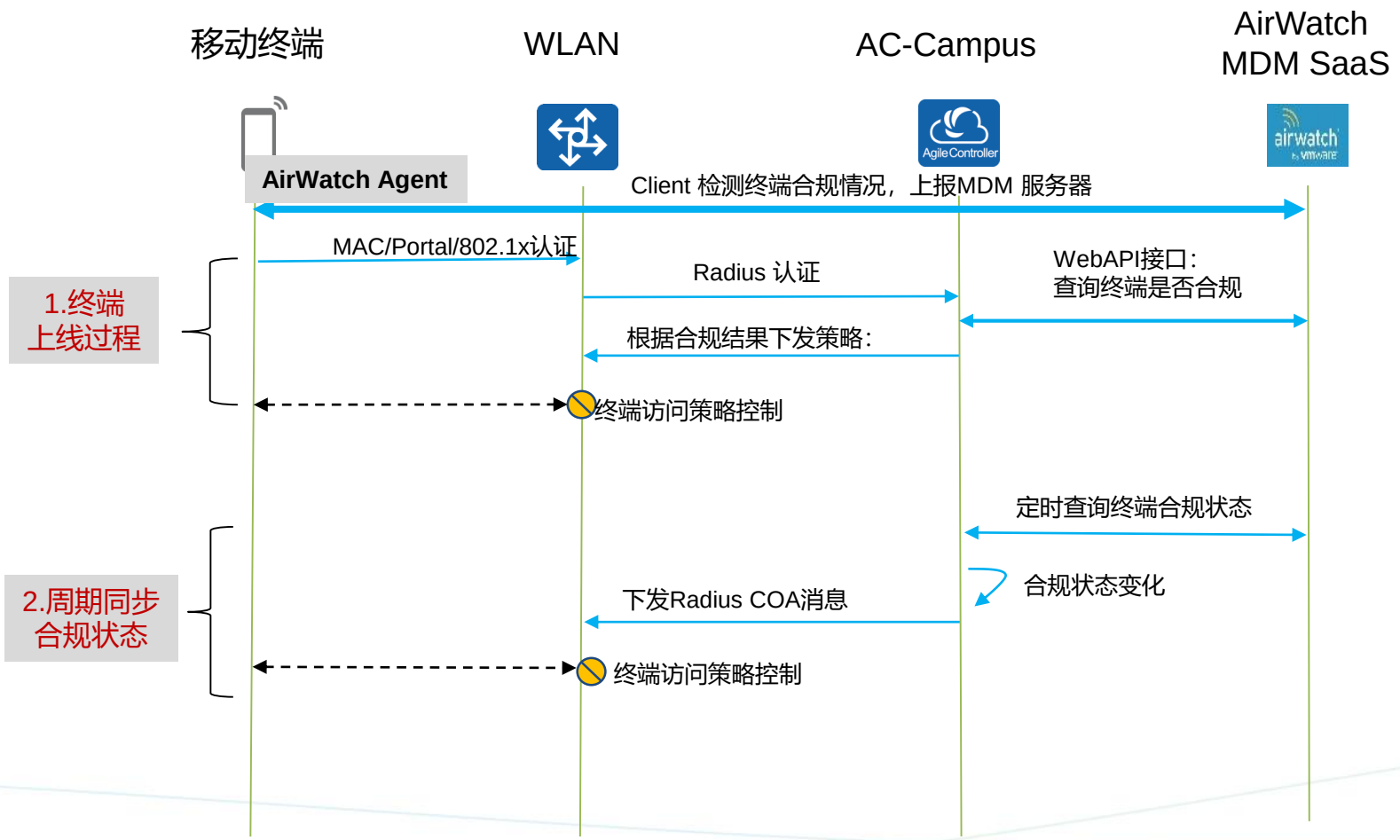
服务器端

- 终端通过AC-Campus 完成NAC认证
- AC-Campus通过**RestAPI**接口集成Airwatch 的**MDM/EMM Saas**服务

AC-Campus与Airwatch注意事项：

- 若客户要求MDM检查设备安全状态，进行网络接入控制，则需要两者进行集成
- 若客户要求进行内容访问等应用控制，可以通过Airwatch 应用层控制，Airwatch 可独立部署，不需要跟AC-Campus集成

