

AD campus方案简介

基础服务部-业务软件

2016年4月

目录

- 网络新趋势
- AD campus方案
- AD campus实施



当前网络IT模型的问题

当今 IT 模型 – 网络运行压力沉重
没有时间再做其他任何事情



80–90%

网络运行



10–20%

实现创新

0 秒

10 秒

100 秒

1,000 秒

10,000 秒

IoT 扩展

繁琐缓慢

难以配置应用程序

难以故障排除

超慢的服务部署速度

Overlay技术给网络的带来好处

■ Overlay网络

- 基础网络可以自动化建立
- 用户标识与位置解耦，终端可以在Fabric内任意移动而IP不变
- 用户标识与策略解耦，网络service任意位置部署



- Overlay网络易于分片，网络资源**虚拟化/池化**。适合用户网络的**动态**建立。由于动态，就更易于**自动化**，更易被controller控制。



引入Overlay技术给园区网SDN策略带来的好处

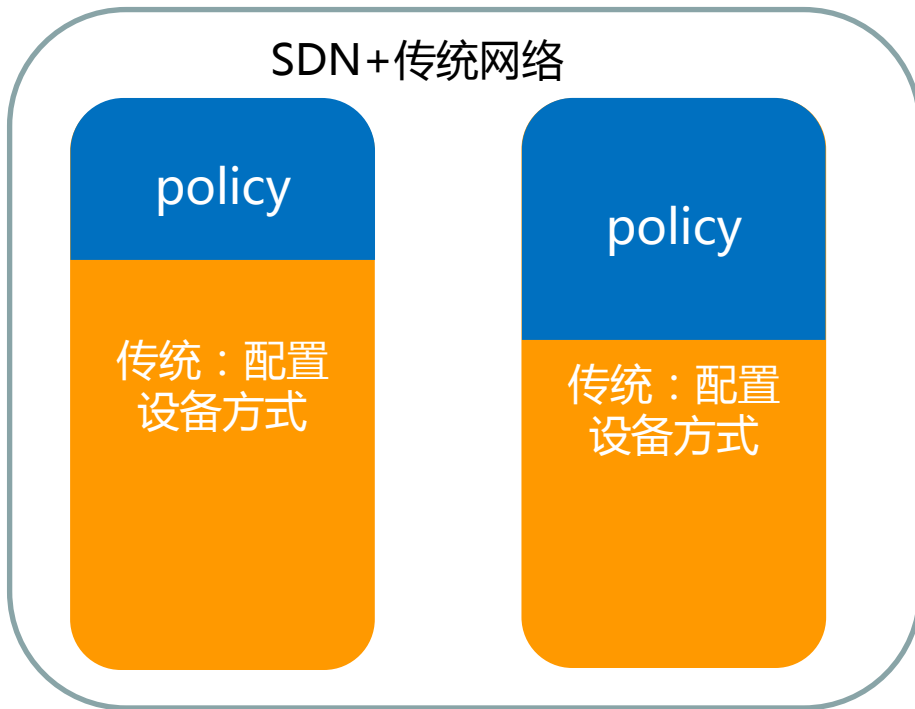
终极目标
本质好处

园区SDN策略在自动化方面的演进：

当前：无SDN



SDN+传统网络



SDN+Overlay网络



Overlay网络强化SDN的战略目标：自动化，业务感知，可编程

目录

- 网络新趋势
- **AD campus方案**
- AD campus实施

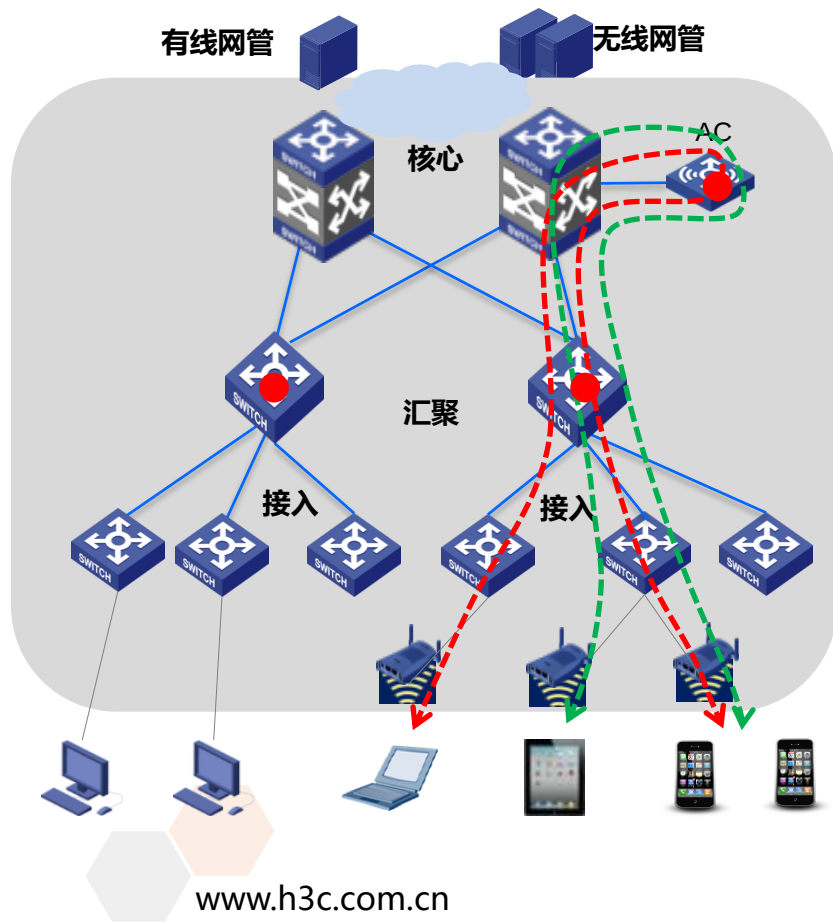


目录

- AD campus方案
 - 有线无线深度统一
 - 策略随行
 - IP绑定



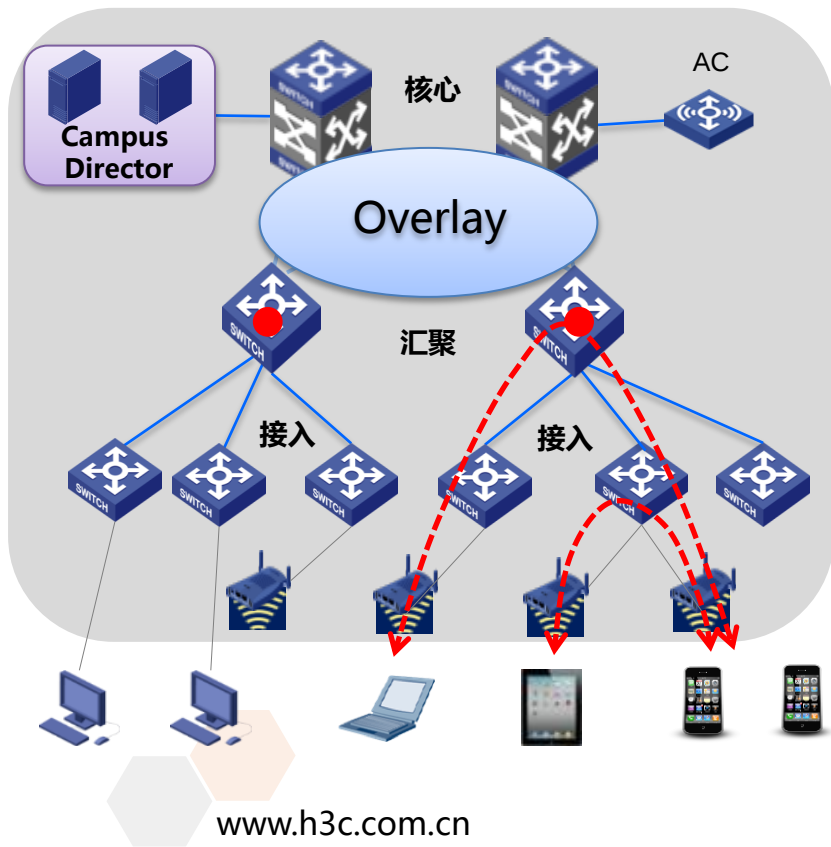
当前园区无线网络的问题



- 无线网络单独建设与管理，与有线网络割裂。
- 无线数据流量集中式转发，AC成为无线网性能瓶颈（尤其在11ac环境下），AC成本高
- 无线网络的策略控制点在AC, 与有线网络的策略控制分离

