日期：2012年11月2日星期五

Huawei Enterprise A Better Way

华为ONE NET园区网技术主打胶片

www.huawei.com/enterprise

HUAWEI TECHNOLOGIES CO., LTD.

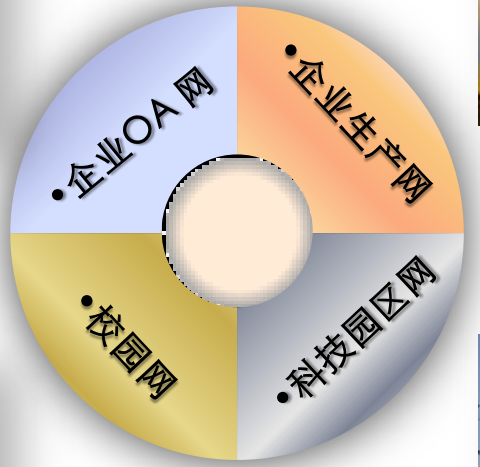
HUAWEI

目录

什么是园区网？

政府、金融、交通、能源……

电力、石油、制造行业……

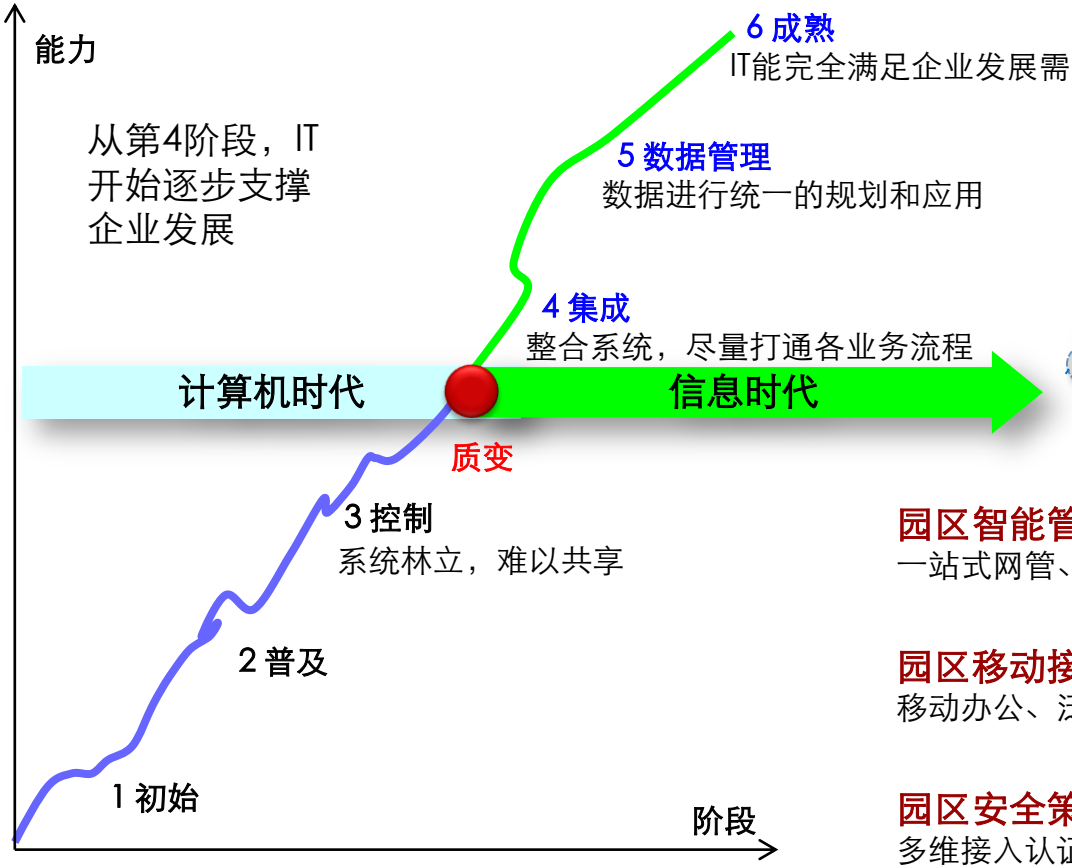


学校园网

高新科技园、软件园 ……

园区分类	小型园区	中型园区	大型园区
终端用户数量	<200	200-1000	>1000

信息时代 需要建设园区网



诺兰模型

企业信息化发展遵循客观规律的经典模型，用于指导企业IT系统建设，分为6个阶段。

园区智能管理：

一站式网管、基于业务的流量监管、快速问题处理

eSight

园区移动接入：

移动办公、泛在移动设备接入、移动安全保障

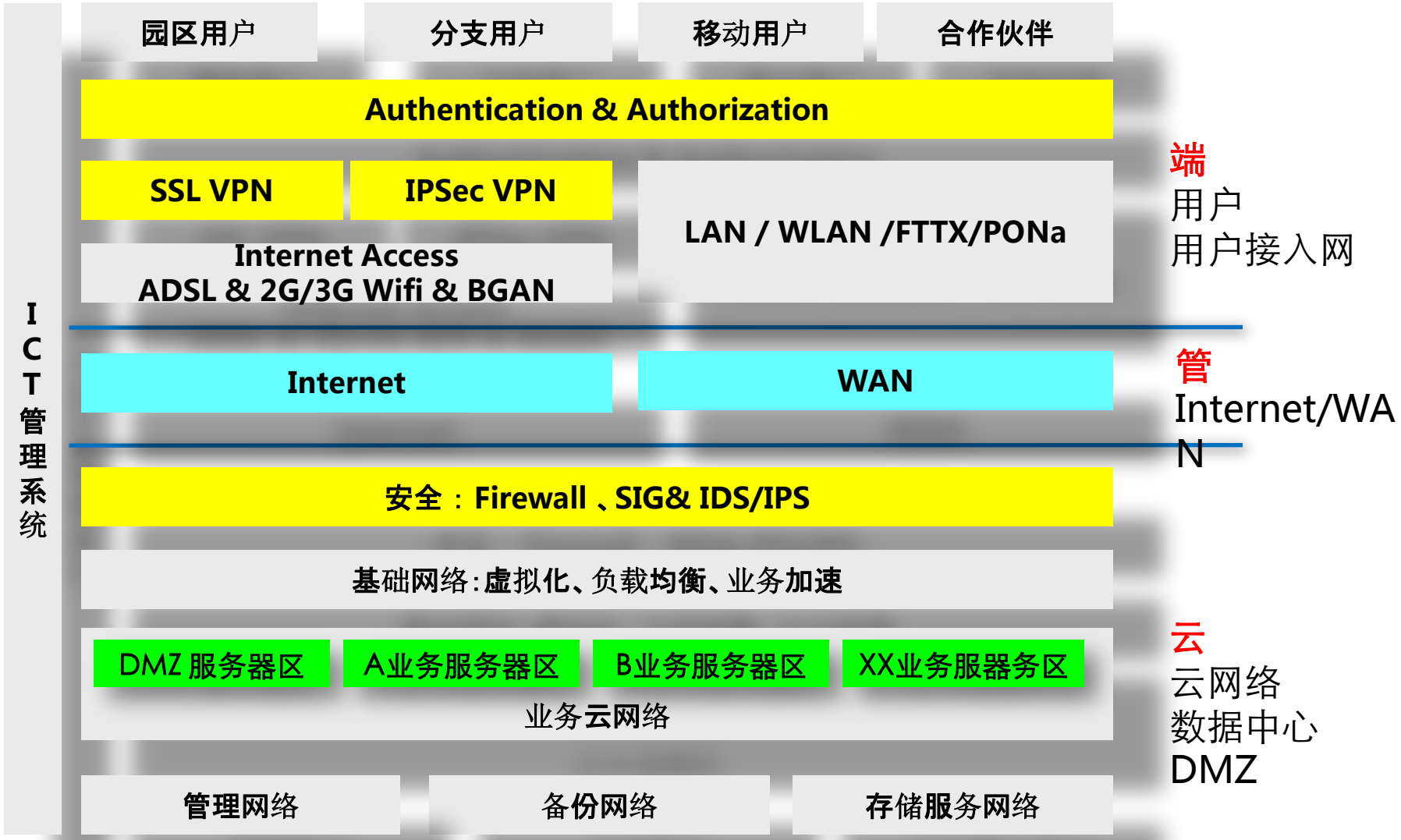
园区安全策略：

多维接入认证、分权分域管理、文件管理、行为监管

智能化园建设：

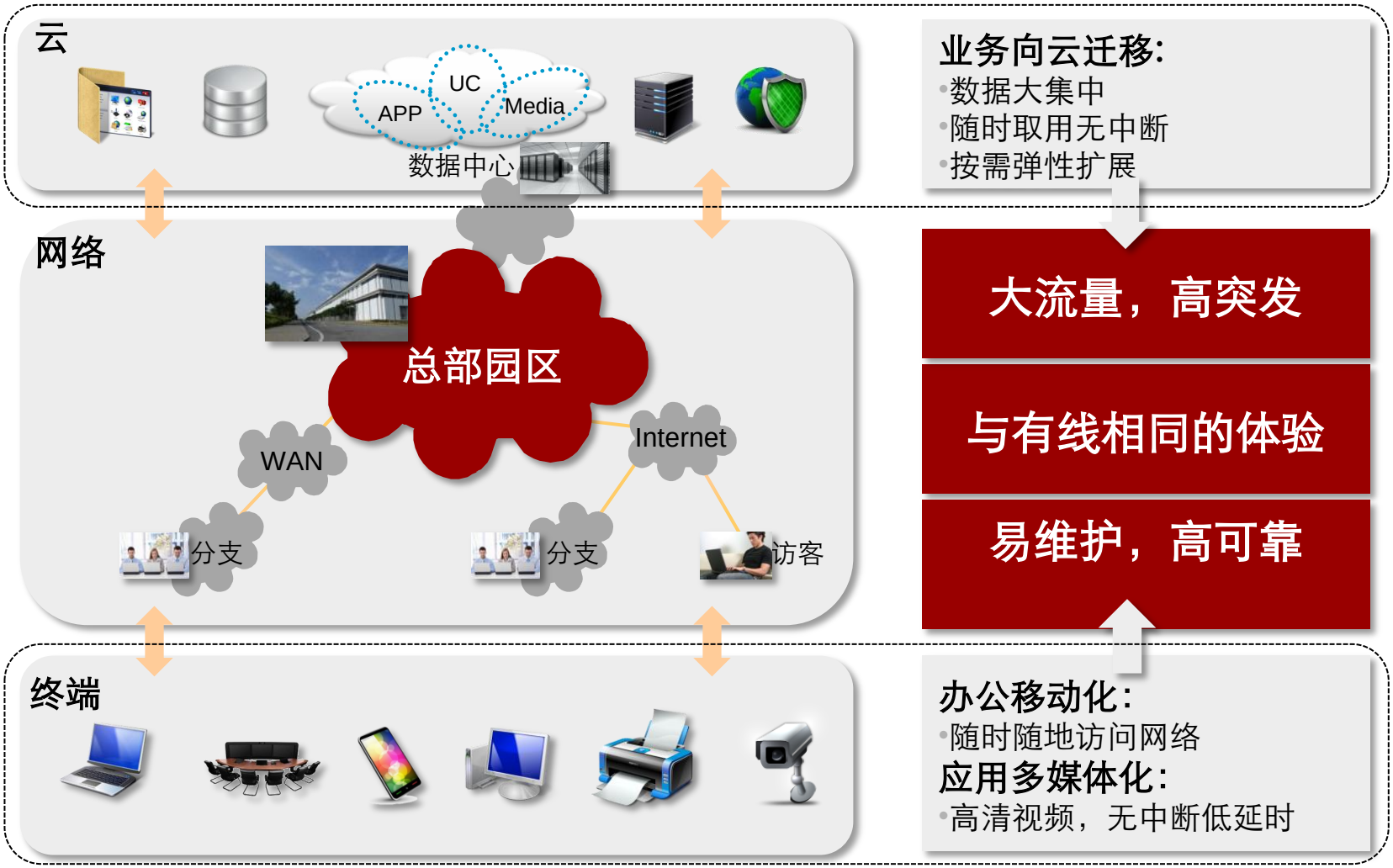
智能能耗管理、快速部署、智能运维、机房精细化管理

企业网信息体系逻辑架构

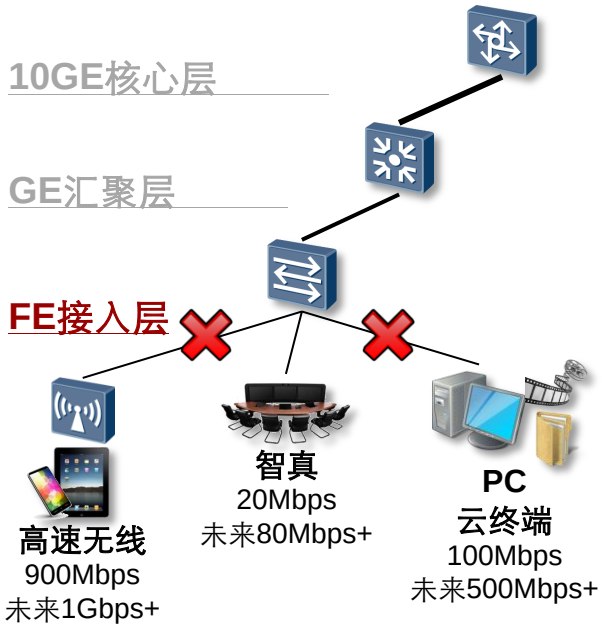


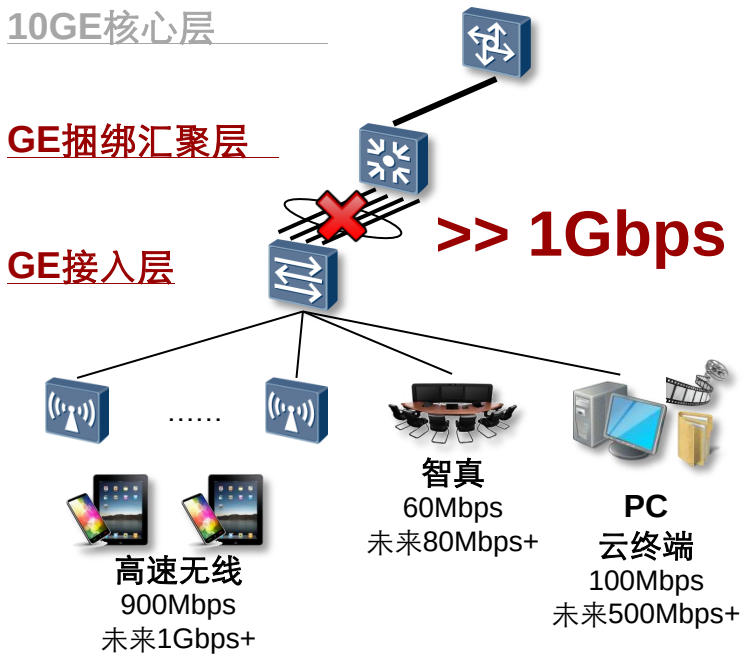
多媒体、云和移动是企业信息化的方向

企业信息化对园区网的影响



挑战一：大流量，高突发





FE接入不能满足无线需求

接入层带宽已经不能满足无线园区、多媒体、大数据拷贝等需求

GE捆绑汇聚不能满足并发需求

- 汇聚层带宽收敛大
- 接入层端口浪费大
- 网络复杂度高

挑战二：与有线相同的体验

无线射频性能

信号覆盖差，需要部署大量AP

多用户接入能力

多用户接入时吞吐量低

安全

多种智能终端接入时权限控制差，直接威胁公司信息安全

挑战三：易维护，高可靠

故障恢复

- 恢复时间长达秒级，不能满足多媒体、云业务的实时需求
- 不能精准定位故障至网元

网络质量管理

- 不能区分严格实时、实时和非实时类业务
- 监控措施占用CPU，影响协议和业务

华为万兆园区网架构

One Net
Connect Everyone, Connect as One

体验

极速灵活　　业务随行　　可靠可视

终端/IT

核心

万兆网络　　移动性　　云承载

方案

万兆 | 虚拟化 | 有线无线一体化 | 智真运维 | 桌面云 | 企业语音 | 能源管理 | IPv6 | NAC

产品

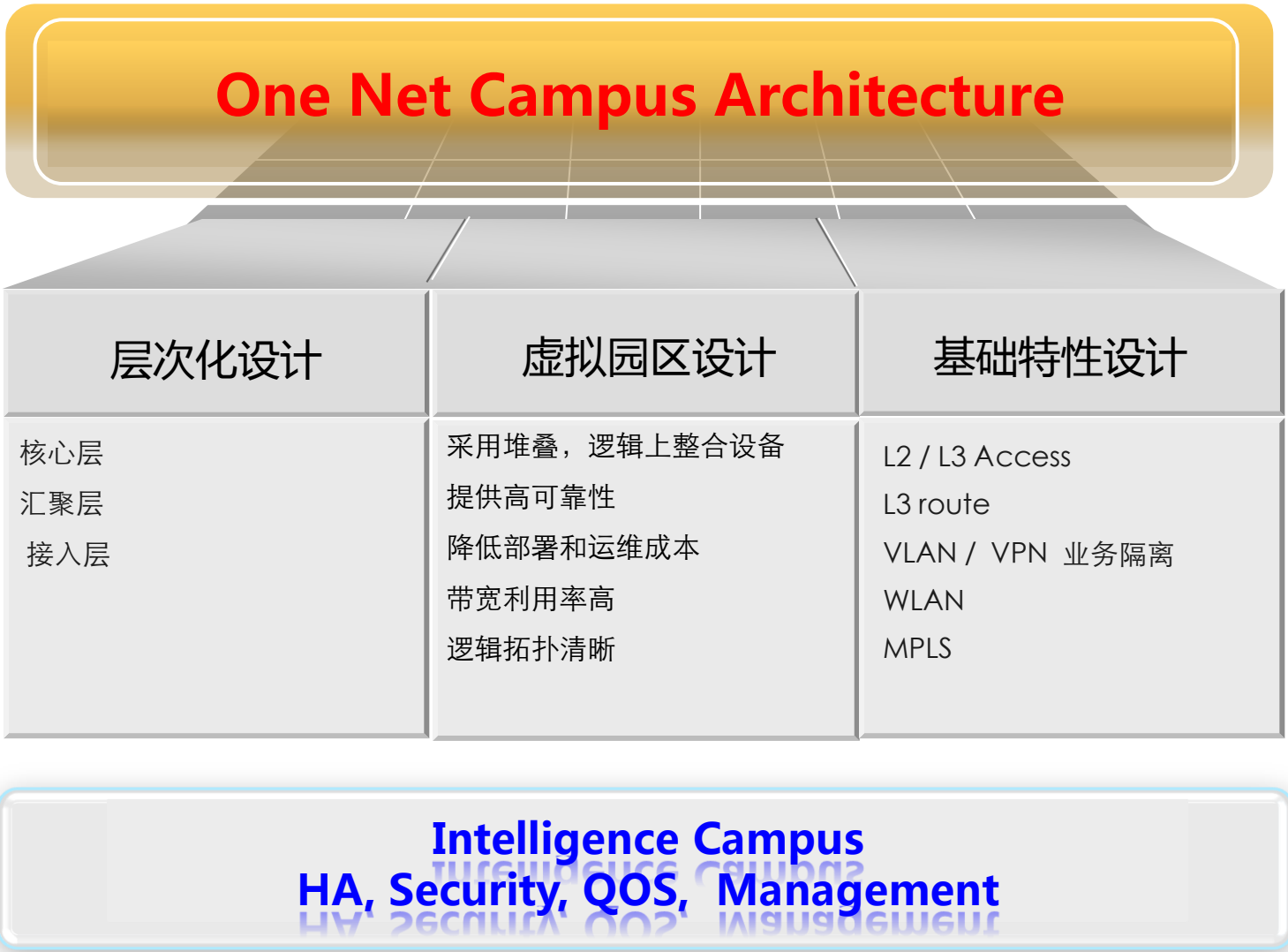
交换机　　路由器　　防火墙　　WLAN　　GPON

目录

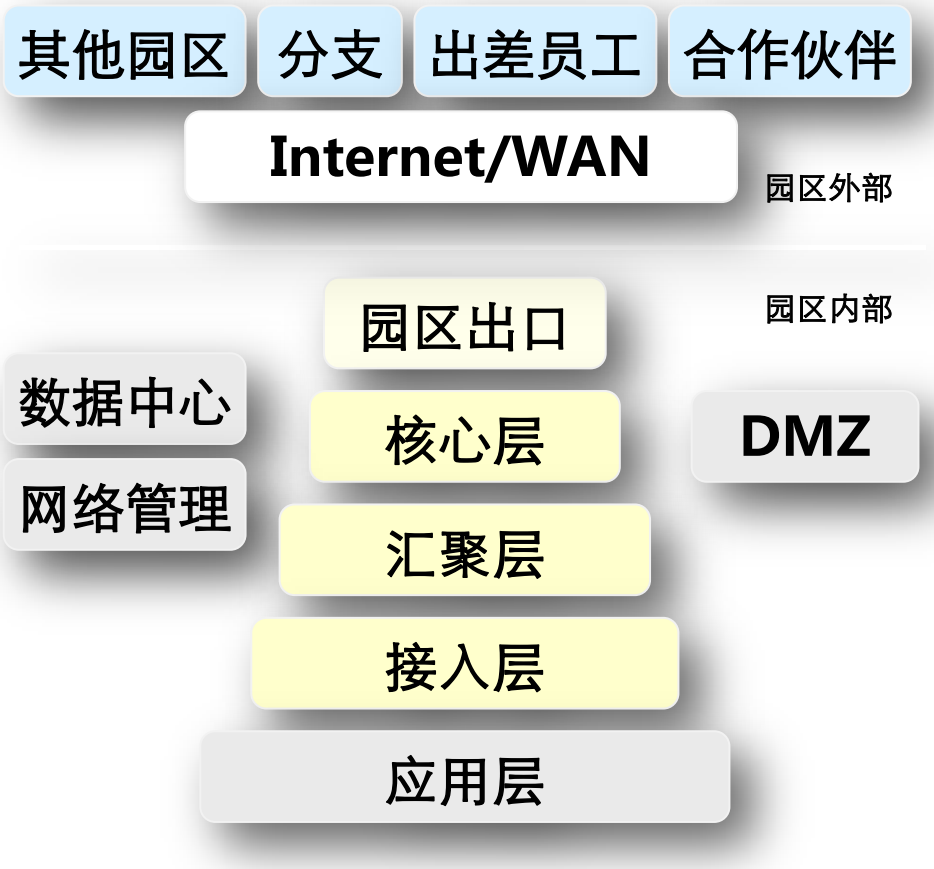
子目录

2 园区网基础解决方案

园区网络体系架构


One Net Campus Architecture
层次化设计
虚拟园区设计
基础特性设计
核心层
汇聚层
接入层
采用堆叠，逻辑上整合设备
提供高可靠性
降低部署和运维成本
带宽利用率高
逻辑拓扑清晰
L2 / L3 Access
L3 route
VLAN / VPN 业务隔离
WLAN
MPLS
Intelligence Campus
HA, Security, QOS, Management

园区网设计概述



基于云、物联网的安全，智能化园区

您的企业可充分利用这些成功设计原则，借鉴成熟案例和方法，建设和优化网络，满足您的业务要求。

层次化结构：核心层、汇聚层和接入层，具有稳定性，可扩展性，可靠性。

模块化设计：园区出口，数据中心，DMZ，网络管理，分支、园区间、出差员工和合作伙伴灵活访问和互联。

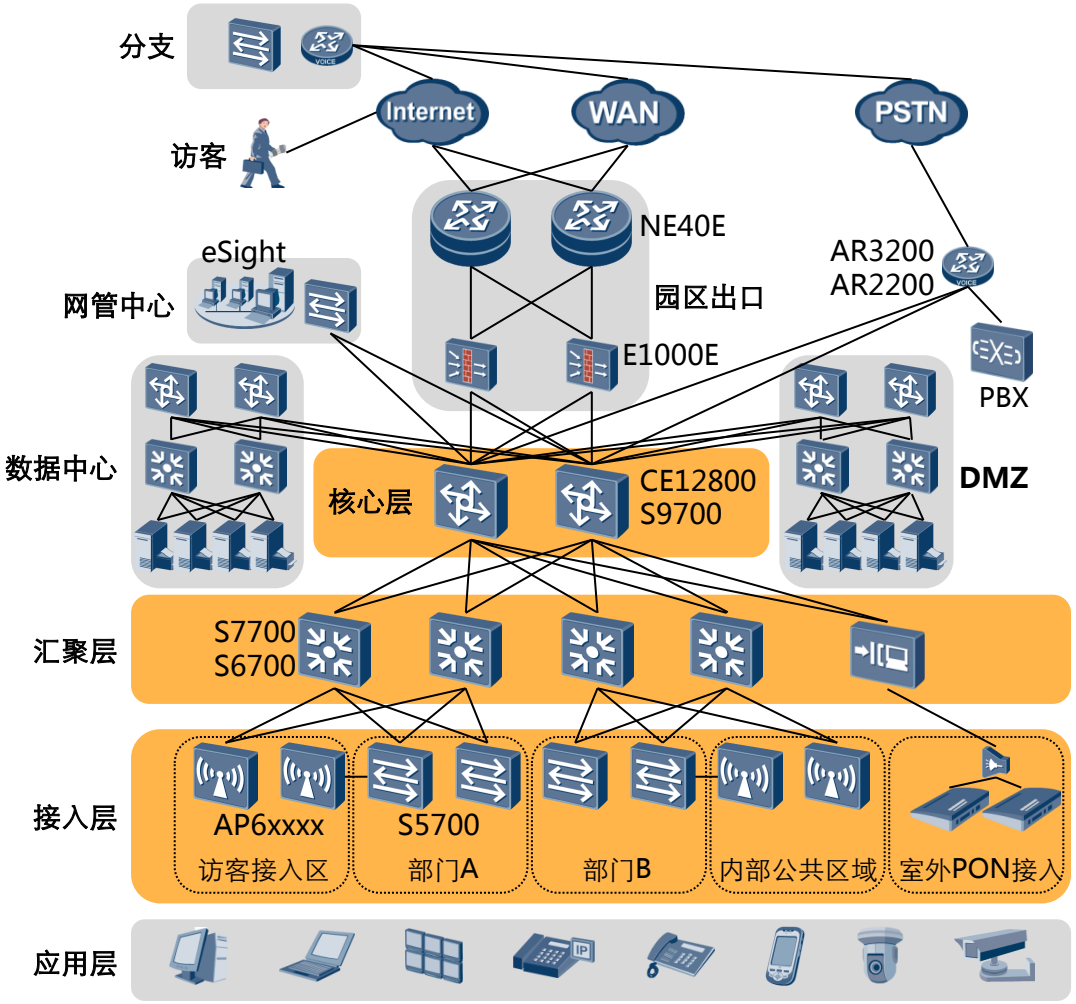
高可靠性设计：关键部位冗余架构与可靠故障恢复迅速。

虚拟化设计：纵向虚拟化提供丰富的隔离和安全，横向虚拟化简化网络、优化流量、易于管理。

整体网络安全设计：防止恶意破坏，保护数据和网络安全。

智能网络设计：全网多业务主动和综合管理，实时分析网络健康状况，积极预防，排除故障，减少损失。

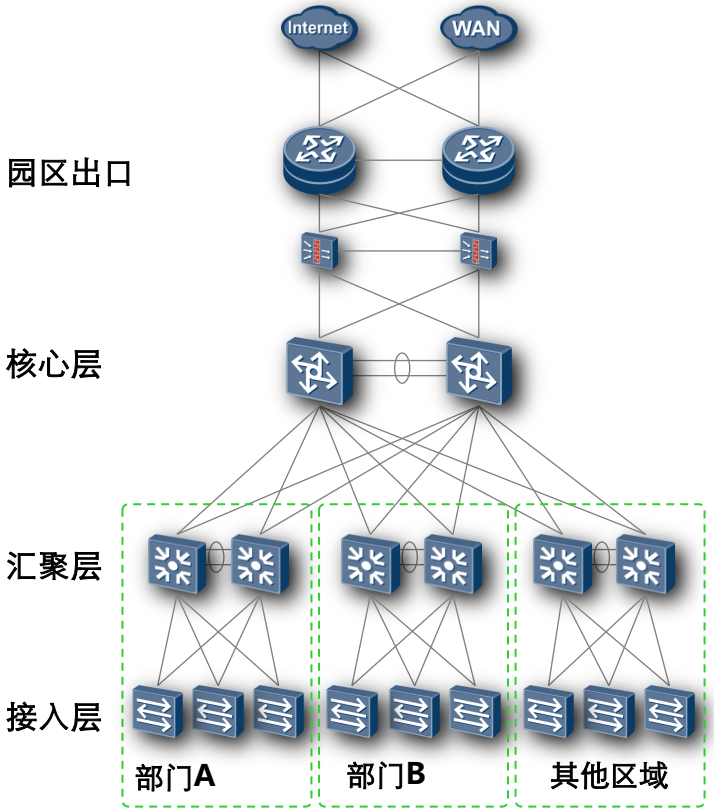
园区基础网络架构



位置	三层组网选型	两层组网选型
核心	40GE核心层 CE12800/S9700系列	10GE汇聚层/核心层 S9700/S7700
汇聚	10GE汇聚层 S9700/S7700系列	NA
接入	S5700系列	
AP	AP6010SN：室内标准型，2*2:2个流，单频 AP6010DN：室内标准型，2*2:2个流，双频 AP6510DN：室外标准型，2*2:2个流，双频 AP6610DN：室外网桥， 2*2:2个流，双频 （AC供电，光口上行） AP6310SN，室分型，2*2:2个流，单频	
AC	AC6605（盒式） S9700/7700 ACU（插卡）	
出口路由器	大中型园区：NE40E系列 中小型园区：AR3200/AR2200系列 支持语音的园区：AR3200/AR2200系列	
防火墙	Eudemon E1000E-X系列	

注：
- S57分为LI/SI/EI/HI，LI为二层千兆交换机，其他为三层千兆交换机。
- 接入AP、IP电话、IP摄像头等可PoE受电的终端时推荐选择PoE交换机，S5700交换机命名中带“PWR”表示为PoE型号。