AirWatch MDM服务对接工作流程图



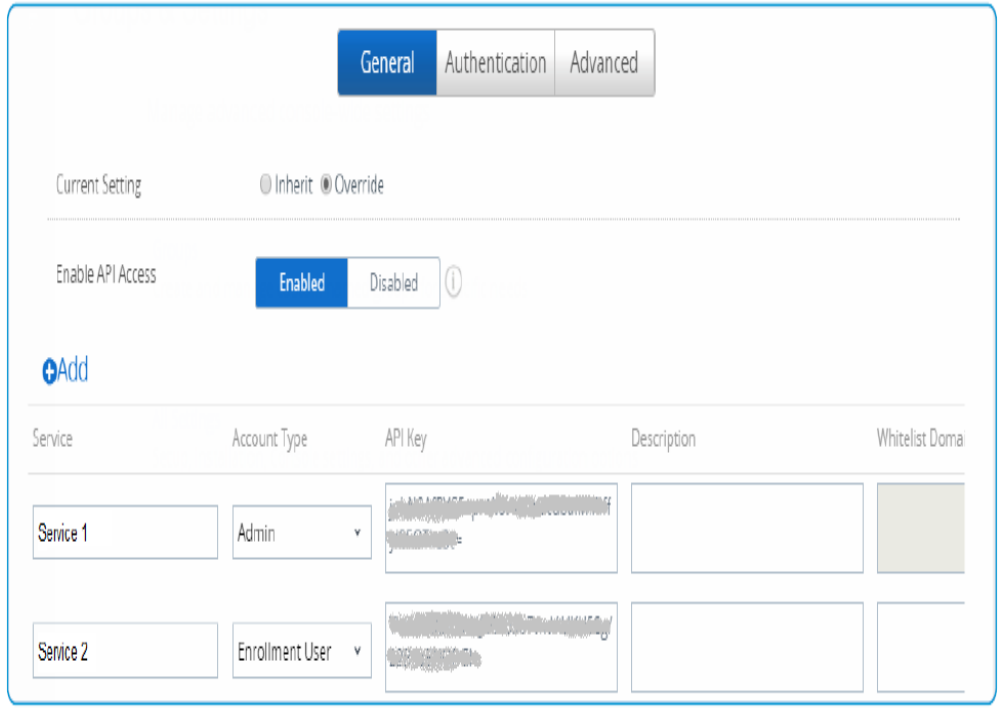
关键过程：

1、 终端上线发起认证时，Agile Controller-Campus 1.0 调用Resf API接口，查询终端合规状态。Controller 根据合规结果，对终端下发相应的授权策略

2、 Agile Controller-Campus 1.0 周期 调用接口，与Airwatch MDM Server同步终端合规状态

相关技术细节可以参见 3ms 技术白皮书
http://3ms.huawei.com/mm/docMaintain/mmMaintain.do?method=showMMDetail&f_id=EDC180603103537246