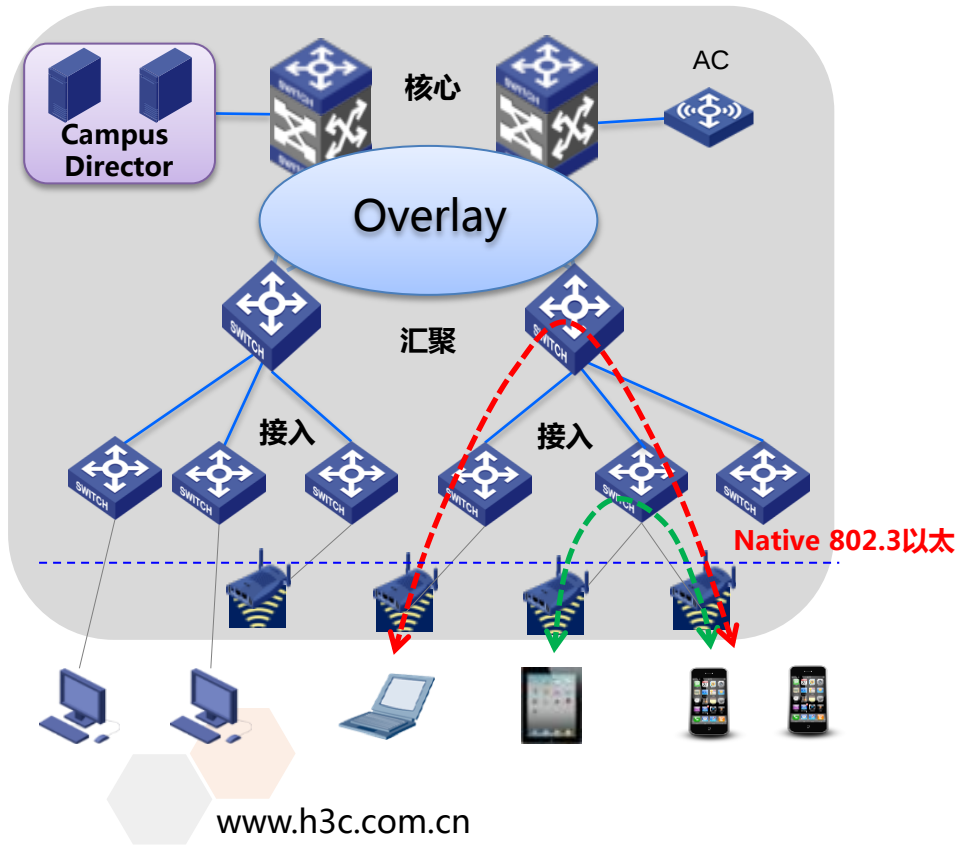
有线无线深度统一的园区网架构

基于统一架构的融合管控：One Network，One Policy，One Management



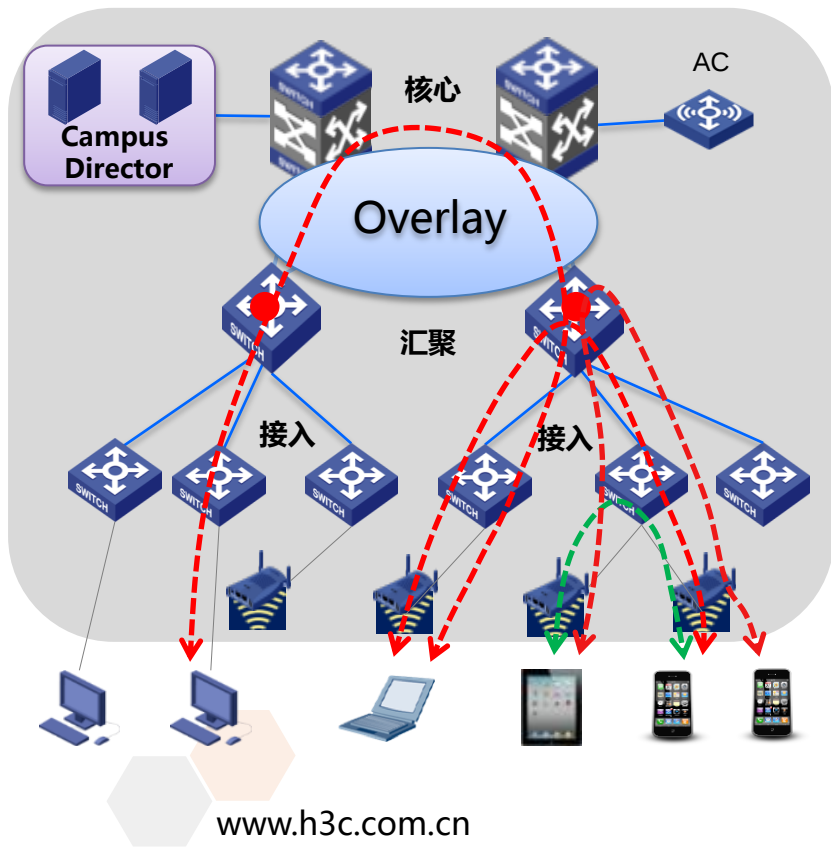
- One Network---统一数据转发
 - 无线流量不做capwap封装，AP上行到交换机的流量为native以太网报文，和有线统一，不再绕行到AC
 - 流量可以统一调度和监控。
- One Policy---统一策略执行
 - 访问控制策略统一由Director提前下发至汇聚层交换机。
 - 有线和无线终端在园区范围内移动和漫游，策略不变。
- One Management---统一网络管理
 - Director统一管理有线和无线网络
 - 有线用户与无线用户统一使用5W1H来划分安全组。

有线无线统一数据转发



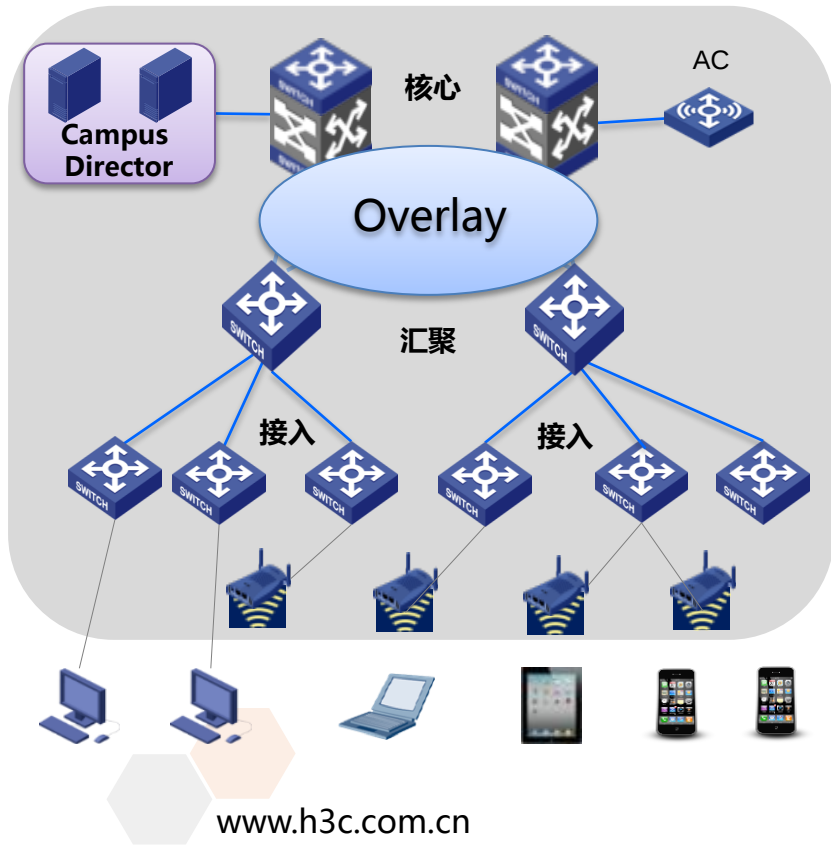
- 无线流量不做capwap封装，AP上行到交换机的流量为native以太报文，和有线统一，不再绕行到AC；
- AC不再处理数据平面，只负责AP射频管理、无线用户认证、终端漫游等；降低AC成本；
- 有线无线流量可以统一调度和监控；
- 无线用户可在全网范围内漫游；

有线无线统一策略执行