分层的星型园区网络架构是基本原则



层次化设计：核心层、汇聚层、接入层，每层功能清晰，架构稳定，易于扩展和易于维护

模块化设计：每一个模块一个部门，部门内部调整涉及范围小，定位问题也容易。

冗余性设计：双节点冗余性设计，适当的冗余性提高可靠性，过度的冗余不便于运行维护

对称性设计：网络的对称性便于业务部署，拓扑直观，便于协议设计和分析。

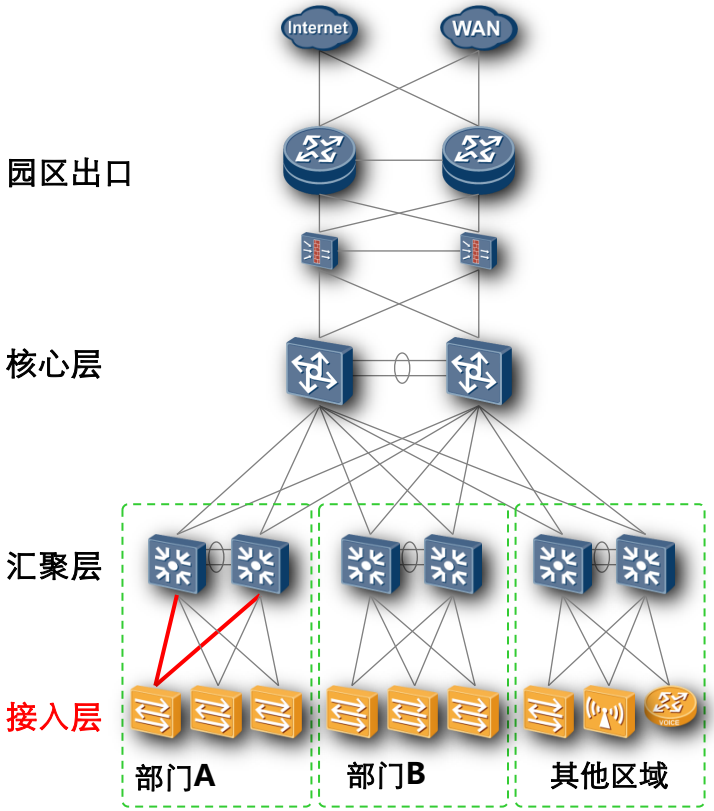
星型网络：

优势：园区网重要的是网络架构简单易维护易部署，环形网络多用于需要节约光纤的网络

破环技术：星型不等于不成环，因此环保护协议运行是必须的，有多种全网破环协议，推荐MSTP

环形网络的应用场景：并非所有园区网都一定是星型的，特殊情况需要特殊考虑，比如地铁调度网络

接入层设计



接入层是最靠近用户的网络，为用户提供各种接入方式，是终端、边缘和IP电话设等备接入网络的第一层，一般都部署二层设备，双归属到汇聚层两个不同的交换机。

要求：

丰富的二层特性：VLAN、IGMP Snooping、环网避免

安全特性：802.1x、端口安全、DHCP snooping、DAI、IP Source Guard，MFF安全

可靠性：系统级的引擎和电源冗余，LAG，iStack等

POE:方便IP电话或无线AP接入

带宽管理：IGMP snooping、QoS等

高密度GE/FE接口，接入交换机数量大，易管理

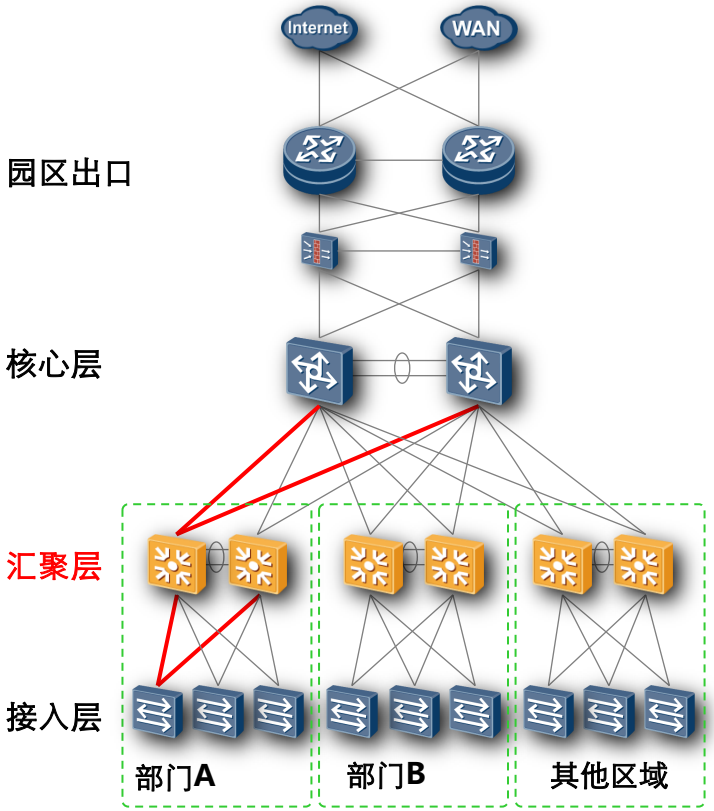
设备推荐

千兆接入场景：S5700交换机，

百兆接入场景：S2700/S3700（三层接入）交换机

接入层设备不仅包括交换机，还包括AP、xPON、xDSL、语音等不同的接入设备

汇聚层设计



汇聚层是部门的核心，转发部门用户间的“横向”流量。同时提供到核心层的“纵向”流量。

对接入层隐藏核心层，作为园区网的配线架，将大量用户接入到互联的网络中，扩展核心层设备接入用户的数量

承担L2/L3边缘的角色。

双归到核心层，并支持接入层的双归

要求：

强转发能力，高端口密度

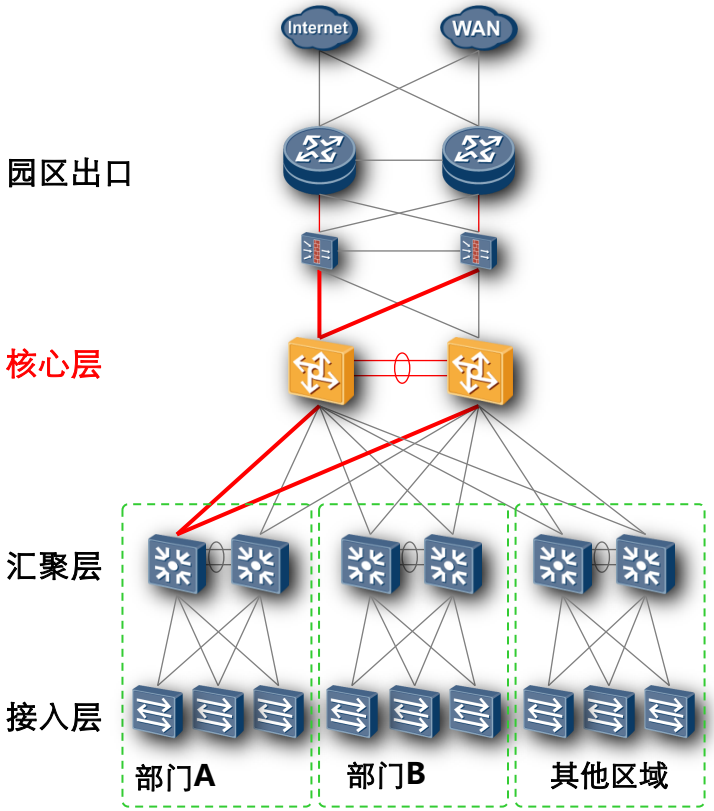
可靠性是最重要的特性，三层支持NSF，二层支持Smartlink

三层特性，承载多业务：VRRP，MPLS，OSPF等

设备推荐：

采用S5700/S7700/S9300系列交换机，通过GE/10G端口连接核心交换机、GE端口连接接入交换机

核心层设计



园区的核心，连接所有汇聚交换机，转发各个部门之间的流量

核心层对3个以上部门规模的企业来说是必须的，除了减少连线、路由Peer之外，让扩展以及日常策略调整也变得简单

全连接结构，保持核心设备配置尽量简单，并且和部门无关

要求：

高密10GE接口，强转发能力

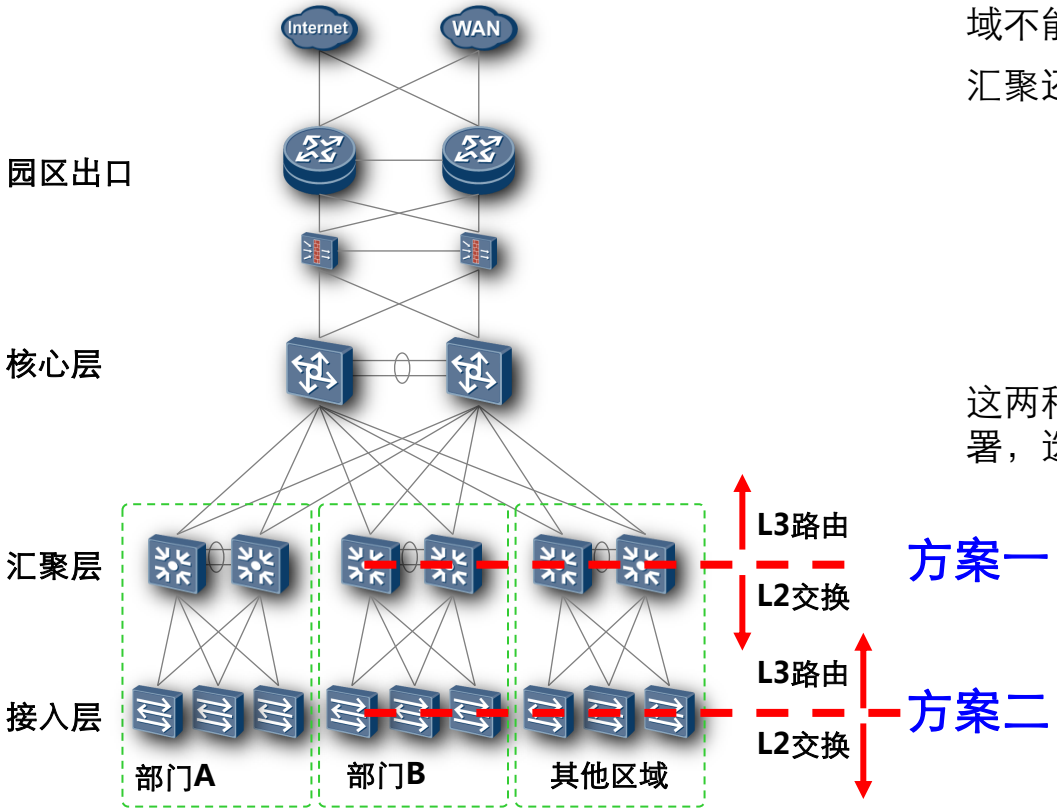
强路由能力，强路由收敛能力，故障快速收敛。

带宽利用率高亮

设备推荐：

采用S7700/S9300高端交换机，通过GE或10GE端口连接汇聚交换机和出口路由器

二三层分界点设计方案



除非没有核心层的小园区网络，否则核心是三层路由这一点业界已经形成共识，原因是二层域不能太大，各部门地址规划独立

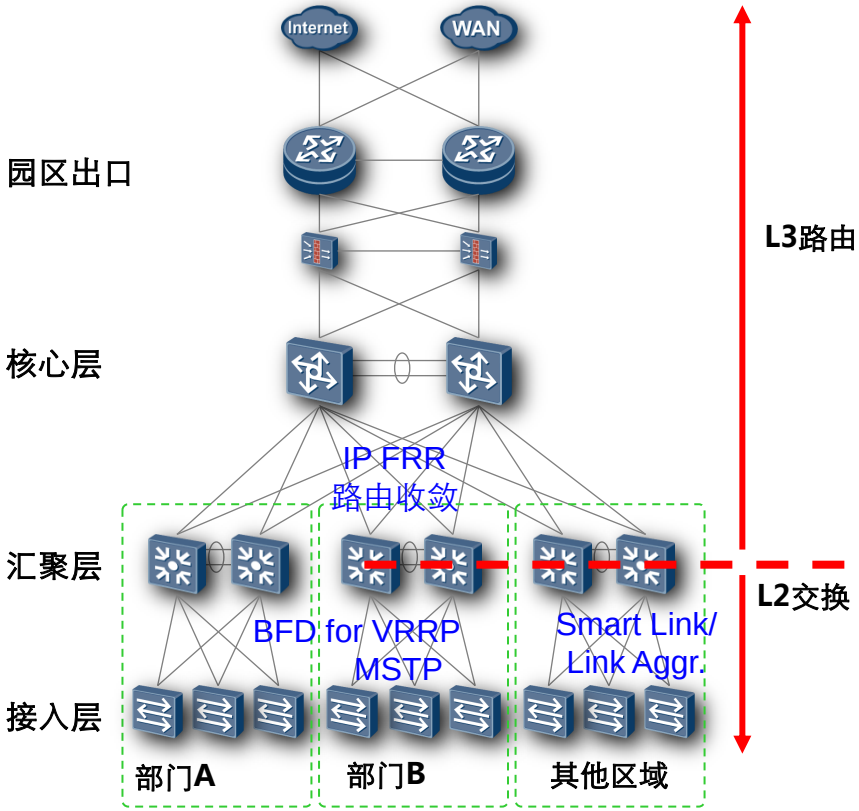
汇聚还是接入作为分界点有两种方案：

方案一：二三层分界即网关设在汇聚设备上，即部门公用网关，采用SuperVlan或者子接口方式进入三层

方案二：二三层分界即网关设在接入设备上，部门多个网关，整网没有二层广播域

这两种方案各有优缺点，根据实际情况进行部署，选择最适合的企业业务的方案

二层接入园区网（推荐方案）



业务流程：

- 接入设备仅仅为用户提供二层接入功能，并根据企业具体情况划分VLAN
- 汇聚设备作为二三层网络的分界点，为用户提供三层网关
- 园区接入侧通过MSTP防止网络环路
- 接入层到汇聚层通过SmartLink或者链路汇聚（CSS）保证设备间可靠性
- 通过BFD + VRRP保证用户网关可靠性
- 园区汇聚、核心、出口均采用三层路由互联，并通过IP FRR做快速路由收敛

优点：

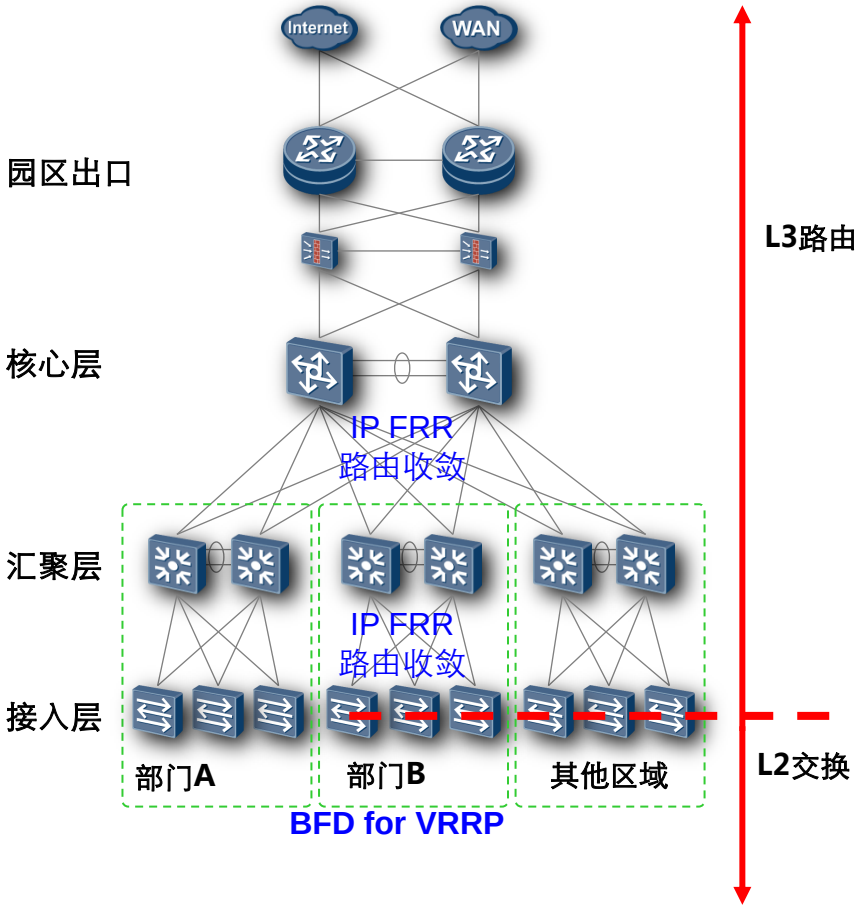
- 低成本，接入侧交换机采用二层交换机，保护和节省用户投资
- 满足部门内特殊业务的二层互通需求

缺点：

- 接入交换机和汇聚交换机之间存在二层环路风险
- 接入交换机和汇聚交换机之间的链路利用率低

上述两个问题,可通过汇聚交换机集群和接入交换机的堆叠技术解决

三层接入园区网



业务流程：

全网路由结构，接入设备是二三层网络的分界点，接入设备作为终端设备的网关，提供二层终结，三层路由；

终端采用SuperVlan或者普通VLAN方式接入网关

全网采用IP FRR做快速路由收敛

优点：

纯三层结构，网络结构简单清晰，不依赖CSS等技术简化网络

扩展性强，网络拓扑依赖度低，可以任意网络拓扑形式扩展

易维护，无二层环路网络风险，无需配置生成树协议

易配置，无需规划二层配置

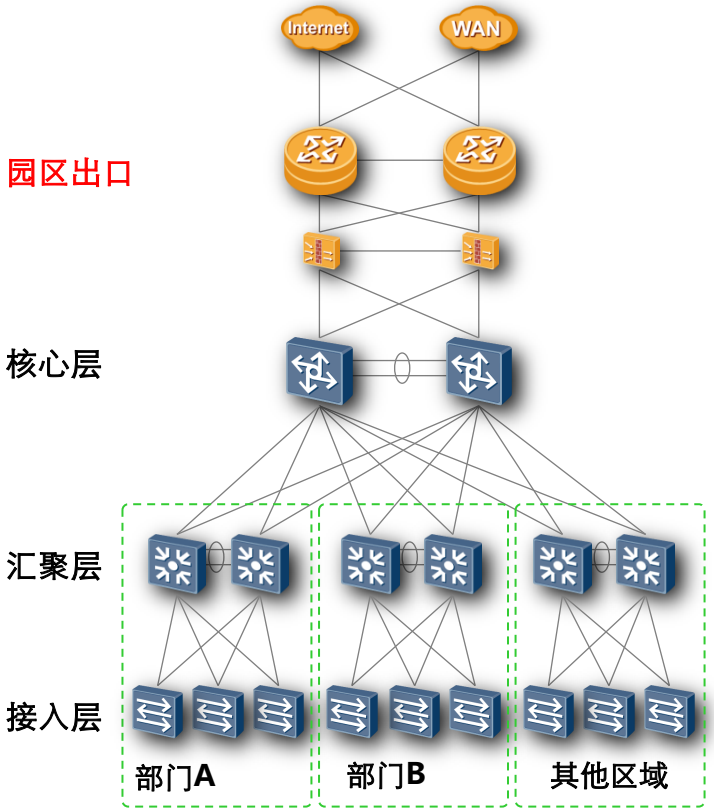
缺点：

成本高，对接入交换机要求较高，导致成本提升

部门内无法进行二层互通，某些特殊业务无法运行

收敛速度相对二层可能会略慢

园区出口



企业广域网和Internet的出口，连接企业的不同园区或分支，出差员工、SOHO，合作伙伴和访客等

配置防火墙、IPS等，根据不同的安全性要求和投资规模选择安全部件

Internet安全性和可靠性低，费用低，WAN安全性和可靠性高，费用高。为保证WAN/Internet链路的高可靠性，可申请两条链路，实现冗余备份，也可以WAN作为主，Internet作为冗余备份。

要求：

支持WAN接口

大路由表

MPLS VPN能力

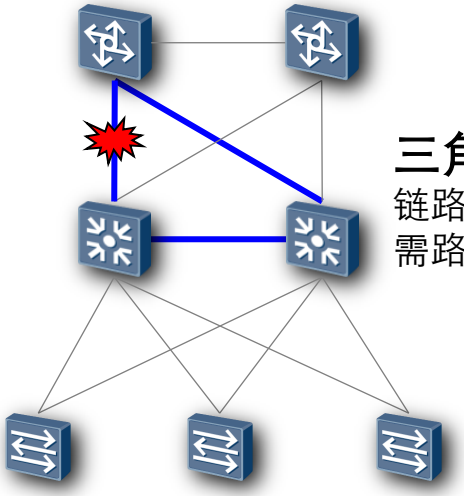
集成或独立DPI、防火墙、IPS/IDS等功能

设备推荐：

一般采用路由器组网，高端场景采用NE40E,低端场景采用NE20E/AR G3路由器，使用WAN接口连接互联网/城域网；

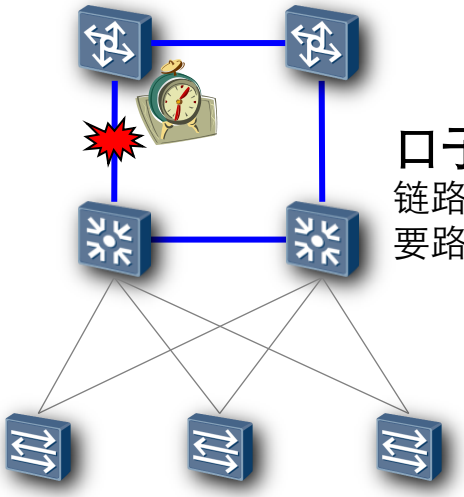
对设备投资低成本方案，可以使用S9300交换机内置WAN板作为企业出口，防火墙旁挂

园区网转发设计



三角型

链路、设备故障无需路由协议收敛



口子型

链路、设备故障需要路由协议收敛

路由转发存在三角型和口子型组网两种组网，三角型组网好于口子型，原因如下：

- 三角型组网链路、设备故障无需路由协议收敛，而口子型需要
- 三角型组网设备及链路利用效率高，而口子型在链路故障时效率低
- 三角型可作ECMP负载分担

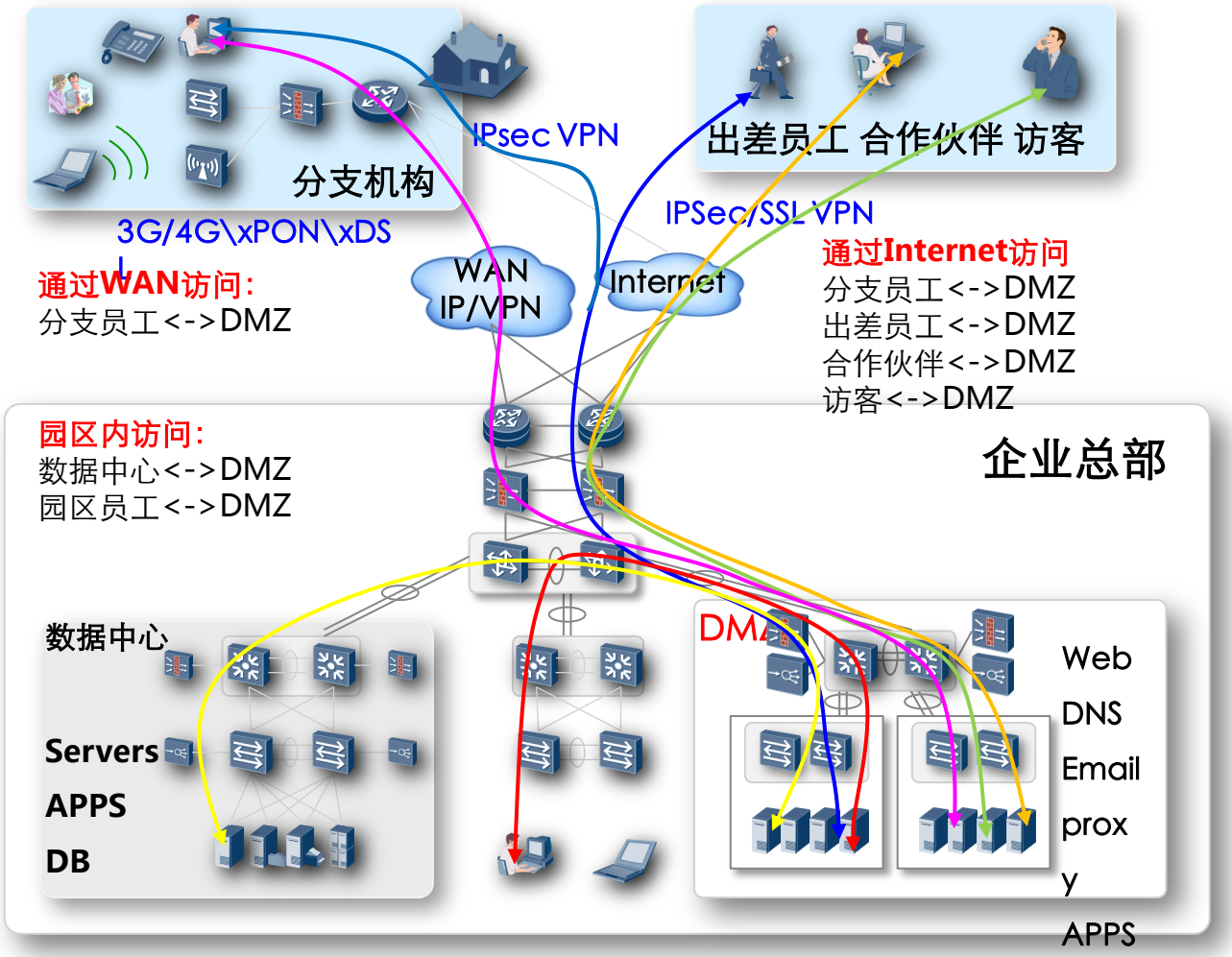
关于负载分担转发根据实际情况配置成ECMP或者UCMP

汇聚以上最好是每条路径都存在备份链路，防止链路故障时出现黑洞

可以通过汇聚设备配置Passive接口减少OSPF Peer的数目

汇聚交换机之间加一条链路有助于在接入交换机上行链路故障时保证回程数据

DMZ 设计



DMZ区是部署对外业务和服务的区域，狭义的DMZ仅对互联网用户提供服务。广义的DMZ区还对内部用户，以及为合作伙伴提供的服务。

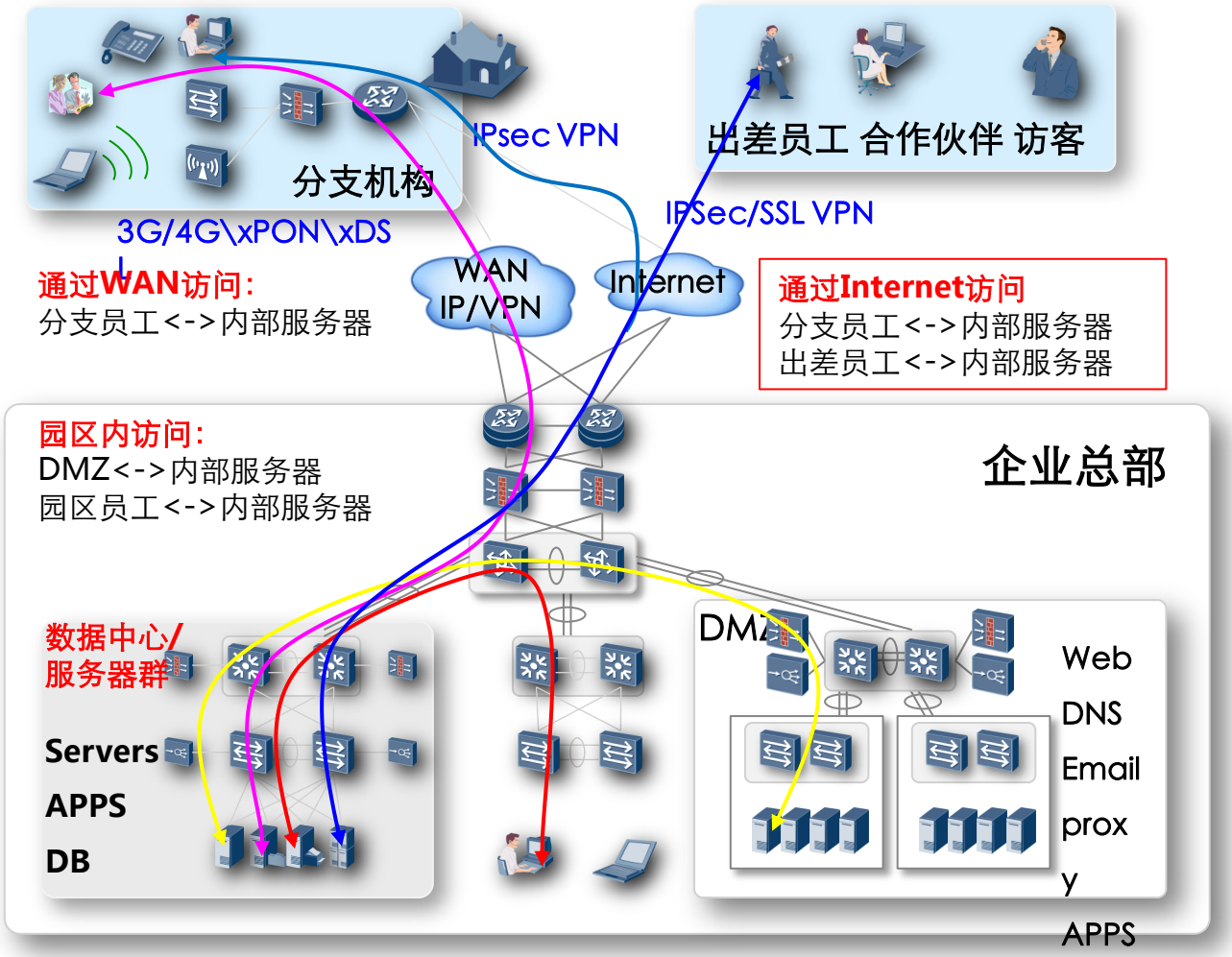
设置DMZ区是出于安全性和业务便利性的考虑。

外部用户可以访问DMZ区的web、ftp等服务，但不能访问到内部的服务。

DMZ区放置对外服务的web、ftp、mail服务器，也放置方便内部用户访问Internet的proxy、dns服务器等

涉及公网和私网转换主要应用NAT、IPSec/SSL VPN、GRE over IP Sec等技术。

内部服务器区设计



内部服务器区是放置为企业内部提供服务的服务器，对外服务所需的APP和DB服务器，建议放在DMZ，规模达到一定程度需要建设专门的数据中心。

内部用户能够造成更大的安全威胁，采取“未经明确允许的就是被禁止的”及“最小授权”的严格安全策略

内部服务器区安全部署重点关注内部子分区的隔离，安照企业组织、密级、业务进行子分区划分。

各子分区共用的设备,不同部门或业务采用虚拟技术隔离，如VLAN、VPN实例

绝秘子分区或业务在物理位置、接入交换机上分开；

网络管理、系统管理在物理位置、接入交换机上分开

涉及公网和私网转换主要应用NAT、IPSec/SSL VPN、 GRE over IP Sec等技术。

子目录

2 园区网基础解决方案

园区IP地址规划

- IP地址的合理规划是网络设计中的重要一环，大型网络必须对IP地址进行统一规划并得到实施。
- P地址规划的好坏，影响到网络路由协议算法的效率，影响到网络的性能，影响到网络的扩展，影响到网络的管理，也必将直接影响到网络应用的进一步发展。
- IP地址规划原则：唯一性、连续性、扩展性、实意性
- loopback地址：为了方便管理，会为每一台路由器创建一个loopback 接口，并在该接口上单独指定一个IP 地址作为管理地址，loopback地址务必使用32位掩码的地址，最后一位是奇数的表示路由器，是偶数的表示交换机，越是核心的设备，loopback地址越小。
- 互联地址：互联地址是指两台网络设备相互连接的接口所需要的地址，互联地址务必使用30位掩码的地址。核心设备使用较小的一个地址，互联地址通常要聚合后发布，在规划时要充分考虑使用连续的可聚合地址。
- 业务地址：业务地址是连接在以太网上的各种服务器、主机所使用的地址以及网关的地址，业务地址规划时所有的网关地址统一使用相同的末位数字，如：.254都是表示网关。
- 园区网内部的IP地址建议使用私网IP地址，在边缘网络通过NAT转换成公网地址后接入公网。
- 汇聚交换机下接入的网段可能有很多，在规划的时候需要考虑路由是可以聚合的，这样可以减少核心网络的路由数目

园区VLAN规划

用户VLAN

用户VLAN即普通VLAN，也就是我们日常所说的VLAN，用来对不同端口进行隔离的一种手段。VLAN通常根据业务需要进行规划，需要隔离的端口配置不同的VLAN，需要防止广播域过大的地方配置VLAN用于减小广播域。 VLAN最好不要跨交换机，即使跨交换机，数目也需要限制

Voice VLAN

Voice VLAN是为用户的语音数据流划分的VLAN，用户通过创建Voice VLAN并将连接语音设备的端口加入Voice VLAN，可以使语音数据集中在Voice VLAN中进行传输，便于对语音流进行有针对性的QoS（Quality of Service，服务质量）配置，提高语音流量的传输优先级，保证通话质量。

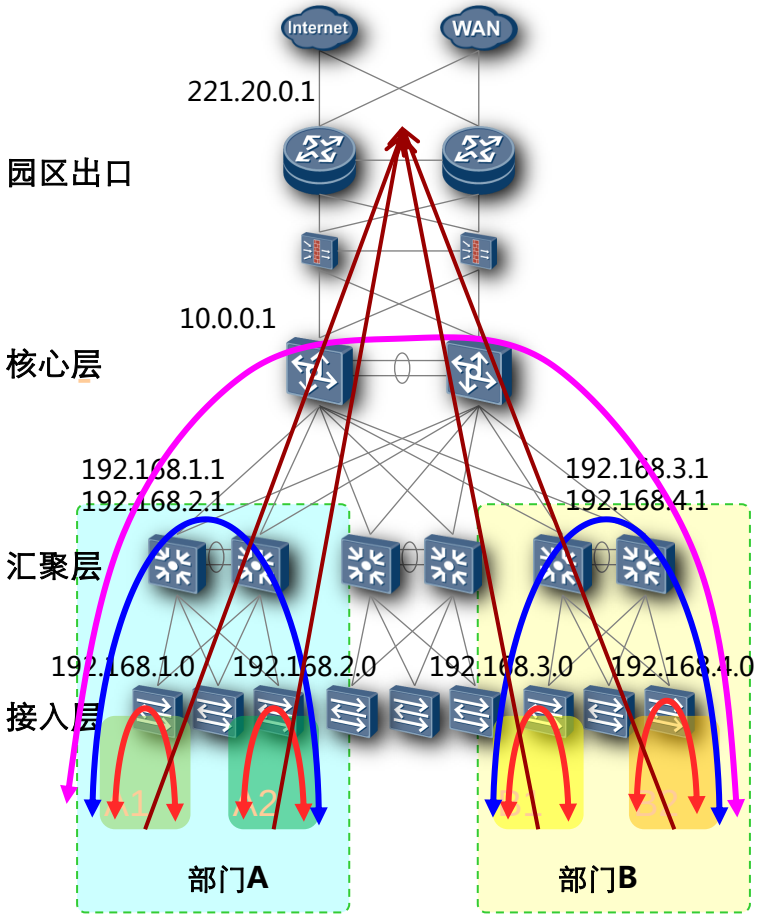
Guest VLAN

网络中用户在通过802.1x 等认证之前接入设备会把该端口加入到一个特定的VLAN（即Guest VLAN），用户访问该VLAN 内的资源不需要认证，只能访问有限的网络资源，用户从处于GUEST VLAN的服务器上可以获取802.1x客户端软件，升级客户端，或执行其他一些应用升级程序（例如防病毒软件、操作系统补丁程序等）。认证成功后，端口离开Guest VLAN加入用户VLAN，用户可以访问其特定的网络资源。

Multicast VLAN

Multicast VLAN即组播VLAN，组播交换机运行组播协议时需要组播VLAN来承载组播流，组播VLAN主要是用来解决当客户端处于不同VLAN中时，上行的组播路由器必须在每个用户VLAN复制一份组播流到接入组播交换机的问题。

园区地址规划和VLAN隔离举例



园区出口：公司内终端接入到Internet或者总部通过出口路由器

从私网地址到公网的NAT转换以及Firewall等功能也集成在一起（也可独立）

语音视讯等业务也在AR上完成终结

终结分支部门或者出差员工接入到公司内部的VPN，并接入到内网

核心层：公司内各个部门之间的互联互通

部门之间的隔离可以通过ACL完成，也可以基于MCE，把不同的部门放到不同的VPN中去

有互访需求的部门通过VPN策略来控制路由发布

汇聚层：部门

子部门之间二层通过VLAN进行隔离，通过三层进行互通，网关设在汇聚交换机上,不同部门之间VLAN可以重合

子部门之间的隔离策略建议通过ACL来完成（手工配置或者NAC下发），也可以使用MCE隔离

接入层：子部门

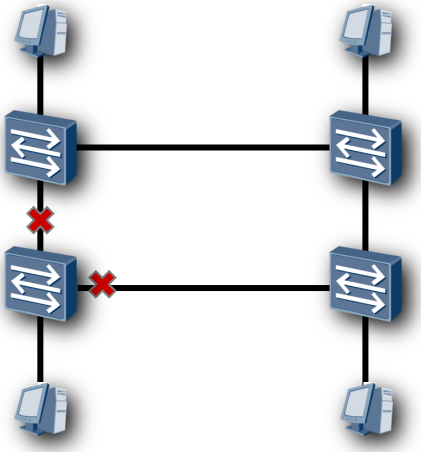
子部门分配独立的IP地址段，通过DHCP申请

部门内根据需要划分VLAN，建议需要隔离的划分不同的VLAN，其他在同一VLAN域内，二层互通；也可以都VLAN隔离，通过SuperVLAN解决网关问题，子部们之间VLAN必须不同

子目录

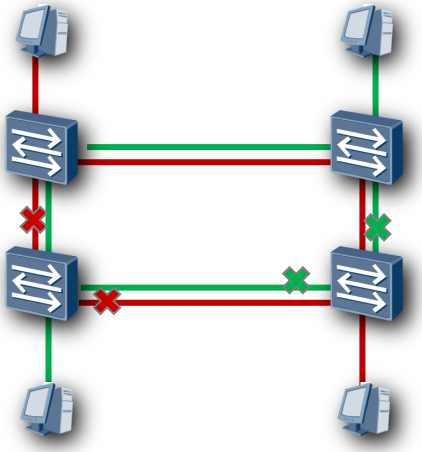
2 园区网基础解决方案

STP/RSTP/MSTP技术对比



STP/RSTP

协议	是否快速收敛	是否支持多实例
STP	X	X
RSTP	√	X
MSTP	√	√

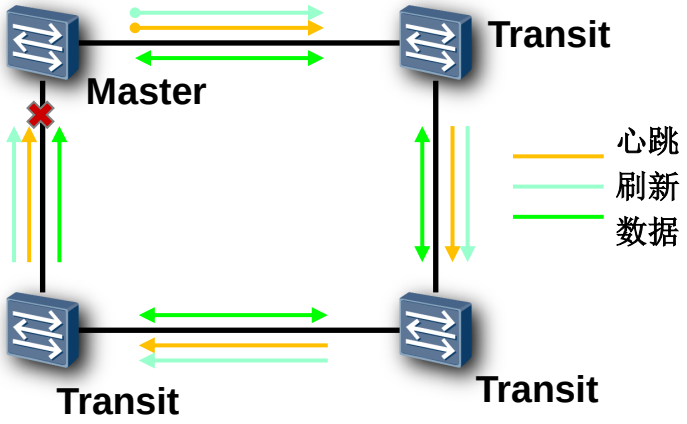


MSTP

在园区网中，MSTP用来避免人为形成环路所造成的广播风暴.
多棵生成树在VLAN间实现负载均衡，不同VLAN的流量安照不同的路径转发

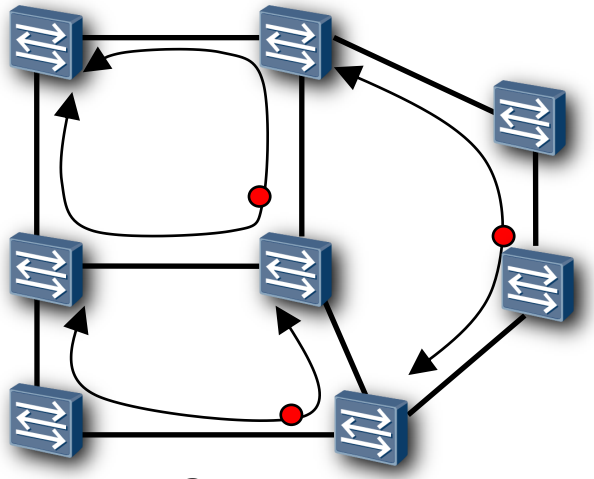
STP: Spanning Tree Protocol, 生成树协议 802.1d-1998
RSTP: Rapid Spanning Tree Protocol, 快速生成树协议 802.1d-2004
MSTP: Multiple Spanning Tree Protocol, 多生成树协议

RRPP/SEP实现快速收敛，SEP支持任意拓扑



RRPP

协议	50ms内收敛	非单独硬件支持	支持环网	支持任意拓扑
STP/MSTP/RSTP	X	√	√	√
RPR	√	X	√	X
RRPP	√	√	√	X
SEP	√	√	√	√



SEP

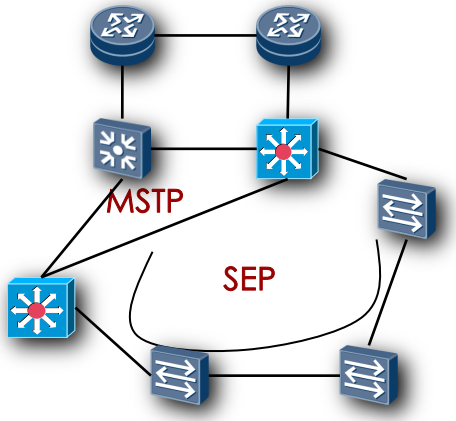
SEP/RRPP协议是专用于以太网的快速环保护协议,达到电信级倒换要求

RRPP当园区网中有环网的时候,能够达到最快的倒换效果

SEP能够适应任何拓扑，并与其他厂商联合组网

RRPP: Rapid Ring Protection Protocol,华为自主知识产权协议
SEP: Smart Ethernet Protection Protocol ， 华为自主知识产权协议

高可靠SEP半环保护



当前问题：
园区接入层目前主要依靠MSTP或RRPP来实现二层组网可靠性，但均存在不足：依赖标准的MSTP协议，业务收敛速度慢，通常在秒级；RRPP收敛快，但必须环上全是同一厂商产品

特色方案

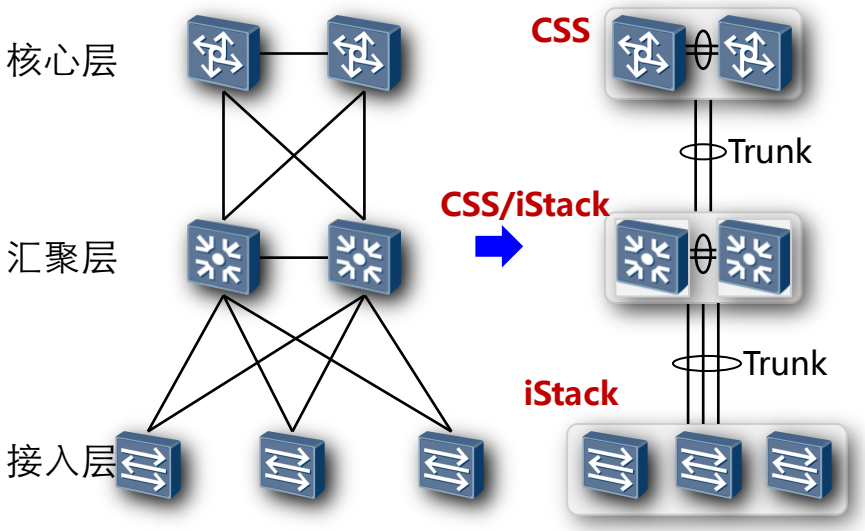
SEP环网保护方案，继承了50ms可靠性保护的快速倒换能

力，大大减少倒换引起的报文丢失

多厂家设备共存、扩容无障碍：可采用半环方案，不受限于环上都是同一厂家设备，破除现网封闭组网限制

优化提升用户的现网收敛速度：SEP通过标准协议向STP通知拓扑变化，优化流量路径，使现网MSTP及时收敛。

CSS+iStack无环以太网技术让可靠性变得简单



高可靠的物理和逻辑拓扑

可靠性机制

2台接入层堆叠，2台汇聚层集群，2台核心交换机集群

设备的可靠性保证

通过堆叠/集群技术保证节点的可靠性；一台设备故障后，另外一台设备自动接管所有的业务

链路的可靠性保证

通过Trunk技术，保证链路包括性； 一条或多条链路故障后,流量自动切换到其他正常的链路

配置简单，不易引入配置故障

不需要配置多数可靠性的协议，如VRRP等,减化配置和维护工作量，减少出错的机率

适应面广

适合于多数有可靠性要求的园区网络，可扩展

子目录

2 园区网基础解决方案

Page 37

BGP路由设计

园区网中使用BGP的场景

路由数量过于庞大，OSPF难以胜任时。

需要大量的使用路由策略或者是业务分流，OSPF等协议不擅长

部署MPLS VPN技术时，用于复杂的隔离策略等。

Router id的规划

BGP的router id与ospf的router id共用一个，与loopback接口地址相同

AS number的规划

由于企业网中都是私有网络，所以BGP使用私有的AS number

IBGP和EBGP的选择

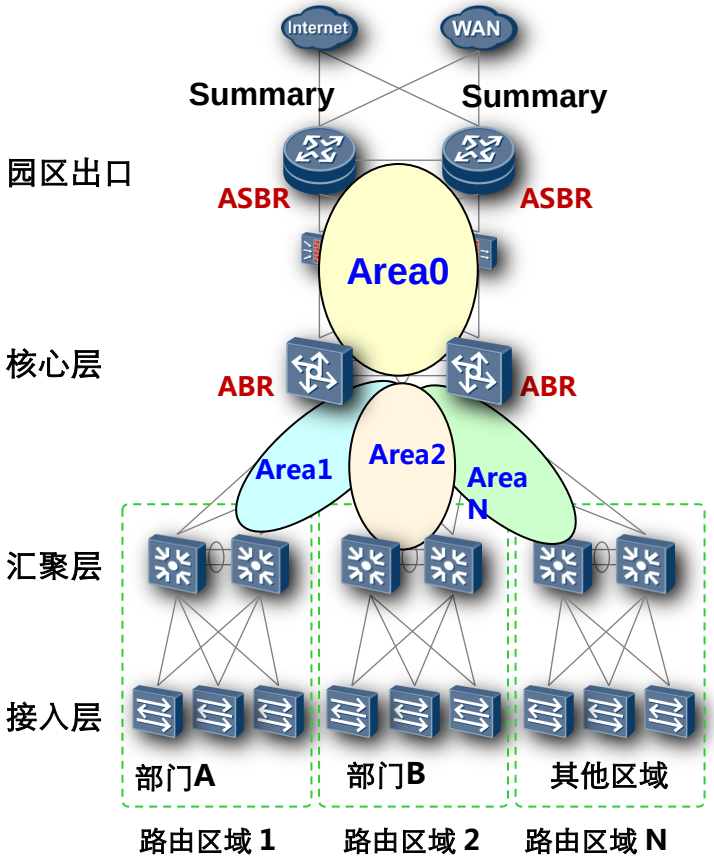
由于企业网的规模通常都不会很大，通常IBGP就可以满足一般的需求了

BGP对设备的要求

BGP协议本身并不消耗很多资源，只有当运行BGP的设备需要学习到很多条路由，需要建立很多邻居关系时才会要求设备自身的性能很高

只要规划得当，任何档次的设备（包括接入层设备）都可以运行BGP协议

园区网IGP路由选择



鉴于园区网内部可能存在不规则区域，且路由节点不是特别多，建议使用OSPF路由协议

每个业务部门区域作为一个单独的OSPF区域

出口路由器和核心交换机作为OSPF的Area0, 出口路由器作为ASBR和ABR，核心交换机为ABR

每个汇聚交换机和核心交换机组网部署为不同的OSPF Area ID 1,2,N

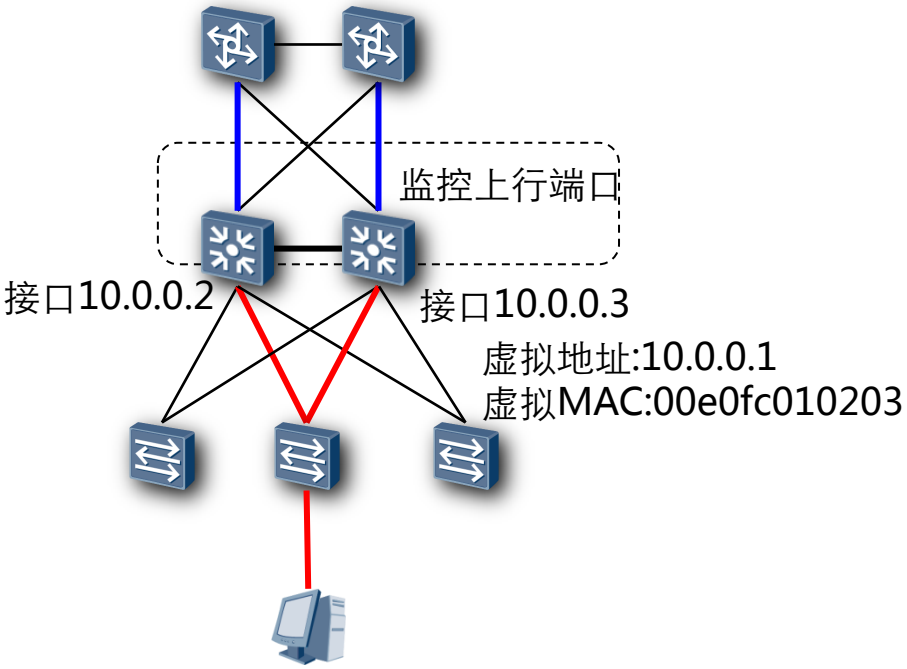
Area 1,2,N 使用OSPF NSSA 区域，限制LSA在区域间的传播

核心交换机和出口路由器, 通过区域汇总，限制区域间传播的LSA条目

一个区域的路由计算和网络调整不会影响其它区域,因故障引起的路由震荡被隔离在区域内部.