AC-Campus 与AirWatch集成配置 – AirWatch端



WMware AirWatch的配置分为两大部分

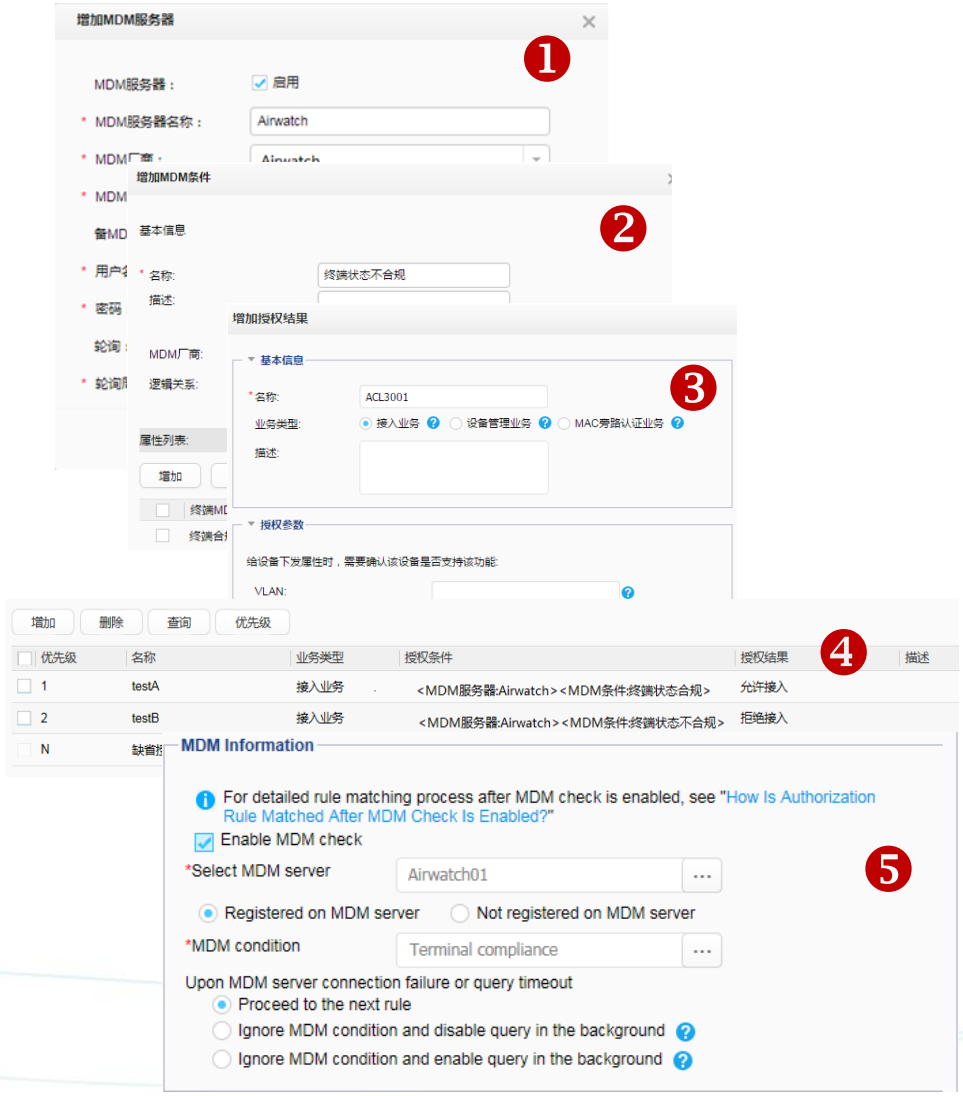
1. 与MDM业务相关配置，该配置请参考Airwatch 配置手册，不在这里描述， 参考配置

2. 与Agile Controller 对接配置， MDM API配置：

a) 登录到AirWatch主页面导航到：Groups & Settings > All Settings > System > Advanced > API >REST API