- 策略集中配置，不区分有线还是无线
- 策略统一由Director提前下发至汇聚层交换机。
- 有线和无线终端在园区范围内移动和漫游，策略不变。

有线无线统一网络管理



- Campus Director统一管理有线无线网络
- 统一配置用户映射策略 (5W1H)
- 网络状态统一呈现

注：

5W1H (Whose、What、Where、When、Who、How)

具体包括

Who -- 接入帐号、终端

When -- 接入时段策略

Where -- 接入设备分组、SSID分组、AP分组

What -- 接入终端类型、操作系统、厂商

目录

- AD campus方案
 - 有线无线深度统一
 - 策略随行
 - IP绑定



传统方案存在的问题

- 传统方案1：静态ACL+动态VLAN
 - 交换机上预先配置ACL，ACL中描述了允许或禁止访问的服务器IP地址或网段，并与入方向的VLAN绑定
 - 用户认证上线时，认证服务器根据用户身份及接入位置等信息将用户分配至不同的VLAN
 - 不同的VLAN内的用户因为绑定的ACL不同，所以其网络权限也不同
- 传统方案1存在的问题
 - 需要提前在每台接入交换机创建VLAN并配置静态ACL，预配置工作量大
 - 增加用户组或修改用户组权限时，仍需要人工逐台交换机更改配置
 - 在允许用户移动的场景下，只能实现用户到资源的访问控制，无法实现不同用户组之间的访问控制