如果部门较少，建议只配置Area0.

VRRP实现网关可靠性



第一跳网关的可靠性即终端接入的可靠性通常使用VRRP协议来保障

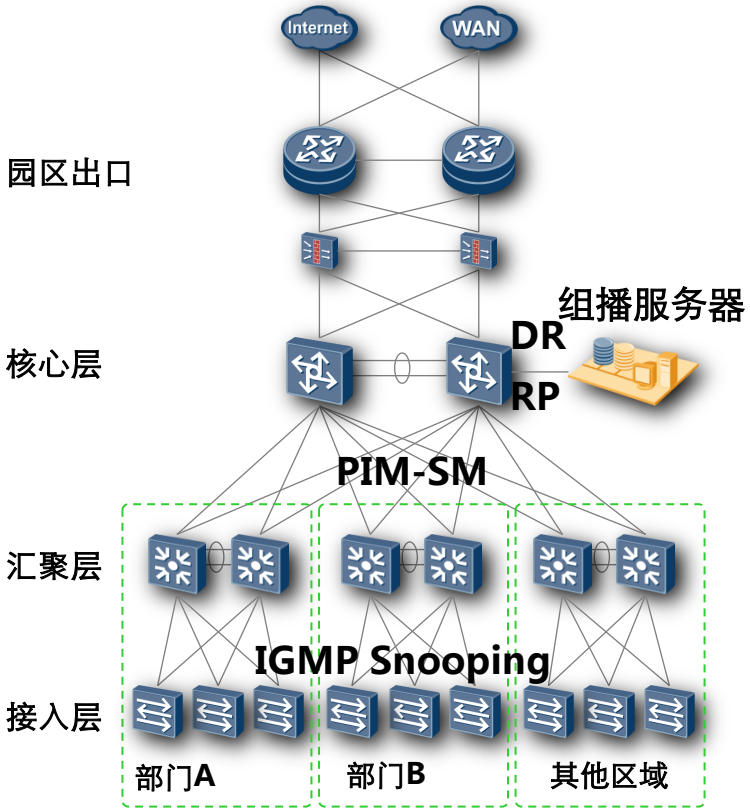
两台网关设备通过一台二层交换机或者设备之间的直连链路交换VRRP报文信息，并向下提供虚拟IP及MAC地址

主用的网关同时监控上行接口，上行链路故障或设备故障时会自动切换

华为支持BFD for VRRP即VRRP+，加速VRRP收敛时间

VRRP适用场景广泛：例如核心交换机三层保护倒换

组播设计



组播在园区网一般用于特殊场景，比如说网上教学、IPTV、VOD等业务，视频监控一般使用单播

采用PIM SM + IGMP Snooping来实现:

- 汇聚交换机到组播源采用PIM-SM协议；在接入交换机通过IGMP Snooping + 组播VLAN实现跨VLAN的组播；终端上部署IGMP

园区网络比较简单时，一般RP设置在和源DR在同一台核心交换机上;园区网络比较复杂时，选取一台性能较高的路由器作为DR

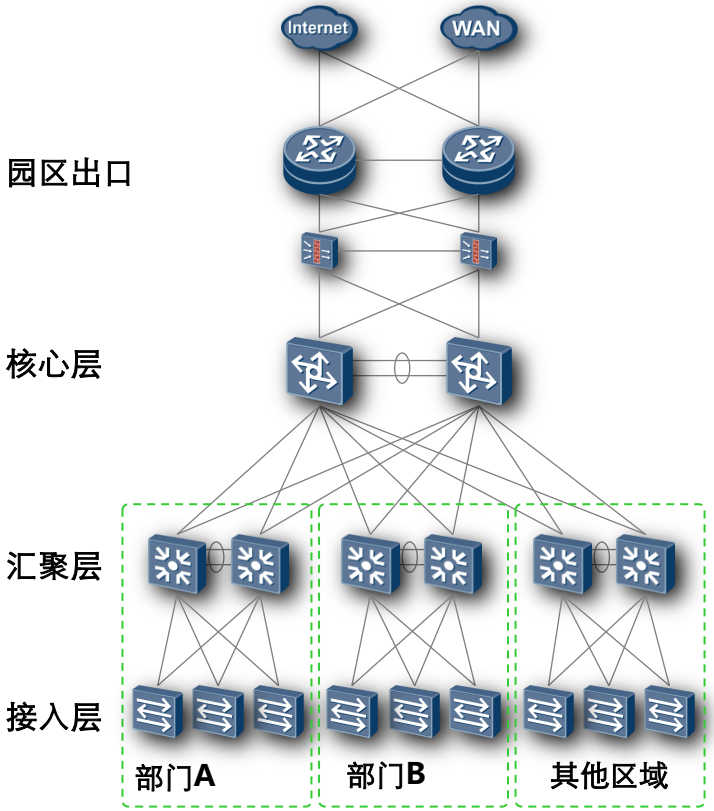
通过RPF检查组播流的合法性

子目录

2 华为园区网基础解决方案

Page 42

可靠性设计



园区网中可靠性可以分为：

设备本身的可靠性：CSS，部件冗余

二层网络的可靠性：SmartLink，MSTP，Trunk，DLDP，SEP，RRPP

三层网络的可靠性： IP FRR，NSF/GR，ECMP/UCMP， VRRP ,BFD等

适当的冗余设计能够有效提升可靠性，如：双归属链路、链路捆绑

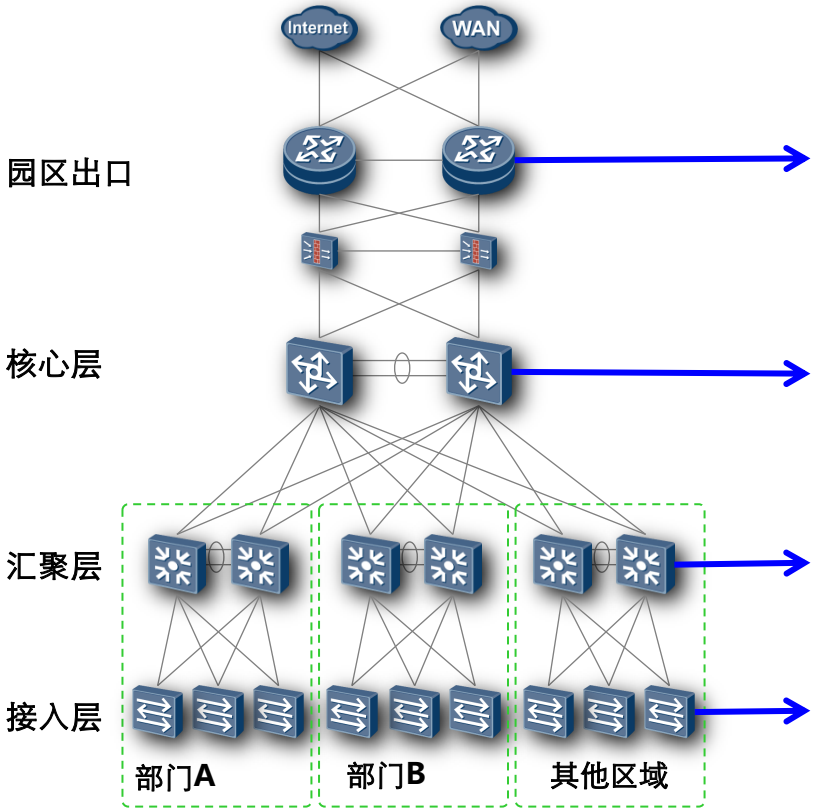
可靠性技术有多种，如何选择取决于业务需要、组网以及设备能力

层次越高的地方对可靠性要求越高

拓扑越简单可靠性肯定越容易保证

设备自身可靠性考虑

设备可靠是整个网络可靠的基础，除非特殊场景否则建议遵循如下基本原则



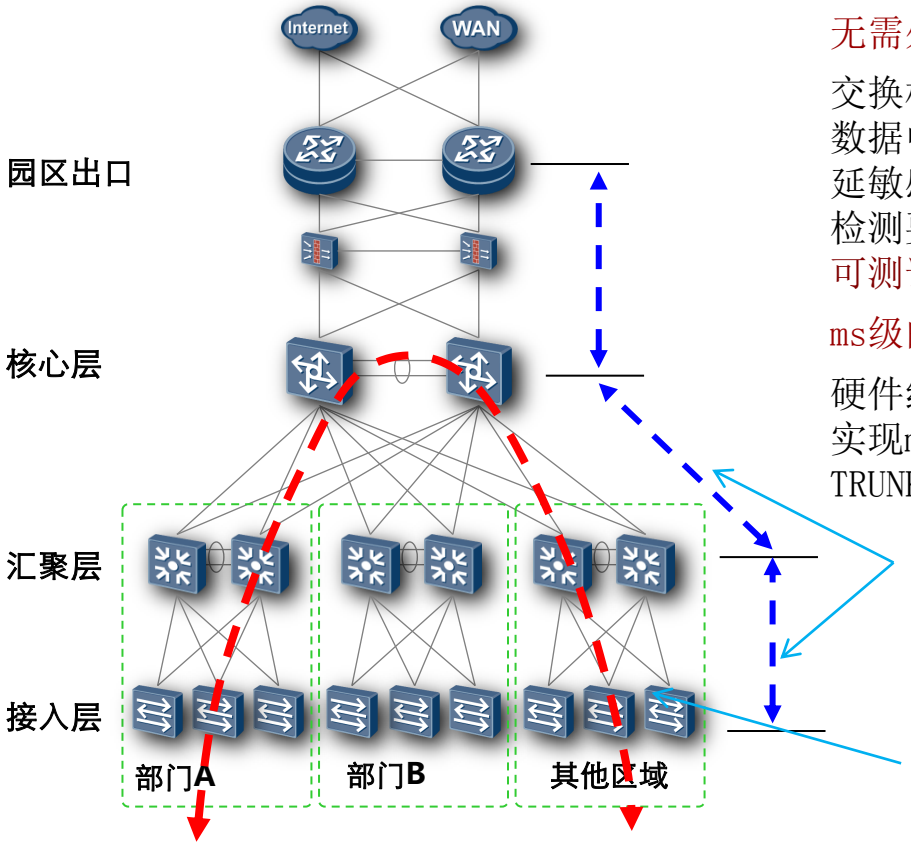
具备电信级可靠性
双上行到不同WAN或者运营商
支持双机热备

具备电信级可靠性，并支持SSO
设备Full Mesh

关键模块冗余备份，特殊情况可单主控
建议堆叠实现双机备份
双链路上行到核心设备

往往对于冗余要求较低，基本不考虑设备自身冗余（特殊场景电源冗余）
双链路上行即可

低延时检测及硬件级故障检测能力



引入S9300的灵活插卡，以及S5700HI，3700HI交换机

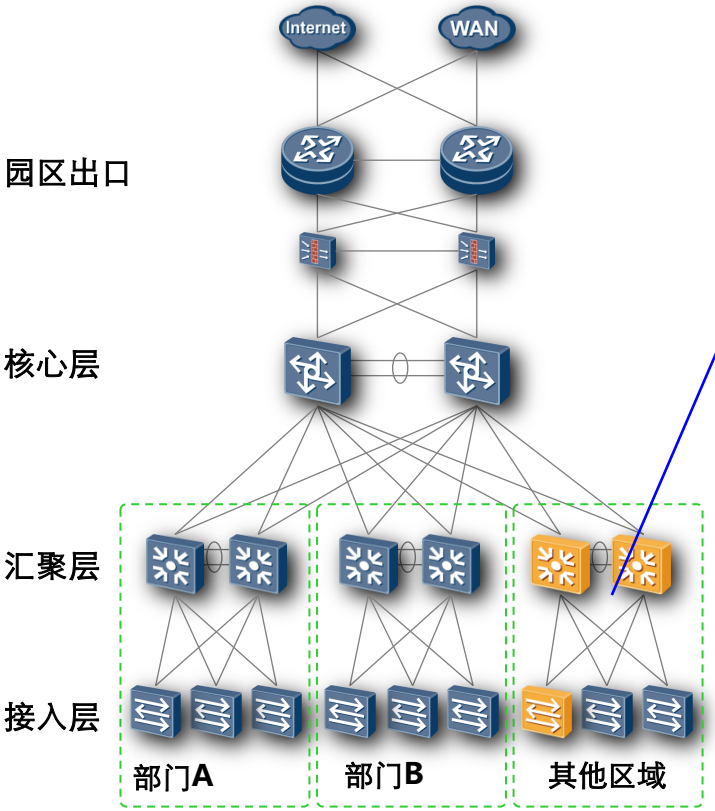
无需外置探针的端到端低延时检测能力

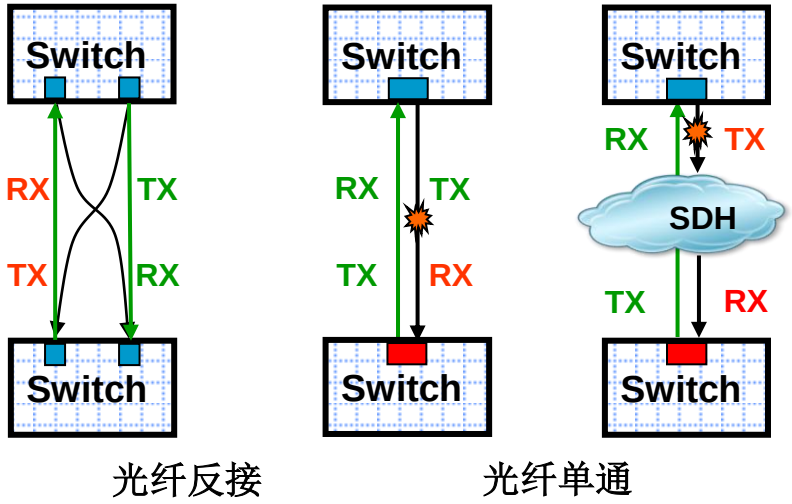
交换机内置硬件探针能力，基于Y1731协议，实现数据中心内端到端的时延检测和监控，服务于时延敏感业务的运维和管理(如金融证券业的低延时检测要求)，免去外挂专业时延检测设备，同时还可测试抖动和丢包率。

ms级的硬件级链路故障检测能力

硬件级的Ethernet OAM链路故障检测机制(3.3ms)，实现ms级故障检测和联动倒换(应用于集群分裂、TRUNK链路选路、路由重选路)；

二层网络可靠性——DLDP



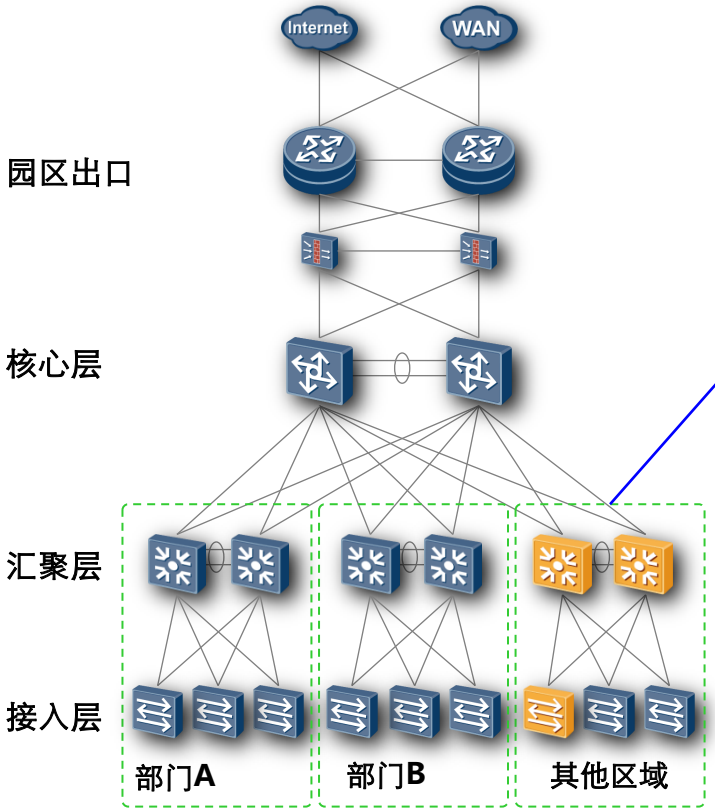


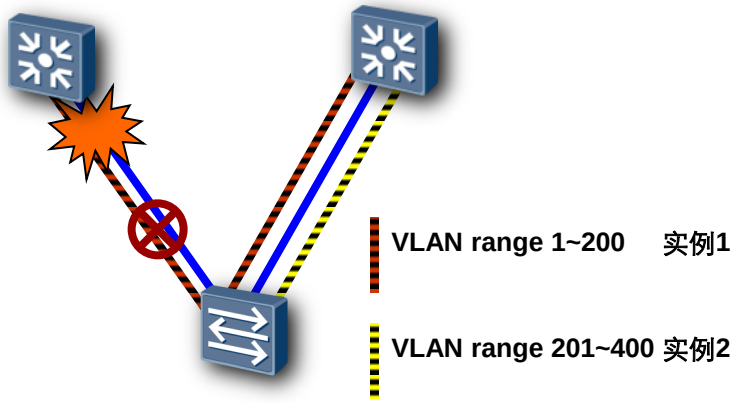
单向链路检测协议 (DLDP)能够检测光纤或者双绞线的链路状态。

如果存在单向连通，DLDP能够自动或者向管理员报告手工关闭端口，避免连通问题。

DLDP能够和RRPP、Smart Link等保护协议联动实现单通保护倒换

二层网络可靠性——Smartlink





Smart Link 是一种为双上行组网提供高效可靠的链路备份、负载分担和快速收敛性能的解决方案

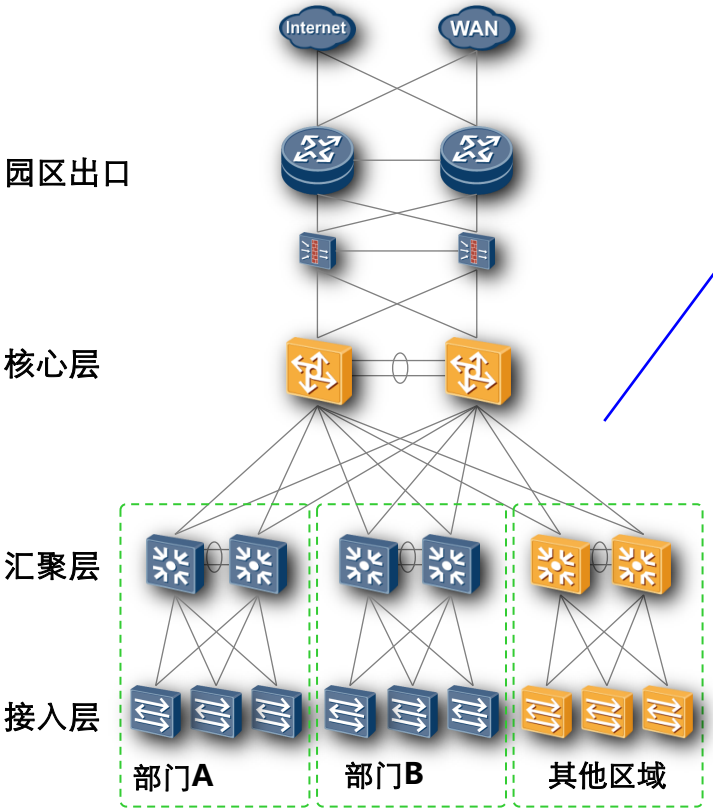
可以在二层也可以在三层组网中使用，通常在园区网接入交换机和汇聚交换机之间使用

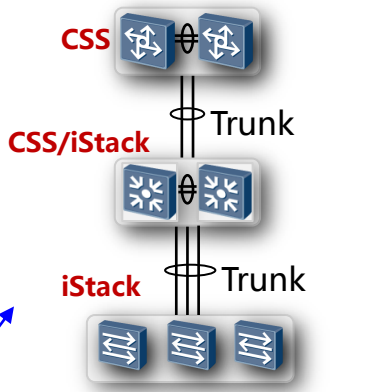
50ms快速保护倒换，自动链路故障恢复

Smart Link多实例实现链路负载分担，华为设备单台最大支持8链路聚合

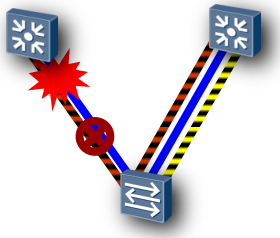
Smart Link与Monitor Link联动，用于监控上行链路，增强可靠性

二层网络可靠性总结

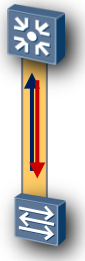




CSS+iStack+Trunk



Smart Link



DLDP

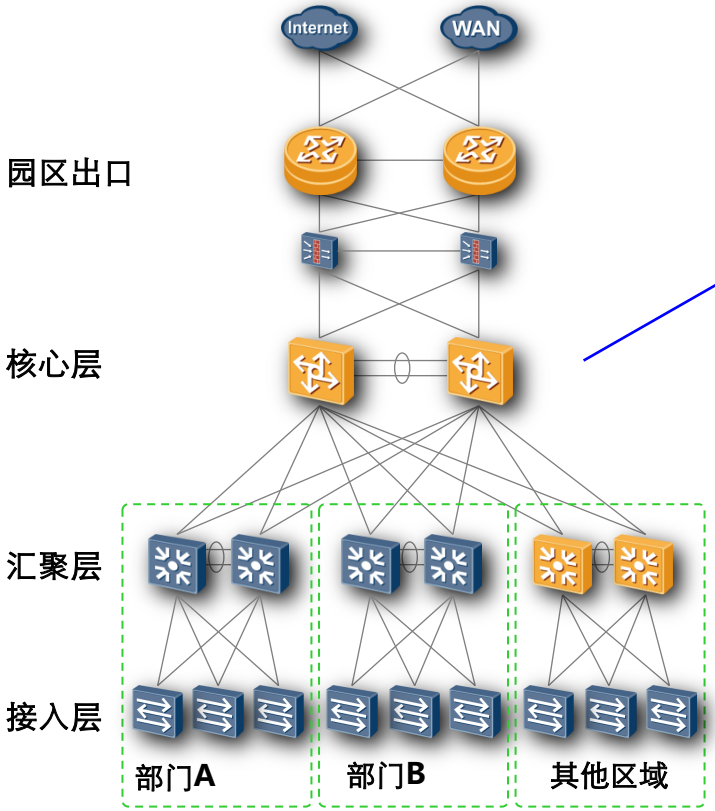
Trunk即链路捆绑是解决两个设备之间可靠性以及带宽扩展的好办法，对于两层都是双设备备份情况下和CSS配合使用，转发路径通过HASH得到，实际情况中根据需要及能力进行3元组、4元组或者5元组HASH，通常在虚拟园区网中使用

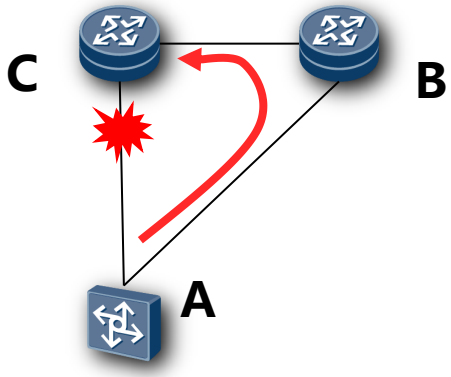
Smart Link 是一种为双上行组网提供高效可靠的链路备份、负载分担和快速收敛性能的解决方案，可以在二层或三层组网中使用，通常在接入到汇聚使用

DLDP部署在设备之间用于检测光纤是否存在单通的情况，发现单通后进行链路阻塞，触发上层进行倒换，避免出现流量黑洞，建议光纤连接的设备间都部署DLDP

在有二层链路时MSTP配置是为了避免误操作成环，这是必须的，通常全网部署

三层网络可靠性——IP FRR





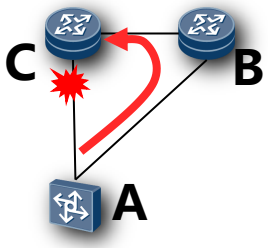
IP FRR：IP Fast Reroute，即IP快速重路由

IP FRR是一种转发快速切换技术，在链路故障时无需等待路由收敛，直接转发切换到备份路径。

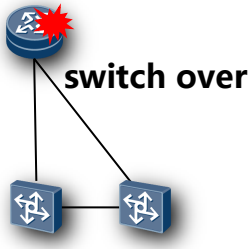
通常在汇聚到核心、核心到出口路由器之间部署

从A到C之间的路径为主转发路径，当A检测到A到C之间的主路径出现链路故障时，快速切换转发下一跳至B，启用备份路径，A-B-C之间的路径为事先建立好的转发路径

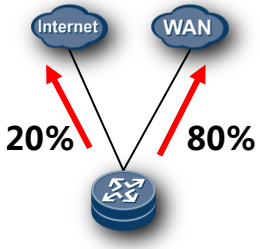
三层网络可靠性总结



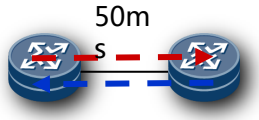
IP FRR



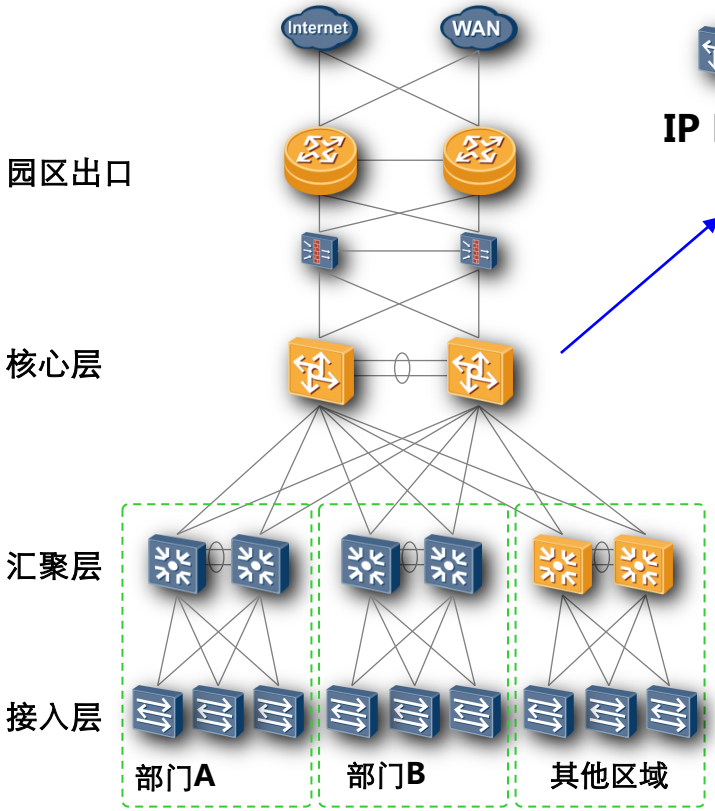
NSF/GR



ECMP/UCMP



BFD



IP FRR在链路故障时无需等待路由收敛，直接转发切换到备份路径，通常在汇聚到核心以及核心到出口路由器之间部署

NSF/GR是设备本身的可靠性的一种，在设备主控倒换时，转发层面不等待控制平面重新计算路由，先保持现有转发路径不变，通常在所有三层设备上部署

ECMP/UCMP解决三层设备之间的转发能力扩展和可靠性问题的，根据实际链路情况和需要配置成等价转发路径或者非等价转发路径，实际转发路径通过HASH得到，根据需要进行3元组、4元组或者5元组HASH，是解决三层多路径的一种非常好的办法，主要用于园区出口连接广域网和Internet的不同运营商

BFD是一种三层检测机制，对相邻转发引擎之间通道故障提供轻负荷、持续时间短的检测。这些故障包括接口，数据链路，甚至可能是转发引擎本身。提供一个单一的机制，它能够用来对任何媒介、任何协议层进行实时地检测，并且检测的时间与开销范围比较宽。

可靠性设计总结

OSS/CSS/部件冗余

主控板、电源模块、风扇框全部冗余且热插拔；状态切换保主用备用主控状态同步；堆叠确保逻辑和物理拓扑高可靠。

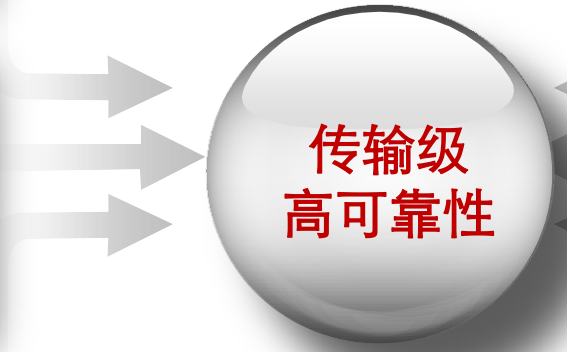
ISSU

不中断业务软件升级能够将由于软件升级而造成的业务中断时间化为最小。

NSF

不间断转发包括GR for OSPF、GR for ISIS、GR for BGP 和GR for LSP，保证网络业务的永续性。

99.999%+



SmartLink/Trunk/DLDP

确保二层链路在各种复杂组网强化连通的强壮和稳定可靠，带宽高利用率。

RRPP/E-VRRP/SEP

快速环保护协议与增强的虚拟路由冗余协议实现50毫秒保护倒换，保证关键业务不中断。

MPLS TE FRR/IP FRR

快速重路由技术能够确保4000条LSP能够在50毫秒内做到主备LSP的状态快速切换，无需等待路由收敛

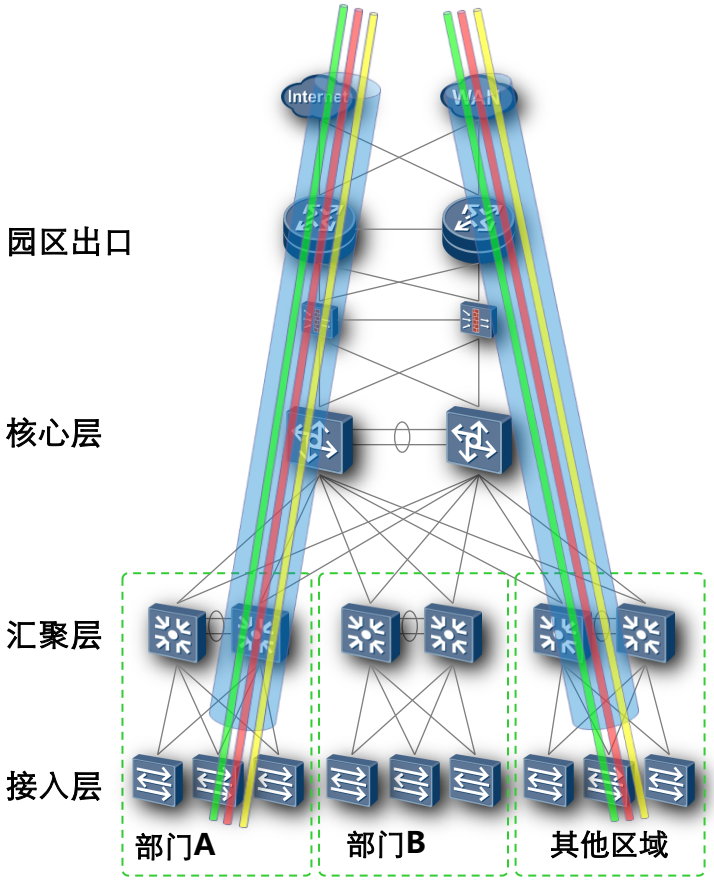
可用性 (%)	MTBF (年)	MTTR (小时)	年中断时间 (分钟/年)
99.99964	33.8	<0.5	1.9
99.99959	24.2	<0.5	2.2
99.99959	24.1	<0.5	2.1