b) 配置 API 账户以及 API Key

AC-Campus 与AirWatch集成配置 – Agile Controller端



1. Agile Controller 上添加AirWatch的**MDM**服务器。选择“系统 > 外部认证源 > MDM服务器配置”，添加AirWatch：

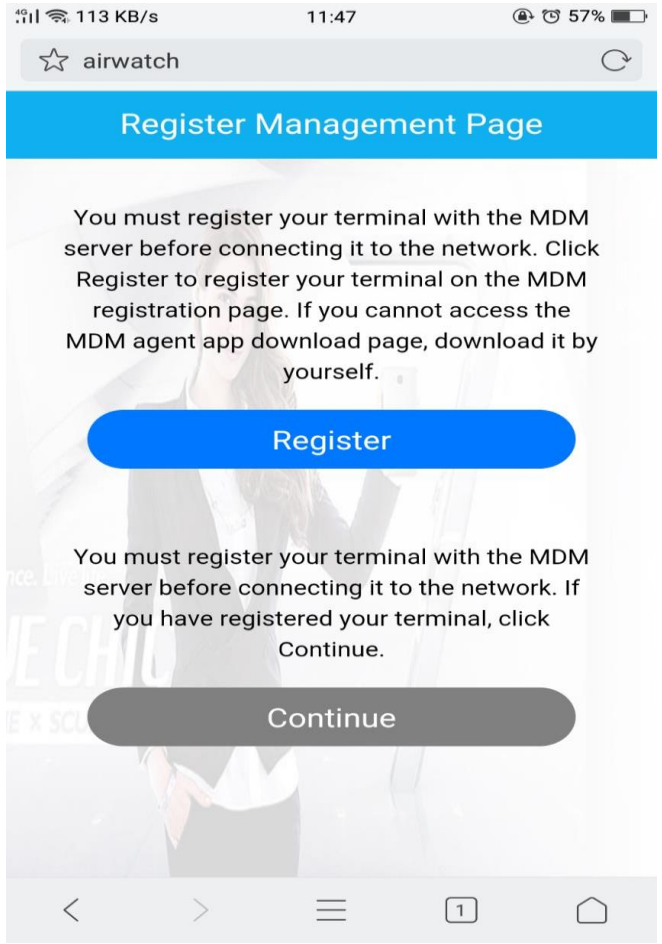
2. 添加**MDM条件**。在授权规则中根据MDM条件授权， 选择“策略 > 准入控制 > 策略元素 > MDM条件”，添加MDM条件

3. **添加授权结果**，分别用于符合MDM条件和不符合MDM条件的移动设备授权。选择“策略 > 准入控制 > 认证授权 > 授权结果”，ACL编号与认证控制设备配置一致：

4. 针对终端状态合规和终端状态不合规分别授权，未注册移动设备使用缺省授权规则，并将缺省授权规则修改为禁止接入，选择“策略 > 准入控制 > 认证授权 > 授权规则”