传统方案存在的问题

■ 传统方案2：静态VLAN+动态ACL

- 在交换机上根据接口静态划分VLAN，在用户认证上线时，认证中心根据用户身份分配关联的ACL。
- ACL跟每个用户——绑定，ACL的具体内容既可以在交换机上预配置，也可以由认证中心动态下发。
- 不同用户因为绑定的ACL不同，所获得的网络访问权限也不同

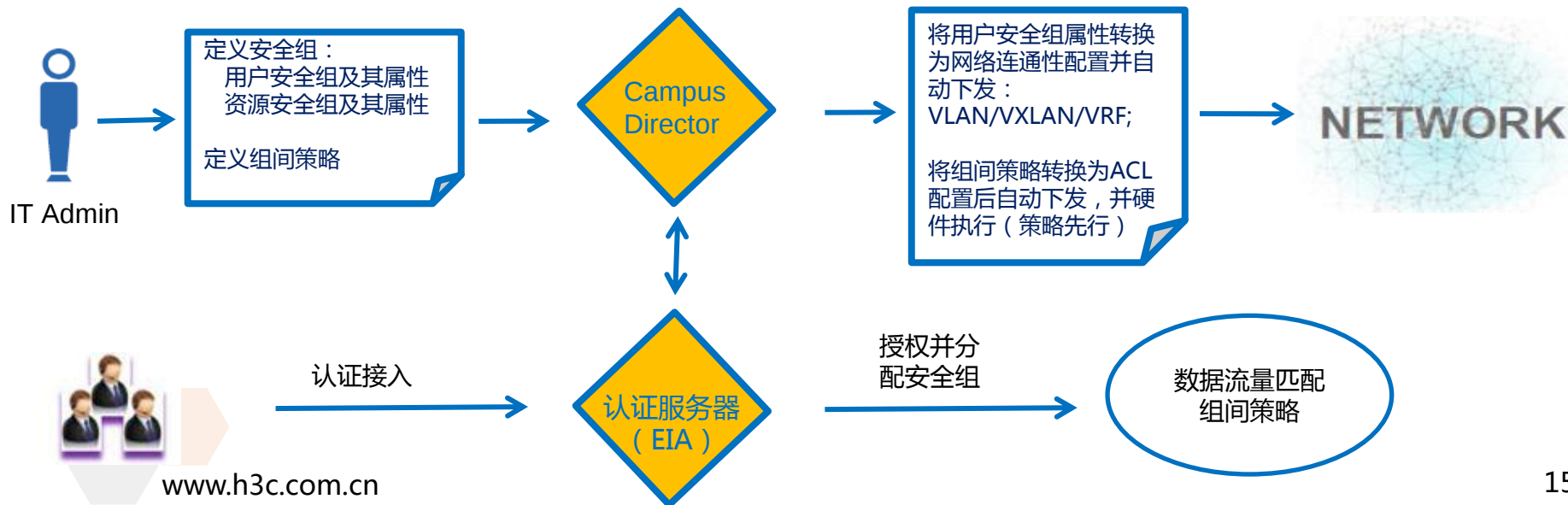
■ 传统方案2存在的问题

- 无法做到VLAN内用户互访的隔离。因为不同类型用户会获得同一网段的地址，用户之间互访隔离的ACL无法提前定义好。
- 虽然ACL可以由认证中心统一下发，以减少交换机上的ACL配置工作量。但是交换机采用硬件匹配ACL，此方案中ACL需要与用户——绑定，即使是同一个组中的不同用户也不能共享ACL。因此实际每条ACL包含的规则数量受限，否则会因交换机处理芯片支持的规则数量（TCAM表项数）不足而无法生效