MTBF 平均故障中断时间
MTTR 平均修复时间

子目录

2 园区网基础解决方案

端到端的QoS部署，保障核心业务和VIP用户



园区网应该是一个无阻塞的网络

园区网部署QoS主要是防止BT等非正常业务流量对园区网关键业务以及关键客户流量形成冲击

QoS的部署需要是端到端的，每一层承担不同的角色

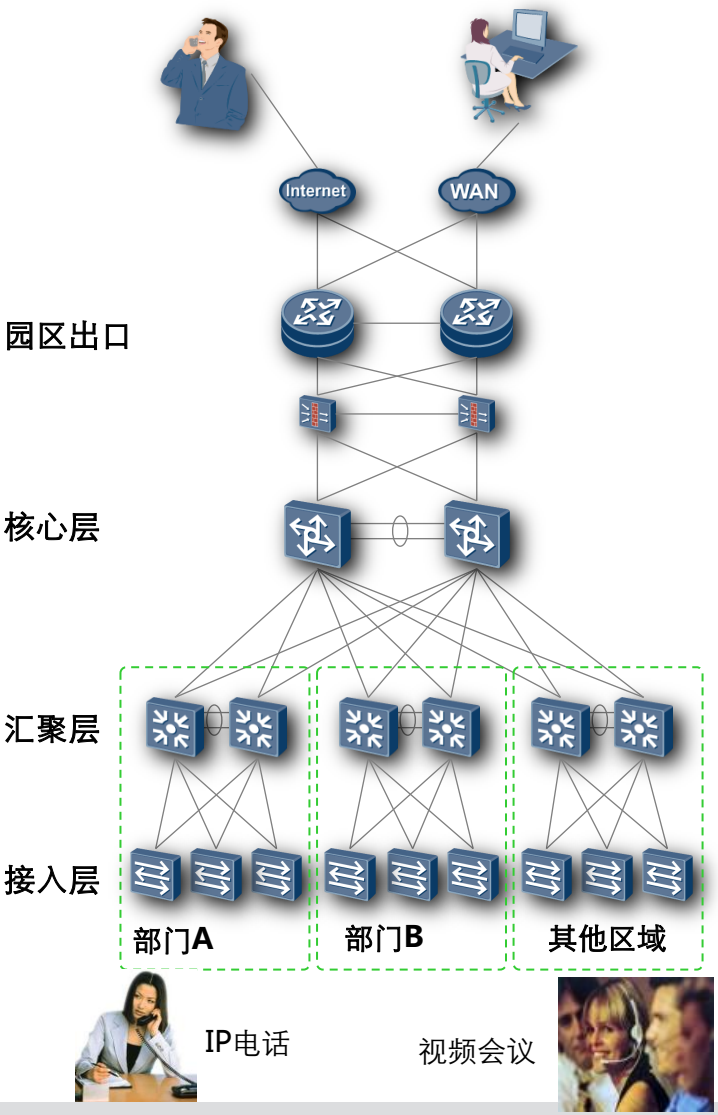
园区网所有节点都需要应用QoS策略

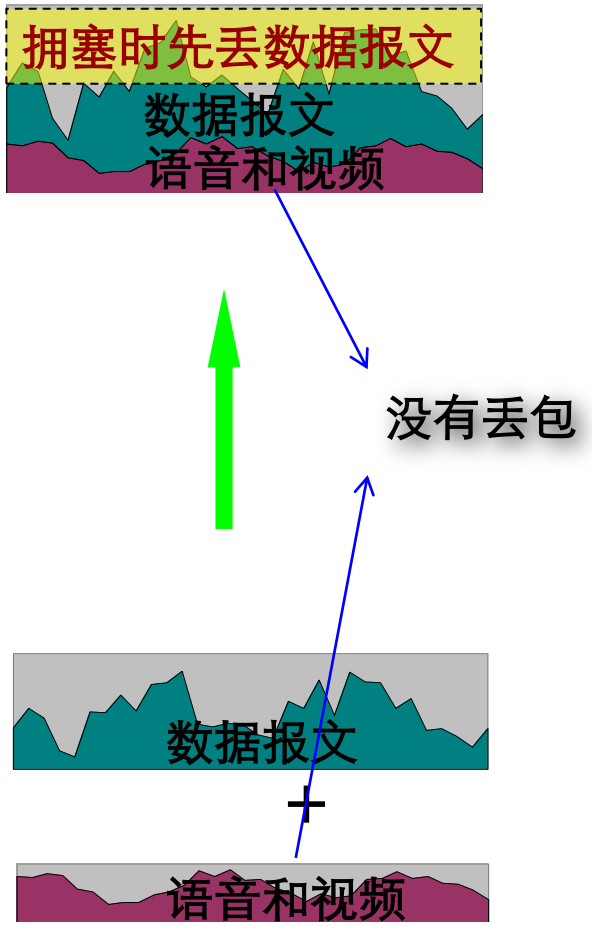
园区网QoS的策略主要是多个应用队列之间进行调度

接入节点通过Remark 802.1p/DSCP进行流量区分，其他节点根据流分类调度

一般情况下采用绝对优先方式（SP）进行调度，特殊情况配置WFQ及HQoS

QoS保障语音业务应用实例

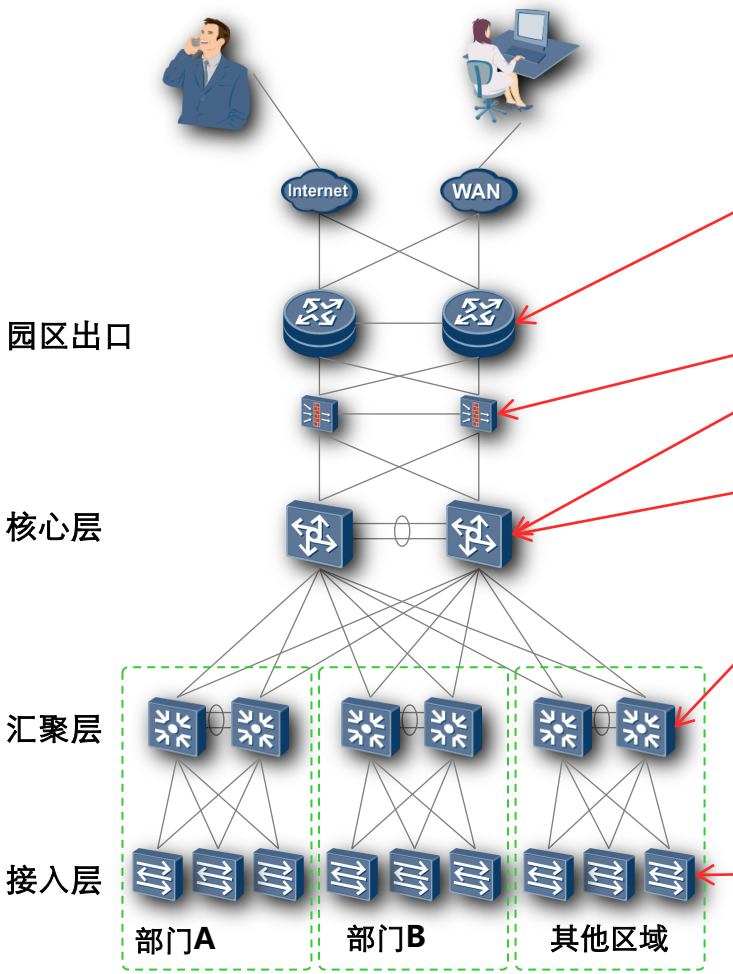




子目录

2 园区网基础解决方案

层次化端到端的园区网络安全



远程安全：

远程接入控制IPSec/SSL VPN

边界防御：

防火墙、IDS/IPS

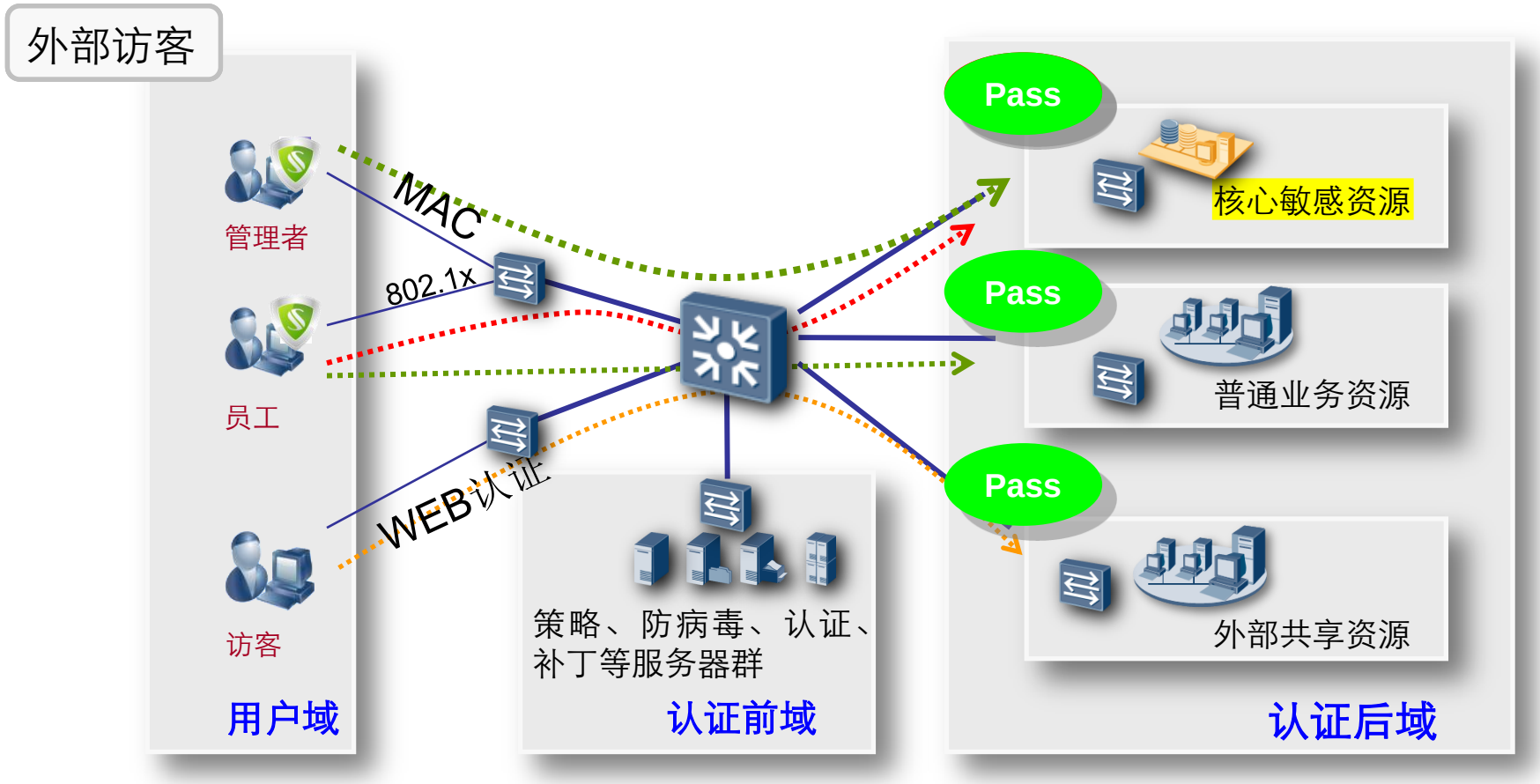
网络监管：

ACL流量控制
DHCP服务器欺诈攻击防范
ARP欺骗攻击防范
IP地址欺骗攻击防范
ARP限速功能
DHCP限速功能
MAC地址表容量攻击防护能力

接入安全：

终端安全接入控制（NAC）
用户隔离
端口隔离

准入控制+病毒清洗+分权分域实现接入安全控制



终端安全控制有两个目的，一是确保终端是干净的，二是确保身份和权限一致

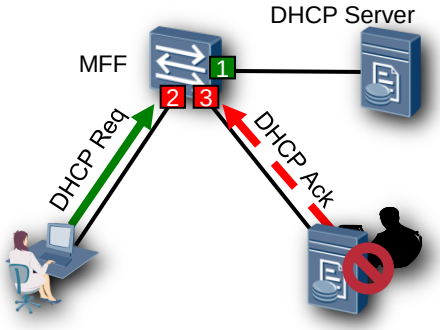
终端认证方式有三种：802.1x认证、MAC认证、WEB认证，认证通过之前只能访问认证前域

NAC客户端和策略服务器配套对用户终端健康状态进行检查（例如检查操作系统补丁、病毒等状态），如果检查不通过，则通知接入设备限制其进入网络

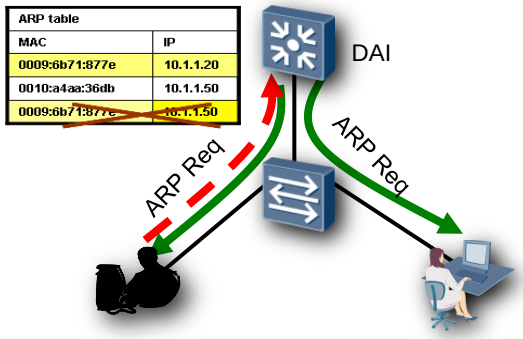
接入认证技术对比

技术比较	MAC	Portal/Web	802.1x	PPPoE
标准化程度	标准	WEB软件厂商私有	标准	标准
封装开销	小	小	小	大
控制方式	数据认证分开	数据认证分开	数据认证分开	数据认证统一
IP地址	无认证	认证前分配	认证后分配	认证后分配
组播支持	好	好	好	差
客户端软件	不需要	不需要	需要	需要
对设备要求	无	私有设备	大多数交换机	BRAS设备
安全性	低	高	高	高
地址仿冒能力	无	弱	弱	强
使用场景	有特殊权限的客户端	外部访客	内部员工	园区网不建议

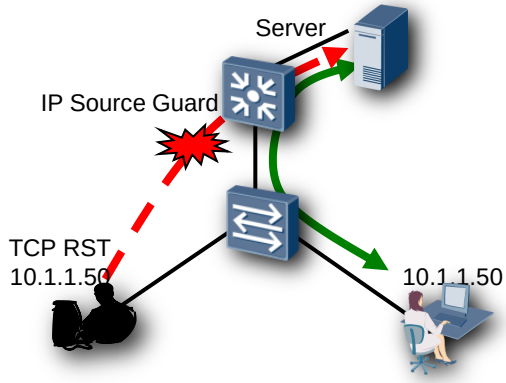
多种监听技术及风暴抑制实现内网安全



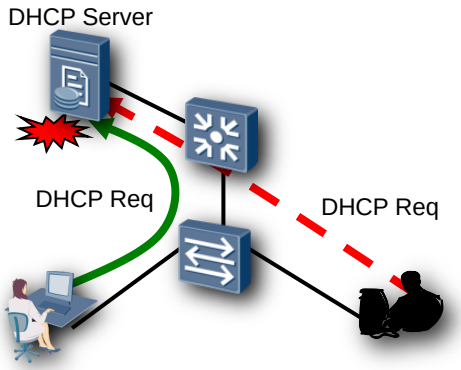
MFF—非法服务器



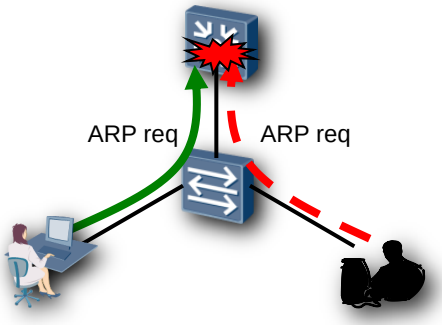
DAI—ARP欺骗



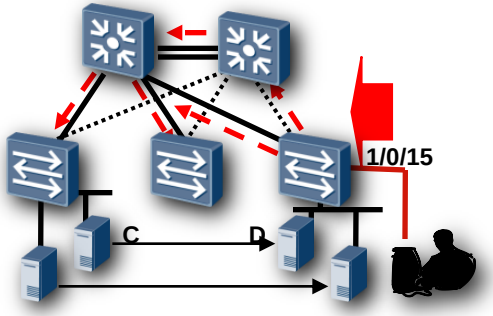
IP Source Guard—IP欺骗



DHCP 限速—DHCP 泛洪



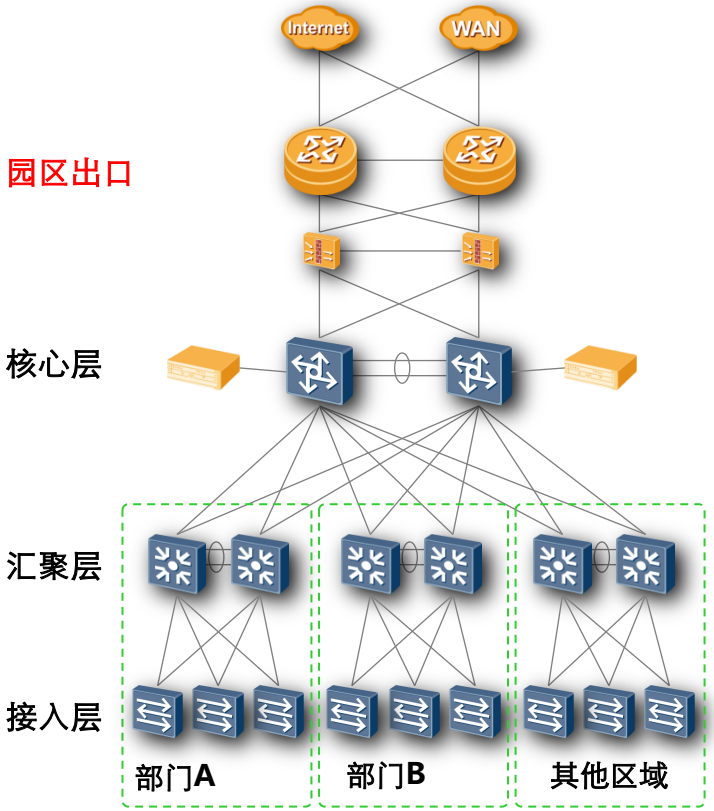
ARP 限速—ARP扫描



MAC 限速—MAC 泛洪

华为系列产品通过支持内网接入边界安全功能，防止内部合法及非法用户对网络进行攻击

边界安全



园区网连接到WAN/Internet等外部网络的边缘区域,

边界访问控制

防护来自internet的威胁，保障内部网络与internet隔离;

安全区域划分,加强安全区域之间访问控制,阻止安全威胁扩散;

网络，应用，数据立体的防御体系能够应对多样的安全威胁;

实时入侵防御

进行全面的攻击检测,事件管理与分析统计

防病毒

文件级病毒扫描，保证病毒检测的完整性;仿真环境，虚拟执行技术，让病毒暴露其不良活动企图或者现出原形;

上网行为管理:

50余种P2P流量的精确识别，K级流量控制;

IM软件的阻断,URL自动化分类过滤,

提高企业工作效率，减少园区网络内部风险，减少法律风险;

统一安全管理

统一的管理平台，提供TCP、UDP、ICMP等服务，服务组，多种IP协议的灵活支持;

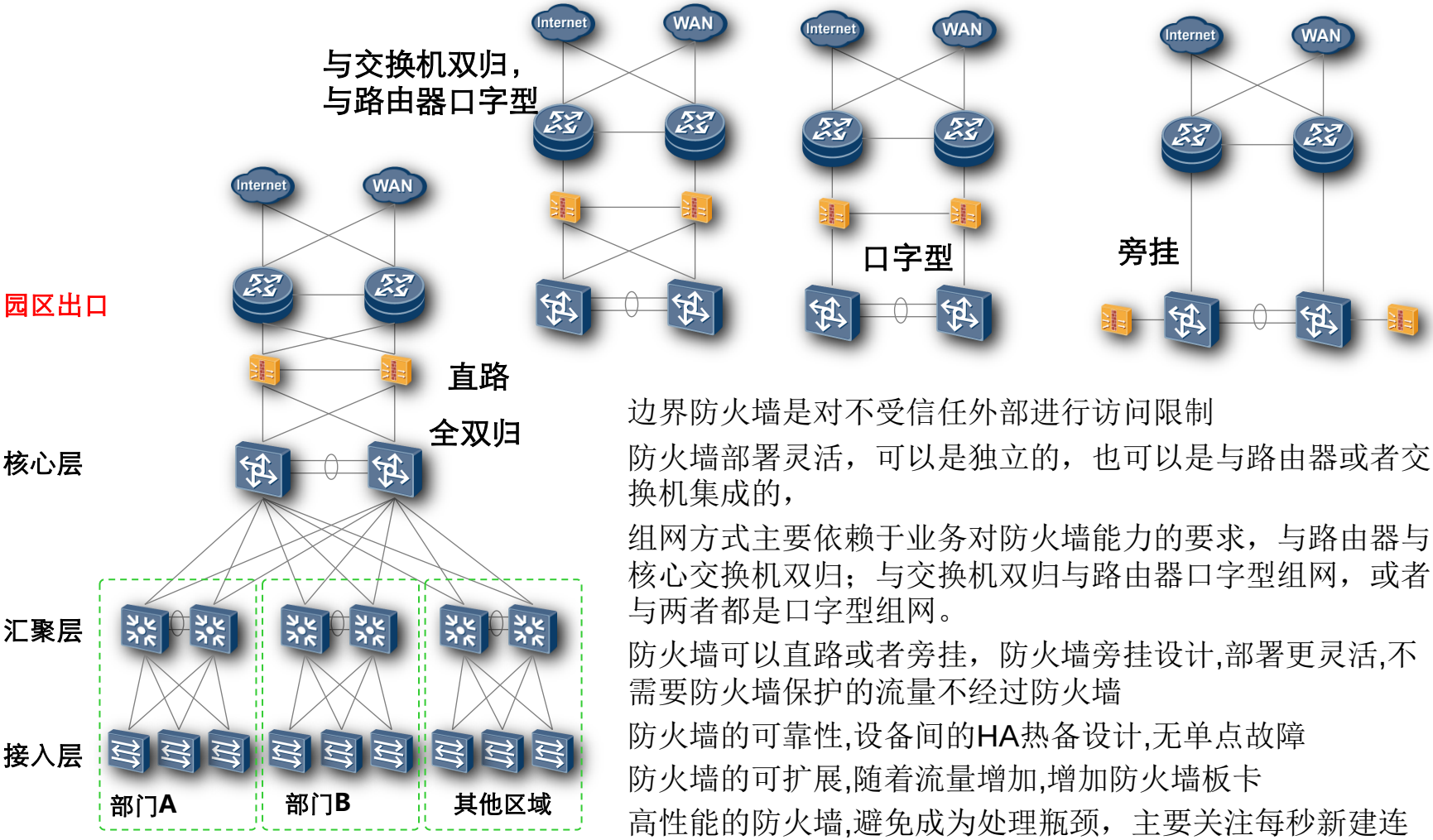
支持安全设备与交换路由设备单台设备和设备组的管理与策略下发。

对所有设备、数据库、服务器、主机进行日志分析管理

提供丰富的报表分析;

降低企业网络运维成本;

防火墙设计



边界防火墙是对不受信任外部进行访问限制

防火墙部署灵活，可以是独立的，也可以是与路由器或者交换机集成的，

组网方式主要依赖于业务对防火墙能力的要求，与路由器与核心交换机双归；与交换机双归与路由器口字型组网，或者与两者都是口字型组网。

防火墙可以直路或者旁挂，防火墙旁挂设计,部署更灵活,不需要防火墙保护的流量不经过防火墙

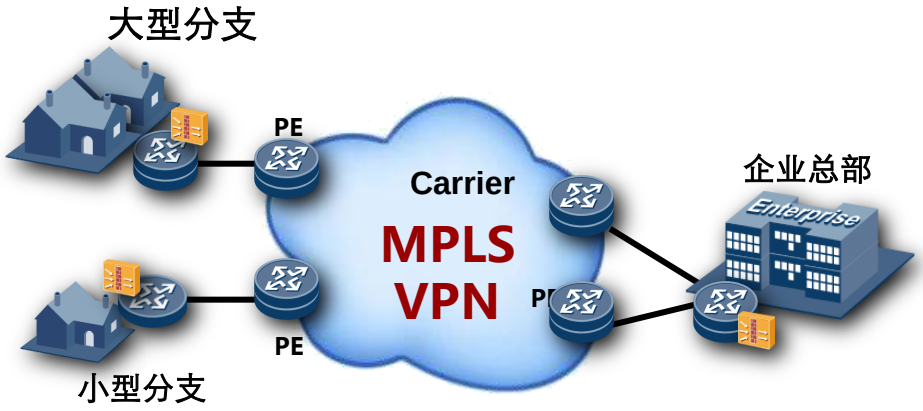
防火墙的可靠性,设备间的HA热备设计,无单点故障

防火墙的可扩展,随着流量增加,增加防火墙板卡

高性能的防火墙,避免成为处理瓶颈，主要关注每秒新建连接数，ACL匹配速度，DDOS识别技术

防火墙虚拟化，可”分割”给不同部门、不同区域使用

远程接入访问——远程接入解决方案建议

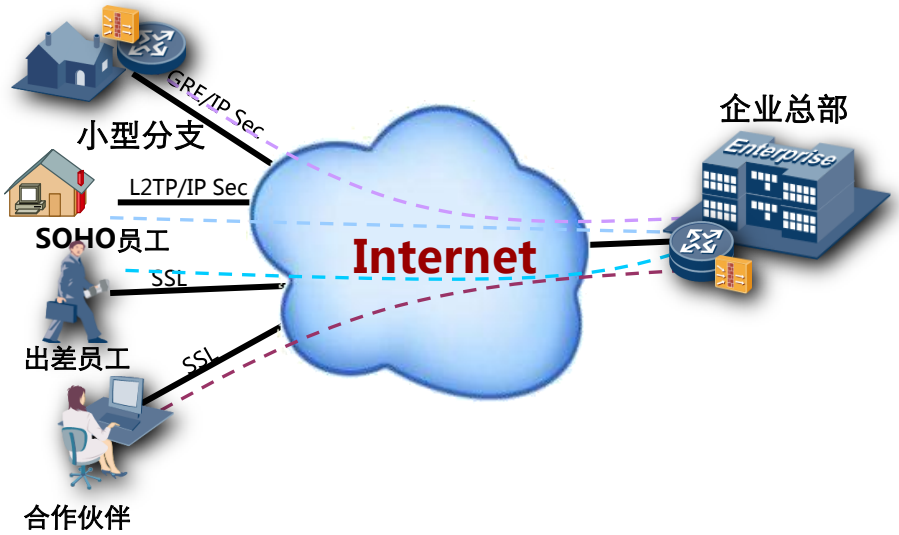


企业多园区互联

没有 广域专网的企业，通过运营商提供的MPLS VPN实现互联

租用运营商固定专线的企业，可以通过MPLS VPN实现内部业务隔离和互访

垂直行业通过自己的专网部署MPLS VPN互通，PE部署在企业出口路由器



Internet远程接入

企业分支通过GRE over IP Sec的方式实现和园区内部门同等业务，并确保安全

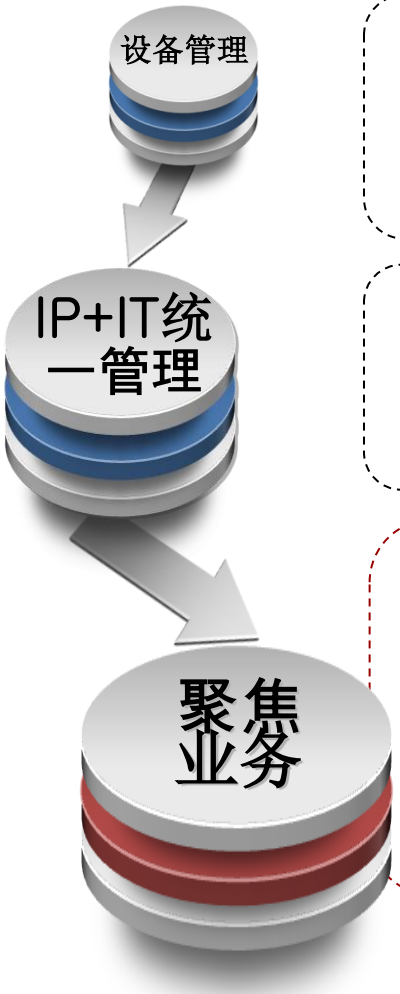
SOHO员工、出差员工通过L2TP或IP Sec VPN方式获得和园区内上班员工相同的权限

合作伙伴以及访客出差人员通过SSL VPN实现和企业互联互通，并且限制某些应用

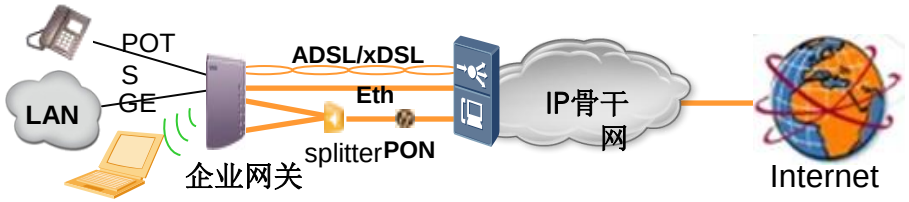
子目录

2 园区网基础解决方案

华为eSight企业运维解决方案

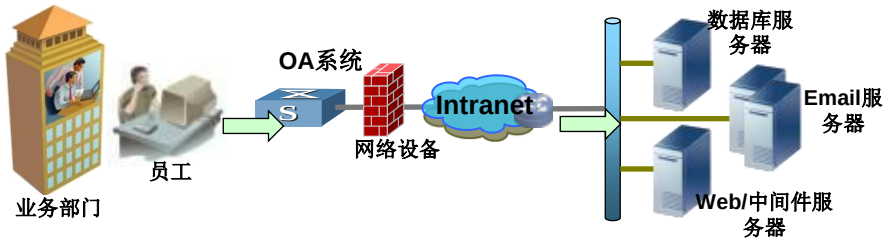


- **多厂商管理,有容乃大：**
  支持对多厂商设备的管理能力

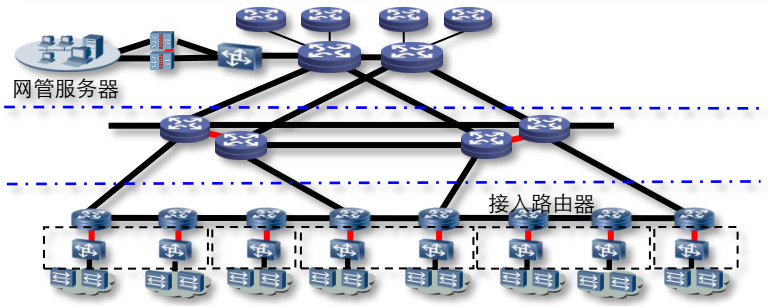


- **IT + IP统一管理：**
  IT设备(服务器、打印机等)、网络设备统一管理

- **面向业务的运维系统：**
  企业业务可视化管理、
  企业内部流量精细化管理
- **精细管理：**
  网络流量分析,聚焦核心业务



多厂商设备管理



HUAWEI H3C ITolP解决方案专家 CISCO ZTE中兴

客户问题：

IP网络是开放的，各厂商混合组网成为企业组网普遍情况。大部分企业不会像运营商一样建设综合网管，新厂商进入导致企业运维人员将面对多套厂商管理系统分而治之的情况，不具备全网设备统一监控的能力，出现网络故障后需要登录到多个网管查看状态，导致管理效率低下。

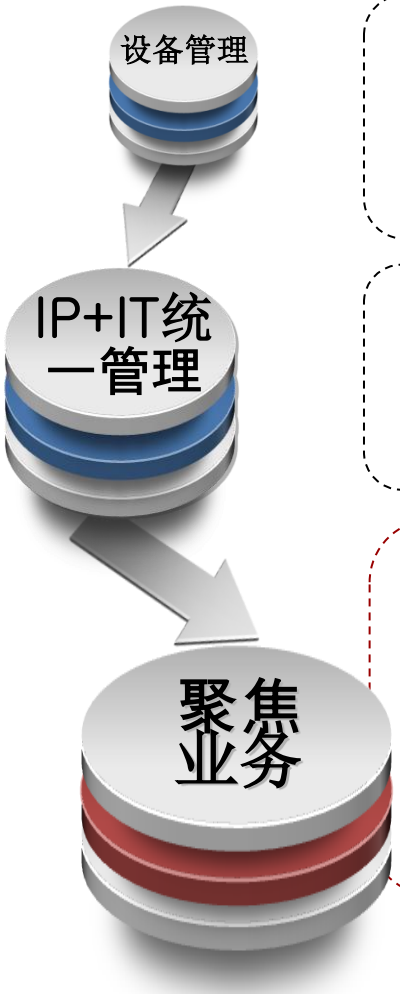
特色方案：

eSight预集成业界主流设备，默认已包含Cisco 20个系列140余款设备、H3C 14个系列130余款设备、其他厂商100余款设备、以及数十款打印机、服务器。企业运维人员不做任何配置，即可管理全网设备，大大提升管理效率。

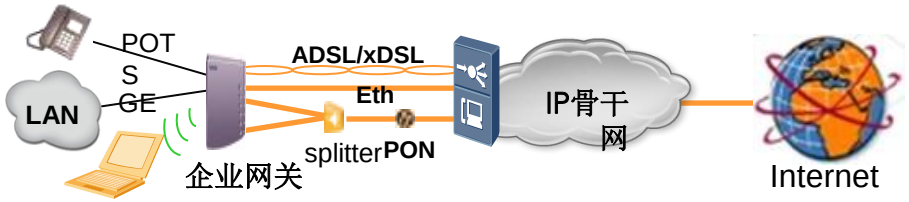
eSight拥有厂商新款设备自动配套能力，通过eSight厂商类型自动识别能力，对于友商新发布的设备也可实现拓扑、告警、性能等管理能力。