5. 配置未注册终端弹出注册页面规则。

AC-Campus 与AirWatch集成结果



未注册终端用户，弹出Portal页面，提示需要注册

网络访问控制：

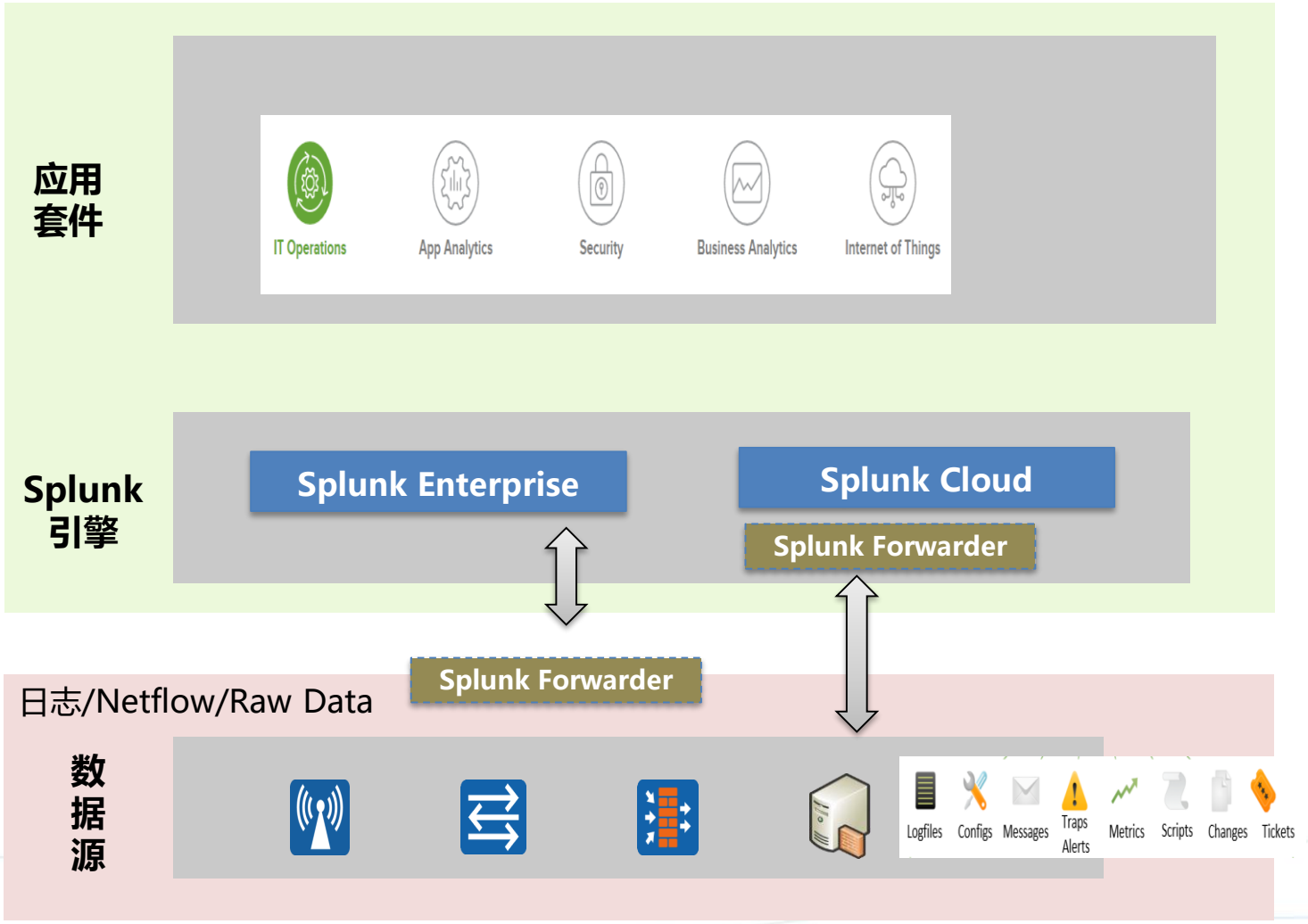
根据移动设备的状态, 终端用户进行网络访问授权

1. 如果移动设备满足管理员在AirWatch所配置的检查策略，能够访问受控域和Internet。
2. 如果移动设备不满足管理员在 AirWatch所配置的检查策略，只能Internet。
3. 如果移动设备未在AirWatch注册，无法访问任何资源。

集成相关限制：

1. 对于Windows 系统终端，Airwatch 仅支持Windows 10 及以上版本
2. 对于Andriod 终端， 中国区禁用Google相关服务，AirWatch无法获取终端MAC地址。 集成方案在中国区以及其他禁用Google服务的地区不可用。