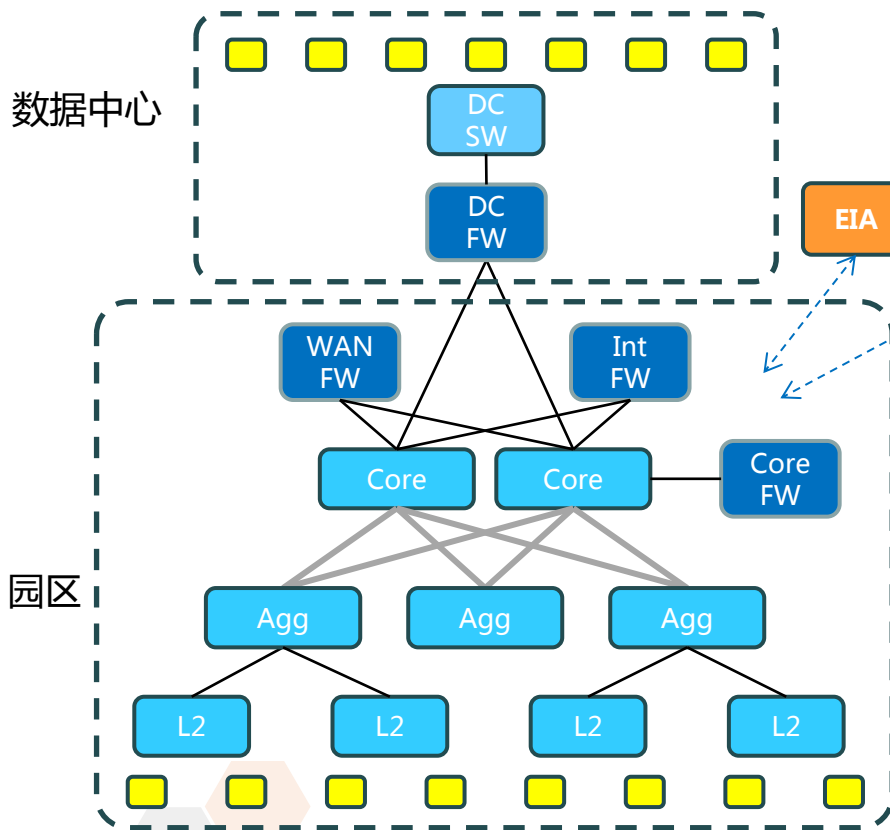


策略随行：方案总体思路

- 采用基于安全组的策略控制替代传统的VLAN/ACL的控制方案
- 管理员定义用户安全组及其属性（VLAN/VXLAN/IP网段）；服务器资源根据其网段或IP地址映射为资源安全组（静态）
- 管理员定义安全组的组间策略，Campus Director将安全组属性转换为网络连通性配置并自动下发，将组间策略转换为ACL配置并自动提前下发到指定的策略执行点（交换机或防火墙），避免了逐台配置交换机的繁琐操作
- 用户上线时，认证服务器根据5W1H条件为用户授权安全组，并将用户放入相应的VLAN/VXLAN；由于该组的策略已经提前下发，从而实现用户无论从什么位置接入，无论采用有线还是无线接入，均能得到其相应的网络策略



策略随行：系统架构



静态资源：数据中心被用户访问的服务器资源

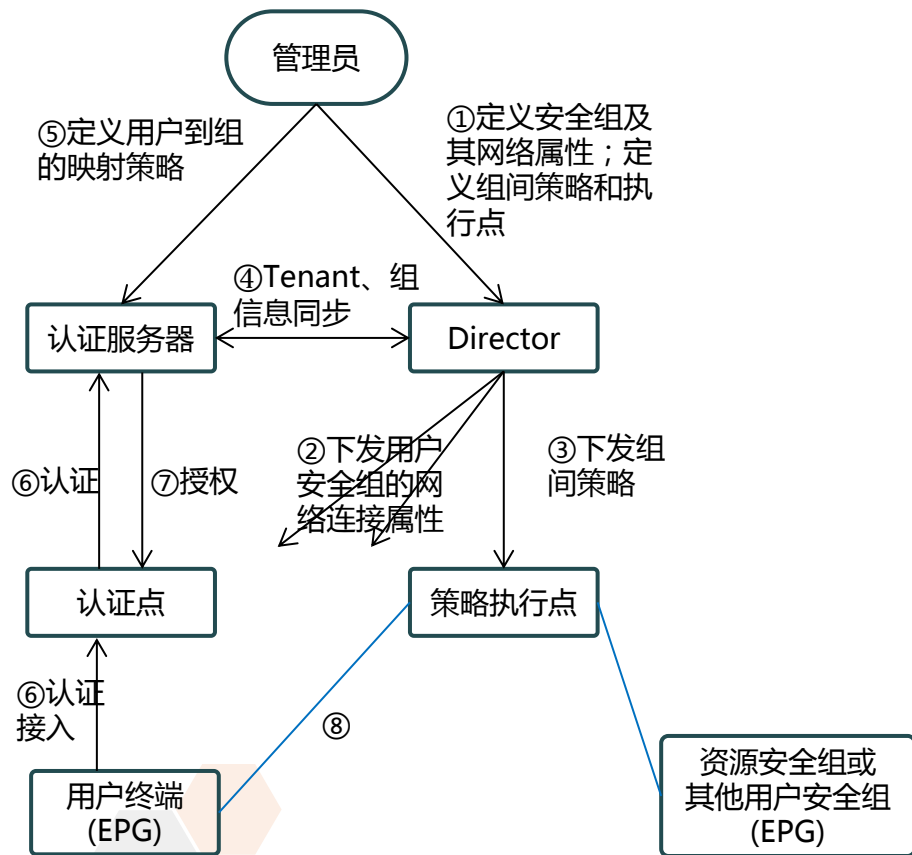
核心交换：负责园区网络各个区域的互联

执行点设备：汇聚交换机或FW, 执行组间策略

认证点设备：对用户终端进行认证，决定是否允许用户接入网络，提供有线、无线接入方式

用户终端：PC/Tablet/手机、打印机/IP Phone/Camera等

策略随行：逻辑架构



- ①管理员定义安全组及其网络属性；定义组间策略
- ②Director将用户安全组网络属性转换为网络连通性配置自动下发到网络设备（接入/汇聚/核心交换机）
- ③Director将组间策略转换为ACL 配置自动下发到指定的策略执行带点
- ④Director将用户安全组信息同步给认证服务器
- ⑤管理员定义用户到用户安全组的映射策略（根据5W1H）
- ⑥用户认证
- ⑦认证服务器将用户授权到某一安全组
- ⑧针对用户数据流量策略执行

策略随行---方案优势

- 策略先行，体验随身：有线无线用户均可移动/漫游，且其业务策略保持不变
- 不仅实现了用户组与资源组的访问控制，还可实现用户组到用户组的访问控制
- 业务策略集中管理，自动化下发，简化运维
 - 全网业务策略集中定义，自动提前下发到策略执行点；
 - 业务策略针对用户组，用特定用户无关；采用自然语言描述，与IP地址无关
 - 不用逐台配置交换机，不用关心不同交换机的ACL配置命令差异
- 可支持用户IP地址绑定，易于审计和追溯