针对业界主流设备深入分析，不仅支持标准的流量采集，还同时支持设备面板、设备CPU利用率等私有属性的管理。

华为eSight企业运维解决方案

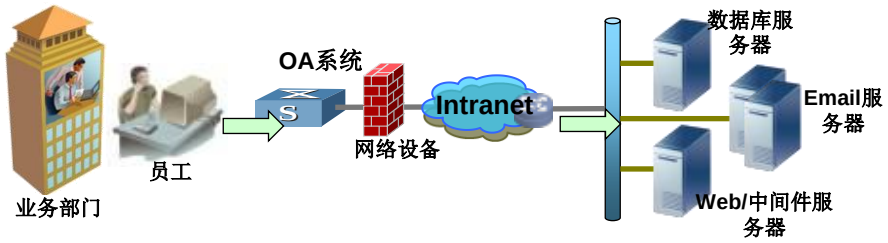


▪多厂商管理,有容乃大：
支持对多厂商设备的管理能力

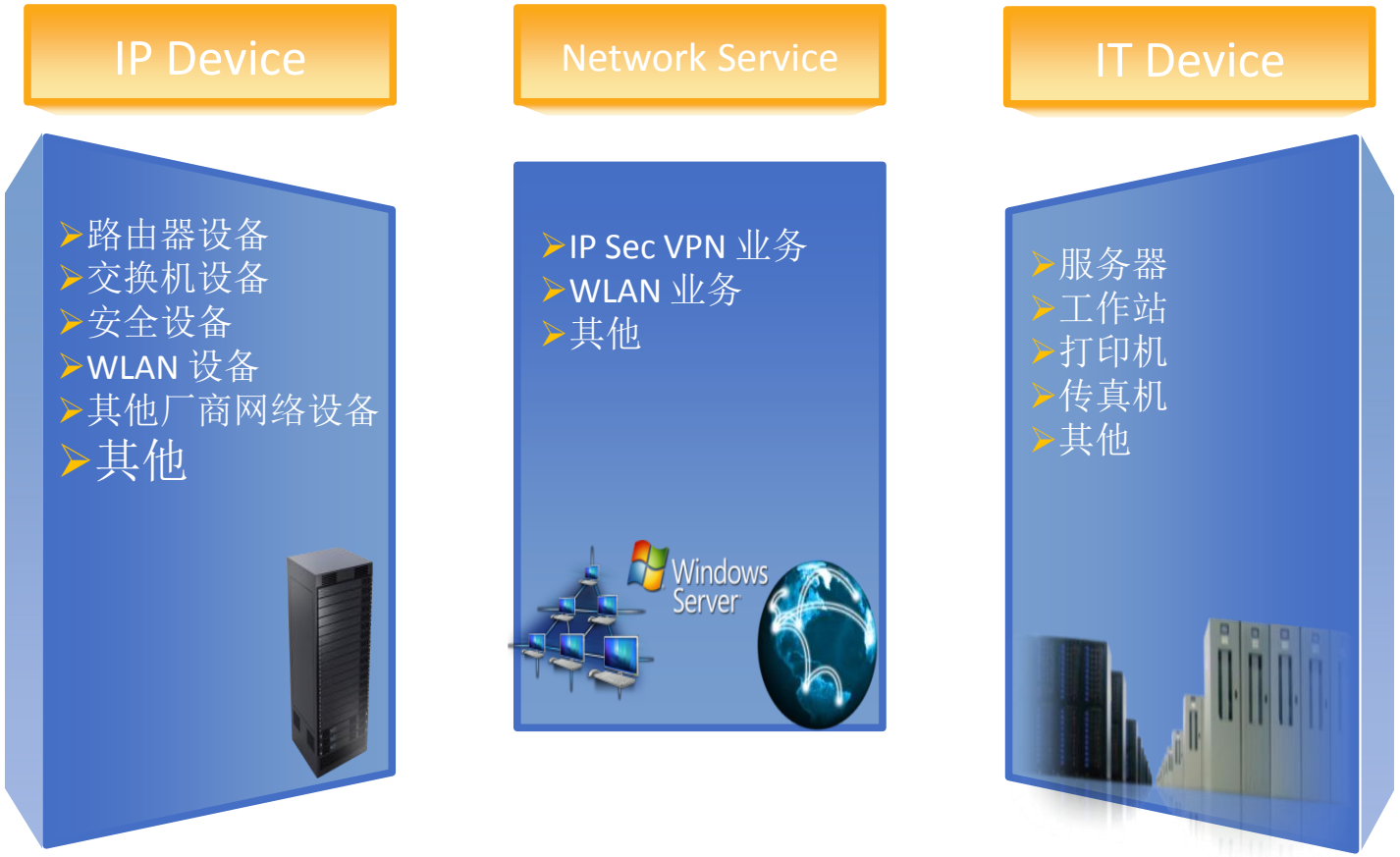


▪ IT + IP统一管理：
IT设备(服务器、打印机等)、网络设备统一管理

▪面向业务的运维系统：
企业业务可视化管理、
企业内部流量精细化管理
▪精细管理：
网络流量分析,聚焦核心业务



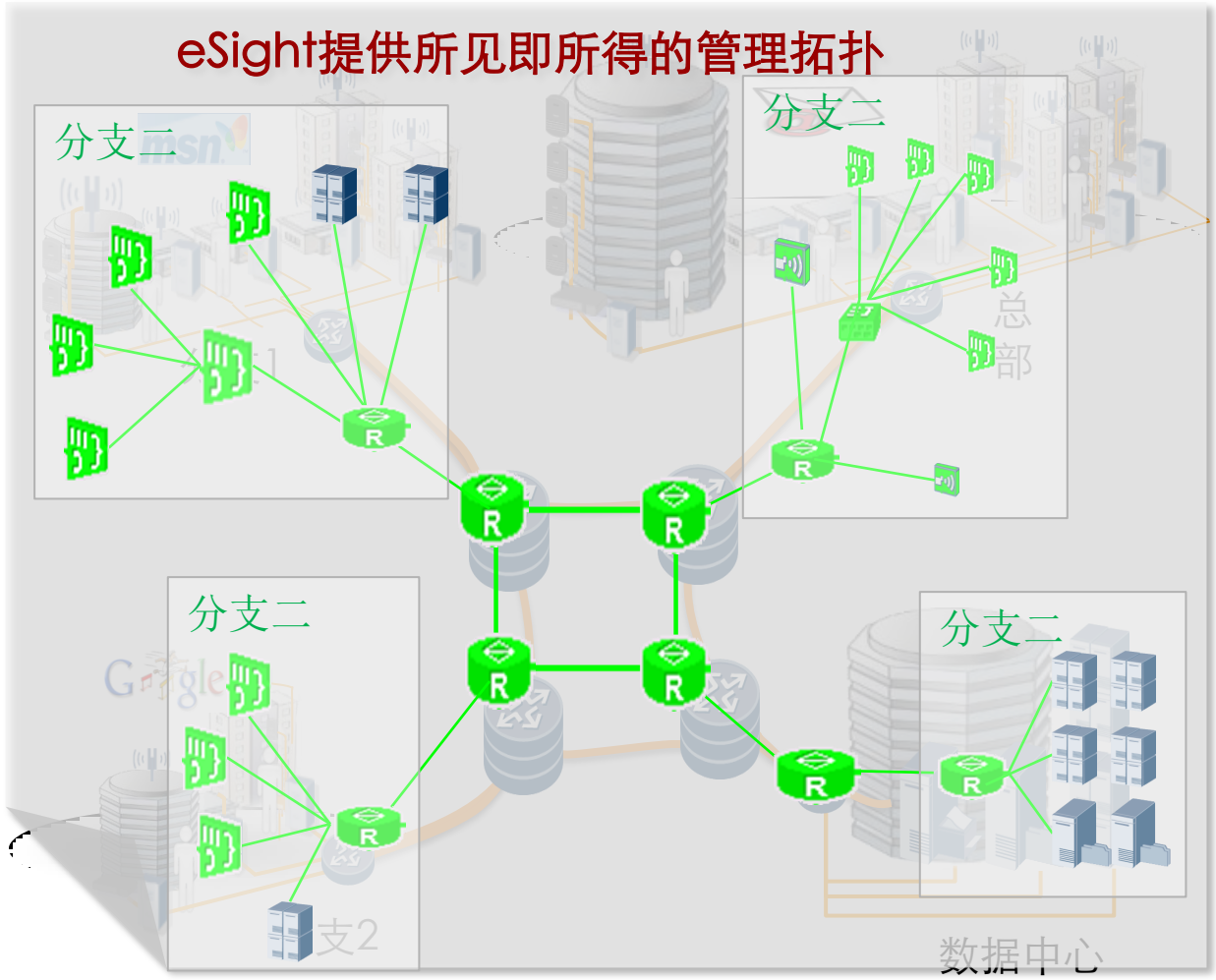
企业资源统一管理



eSight 支持统一管理 IP & IT 设备。

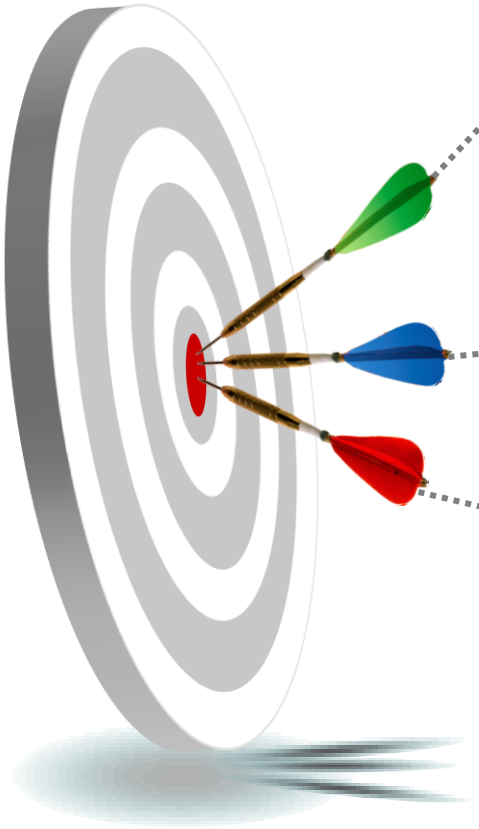
eSight 支持统一管理 IP & IT 业务。

可视化的企业统一视图



- 自动发现：自动发现网络资源，网络链路自动创建。
- 统一视图：提供IT&IP一体化拓扑视图，全面管理企业资源
- 实时呈现：呈现子图、网元、链路、网元状态，实时了解网络的运行情况
- 灵活定义：按用户信息保存网元位置、支持拓扑背景图和自定义图标功能，各种Tips信息，企业结构一目了然

全方位的企业故障监控



全面的故障类型

- 基于IP设备的告警
- 基于IT设备的告警
- 基于业务应用的告警

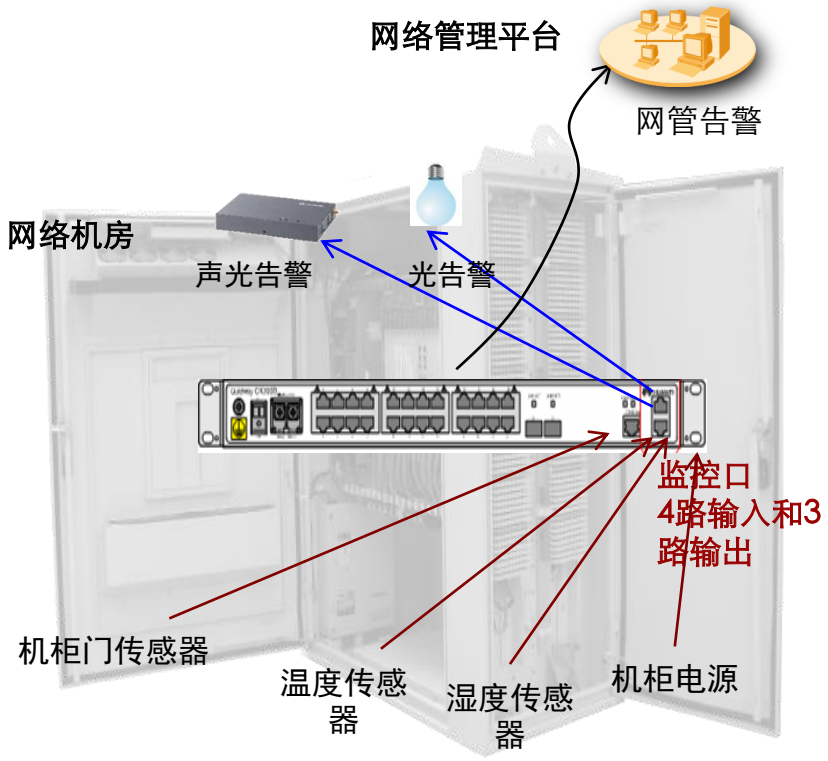
实时的故障监控

- 7*24 不间断的故障监控
- 实时的故障提醒
- 及时的故障远程通知

丰富的故障统计

- 故障分布情况统计
- 链路通断情况统计
- 设备健康性统计

机房精细化监控



需求：

1：传统用户机房的设备管理都是亡羊补牢型的，如：设备高温烧毁了，才发现网络故障，电源坏了，才赶去维修。

而如果能够在温度或电源发生异常时就及时知会网络管理员，就会避免最终设备失效带来的长时间断网以及重大维修。

2：电力不稳地区，设备突然掉电重启，管理员无法判断具体原因。

设备掉电前瞬间如果能上报网管掉电，则可以时网络管理员及时处理。

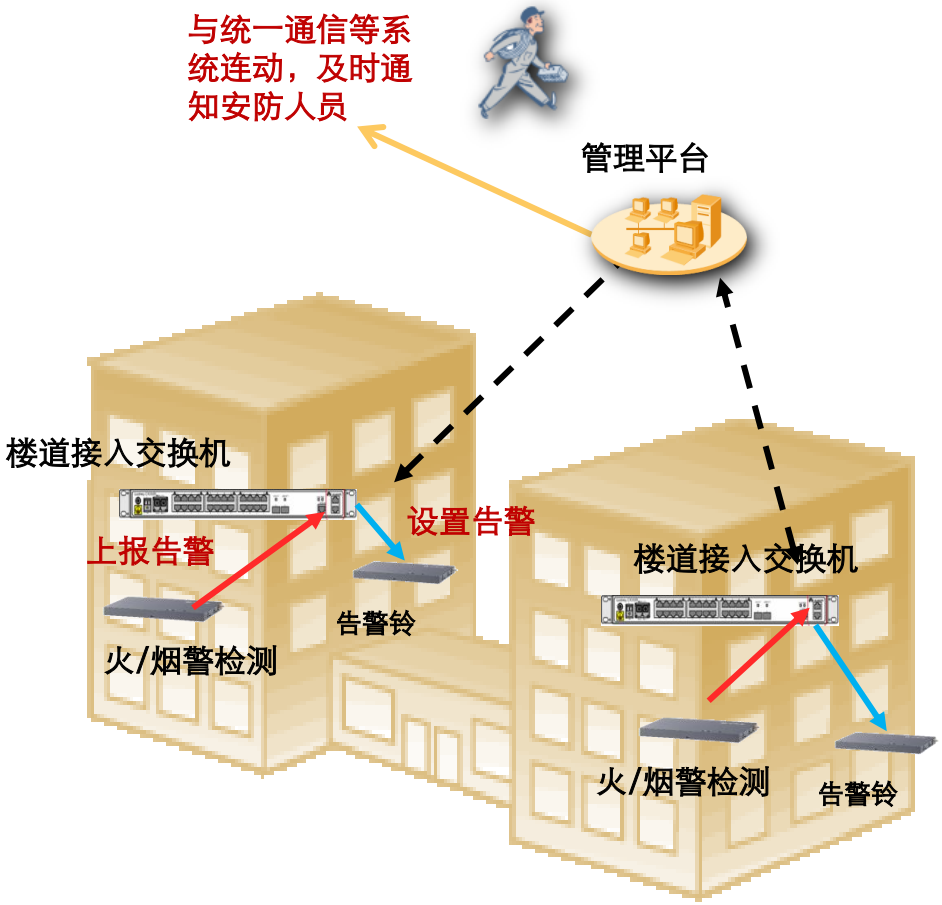
特色方案：

通过引入S3328TP-EI – MC盒式交换机，支持环境监控口，支持4路信号输入和3路信号输出，实现机房环境在网络平台上的统一监控，提前对异常进行感知并上报网管，同时根据需要进行声光告警。如与接入网E系列机柜一起实现机柜门、温度、湿度的告警监控。

Dying gasp功能 （S3328TP-EI – MC 和S5306TP-LI）

实现断电瞬间告警发送，通知管理员设备复位是由于供电异常所致

辅助智能楼宇安防监控

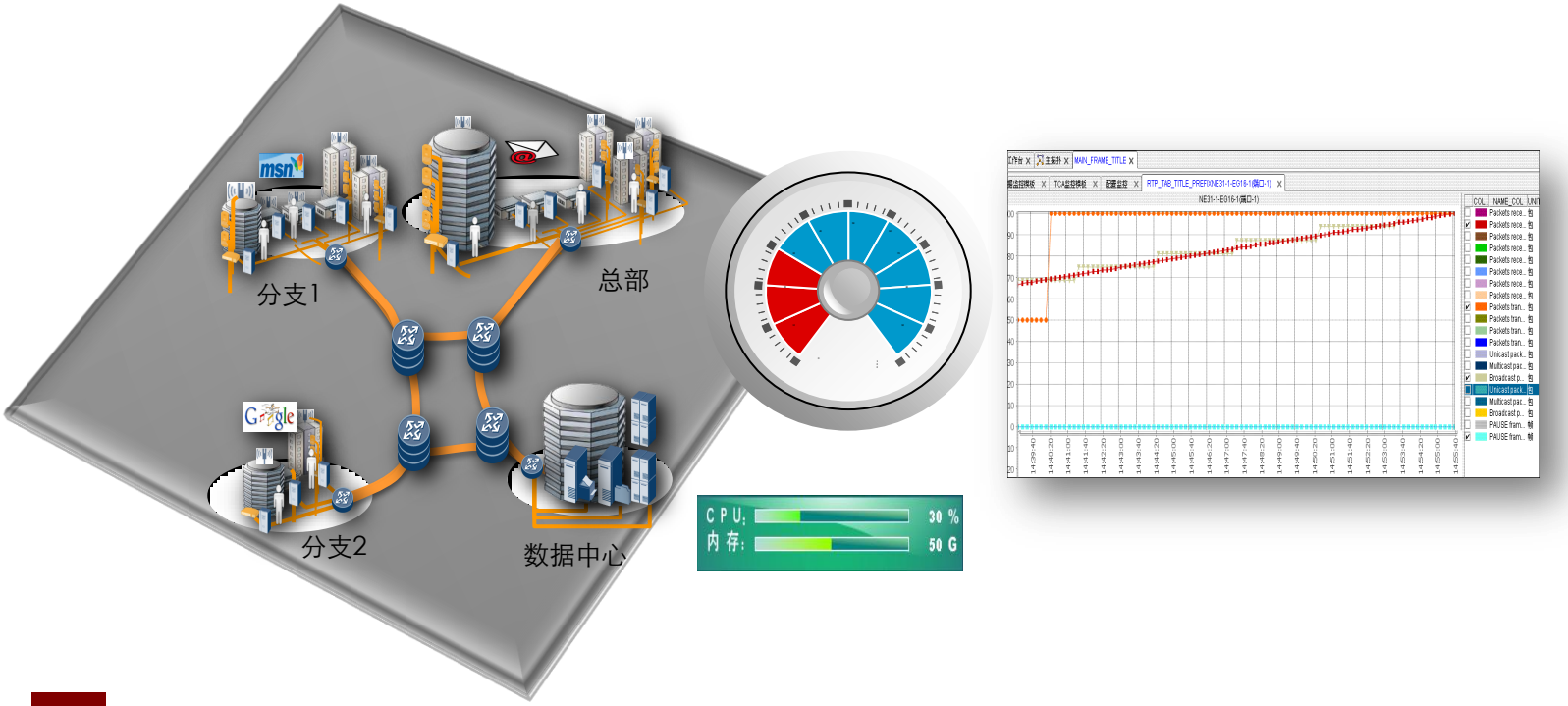


客户问题：
智能楼宇建设中，对火警，盗警等安防检测主要是通常的闪灯，声音报警等手段，如何能够将各种报警信息汇总到统一管理平台，以便进行灵活处理

特色方案：
通过网络设备监控口，实现安防告警信息IP化，灵活处理告警：在触发声光告警的同时，短信及时通知安防人员

与IP视频监控联动，实现统一安防： 网络管理平台通过上报告警的网络设备判断告警位置，切换视频监控查看现场状态，指挥救援

企业网络监控性能管理能力

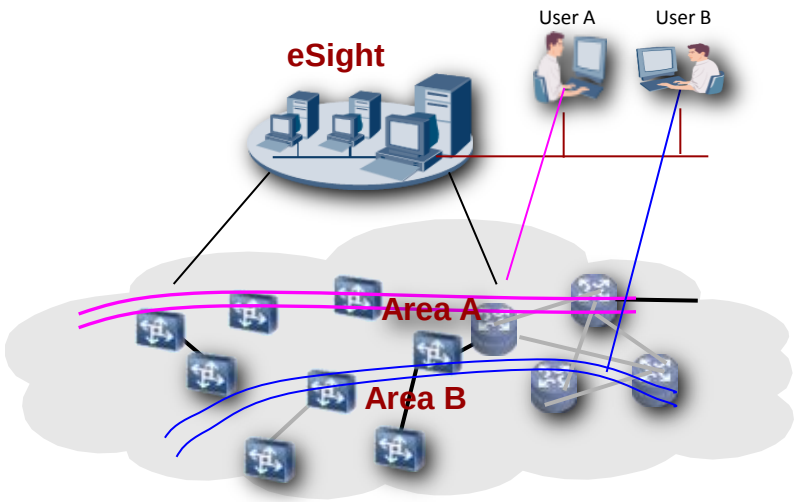


1 提供图形方式呈现性能数据，直观了解企业设备、服务器等资源设备性能情况

2 提供性能阈值告警能力，企业网络健康度实时了解，保障企业业务承载网络健康性

3 自动创建设备基本性能监控，支持批量创建同类性能监控实例，方便客户轻松操作

分权-分域-分时 的用户管理



- **日志**
  用户使用情况全记录。

- **权限**
  用户操作权限全可控。
- **区域**
  用户管理范围全可管。

eSight Solution

分权

- 为不同用户分配不同权限，并记录操作日志

分域

- 设置用户管理区域，限定用户管理范围。

分时

- 可设定用户有效时间、有效期。

eSight智能配置工具

eSight智能报表

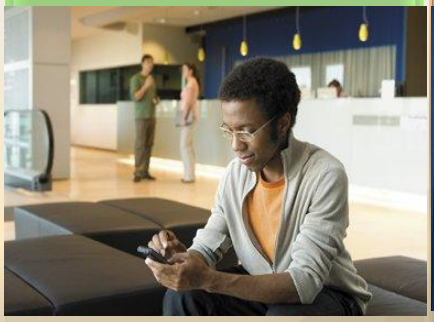
报表类型自定义

★支持报表类型定义
★丰富的报表展现方式

报表数据自定义

★支持报表数据字段的自定义
★支持报表设计的预览

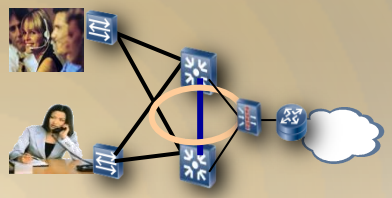
报表生成自定义

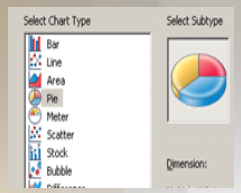


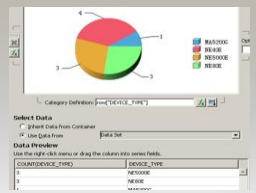
★支持日报、周报等周期报表
★支持实时统计报表

报表分发自定义

★支持报表自动分发设置
★支持E-mail、FTP等多种分发方式







eSight智能配置工具

Difficulties

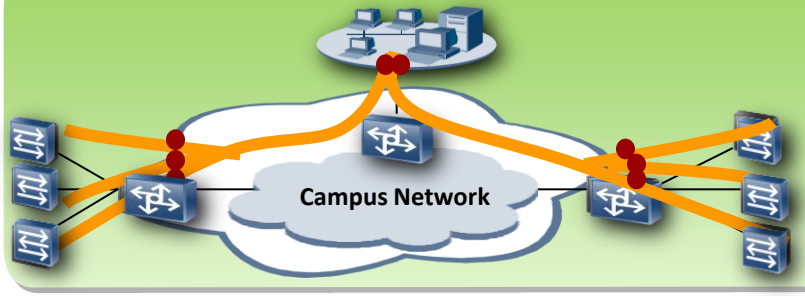
低效的海量设备管理

Do the same thing again and again!

Low efficiency and increasing costs

It takes a long time to configure such a large number of devices.

eSight Smart Configuration

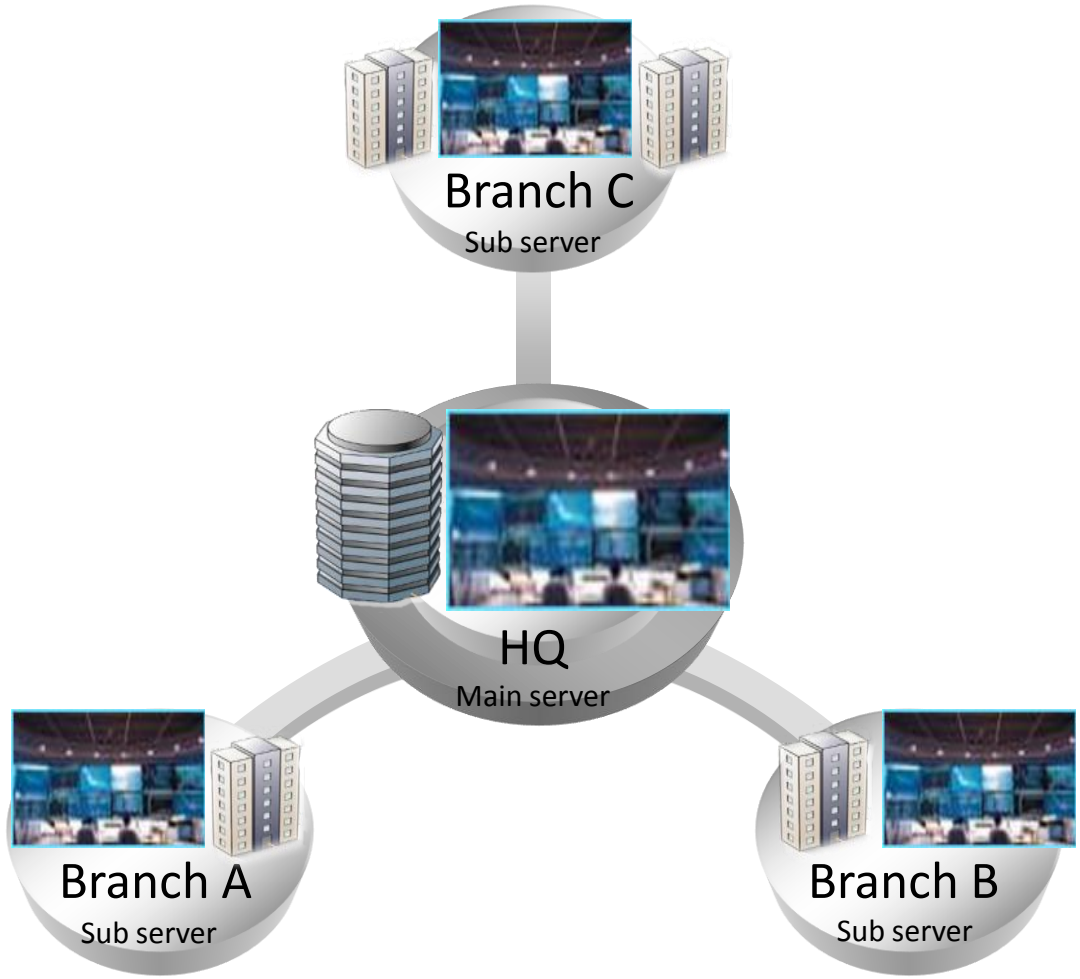


★ 基于命令行模板的设计。
★ 基于命令行的校验。
★ 支持差异化配置批量下发。
★ 支持华为路由器、交换机等全系列设备。

eSight能够帮助您有效管理您的网络配置

Solutions

分级的管理架构



- eSight 支持分级的网管架构。
- 每个子服务器均可以作为单独的系统独立运作，也可以作为分布式子系统统一管理。
- 子服务器支持传输数据给总服务器，在总服务器进行统一管理。
- 总服务器管理员可以透明的登录到各个子服务器，并支持在总服务器上监控每个子服务器的状态。
- 每个服务器之间的通讯带宽要求为4M。

Annotation:

NMS

Data stream

eSight 开放的企业管理平台

统一的
北向接口

- 统一北向接口快速集成

两类
集成模式

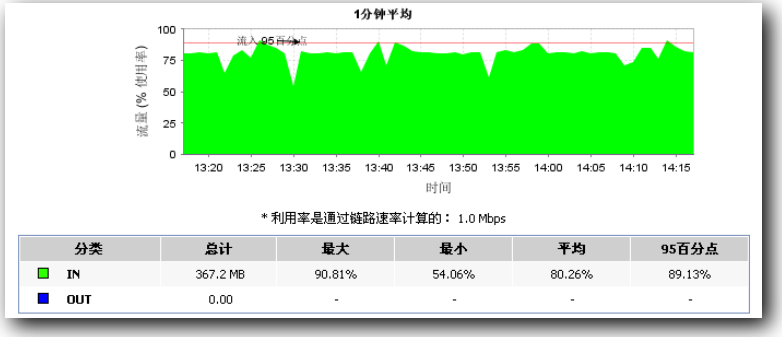
- eSight集成企业现有管理系统，统一资源和告警
- eSight开放的API和数据库接口供企业应用集成

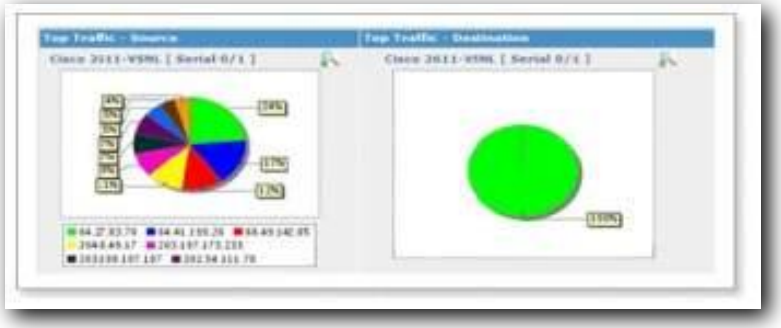
三步
设备集成

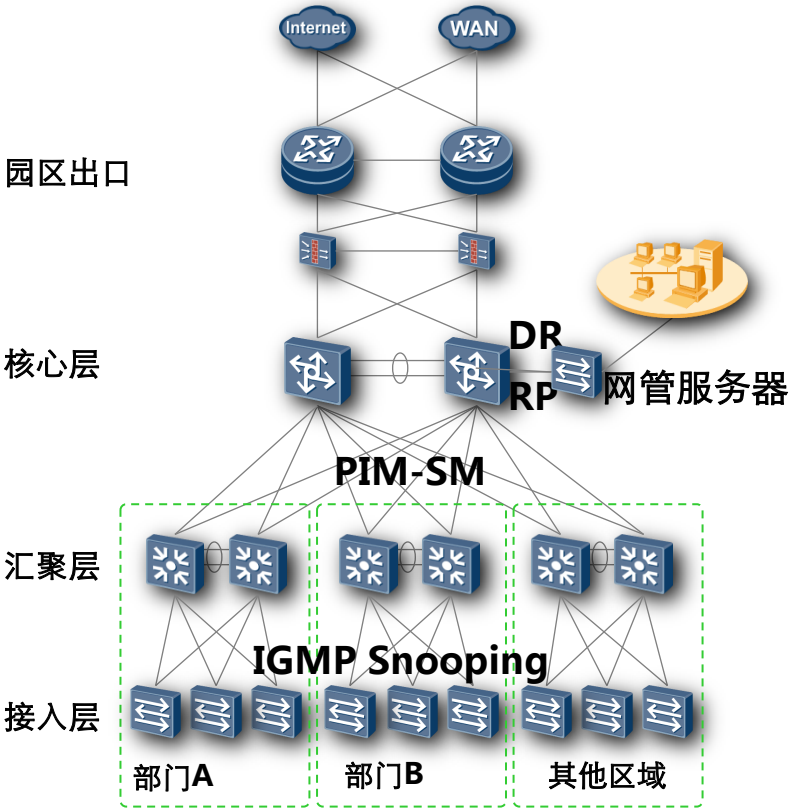
- 定义设备类型
- 定义私有告警
- 定义私有性能

精细化流量管理

全面、直观







- **支持业界主流网流技术：**如NetStream、NetFlow、 sFlow、cflowd、J-Flow和IPFIX；
- **基于业务的统计一目了然：**能深入分析应用、源、目的、QOS等报文参数，输出各种TOP报表，重点业务重点监控。

真正面向业务的SLA管理，给你的网络质量打分

nqaJitterStatsMinOfPositivesSD	源到目的抖动值为正值的最小值	毫秒
nqaJitterStatsMaxOfPositivesSD	源到目的抖动值为正值的最大值	毫秒
nqaJitterStatsNumOfPositivesSD	源到目的抖动值为正值的数目	个数
nqaJitterStatsSumOfPositivesSD	源到目的抖动值为正值的和	毫秒
nqaJitterStatsSum2OfPositivesSD Low	源到目的抖动值为正值的平方和低位	无单位

客户问题：

网络质量对大部分用户而言是个看得见但摸不着的东西，传统的SLA方案给用户一大堆无法理解的参数概念，对用户的专业能力要求高，无法真正指导广大一般用户对网络质量评估。

特色方案：

真正面向业务的SLA管理：通过实际业务特点预定义视频、语音、实时应用、门户网站等业务类型，最真实反映业务质量；如门户网站业务类型已经自动整合HTTP、DNS、TCP Connection等NQA测试例。