Splunk集成原理



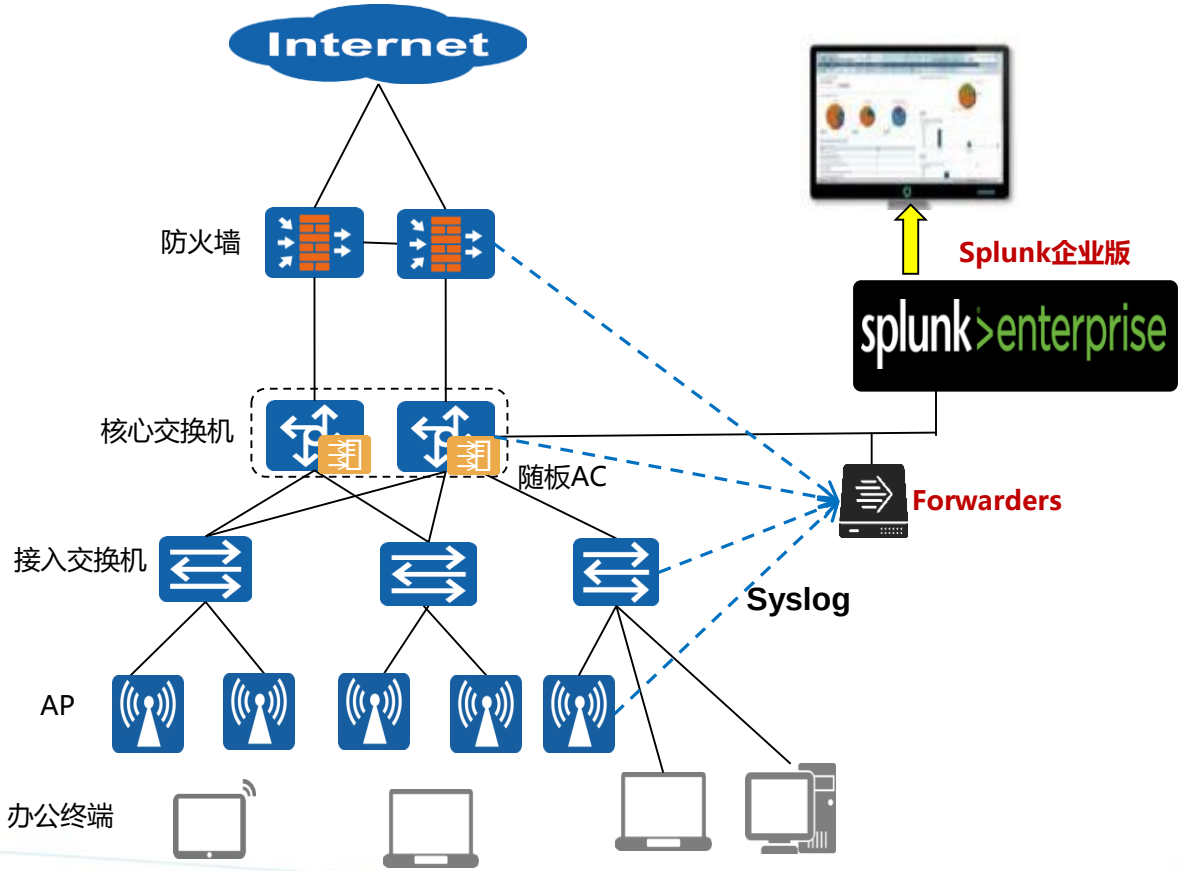
Splunk集成分为几个部分

1. **数据源**： **Splunk**使用Splunk Forwarder 从各种端点采集数据信息。Splunk Forwarder 可以本地部署，也可以云部署。园区网络中各种网络设备可以作为数据源。

2. **引擎**： 实现数据接收、存储、索引数据。可以本地部署，也可以云部署。

3. **应用套件**： 可以自定义应用规则，进行结果呈现。

Splunk集成方式



集成方式

1. 园区网络设备配置syslog，上送至Splunk Forwarder。 配置命令： info-center loghost x.x.x.x
2. Splunk上配置相关分析应用实例
3. 则在Dashboard 上看到相应的结果

注意事项

1、 **Splunk** 相关应用实例，可以作为App 在Splunk 官方发布。Cisco 已经发布了大量App.

2、 我司园区网络设备支持标准syslog与Splunk集成，除此以外的深度集成需要开发定制

敏捷园区互联互通能力总结

类型	子类型	示例	兼容能力	注释及后续计划
❶ **网络协议**	Layer2/Layer3/HA	PVST/EIGRP/HSRP	★★★★☆	网络协议兼容性较好
❷ **终端设备**	IT	IP Phone/AP	★★★★	新终端测试来源，市场分析，项目触发。
	OT	Scanner, Printer	★★★☆	对接OT设备少，后续会增强
❸ **NAC**	**NAC+ Huawei device**	ISE	★★★★	与ISE 2.X兼容性较好，计划纳入更多的NAC Server, 如 NPS, Free Radius etc.
	AC1.0+Other Vendor Device	Cisco	★★★	与友商设备只做过初步对接，没有经过系统完整的验证和测试
	Device Admin	TACACS+	★★★☆	支持标准协议，经过基本的验证。
❹ **NMS**	**Network Manager**	Solarwinds	★★★★	标准SNMP协议支持较好，与Solarwinds集成验证过，兼容性较好，目前正对HP, CA NMS验证。
	Log System	Kiwisyslog	★★★☆	支持标准的**Syslog**协议，但没有实际对第三方Log系统进行过验证。
❺ **第三方增值系统**	**MDM**	AirWatch	★★★☆	只跟跟Airwatch的SaaS平台对接过。 无实际落地案例，后续其他厂商集成基于项目触发。
	SIEM	Splunk	★★★	支持通过标准syslog协议对接
	LBS	Bluetooth Beacon	★★★	eSight定位引擎能力较弱，不支持商用。定位方案依赖于第三方合作伙伴。
	Social Login	Facebook	★★★★☆	集成能力较强，与主流社交账号都有集成方案。

Thank You.