目录

- AD campus方案
 - 有线无线深度统一
 - 策略随行
 - IP绑定



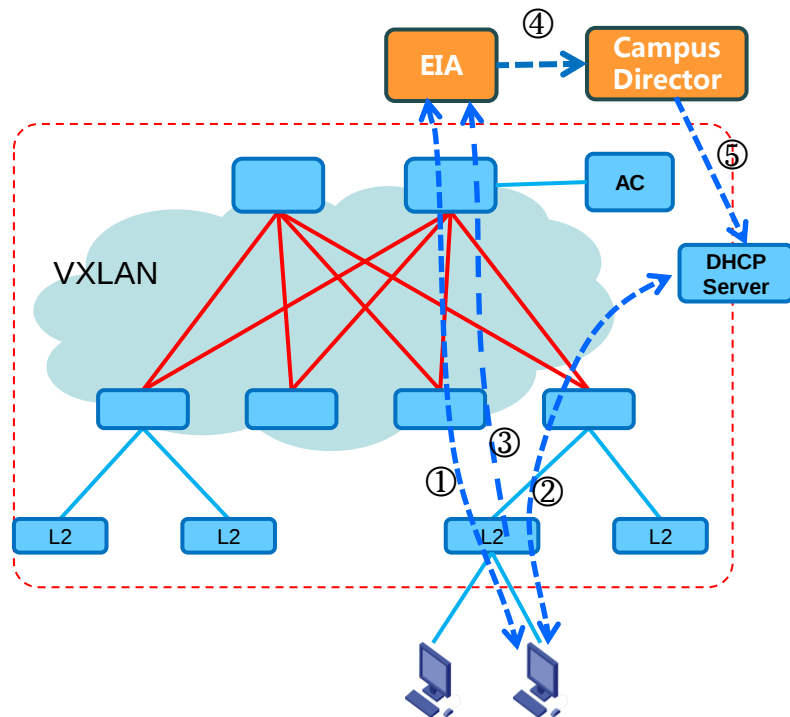
用户账号和IP地址绑定

■ IP绑定总体流程

- ① 终端向EIA进行认证
- ② 终端在业务VLAN内通过DHCP Relay到DHCP server申请地址。
- ③ Access设备作为NAS，捕获终端IP，通过RADIUS计费报文将终端IP上报EIA。
- ④ EIA和Director交互，告知上线终端IP/MAC等信息。
- ⑤ Director判断绑定标记，若需要绑定则通过agent向DHCP server设置地址绑定（MAC+VLAN→IP）。
- ⑥ 终端后续上线DHCP申请时均获得绑定的IP地址。

■ 带来的好处

- 根据IP地址即知用户，易于审计及追溯
- 满足强绑定场景（如招商银行）
- 满足特殊应用（如财务软件License和Client端的IP绑定）



目录

- 网络新趋势
- AD campus方案
- AD campus案例讲解



目录

■ AD campus案例讲解

第一步：网络自动化部署

第二步：业务部署



AD campus方案中第一步是网络自动化部署，自动化阶段是设备空配置上电，获取并加载基础配置文件、构建Underlay网络的过程。这个自动化过程目前campus方案中尚未支持，后续会合入。

暂时的策略先手工进行配置：

- 1、配置设备之间路由可达，以及配置好bgp邻居。
- 2、配置SNMP、TELNET参数，将设备加入管理软件中。
- 3、设备使能NETCONF，并配置用户名密码。

然后进入到管理页面的设备详细信息页面添加NETCONF参数，如下：

SOAP/HTTP	
传输层协议	SOAP
访问URL协议	HTTP
端口号 (1-65535)	80
访问路径	/soap/netconf/
用户名	h3c
用户密码	*****

修改 删除

+

返回



配置完成Telnet、Netconf之后，进入Overlay管理页面，如下。点击右上方设备管理，导入VTEP设备，导入成功后系统会自动对VTEP设备进行一次同步，也可以手工点击同步。

The screenshot shows the iMC 7.0 interface. The left sidebar contains a menu with 'Overlay管理' highlighted. The top right of the interface has a '设备管理' button highlighted in a red box. The main area displays the 'VXLAN列表' (VXLAN List) page, which includes a table of VXLAN configurations.

	VXLAN ID	设备名称	VSI名称	隧道接口	ARP抑制	是否监控	操作
☐	1033	105(10.153.149.120)	vsi1033		否	否	...
☐	1036	105(10.153.149.120)	vsi1036		否	否	...
☐	24	105(10.153.149.120)	Auto_L3VNI24_13		否	否	...
☐	1037	105(10.153.149.120)	vsi1037		否	否	...
☐	1034	105(10.153.149.120)	vsi1034		否	否	...
☐	1035	105(10.153.149.120)	vsi1035		否	否	...
☐	4094	105(10.153.149.120)	4094	1, 2	否	否	...
☐	1032	105(10.153.149.120)	vsi1032		否	否	...
☐	14	105(10.153.149.120)	vsi10	3	否	否	...

注：设备在下发VXLAN的时候会查这里的VXLAN列表，计算出不包含在此表中的最小VXLAN ID，所以建议在下发配置之前确保这里的同步操作结果成功，否则在创建私网和二层网络域时可能在不同的VSI下绑定相同的VXLAN，会使配置下发失败。

目录

■ AD campus案例讲解

第一步：网络自动化部署

第二步：业务部署



进到业务>业务规划页面，页面初始如下。首先选择组网方案点确定（我们以Vxlan组网为例），然后配置下面的通用组策略参数（认证需要的domain和radius参数，相应配置会下到Access设备上），点确定。