给你的网络质量打分：不需要理解复杂的SLA概念，eSight结合华为多年网络管理实践，将结果转化为直观的分数给你，就像360检查计算机的质量一样Easy

目录

成熟的万兆园区产品系列

GE接入层设备

S5700LI/S5700SI/S5700EI
S5700HI/S5710EI系列

10GE汇聚层设备

S7700/S6700系列

40G/100G核心层设备

CE12800/S9700系列

园区网出口路由器

NE40E系列

语音&安全路由器设备

AR3200/2200/1200系列

WLAN设备

AP/AC系列

AP6010SN
AP6010DN
AP7110DN
AP6310SN
AP6510 DN
AP6610 DN

AC6605

AC插卡

华为端到端IP产品与解决方案

目录

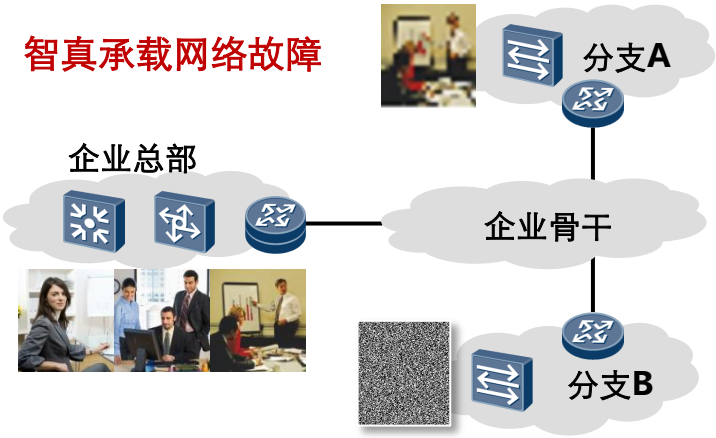
Page 83

子目录

4 园区网业务场景解决方案

智真运维客户需求

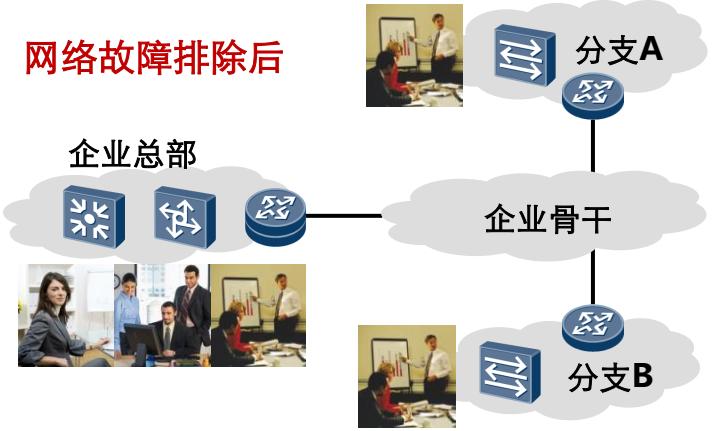
智真承载网络故障



智真承载网络缺乏高效运维检测手段

- 网络质量难以有效评估
- 故障网段难以快速定位

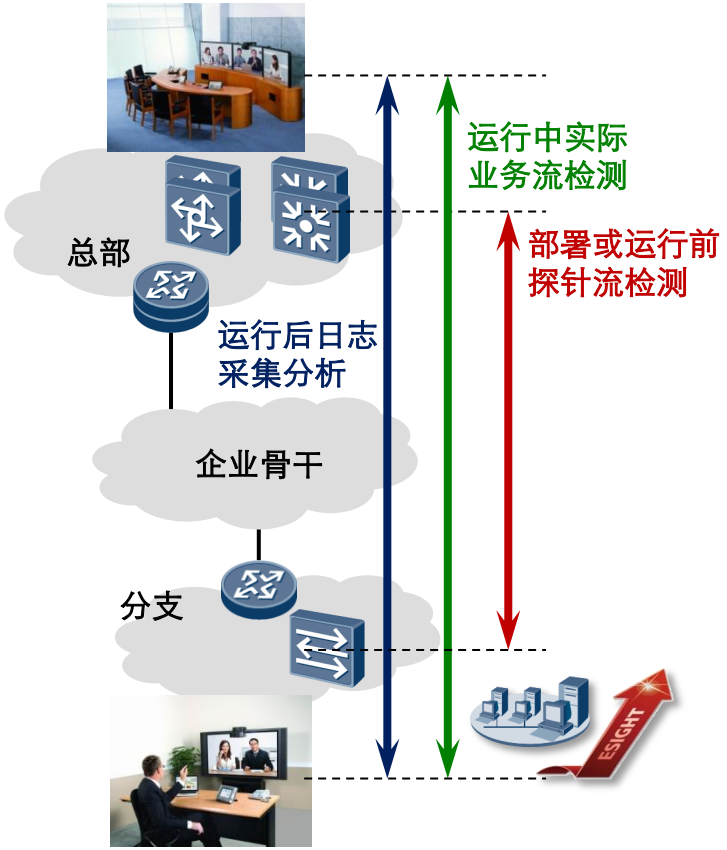
网络故障排除后



智真承载网络质量评估与故障定位方案

- 会前基于硬件探针检测
- 会议中基于实际业务流检测
- 全路径分段显示丢包/时延/抖动/QOS

智真运维总述：会议前/中/后可视化检测和定位



会议前/中/后故障定位与可视化显示

部署或会议前：

全路径检测

会议中：

实际业务流检测

会议后：

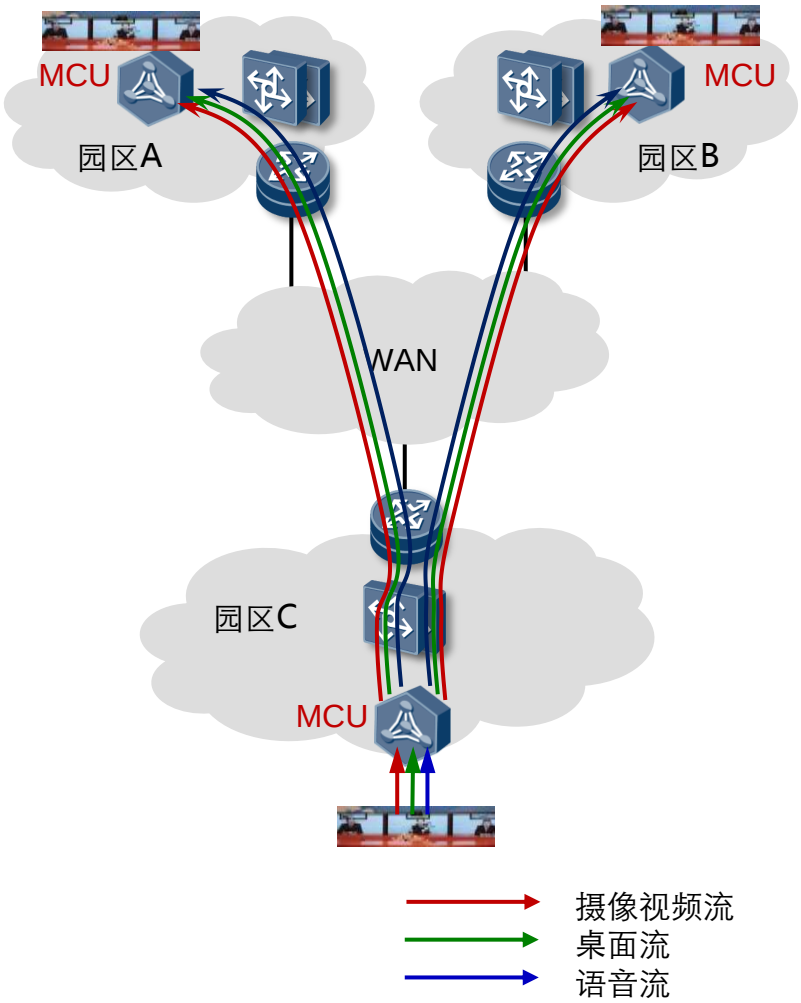
故障日志记录

分段显示：

抖动、丢包率、时延

精确、快速定位

智真业务流量模型



智真流量模型

每终端收发各三条流量

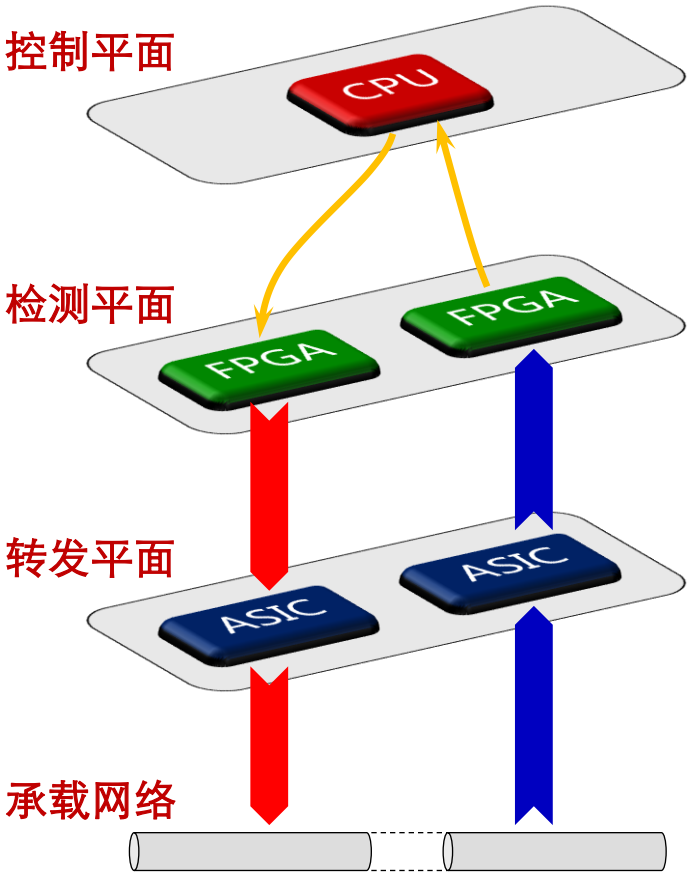
摄像视频流/桌面流/语音流

MCU复制单播流，发送给各接收端

运维检测目标

针对单条码流网络质量检测

高精度硬件探针检测



场景与挑战

智真属于高带宽消耗业务，软件构造仿真数据流严重占用主控CPU资源；

传统板间通信队列导致检测时延、抖动误差较大；

解决方案

检测/控制平面分离设计，专用硬件实现；

部署华为带检测平面硬件设计产品；

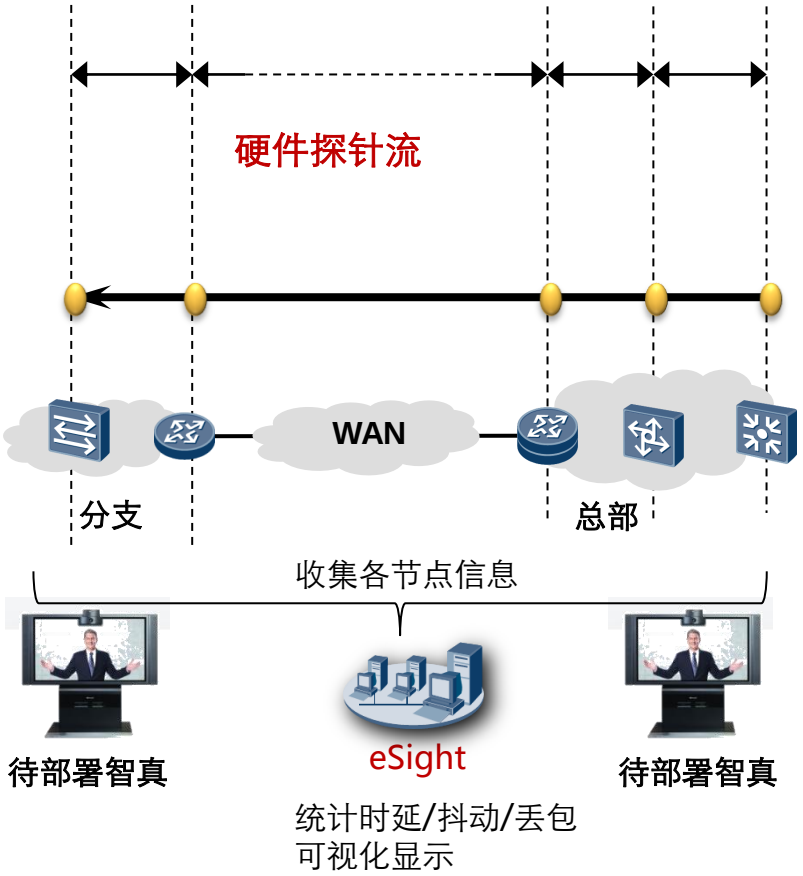
推荐9700/7700/5700H系列；

客户价值

专用硬件发送探针流，CPU零占用；

比业界精度提高20%；

部署前/会议前可视化检测和定位



场景与挑战

在智真系统部署前以及会议开始前；

需要提前检测承载网络能否满足要求；

可视化分段显示网络质量数据；

解决方案

eSight启动检测，端点设备发送探针报文；

路径节点设备进行时延/抖动/丢包统计；

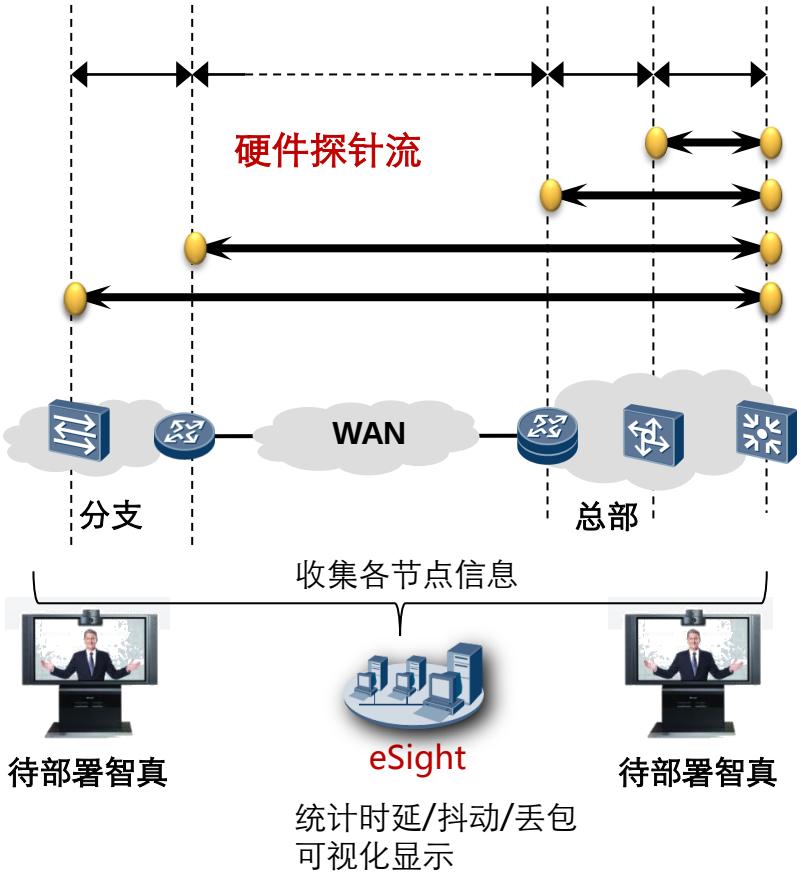
eSight收集数据，计算结果并可视化显示；

接入交换机支持硬件探针；

客户价值

在智真业务部署/应用前，根据eSight网管提供的网络质量可视化图表，指导网络部署/优化/故障排查等工作

视频迟滞故障检测——时延分段显示



场景与挑战

数据时延过大影响图像和语音的实时性；

造成图像语音不同步/反应滞后等问题

解决方案

终端交换机硬件探针流进行双向时延测试；

路径节点设备NQA双向报文返回；

网管故障时延分段显示；

路径节点支持NQA双向报文返回功能；

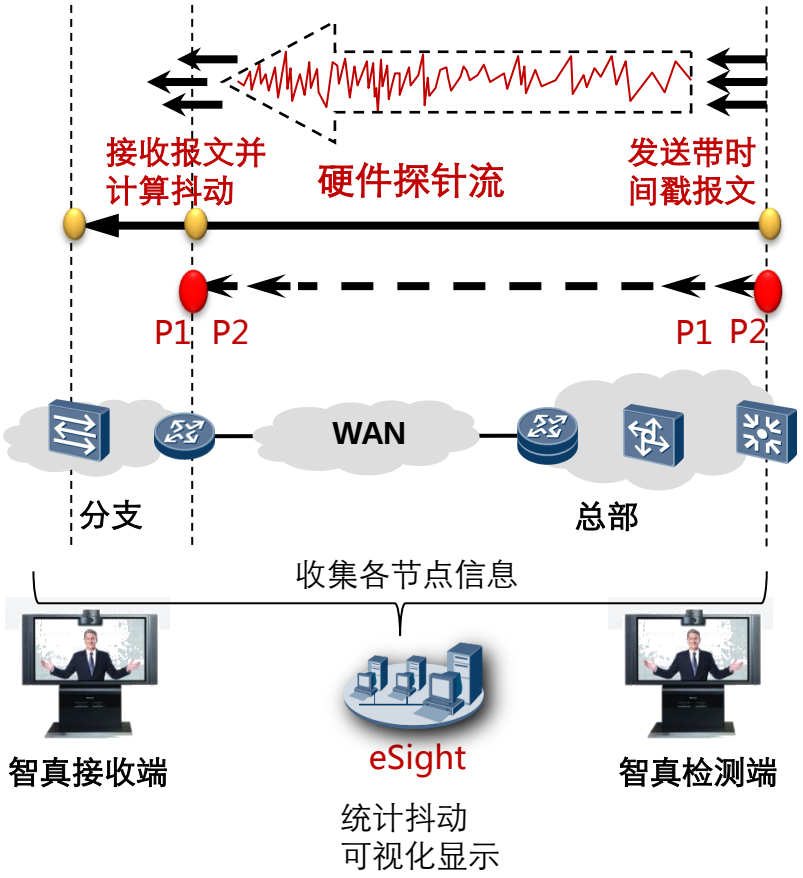
路径节点部署企业交换机和AR产品；

路径节点设备支持三层业务；

客户价值

分段时延显示，以此为依据排查网络故障或优化网络；

视频顿挫故障检测——抖动分段显示



场景与挑战

智真数据传输中发生网络抖动；

图像不连贯；

视频顿挫感；

严重时花屏/语音断续/视频语音失同步；

解决方案

eSight启动检测，端点设备发包测试；

路径各节点设备通过时间戳计算出抖动值；

eSight网管收集各节点数据并可视化显示；

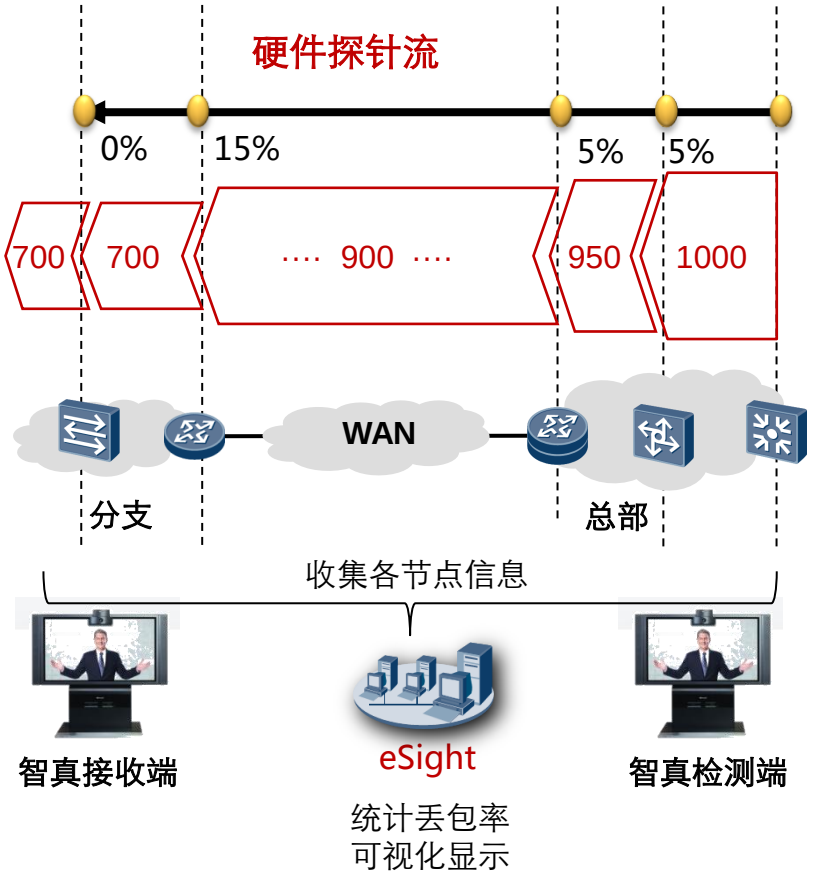
路径节点部署企业交换机和AR产品；

路径节点设备支持三层业务；

客户价值

一键检测网络抖动并可视化显示，以此为依据排查网络故障或优化网络；

视频花屏故障检测——丢包率分段显示



场景与挑战

智真数据传输中丢包率过高影响用户体验，

马赛克/ 花屏/丢帧；

语音断续/杂音；

严重时导致业务中断；

解决方案

eSight网管启动检测，端点设备发包；

路径各节点通过探针流报文数计算丢包率；

eSight网管收集各节点数据并可视化显示；

根据eSight统计结果优化网络；

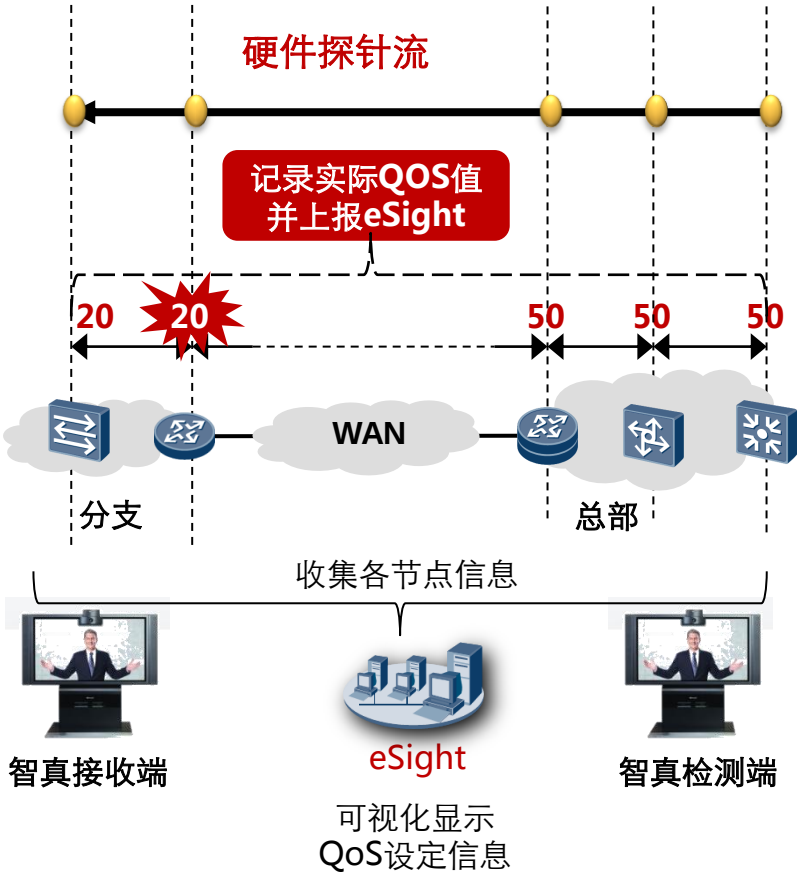
路径节点部署企业交换机和AR产品；

路径节点设备需要支持三层业务；

客户价值

一键检测网络丢包率并可视化显示，以此为依据排查网络故障或优化网络；

网络QoS部署异常检测——QoS信息分段显示



场景与挑战

承载网络中某些节点的QoS设置不合适；

智真网流QoS优先级被修改；

QoS功能无法保证智真业务数据流质量；

解决方案

各节点记录数据流QoS优先级；

eSight网管收集数据并可视化显示；

路径节点部署企业交换机和AR产品；

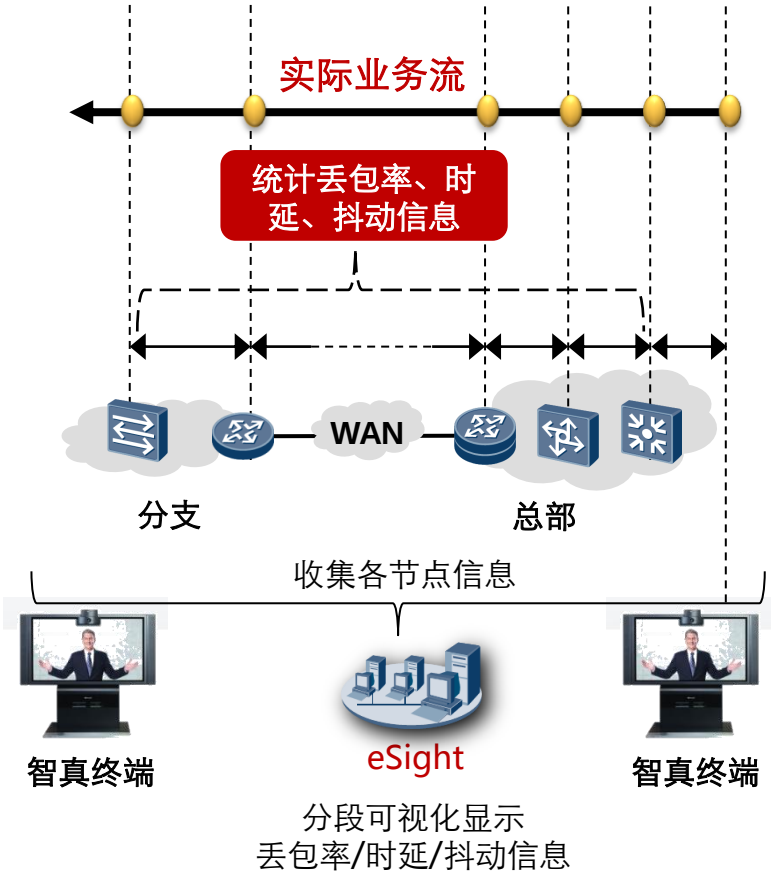
路径节点设备需要支持三层业务；

客户价值

一键获取智真流经过各节点时QoS信息；

将QoS信息可视化显示，指导网络优化；

会议中和会议后可视化检测和定位



场景与挑战

会议中需要快速故障定位手段；

会议中不能产生探针流；

会议后需要日志记录，便于网络故障定位；

解决方案

智真承载网络各节点记录网络参数；

eSight网管收集各节点数据并可视化显示；

日志记录便于会后提供故障排查信息；

路径节点部署企业交换机和AR产品；

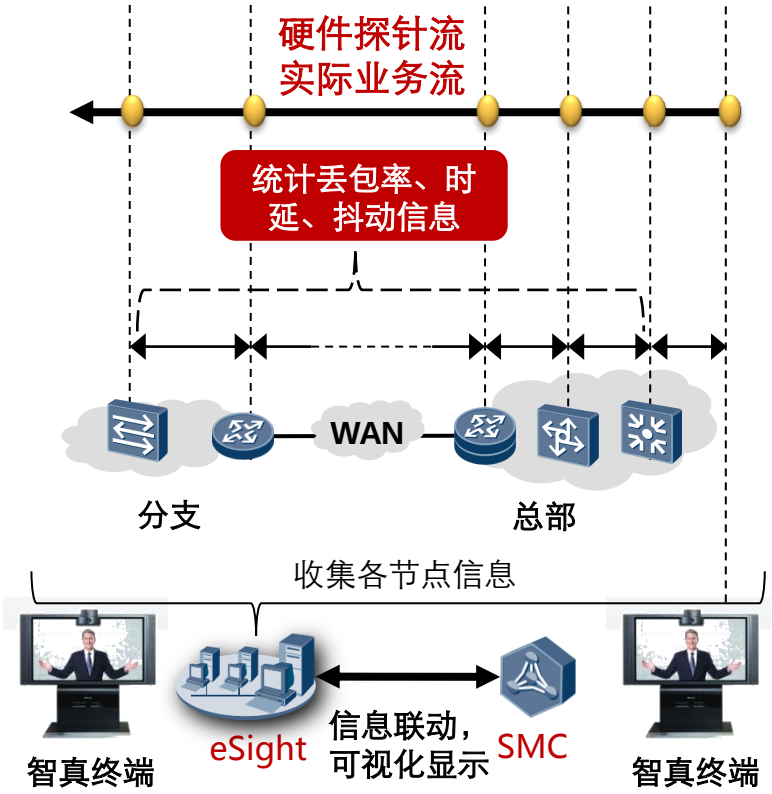
路径节点设备需要支持三层业务；

客户价值

会议中一键检测网络质量，或会议后日志记录网络故障段，并可视化显示；

提供快速排查网络故障的依据。

智真SMC界面可视化故障显示



场景与挑战

智真承载网络在时延/抖动等超过容忍阈值时，需要启动全路径故障网段检测；

可视化显示检测结果/在日志中记录；；

解决方案

端到端监控和全路径检测功能一键联动；

在智真SMC平面可视化显示故障段；

路径节点部署企业交换机和AR产品；

路径节点设备需要支持三层业务；

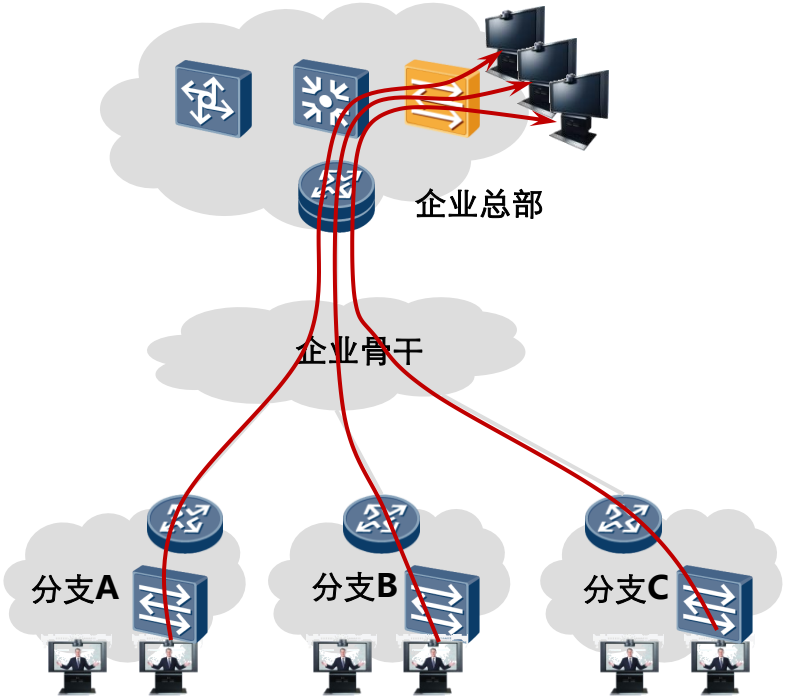
客户价值

会议中自动检测网络质量，或会议后日志记录网络质量参数；

同时在网管/SMC控制台可视化显示；

提供快速排查网络故障的依据。

多会议并发故障检测场景



多条探测流量经过路径节点，
通过五元组
[SIP/DIP/SPort/DPort/Protocol]
区分多实例，进行网络参数统计

场景与挑战

单交换机下部署多个智真终端，需要同时启动多个探测数据流；

路径节点设备可能有多条流量需要统计；

解决方案

交换机可模拟多个探测流；

路径节点设备支持多实例流量统计；

网管支持多实例信息收集和显示；

多实例通过流量五元组识别；

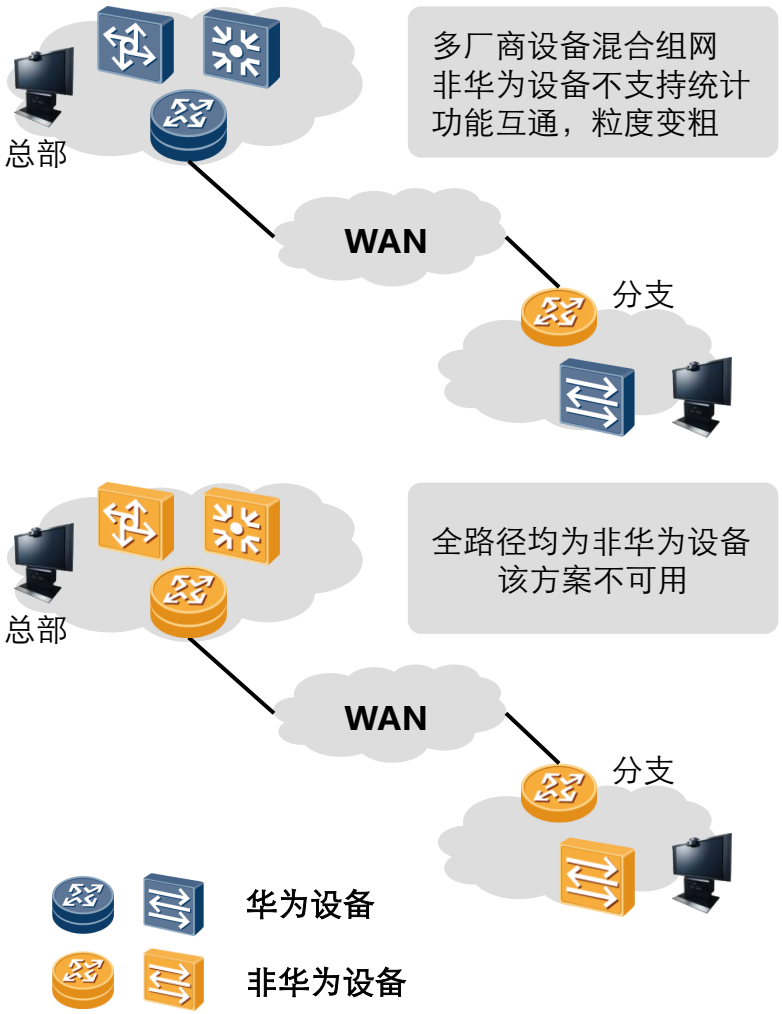
路径节点部署企业交换机和AR产品；

路径节点设备需要支持三层业务；

客户价值

可以同时对多条智真业务流进行检测统计；

兼容多厂商设备检测场景



场景与挑战

组网可能涉及多厂商设备；

非华为设备不支持统计功能；

解决方案

路径中非华为设备节点直接透传；

网段故障检测粒度变粗；

不影响整网统计功能；

路径节点设备可以采用多厂商设备；

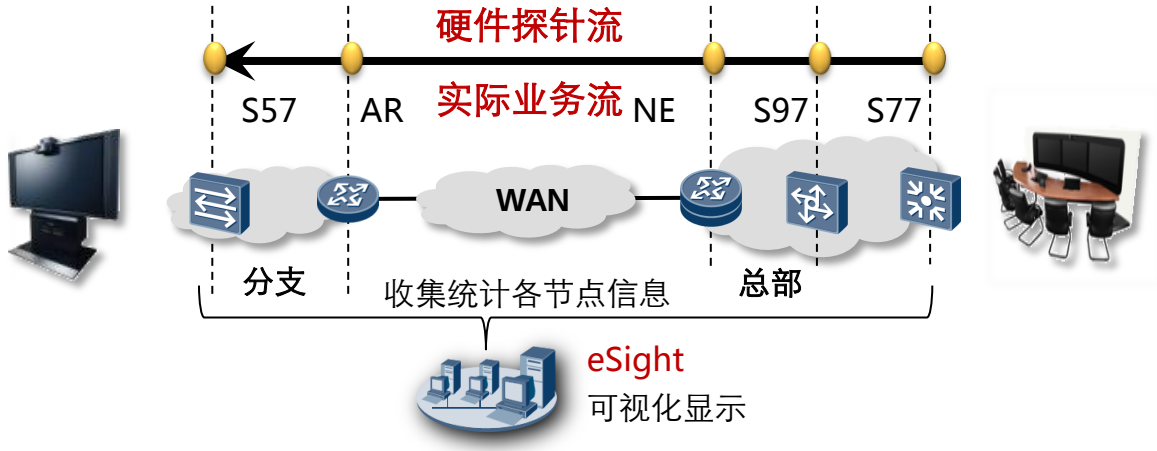
终端交换机必须是华为设备；

网管必须是华为产品；

客户价值

保护现有投资，兼容原有非华为设备；

智真运维产品功能组合



智真运维方案产品组合

交换机产品	路由器产品	eSight网管	智真产品
支持硬件探针 支持流统计 支持三层业务 S57HI/S37HI S97/S77	支持流统计 AR12xx AR22xx AR33xx	支持检测启动 支持统计数据收集 支持可视化显示	支持一键式检测 支持模拟探测流 支持可视化显示 SMC 2.0

智真运维方案总结

类型	部署前	智真会议前	智真会议中	网真会议前	网真会议中	备注
时延	支持	支持	不支持	支持	不支持	华为智真系统支持网管/SMC同步显示功能
抖动	支持	支持	支持	支持	支持	
丢包率	支持	支持	支持	支持	支持	
QOS	支持	支持	支持	支持	支持	
多实例	支持	支持	支持	支持	支持	

Enterprise Router

Access Router AR G3

AR 200 AR 1200 AR 2200 AR 3200

Network Management

eSight

LAN Switch

Core Switch

CE12800 S9700

Aggregation Switch

S7700 S6700

Access Switch

S5700

智真运维方案竞争力分析

华为方案

网管和智真SMC均支持全路径故障分段检测和显示；

智真会议前/部署前，支持硬件探针，测量精度高；

会议中可采用实际流量监控并分段故障显示；

支持QOS更改全路径显示；

支持非华为终端与设备互通；

路径非华为设备透传(检测粒度变粗)

CISCO方案

成熟IP SLA；

能够支持部署前/会议前/会议中分段显示；

支持硬件测试；

仅网真设备支持故障显示，网管不支持；

支持QOS更改全路径显示；

不兼容非思科终端和设备；

H3C方案

仅支持端对端质量测量，不支持网络故障分段显示；

不支持硬件探针，测量精度低；

成熟NQA方案，配套网管支持测试显示；

不支持会议中实际业务流量监控；

不支持流量QOS更改监控；

不兼容非H3C终端和设备；

华为方案支持全路径检测时延/抖动/丢包率，检测数据分段可视化显示；
华为方案兼容CISCO网真终端以及非华为网络设备；
华为和CISCO在智真运维保持领先地位，H3C完全无此方案；

选型建议

所有参与统计的网络设备需要支持三层路由（二层交换机不支持流量统计）；

端点交换机需要支持硬件探针，只有框式交换机以及S5700HI支持；

网管收集统计数据功能是必选组件；

智真运维方案2013年3月份提供交付；

部署建议

智真业务需要高质量网络；

建议三层汇聚层直接接入走专线；

汇聚层部署三层框式交换机以支持硬件探针；

子目录

4 园区网业务解决方案

目录

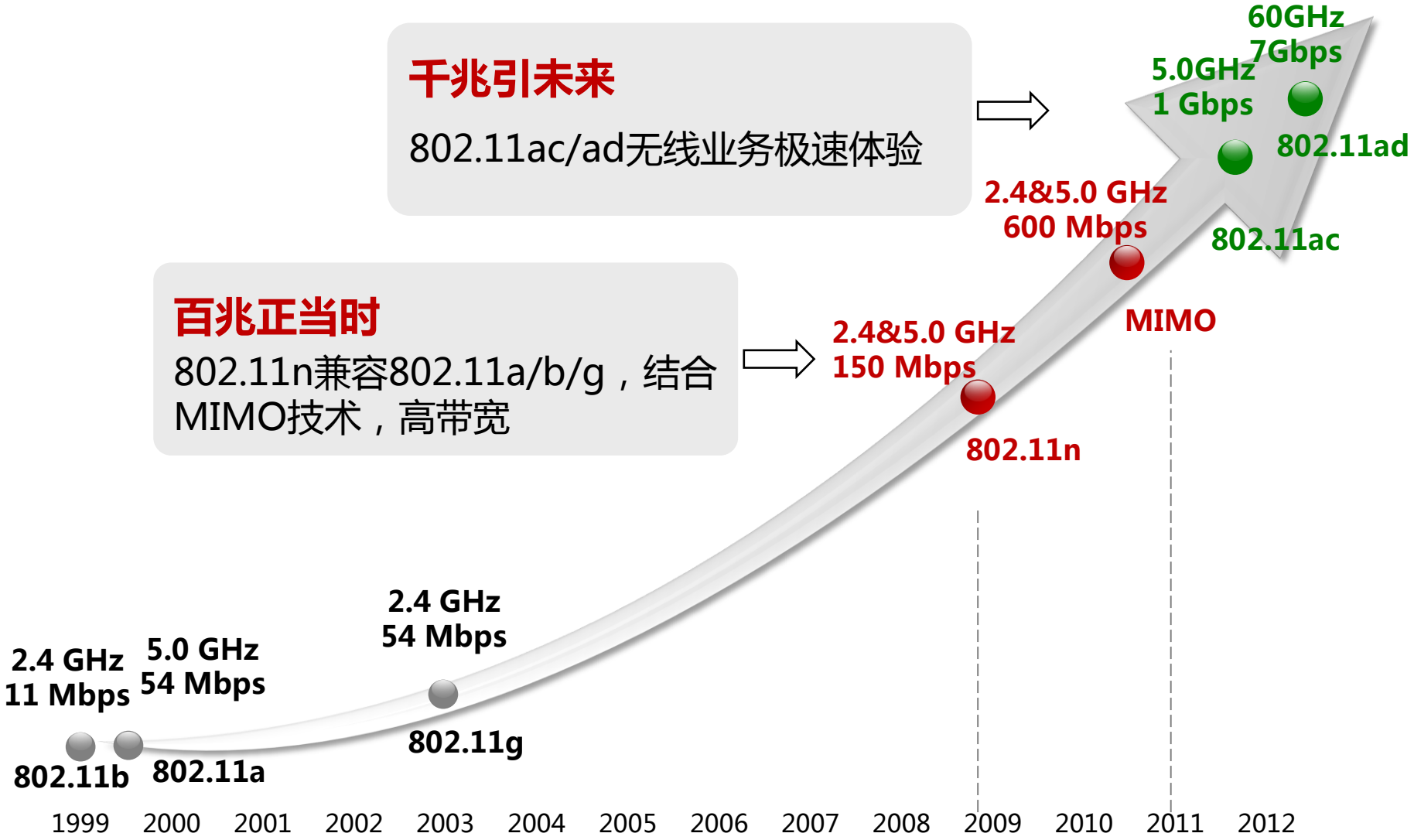
WLAN发展趋势：高带宽、高频率

千兆引未来

802.11ac/ad无线业务极速体验

百兆正当时

802.11n兼容802.11a/b/g，结合MIMO技术，高带宽

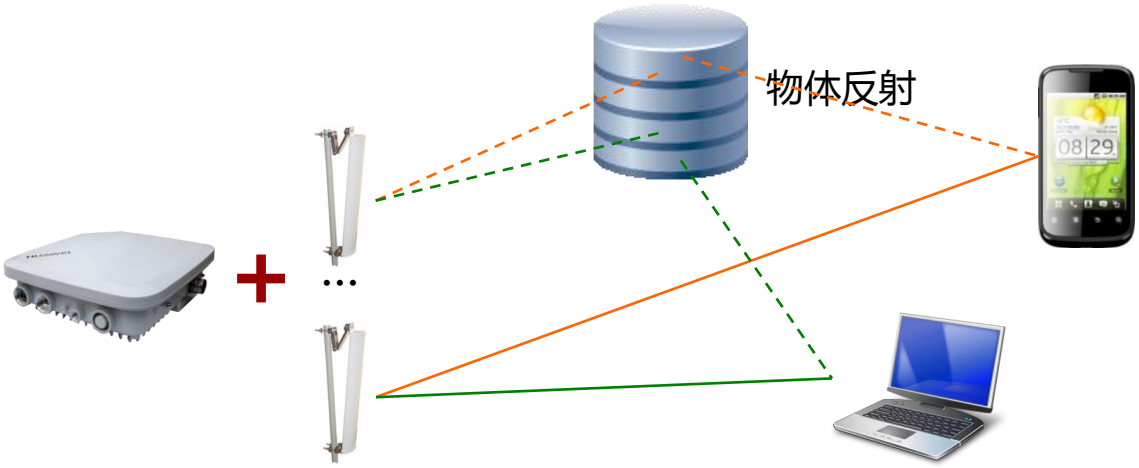


IEEE802.11标准简介

标准名称	发布时间	工作频率	理论速率	实际速率	备注
802.11b	1999	2.4GHz	11Mbps	6Mbps	早期标准
802.11a	1999	5.0GHz	54Mbps	22Mbps	应用很少
802.11g	2003	2.4GHz	54Mbps	22Mbps	早期标准
802.11n	2009	2.4/5.0GHz	150Mbps	75Mbps	结合MIMO技术，理论速率600Mbps
802.11ac	2012	5.0GHz	1Gbps	400～500Mbps	802.11n下一代标准
802.11ad	发展中	60GHz	7Gbps	发展中	面向家庭高清娱乐设备

理论速率指物理层（PHY）连接速率，由于无线信道开销比较大，实际速率一般只有理论速率50%左右。例如，802.11n单天线情况下理论速率150Mbps，实际可用速率只有75Mbps。

WLAN发展趋势：MIMO技术、智能天线



MIMO是智能天线技术的重大突破

在不增加带宽的情况下，**成倍提高系统的容量和频谱利用率**

链路的发端和收端都使用多副天线，将多径传播变为有利因素

具有2×2、3×3、4×4等方式。

MIMO(Multiple Input Multiple Output)