配置组网方案

提示

配置组网方案后，方可使用Campus其他功能，注意组网方案配置后不允许修改。

组网方案

☐ VLAN ☒ VxLAN

确定

通用组策略参数配置

提示

配置设备/接口使能802.1X认证需要的参数信息及Access接口配置的PVID信息，注意必须配置，否则通用组策略不生效。请在配置组网方案后进行配置。

域名分隔符 *

共享密钥 *

认证服务器IP *

认证方法

CHAP

PVID *

确定

注：该操作一旦确定后，当前版本无法修改或者删除。

业务规划（续）

然后业务规划页面会变成如下页面，系统预置3个设备组和7个接口组。点击自动导入设备及接口，系统会自动将相应角色的设备导入到相应设备组里。

点击自动导入设备及接口，系统会自动将相应角色的设备导入到相应设备组里。

注意：从设备组里删除设备或接口会执行相应的undo命令。

Dashboard

首页

拓扑

资源

业务

业务规划

安全组策略

接入用户

接入策略

Overlay管理

设备组

接口组

自动导入设备及接口

刷新

组名	描述	组策略	部署结果	修改
Director-spine设备组				
Director-leaf设备组				
Director-access设备组				

设备组

接口组

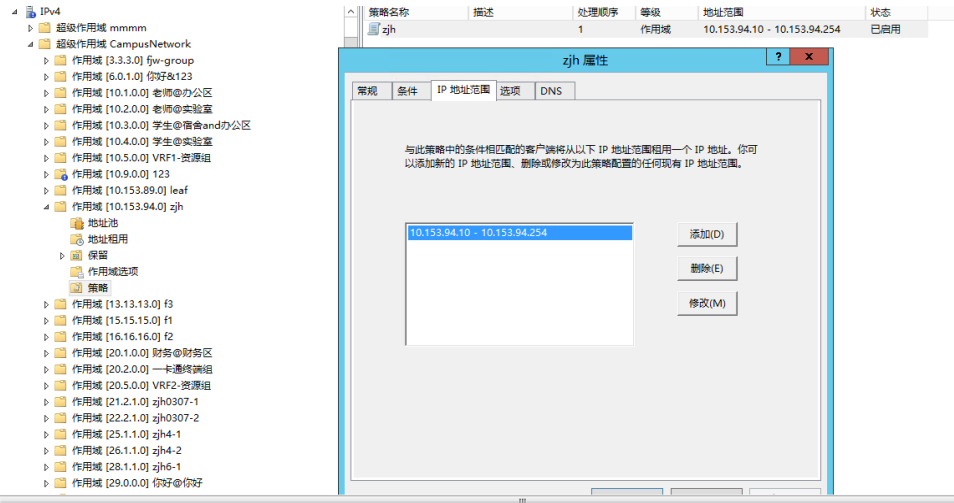
自动导入设备及接口

刷新

组名	描述	组策略	部署结果	修改
Access上行接口组	Access设备上的上行接口，需要Trunk所有VLAN。			
Access设备上的下行Access接口组	Access设备上的下行Access接口组，用于连接视频监控设备/打...			
Access下行Trunk接口组	Access设备上的下行接口，用于连接AP/语音设备，需要Trunk...			
Access下行认证接口组	Access设备上的下行接口，需要使能802.1X认证。			
Leaf上行接口组	Leaf设备上的上行接口组，需要Trunk所有VLAN。			
Leaf下行接口组	Leaf设备上的下行接口组，需要Trunk所有VLAN。			
Spine下行接口组	Spine设备上的下行接口组，需要Trunk所有VLAN。			

业务规划（续）

将DHCP服务器加入监控软件中，需要在DHCP服务器上安装iMC DHCP Plug插件，使其能成功识别到业务规划
右上角DHCP配置页面，如下：



注意：

- 1、DHCP server要配置双网卡：第一个网卡是管理IP，即加入管理软件用第一个网卡IP。另一网卡接入overlay，使用对应的VLAN/VXLAN作为控制通道（走DHCP Relay报文、NAS和EIA之间的认证报文）。
- 2、增加超级作用域，策略中分配的IP地址段包含DHCP Server业务IP网段。

安全组策略

配置顺序大致如下：

增加私网、增加二层网络域、增加安全组、增加资源组、增加访问策略模板、配置组间策略。

1、增加私网会向所有spine和leaf下发vpn实例和一个vsi虚接口，虚接口下绑定这个vpn实例并指定l3-vni，用于不同vxlan之间的三层转发。

私网部署详细信息

私网名称	Campus-VRF1	VPN名称	vpn1455701910469		
设备名称	设备分组	方法参数	完成时间	操作结果	
▼ 105(10.153.149.120)	Director-spine设备组				
部署:创建VSI虚接口		VPN实例名称:vpn1455701910469 VSI虚接口:1082 三层VXLAN ID:72	2016-02-17 17:38:38	成功 ^①	
部署:创建VPN		VPN实例名称:vpn1455701910469	2016-02-17 17:38:32	成功 ^①	
▼ vtep1(10.153.149.101)	Director-leaf设备组				
部署:创建VSI虚接口		VPN实例名称:vpn1455701910469 VSI虚接口:1082 三层VXLAN ID:72	2016-02-17 17:38:39	成功 ^①	
部署:创建VPN		VPN实例名称:vpn1455701910469	2016-02-17 17:38:33	成功 ^①	
▼ vtep2(10.153.149.102)	Director-leaf设备组				
部署:创建VSI虚接口		VPN实例名称:vpn1455701910469 VSI虚接口:1082 三层VXLAN ID:72	2016-02-17 17:38:42	成功 ^①	
部署:创建VPN		VPN实例名称:vpn1455701910469	2016-02-17 17:38:36	成功 ^①	



安全组策略（续）

2、创建二层网络域会向所有设备下发相同的vlan，向spine和leaf下发vxlan，向leaf的所有AC口下发服务实例。

二层网络域部署详细信息					
名称	二层网络域1	私网名称	vpn1455701910469	VLAN ID	1084
Vxlan ID	74	子网	10.1.0.0/255.255.255.0	网关IP	10.1.0.1
设备名称	设备分组	方法参数	完成时间	操作结果	
▼ 105(10.153.149.120)	Director-spine设备组				
部署:创建VXLAN和VSI		VSI名称:vsi1084 VXLAN ID:74 ARP泛洪抑制:0 VSI模式:2	2016-02-17 19:53:21	成功	?
部署:创建Vlan		VLAN ID:1084	2016-02-17 19:53:14	成功	?
▶ vtep1(10.153.149.101)	Director-leaf设备组				
▼ vtep2(10.153.149.102)	Director-leaf设备组				
部署:创建服务器实例		VSI名称:vsi1084 接口索引:207 服务ID:1084 以太网帧匹配规则:4 Vlan规则:1084	2016-02-17 19:53:29	成功	?
部署:创建服务器实例		VSI名称:vsi1084 接口索引:199 服务ID:1084 以太网帧匹配规则:4 Vlan规则:1084	2016-02-17 19:53:26	成功	?
部署:创建VXLAN和VSI		VSI名称:vsi1084 VXLAN ID:74 ARP泛洪抑制:0 VSI模式:2	2016-02-17 19:53:24	成功	?
部署:创建Vlan		VLAN ID:1084	2016-02-17 19:53:18	成功	?
▼ S5130_28S(10.153.149.202)	Director-access设备组				
部署:创建Vlan		VLAN ID:1084	2016-02-17 19:53:16	成功	?
▶ 10.153.149.200(10.153.149.200)	Director-access设备组				