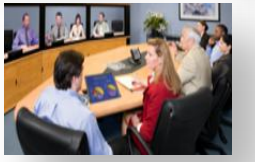
WLAN发展趋势：适应广、无处不在

校园

电力

山川

石油、制造业



企业办公

港口、码头

软件园

机场、酒店……

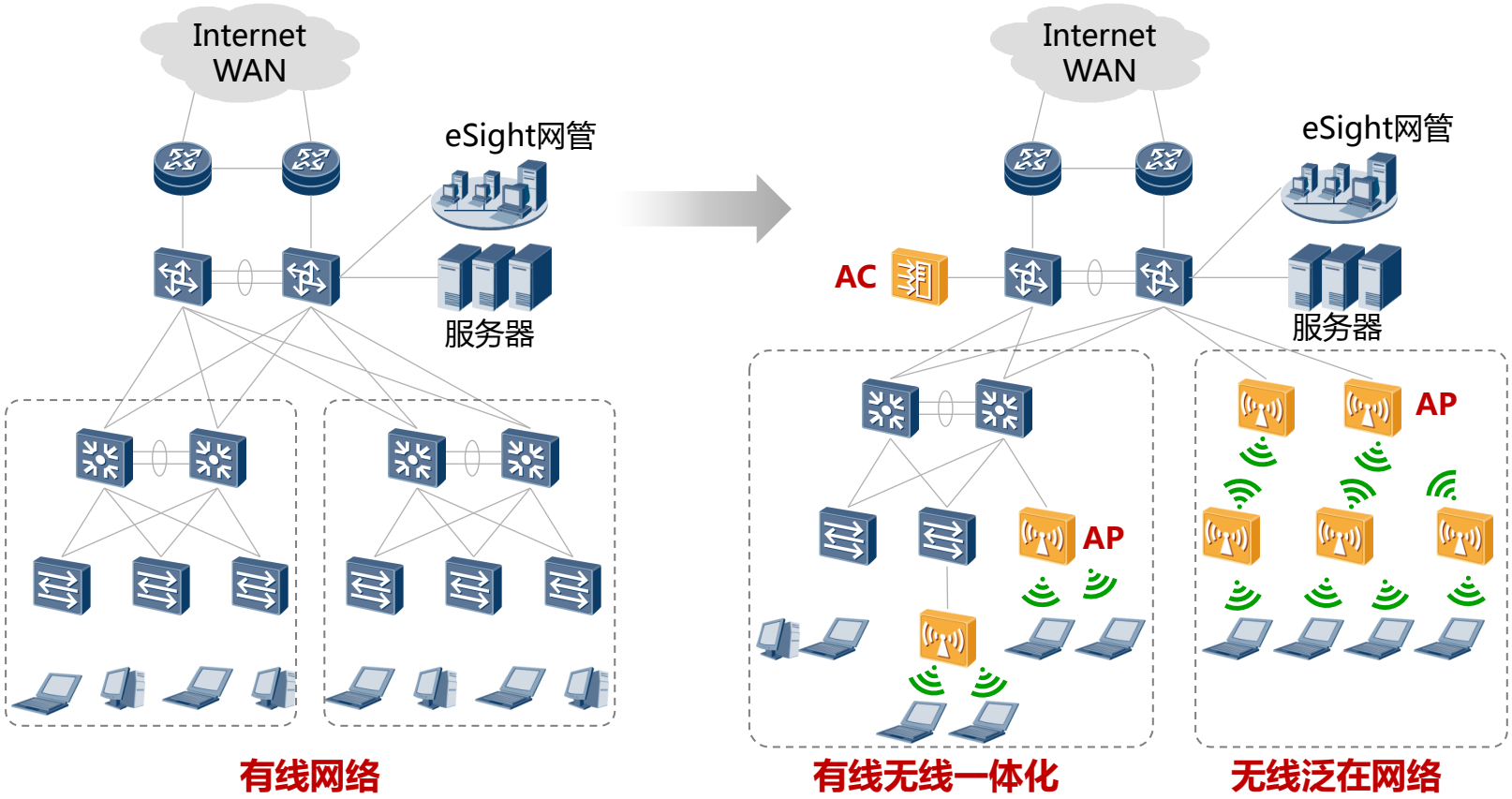
WLAN的独特优势

- 移动办公
- 热点覆盖
- 数据回传
- 定位
- 物联网

广泛的部署能力，应用于所有行业

例如：教育、政府、能源、交通、物流、医疗、企业、商业、电力、金融等等

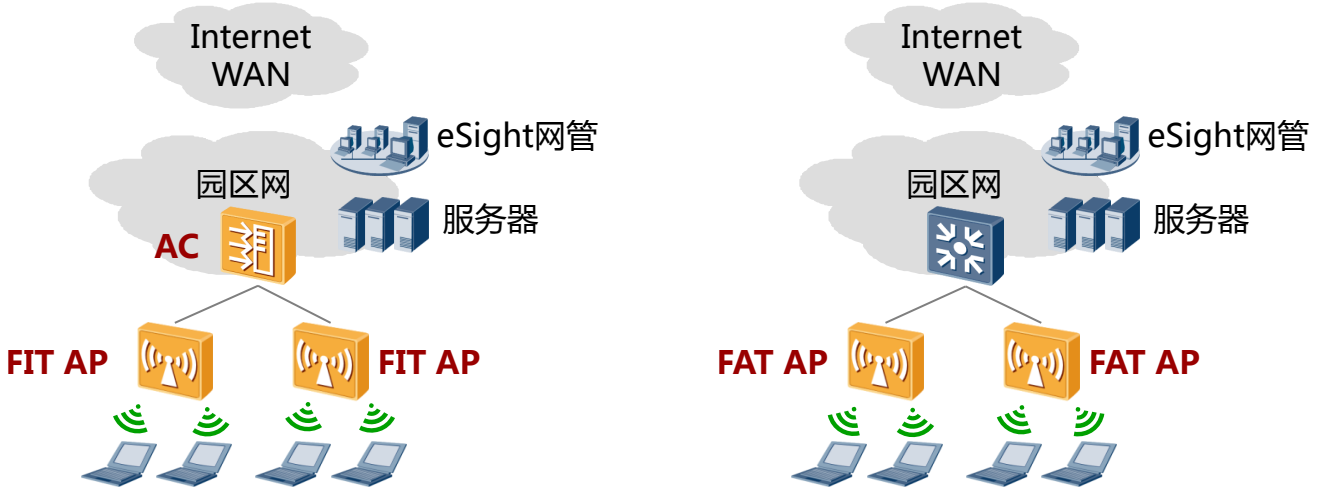
可平滑演进的无线网络，保护投资，节省建网TCO



WLAN 建网优势	无需开挖沟槽，缩短建网周期 终端灵活接入，网络扩展性强

目录

WLAN网络中AP部署：FAT AP和FIT AP

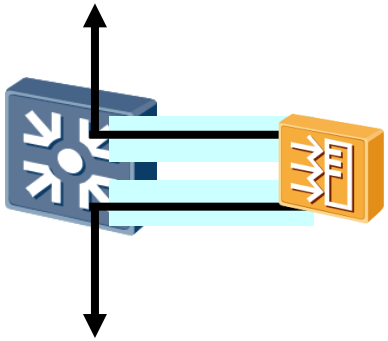


	FIT AP架构	FAT AP架构
应用场景	主流 目前是企业、运营商的通用方案	非主流 早期采用的方案
方案部署	集中式架构 AC和AP协同完成无线接入功能 AC集中管理和控制多个AP(称为“瘦AP”)	自治式架构 不需要AC设备 AP完成无线接入功能(称为“胖AP”)
运维管理	便于AC集中管理、集中认证和实施安全策略	大量配置AP，软件升级等管理操作成本高

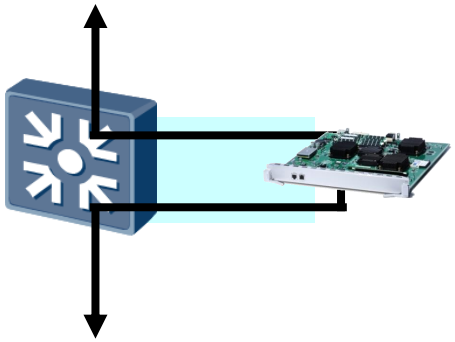
AP(Access Point) 无线接入点 AC(Access Controller) 无线控制器

AC部署方式：旁挂式和直连式

独立AC直连式



独立AC旁挂式



AC业务卡集成到框式交换机

直连式

主要用于中小型园区

所有流量要经过AC

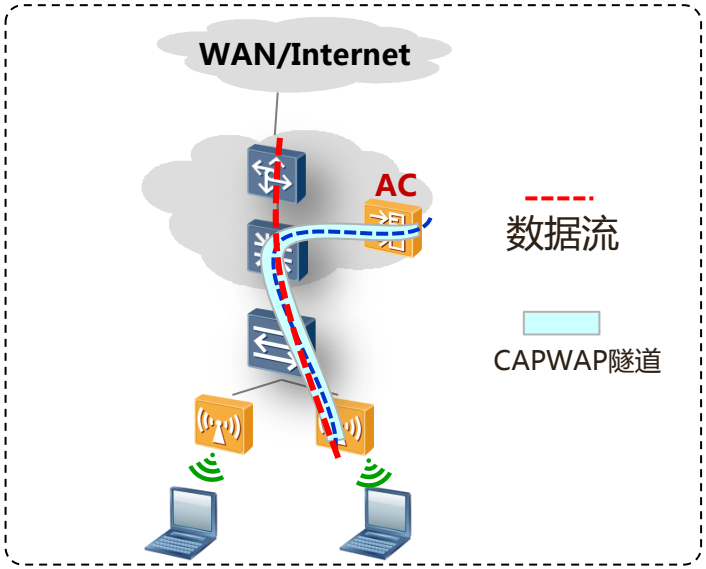
如果AC故障，所有流量受影响，**部署风险高**

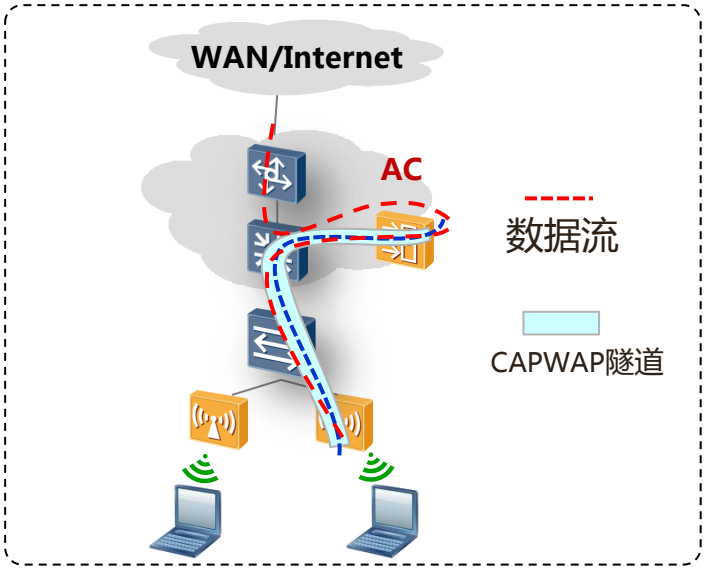
旁挂式

主要用于网络改造、大中型园区

建网有优势，推荐规划

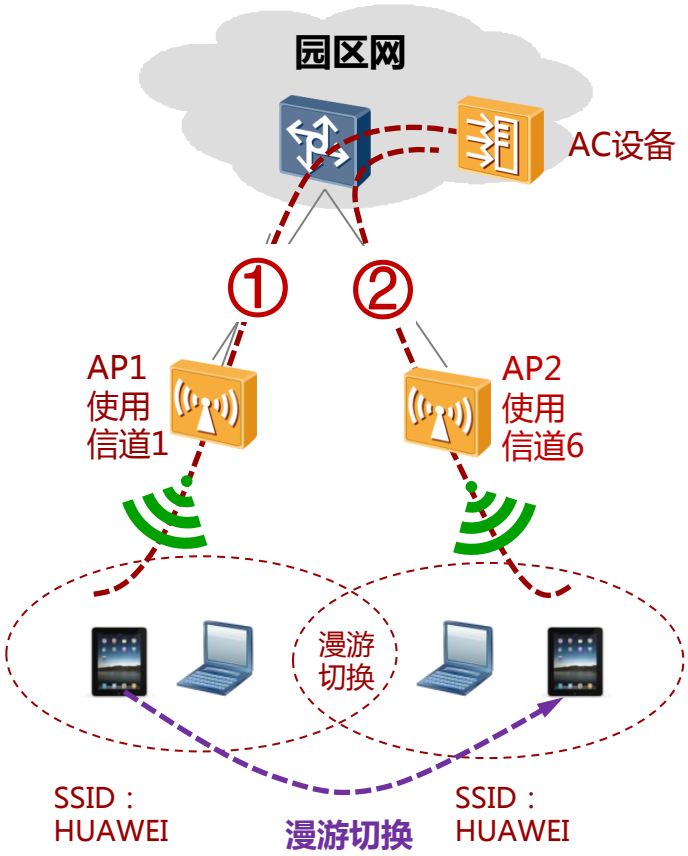
WLAN转发模式:本地转发和集中转发





	本地转发模式	集中转发模式
管理报文	AP管理流封装在CAPWAP（无线接入点控制协议）控制隧道中，到达AC终止	
业务报文	AP业务流不加CAPWAP封装，而直接由AP发送到交换设备直接转发	业务数据报文由AP统一加CAPWAP封装，到达AC实现转发
认证报文	802.1x、Portal等认证报文即可走业务隧道，也可走控制隧道转发流程。	数据报文（包括认证报文）走业务隧道。
优势	数据流量不经过AC，AC负担小，万兆园区推荐方案。	流量全部经过AC，更容易对无线用户实施安全控制策略。

WLAN网络漫游，用户快速切换



① 解除用户和AP1间的关联

② 建立用户和AP2间的关联

漫游概念

用户终端从一个AP覆盖范围移动到另一个AP覆盖范围，用户无需重新登录和认证。

漫游过程举例

终端与AP1已经建立关联，切换到AP2流程如下：

（1）客户端在各信道中发送请求帧。AP2收到请求后，发送应答。AC基于AP信号的强弱，确定与哪个AP关联。

（2）客户端通过向AP1发送解除关联信息，解除与AP1间的关联。

（3）客户端向AP2发送关联请求，AP2使用关联响应做出应答，建立用户与AP2间的关联。

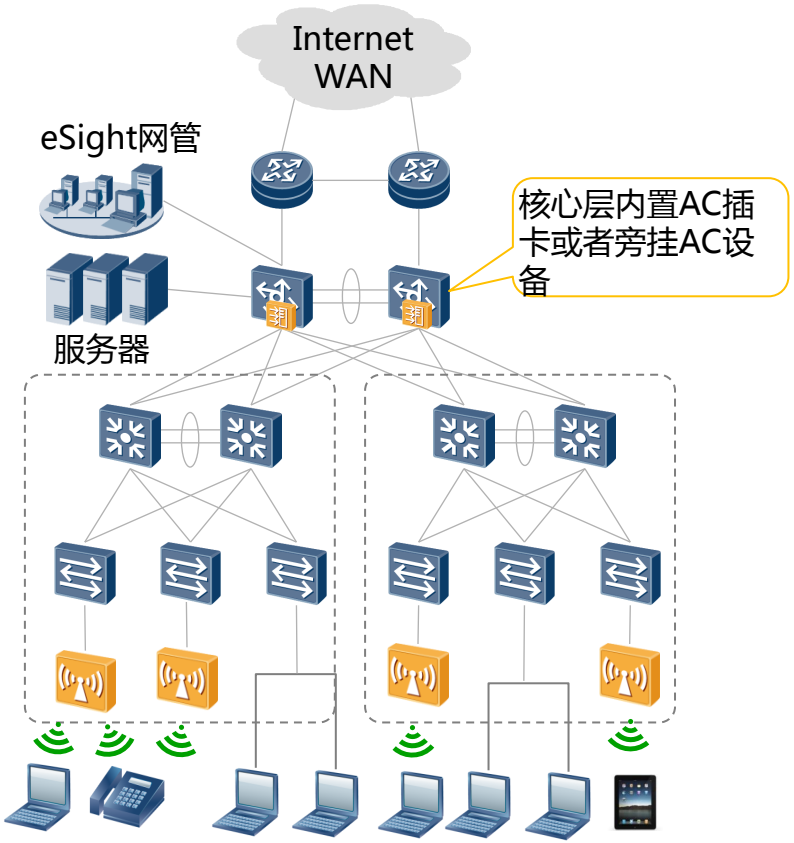
注意事项

（1）漫游切换需要保证SSID相同，即两台AP切换区域需要配置相同的SSID。

（2）漫游切换AP必须是同一个控制器AC管理。

我司不支持跨AC漫游，宣传时注意

大中型园区网络WLAN部署方案



应用场景

终端规模在200以上的大中型园区网，定位于大中型企业总部、大型分支机构、高校、机场等场所。

网络改造，增加园区无线覆盖。

方案部署

在园区网的核心层部署AC设备，主备方式，由AC统一管理AP和无线用户。

AC设备推荐核心交换机（如S97/77等）上直接配置插卡式AC，方便管理；

也可采用旁挂独立AC设备（如AC6605）。

客户价值

方便运维：核心层集中部署AC，有线无线一体化管理。

高可靠性：主备AC方案。

万兆园区网主推方案。

小型园区网络（万兆）WLAN部署方案

应用场景

小型园区或者分支，网终端规模在100～200之间。

方案部署

核心/汇聚层合一的扁平化网络，较少考虑网络可靠性和网管系统。

对于小型万兆园区，核心层采用S7700，内置AC插卡。

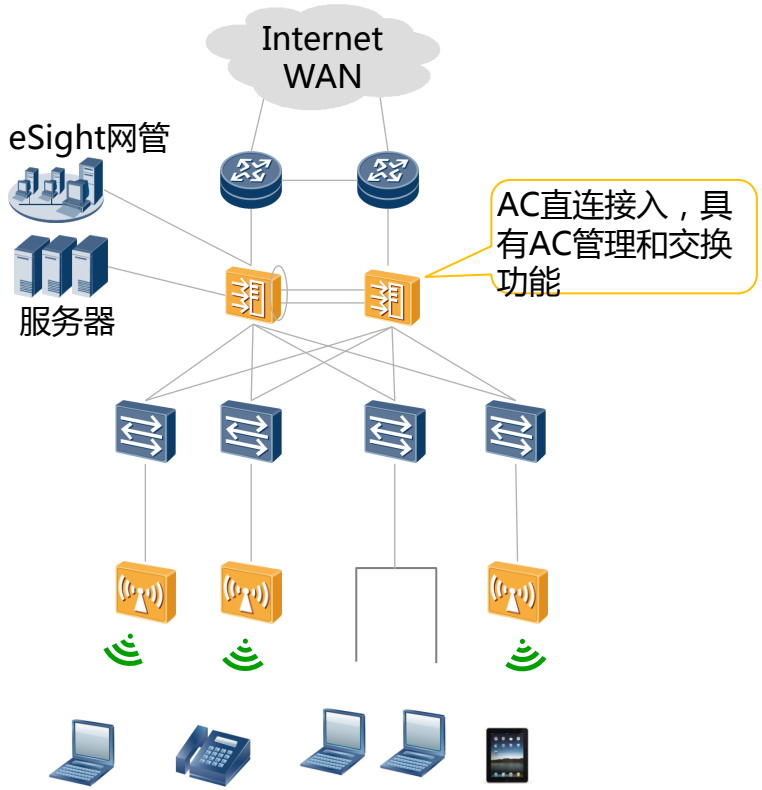
也可采用旁挂独立AC设备（如AC6605）。

客户价值

架构简单：扁平化网络。

节省投资：按需裁减备用设备、网管系统和服务器等设备。

小型园区网络（普通）WLAN部署方案



应用场景

小型园区或者分支，终端规模在100～200。

方案部署

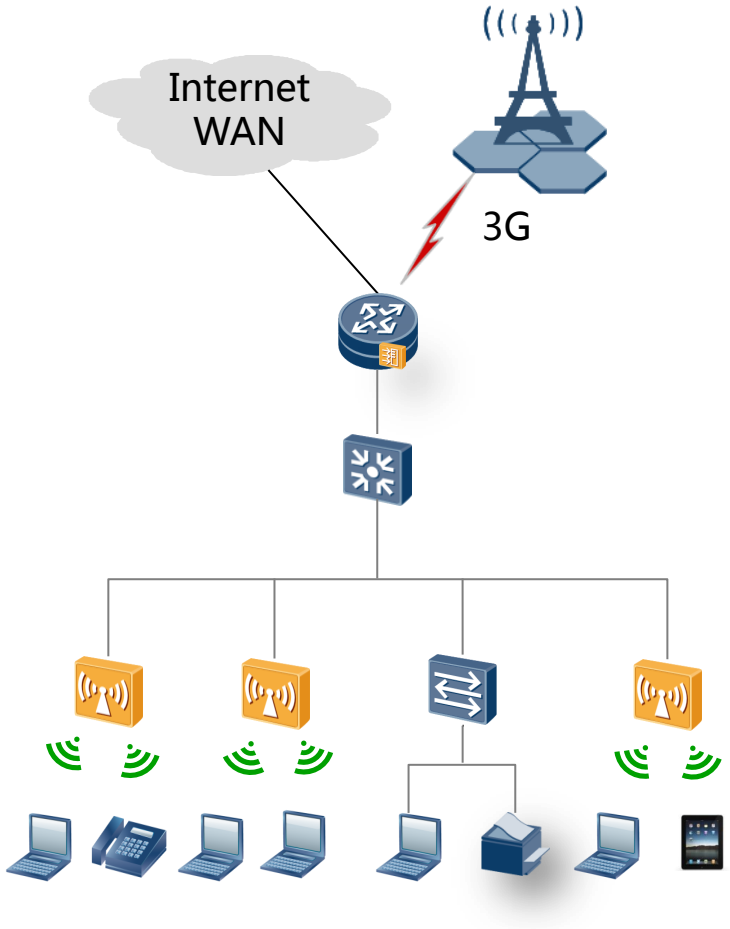
小型园区网规模较小，核心/汇聚层可以合一，扁平化网络可采用独立AC设备，如AC6605等。

客户价值

架构简单：扁平化网络，有线无线一体化管理。

高可靠性：AC主备冗余方案。

SOHO型园区网络WLAN部署方案



应用场景

定位于微型企业或者办事处等场景，终端规模在100以下。

方案部署

园区出口AR集成AC，如选取AR1200作为接入路由器。

汇聚层设备选取PoE交换机，如S3700。

客户价值

组网简单：扁平化网络，不考虑主备。

部署容易：无网管等系统，即插即用。

基于业务划分SSID的WLAN网络

SSID映射以太网中的VLAN（Service Set Identification）

业务VLAN主要用于区分不同的业务类型或用户群体，在WLAN中SSID也同样可以承担相应的工作。因此，在业务VLAN的规划中必须综合考虑VLAN与SSID的映射关系，映射关系有1:1/1:N/N:1/N:N 四种。

AP可配置多个 SSID，构建VAP（Virtual AP）

单频AP可支持16个SSID，双频AP可支持32个SSID。一个AP配置多个SSID，可划分为多个VAP，每个SSID对应一个VAP，AC针对VAP进行策略下发，VAP根据策略进行终端与业务管理。

无线网络一般按照业务类型划分不同的SSID

如右图所示，针对三种不同的无线业务，在AP上设置了3个SSID：

SSID1用于无线办公、SSID2用于访客区域和SSID3用于语音业务。

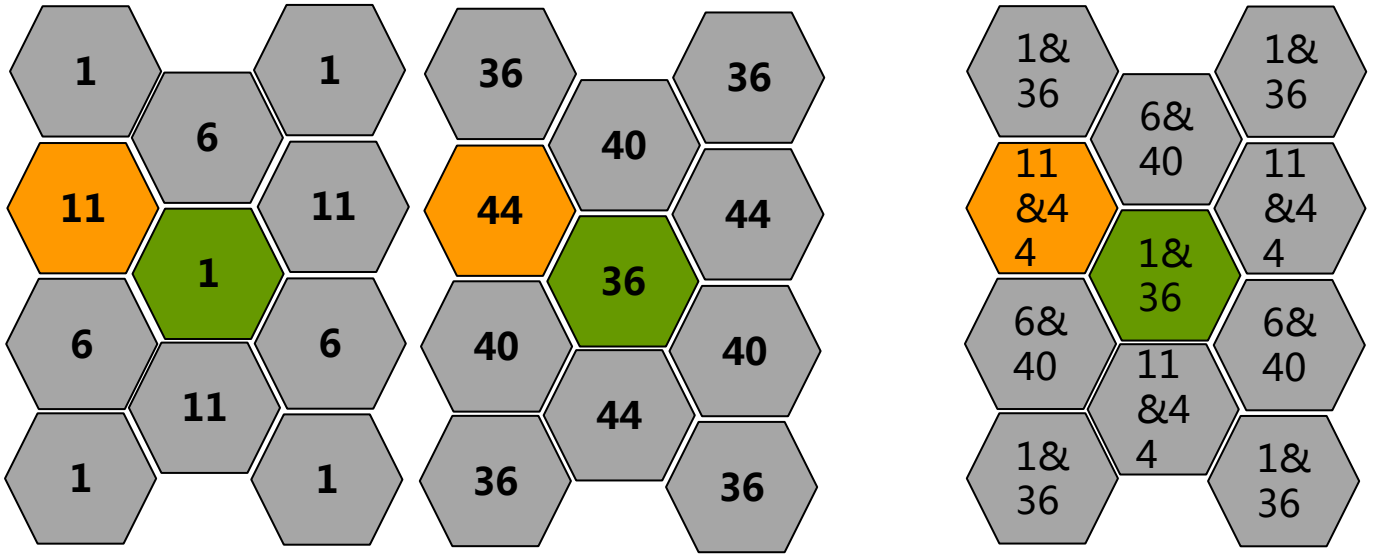
WLAN无线信道划分

为了保证信道间互不干扰，需要对WLAN网络的信道统一规划，WLAN网络主要有两个频段：2.4GHz和5.0GHz。

2.4GHz频段信道划分：

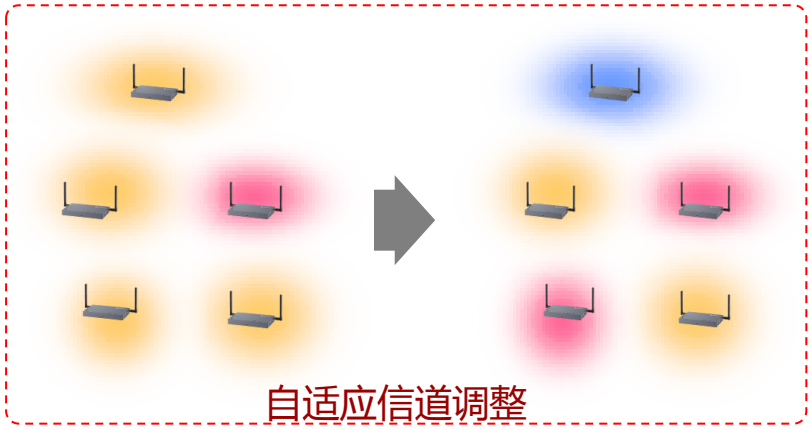
	2.4GHZ频段信道	5.0GHZ频段信道
频率范围	2.4 - 2.4835GHz的连续频谱，信道编号1~14	分配的频谱并不连续，主要有两段：5.15-5.35GHz、5.725GHz-5.85GHz
HT20信道划分	802.11b/a/g/n使用的信道，带宽为20M，如上图，可用不重叠频道只有3个，一般选取1、6、11三个不重叠信道。	5.15-5.35GHz有8个不重叠信道：36、40、44 、48 、52 、56、60、64； 5.725GHz-5.85GHz有4个不重叠信道：149、153、157、161。
HT40信道划分	802.11n使用的信道，2个20MHZ信道捆绑，信道带宽为40M，受频率限制，只支持1个不重叠信道	5.15-5.35GHz有4个不重叠信道 5.725GHz-5.85GHz有2个不重叠信道

WLAN信道蜂窝式无线覆盖



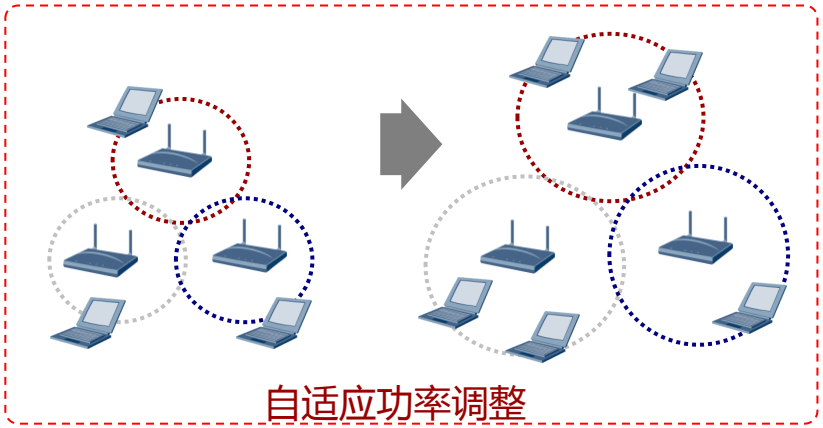
	单频段蜂窝	双频段蜂窝
覆盖要求	相邻区域使用无交叉干扰的信道， 如2.4GHz频段使用1、6、11信道， 5.0GHz使用36、40、44频段。	采用2.4GHz和5.0GHz混合部署，有效实现用户接入负载分担。
	适当调整AP发射功率，避免跨区域的同频干扰。	
部署效果	实现无交叉频率重复使用	高密度覆盖接入场景，提高用户接入能力。
注意：信道使用具有地域、国家差异，规划中需要和部署企业咨询。		

自适应信道、功率调整，简化业务部署



自适应信道调整

支持信道自动扫描功能，自动探测周边的AP、使用的信道以及干扰，结果上报AC，触发信道自适应调整。



自适应功率调整

根据无线终端接入的距离及数据交换容量，自动调整无线信号发射功率。

目录

WLAN安全协议标准

Open System

符合WiFi的终端都可接入，一般用于有众多用户的运营网络。

WEP（Wired Equivalent Privacy）

有线对等加密，主要用来保护WLAN空口信号的信息安全。

应用于小规模/低安全需求的WLAN网络（SOHO/家庭热点等）。

WPA/WPA2（Wi-fi Protected Access）

802.1x认证体系、密钥体系、密钥管理、加密与认证协商以及TKIP加密，WPA2增加了预认证和CCMP加密，同时兼容WPA

广泛应用于各种大、中型WLAN网络和公共场合。

WAPI（Wireless Authentication Privacy Infrastructure）

认证框架采用基于证书的双向认证机制，支持AP与STA之间的双向鉴别。

中国标准，亟需大力推广与支持。

WLAN用户接入认证技术

Portal认证

也称为WEB认证，通过Web认证页面，输入用户帐号信息，实现对用户身份的认证。无需客户端，安全性稍低，广泛应用于园区网中。

802.1X认证

使用EAP（Extensible Authentication Protocol）认证协议，实现客户端、设备端和认证服务器之间认证信息的交换。

需客户端支持，安全性高，园区网主推方案。

MAC认证

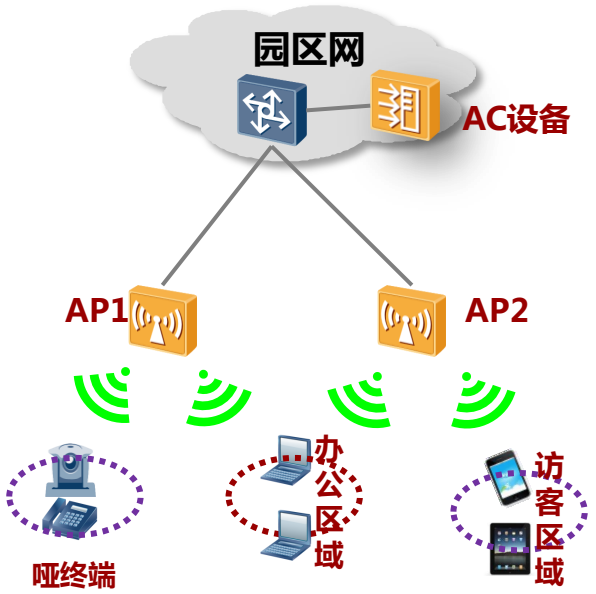
MAC地址作为身份凭据到认证服务器进行认证。

主要用于IP电话、打印机等哑终端设备

PPPoE认证

PPPoE实现广播链路上点对点通讯的协商，通过拨号软件输入用户信息到远端服务器进行认证。

需客户端支持，一般用于运营商网络，企业网不推荐使用。



如上图，哑终端通过MAC认证接入，办公区域通过802.1X或Portal认证接入，访客区域通过Portal认证接入，多种认证技术保证WiFi终端安全接入，从源头上消除安全威胁。**【相关认证技术细节请参见园区网NAC专项方案】**

WLAN无线用户接入技术对比

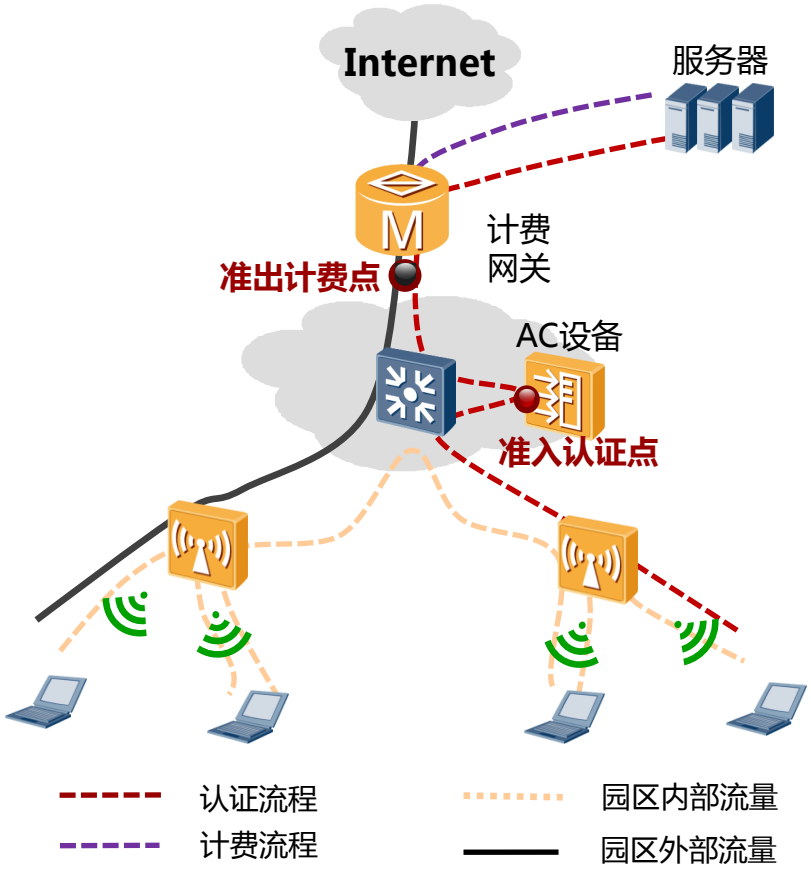
无线接入认证技术和安全协议对应关系如下：

认证方法	安全协议	安全性	封装开销	地址分配	客户端软件	应用场景
MAC认证	Open System	低	小	认证后分配	不需要	手持PDA、IP电话等哑终端设备
	WEP/WPA/WPA2+PSK	低	小	认证后分配	不需要	场景同上，需要额外的PSK密码
Portal认证	Open System	中	小	认证前分配	不需要	中小型园区网络
	WEP/WPA/WPA2+PSK	中	小	认证前分配	不需要	场景同上，需要额外的PSK密码
802.1X认证	WEP/WPA/WPA2	高	小	认证后分配	需要	大中型园区网络
PPPoE认证	Open System	低	大	认证后分配	需要	运营商市场
	WEP/WPA/WPA2+PSK	低	大	认证后分配	需要	场景同上，需要额外的PSK密码