安全组策略（续）

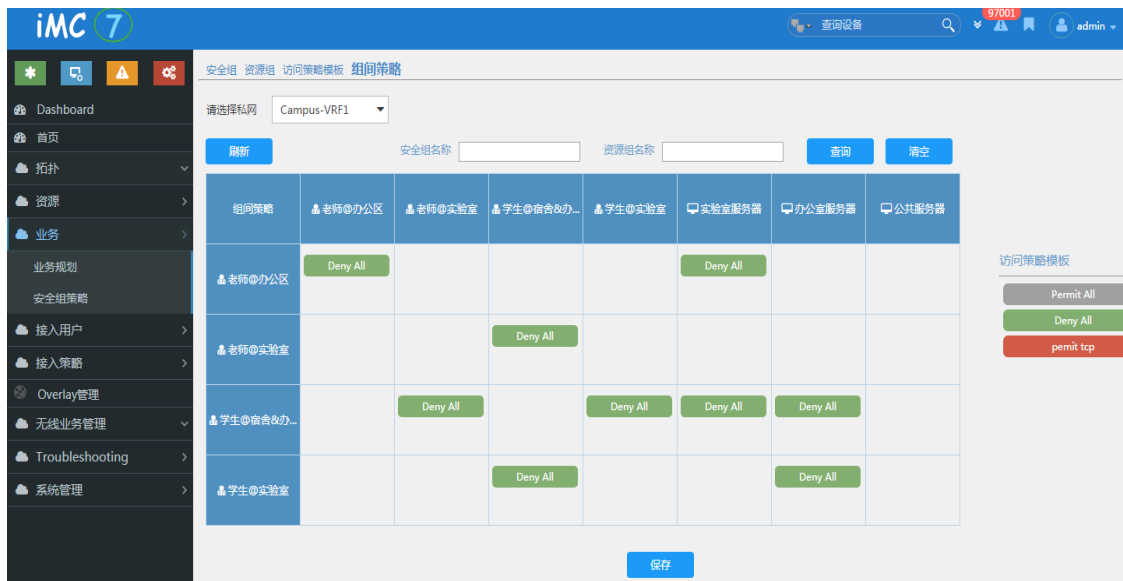
3、创建安全组会向spine和leaf下发vsi虚接口，作为分布式网关。同时会在DHCP服务器上增加相应的子网，可以在业务规划>DHCP配置里看到，这个子网是用户在创建二层网络域中配置的。

安全组部署详细信息

安全组名称	老师@办公区	二层网络域	二层网络域1		
设备名称	设备分组	方法参数	完成时间	操作结果	
▼ 105(10.153.149.120)	Director-spine设备组				
部署:创建VSI虚接口		VPN实例名称:vpn1455701910469 VSI名称:vsi1084 VSI虚接口:1084 网关类型:1 IP地址:10.1.0.1 掩码:255.255.255.0 本地网关接口:1 MAC地址:1000-1000-0001 使能ARP代理:1	2016-02-17 20:00:36	成功 ^②	
▼ vtep1(10.153.149.101)	Director-leaf设备组				
部署:创建VSI虚接口		VPN实例名称:vpn1455701910469 VSI名称:vsi1084 VSI虚接口:1084 网关类型:1 IP地址:10.1.0.1 掩码:255.255.255.0 本地网关接口:1 MAC地址:1000-1000-0001 使能ARP代理:1	2016-02-17 20:00:37	成功 ^②	
▼ vtep2(10.153.149.102)	Director-leaf设备组				
部署:创建VSI虚接口		VPN实例名称:vpn1455701910469 VSI名称:vsi1084 VSI虚接口:1084 网关类型:1 IP地址:10.1.0.1 掩码:255.255.255.0 本地网关接口:1 MAC地址:1000-1000-0001 使能ARP代理:1	2016-02-17 20:00:38	成功 ^②	

安全组策略（续）

- 4、增加资源组不会向设备下发配置，只是指定一些IP，用于访问策略。
- 5、访问策略模板，系统预置了两个访问策略模板Permit all和Deny all，用户也可以根据需要自定义。
- 6、配置组件策略，选择私网，配置其组间策略，拖拽访问策略模板到相应格子，点击保存按钮即可将acl下发到相应的vsi虚接口下，提示保存组间策略成功。



此处是一个典型案例



Microsoft Office
Word 文档

AD campus组网—DR2000应用驱动园区软件简介.pptx - Microsoft PowerPoint

开始 插入 设计 动画 幻灯片放映 审阅 视图 加载项 格式

幻灯片 大纲

安全组策略 (续)

H3C

4. 增加资源组不会向设备下发配置, 只是指定一些IP, 用于访问策略。

5. 访问策略模板, 系统预置了两个访问策略模板Permit all和Deny all, 用户也可以根据需要自定义。

6. 配置组件策略, 选择私网, 配置其组间策略, 拖拽访问策略模板到相应格子, 点击保存按钮即可将ad下发到相应的vsi虚接口下, 提示保存组间策略成功。

IMC ?

单击此处添加备注

此处是一个典型案例

Microsoft Office Word 文档

幻灯片 32/33 "H3C_PPT_标准模板V3.1" 中文(简体, 中国) 100%

19:11 2016/4/14

谢谢！