当前WAPI在企业网和运营商中应用很少，一般作为准入门槛测试。

园区网中，从安全性和易部署性等多方面考虑，**推荐园区802.1X + WPA2的认证机制，无线哑终端采用MAC认证，访客区域采用Portal认证。**

WLAN网络认证、安全、计费方案概述



应用场景

校园网、广电网、酒店等行业具有运营需求，要求认证、安全和计费功能。

解决方案

AC集中认证和授权，统一控制。

出口计费服务器统一计费。

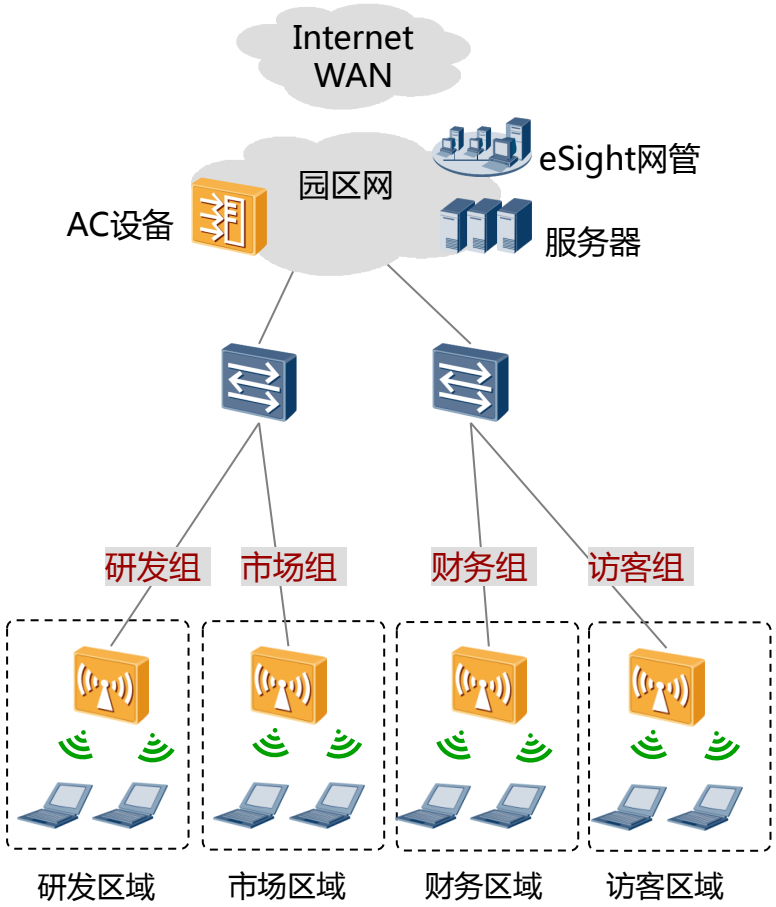
数据本地转发，不经过AC，提升网络性能。

客户价值

用户集中认证，数据流量本地转发，安全管理和网络性能做到完美结合。

各功能组件按需选择，提供多套认证和计费方案。

基于用户组的精细化策略控制



用户组概念（User Group）

是指具有相同安全、策略等属性的一组用户（终端）的集合。例如：网络划分成研发、财务、市场、访客等用户组，不同用户组可授予不同权限。

基于用户组策略部署

基于不同部门划分用户组：

（1）访客组内用户进行二层隔离，限制互访；

（2）研发组和市场组隔离，限制研发和市场人员互访；

（3）市场组用户限速10M，研发组不做限速；

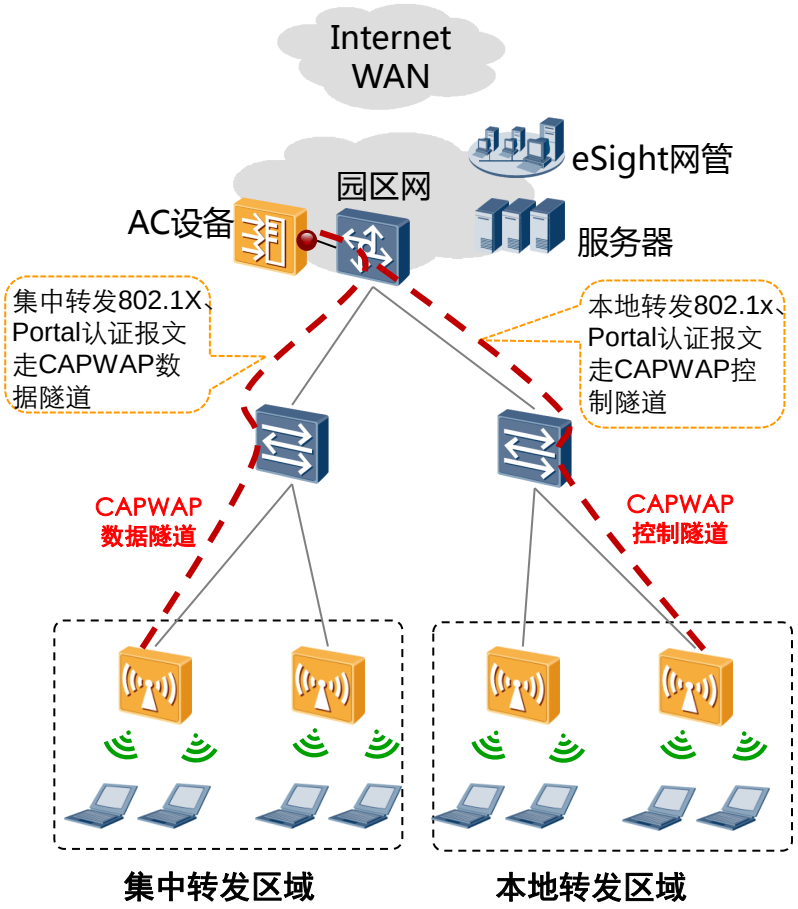
（4）财务部门需要较高安全，访问权限受控，只能访问特定服务器。

客户价值

1）基于用户组下发ACL，节省ACL资源；

2）授权到AP，提供业界细粒度的用户策略控制能力。

无线用户AC集中认证



无线用户AC集中认证

AC上集中认证，用户集中管理。

（1）用户认证通过后，授权通过AC控制隧道下发到AP，精细化控制用户访问权限。

（2）用户漫游、策略下发等由AC灵活控制。

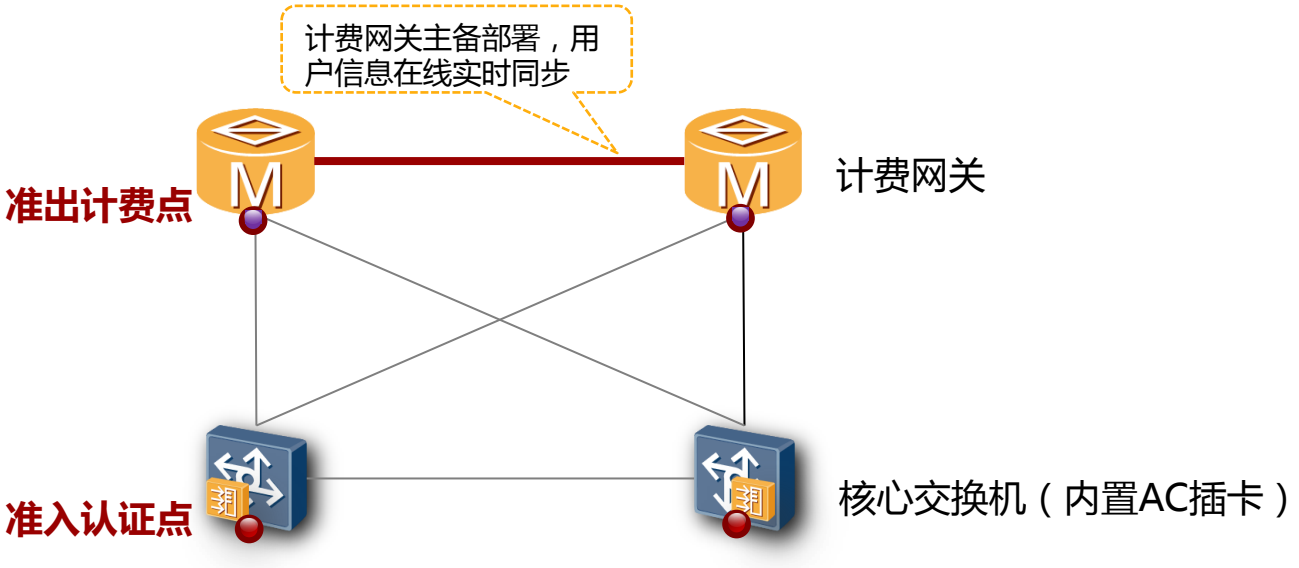
两种转发场景

集中认证，要保证认证协议能够上送AC处理。

（1）集中转发场景，802.1X、Portal认证报文作为数据流量，通过CAPWAP数据隧道上送AC。

（2）本地转发场景，通过配置，802.1X、Portal认证报文进入CAPWAP控制隧道，上送到AC设备，完成认证过程。

园区出口计费网关部署



计费网关部署

计费网关一般作为准出设备，部署在园区出口，对出园区的用户报文进行计费。

两种部署方式:单机和主备，为提升园区网络可靠性，推荐采用主备方式。

网关主备之间数据同步

可以做到用户数据实时同步。用户在任一设备上线后，在线信息会同步到对端设备，保证两台计费网关信息一致。

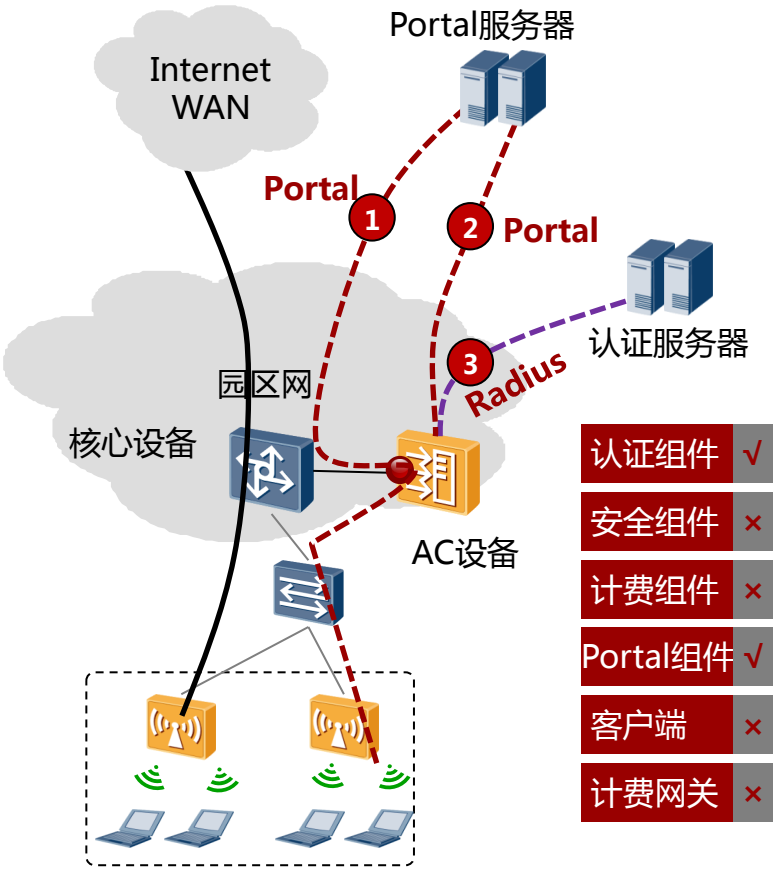
认证、安全、计费系统组件

认证、安全、计费方案需要服务器、客户端、计费网关三部分组成，其中服务器系统可分为认证、安全、计费、Portal等四个组件，各组件功能如下表：

序号	组件名称	功能描述	备注
1	用户认证组件	支持MAC、802.1x、Portal、PPPoE等接入认证和相关统计报表。	必选
2	安全管理组件	通过和客户端联动，支持终端补丁、防病毒等安全检查和修复功能。	可选
3	用户计费组件	支持基于时间和流量计费。	与序号4同时选用
4	计费网关	部署在园区网出口，实现出外网报文计费，包括基于时间和基于流量计费两种方式。	与序号3同时选用
5	Portal组件	弹出用户定制的认证页面，提供方便的用户自助服务平台，实现用户Portal接入认证。	可选
6	客户端软件	通过和服务器联动，完成接入认证、安全检查、用户计费等功能。	可选

除用户认证是必选组件外，其他组件可基于现网需求选择。

WLAN认证方案



应用场景

中小型企业，需控制用户接入，同时企业员工较少，无需终端健康检查等。

方案部署

选择802.1x或者Portal认证。以Portal认证为例，服务器采用TSM系统，认证和Portal服务器可在同一台服务器上。认证过程如下：

（1） 用户通过WEB认证，认证报文到AC后，通过Portal协议向Portal服务器发起认证。

（2）Portal服务器把用户信息回传给AC设备。

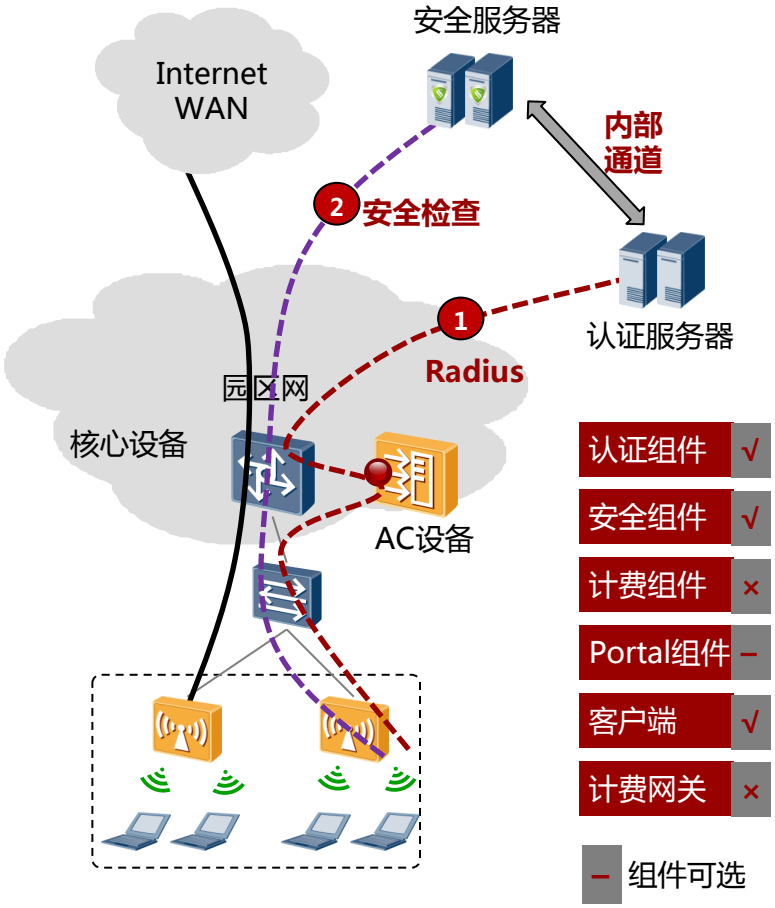
（3）AC设备和认证服务器通过Radius协议完成用户准入认证。

客户价值

无需客户端，通过WEB面或者操作系统自带客户端（802.1X）完成。

服务器组件按需选择，节省用户投资。

WLAN认证+安全方案



应用场景

适合政府、企业等对于安全要求较高的行业客户。

方案部署

服务器采用华为TSM系统，以802.1x认证为例：

（1）802.1x报文到达AC后，通过Radius协议向认证服务器发起认证。

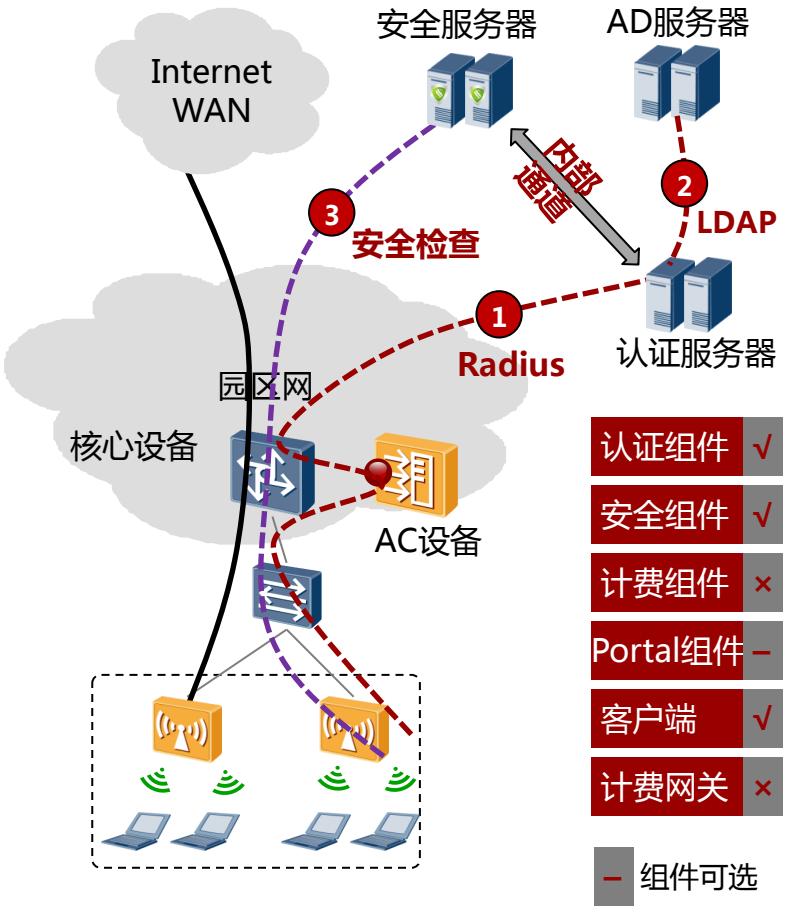
（2）安全服务器和客户端配合，完成终端病毒库、补丁等健康检查，并可和软件服务器联动，进行终端修复操作。

客户价值

准入控制+安全检查，提升内网安全。

服务器组件定制化选择，节省用户投资。

WLAN认证+安全+AD方案



应用场景

适合已经使用LDAP服务器管理用户，对于内网安全要求较高的企业。

方案部署

服务器组件采用华为TSM系统，认证和安全服务器一般部署在同一台服务器上；LDAP服务器为微软AD域服务器：

（1）无线用户认证报文到AC后，通过Radius协议向认证服务器发起认证。

（2）认证服务器和AD服务器通过LDAP协议获取用户信息，完成认证过程。

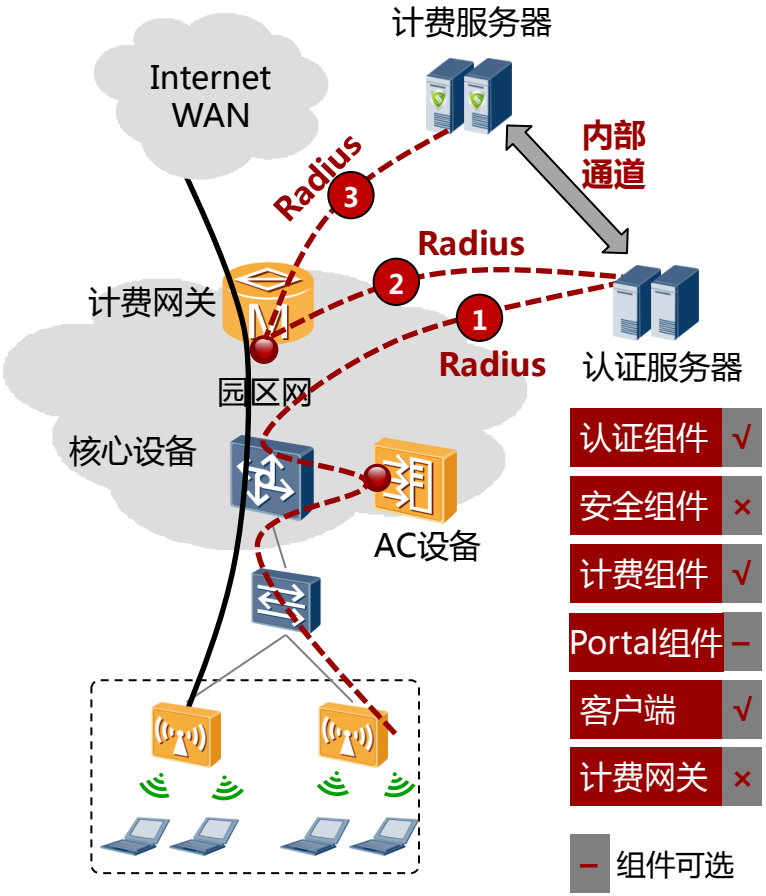
（3）安全服务器和客户端配合，完成终端病毒库、补丁等健康检查，并可和软件服务器联动，进行终端修复操作。

客户价值

准入控制+安全检查，提升内网安全。

和现有AD对接，保护用户投资。

WLAN网络认证+计费方案



应用场景

适合教育、酒店等有计费要求的行业网，对于内网安全要求相对较低的客户。

方案部署

服务器组件采用合作方产品，认证和计费服务器一般部署在同一台服务器上；计费网关一般选择合作方产品，大型行业网可使用ME60：

（1）无线用户认证报文到AC后，通过Radius协议到认证服务器完成内网准入认证。

（2）认证服务器通过Radius协议，主动通知计费网关进行准出认证，打开外网权限。

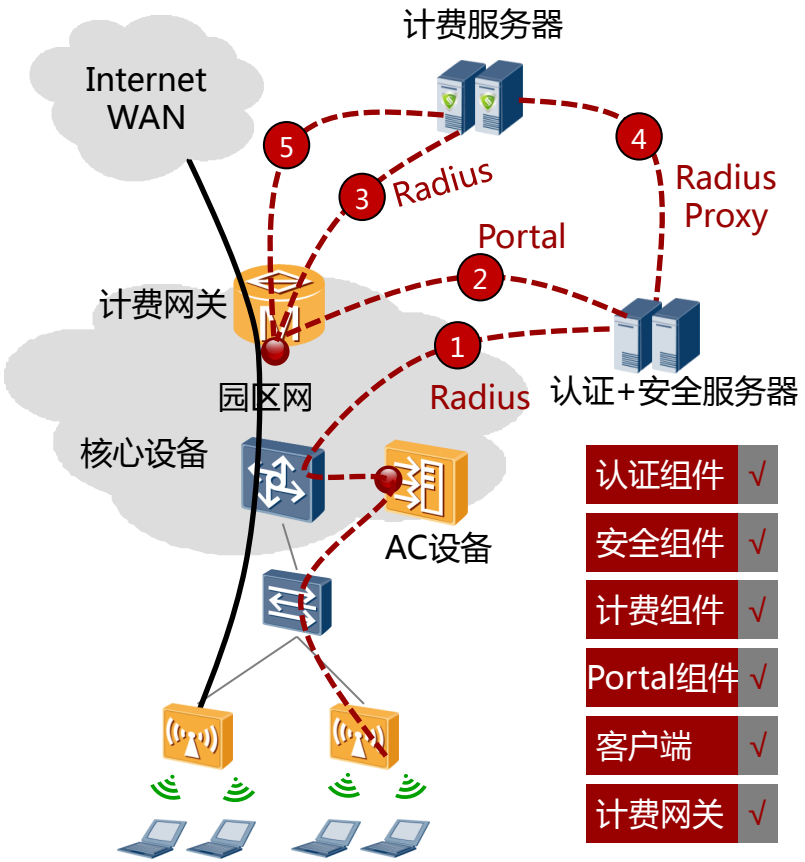
（3）用户访问外网，计费网关开始计费，并向计费服务器通告计费信息。

客户价值

准入准出一次认证，提升用户体验。

计费网关按需选择，节省用户投资。

WLAN网络认证+安全+计费方案



应用场景

适合教育、能源等有计费需求的行业，客户对内网安全也有较高的要求。

方案部署

服务器采用TSM系统，计费服务器和计费网关采用第三方产品，大型园区使用ME60:

（1）认证报文到AC后，通过Radius协议到认证服务器完成内网认证。

（2）认证服务器的Portal组件主动向计费网关发起Portal认证，进行外网准出认证。

（3）计费网关通过Radius协议向服务器请求用户信息。

（4）计费服务器作为Radius Proxy，从认证服务器获取用户信息，完成准出认证。

（5）用户访问外网，计费网关开始计费，并向计费服务器通告计费信息。

客户价值

一次认证，提升用户体验。

用户数据集中管理，方便系统维护。

方案比较和产品选型

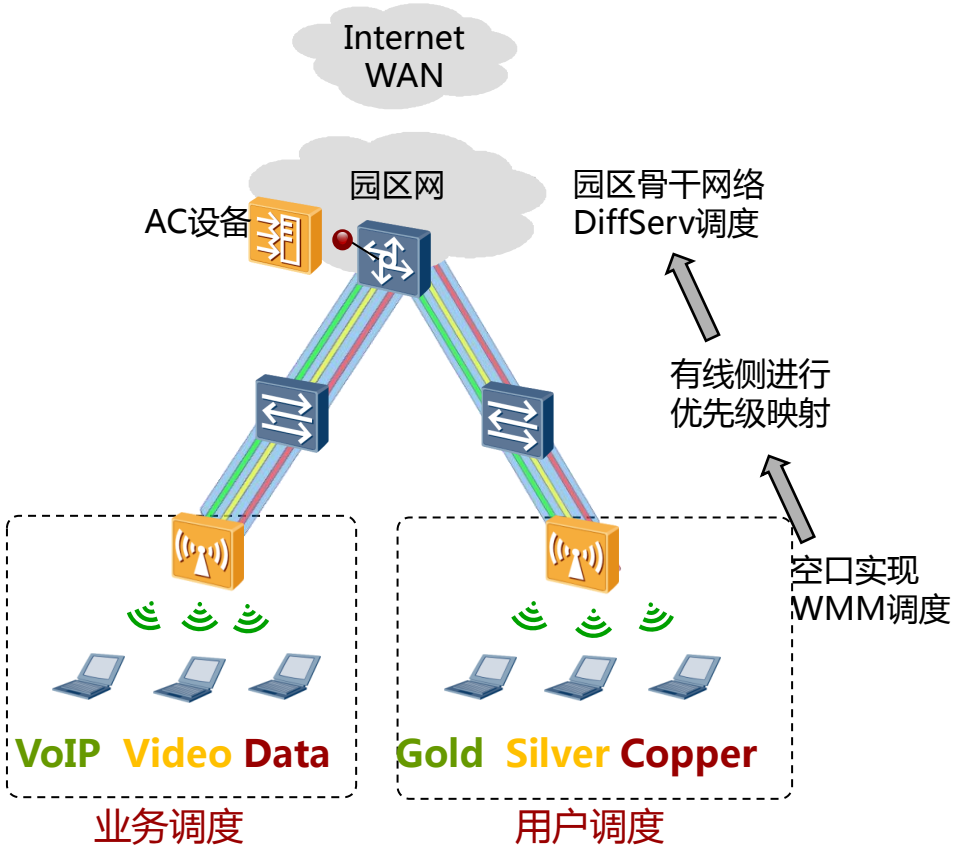
编号	方案名称	服务器组件				客户端	计费网关	应用场景
		认证	安全	Portal	计费			
1	认证	TSM	不需要	TSM	不需要	不需要	不涉及	中小型企业，对于终端安全没有过多要求。
2	认证+安全	TSM	TSM	TSM	不需要	TSM	不涉及	大中型企业等对内网安全要求较严格的市场。
3	认证+安全+AD	TSM	TSM	TSM	不需要	TSM	合作方或ME60	LDAP服务器管理用户，内网安全要求较严格。
4	认证+计费	合作方	合作方	合作方	合作方	合作方	合作方或ME60	校园、广电、酒店等需要计费的行业市场。
5	认证+安全+计费	TSM	TSM	TSM	合作方	TSM	合作方或ME60	教育、能源等需要计费的行业市场，同时内网安全要求较严格。

在国内，合作方有深澜（推荐销售）、城市热点（转售）等厂商，可提供方案4和方案5的服务器组件、客户端和计费网关。

基于现网容量，计费网关可选择合作方产品或者ME60，一般广电、运营商市场推荐ME60产品，校园网、酒店等行业采用合作方计费网关。

目录

WLAN网络QoS调度解决方案



应用场景

定位于大、中型园区网络

方案部署

无线空口做WMM调度

有线侧进行优先级映射

园区网做DiffServ调度

客户价值

保证核心业务服务质量

保证VIP用户业务体验

WMM（ Wi-Fi Multimedia，Wi-Fi多媒体）调度后，在有线侧进行优先级映射，在核心层、汇聚层实现DiffServ调度，最大程度保障核心业务和VIP用户服务质量。

无线空口WMM调度技术

- 信道竞争原理EDCA (Enhanced Distributed Channel Access)

  在占用信道发送数据前，终端Station（或者AP）会监听信道。当信道空闲时间大于或等于终端空闲等待时间时， 则在竞争窗口范围内，终端随机选择退避时间进行退避，最先结束退避的终端竞争到信道。

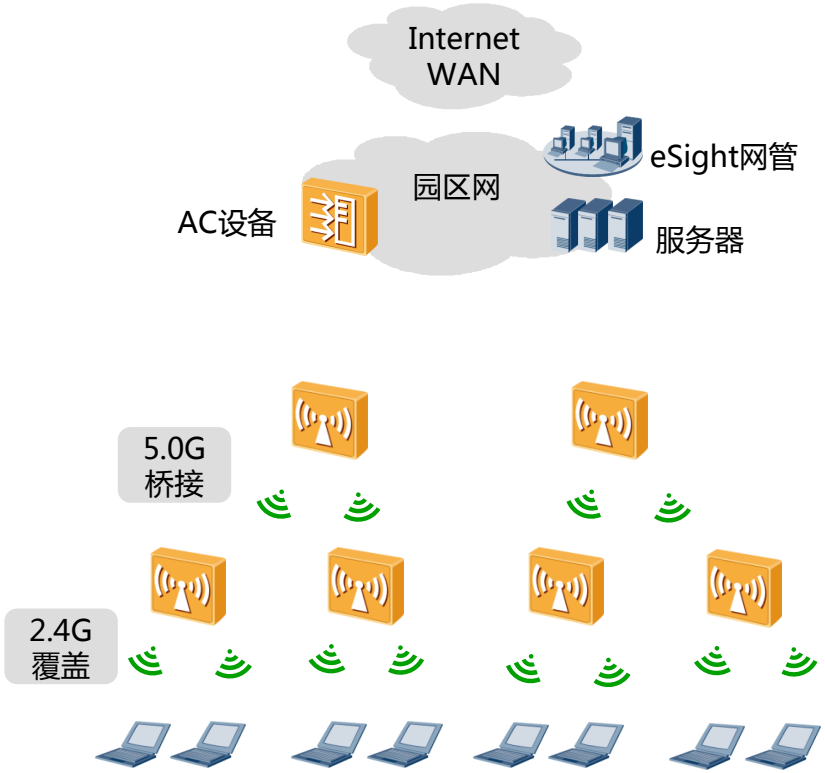
- WMM（Wi-Fi Multimedia）是一种无线QoS协议，在无线空口上，WMM将数据报文通过4个优先级队列发送，每个优先级队列占用信道的机会不一样，从而保证语音、视频等应用在无线网络中有更好的质量。

WMM队列	User Priority（802.11e）
Voice	6或7
Video	4或5
Best Effort	2或3
Background	0或1

无线数据有线侧优先级映射原理

<table>
<tr><th></th><th>数据报文本地转发</th><th>数据报文集中转发</th></tr>
<tr><td rowspan="2">上行无线报文到有线报文优先级映射</td><td colspan="2">AP接收到无线客户端发送的802.11（无线）数据报文后，将其转换为802.3（以太网）报文，然后向网络侧继续转发。</td></tr>
<tr><td>对于信任的客户端，实现802.11e到外层优先级802.1p、DSCP映射；对于不信任的客户端，可以直接指定802.1p、DSCP的优先级</td><td>对于信任的客户端，实现802.11e到外层隧道优先级Tunnel-802.1p、Tunnel-DSCP映射；对于不信任的客户端，可以直接指定隧道Tunnel-802.1p、Tunnel-DSCP的优先级</td></tr>
<tr><td rowspan="2">下行有线报文到无线报文优先级映射</td><td colspan="2">AP接收到802.3以太报文后，将其转换为802.11报文；
空口上依据报文中802.11e优先级（UP）选择不同的WMM队列发送给用户终端。</td></tr>
<tr><td>需要完成802.1p到802.1e优先级映射</td><td>在AC上实现DSCP优先级到外层隧道Tunnel-DSCP映射，802.1p优先级到Tunnle-802.1p优先级映射。</td></tr>
</table>

WLAN无线回传解决方案



应用场景

大型仓库、港口码头、山川河流等恶劣环境，不适合部署线缆。

乡村、郊区或者野外等人员稀疏环境，进行局部热点覆盖。

方案部署

无线网桥通过P2P/P2MP桥接功能，实现热点区域覆盖和数据回传。

无线网桥协议WDS，支持自动发现AC，实现远程自动配置。

客户价值

降低传统有线网络依赖，节省费用。

突破恶劣地域限制，缩短建网周期

WDS：Wireless Distribution System

无线网桥P2P传输性能指标

工作频段	环境	天线增益	典型距离下802.11n HT20 /HT40吞吐量（Mbps）					
			500m	1km	2km	5km	10km	频宽
2.4G 无线覆盖	市区	11dBi	80	80	45	15	/	HT20
		14dBi	80	80	80	36	15	HT20
		17dBi	80	80	80	60	36	HT20
	郊区/农村	11dBi	80	80	70	32	12	HT20
		14dBi	80	80	80	55	32	HT20
		17dBi	80	80	80	80	55	HT20
5.0G 无线回传	市区	11dBi	55/90	30/45	6/9	/	/	HT20/HT40
		15dBi	80/160	60/95	30/45	/	/	HT20/HT40
		18dBi	80/160	80/160	50/80	12/15	/	HT20/HT40
		21dBi	80/160	80/160	80/135	32/50	10/15	HT20/HT40
	郊区/农村	11dBi	80/160	80/135	45/65	8/13	/	HT20/HT40
		15dBi	80/160	80/160	48/70	10/15	/	HT20/HT40
		18dBi	80/160	80/160	80/120	30/45	8/12	HT20/HT40
		21dBi	80/160	80/160	80/160	50/80	27/40	HT20/HT40

2.4G频段用于用户接入覆盖及设备维护，无线回传推荐5.0G频段，传输距离控制在5KM以内。

P2P无线回传带宽影响因素：应用环境、传输距离、天线增益、频宽等直接相关，规划时需要关注。

无线网桥P2MP传输性能指标

点对多点（P2MP）网桥吞吐量性能评估，需在点对点（P2P）网桥数据基础上考虑吞吐量系数。

P2MP	网桥上行因子	网桥下行因子
M=1	1	1
M=2	0.57	0.285
M=3	0.54	0.18
M=4	0.54	0.135
M=5	0.48	0.096
M=6	0.48	0.08

P2MP链路带宽计算

5G频点，18dBi天线，频宽HT20，2km距离下P2P吞吐量80Mbps。

当采用一点对三点的网桥，吞吐量计算如下：

网桥节点带宽：80*0.54=43.2Mbps

分支链路带宽：80*0.18 = 14.4Mbps

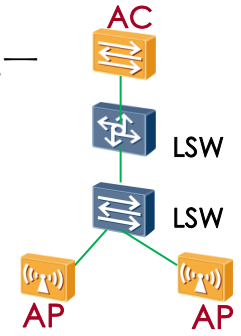
即该级网桥链路总带宽从80Mbps下降到43.2Mbps，而每一条链路只有14.4Mbps。

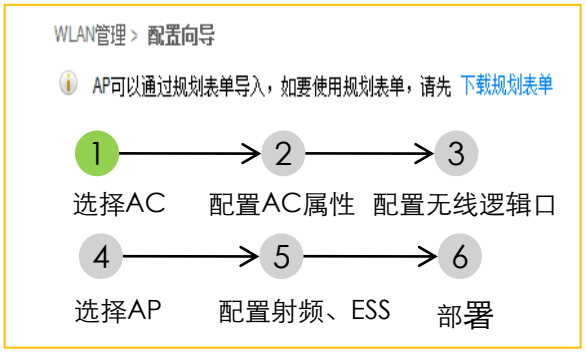
网络规划中，P2MP网桥推荐不要超过4个，无线回传距离控制在5KM。

eSight网管让WLAN网络部署更加简单

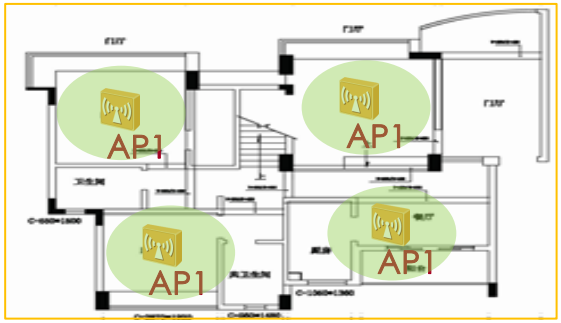
AP上电后自动进入版本加载，无需人工干预；
网管实时监控升级任务，控制升级进程。

有线、无线设备统一管理；
可视化网络拓扑。





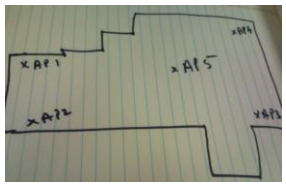
AP配置通过规划表单批量导入；
业务发放向导式配置。



位置拓扑，可视化射频管理；
快速识别非法AP能力。

设计优化服务让WLAN业务承载更可靠

服务前



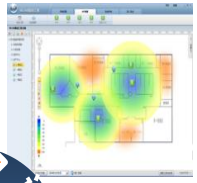
手工规划

服务后

专业工具

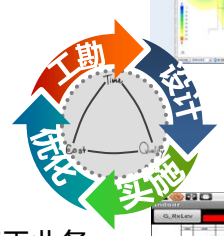
•易携带全覆盖

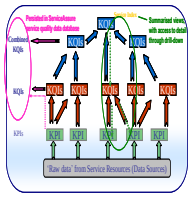
•干扰检测



•专业自动布放算法

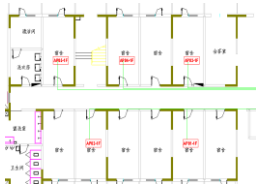
•覆盖效果仿真





•基于业务的指标体系

•业务质量一键测试



合理的网络设计

稳定的网络运行

可预见	降成本	传经验
● 95%↑ 以上区域信号质量保证 ● 可视化规划场强、吞吐率、信噪比、设备数量、设备位置以及线路	● 可合理规划设备投资，建网周期提升30%↑ ● 后期网络运维问题减少20%↓	● 100+↑ 以上项目经验，固化到专业设计、评估工具 ● 专业的规划评估报告，提升运维技能

认证、安全、计费方案产品家族

华为产品

TSM系统服务器组件

TSM客户端软件

ME60

深澜软件

深澜软件 www.srun.com

Srun服务器组件

深澜软件 www.srun.com

Srun 客户端软件

国内推荐销售

Srun 3000

城市热点

Dr.COM

Dr.COM服务器组件

Dr.COM

Dr.COM客户端软件

国内推荐销售

Dr.COM计费网关
2013/2133/2166

华为WLAN产品家族

AP设备

AP6010SN（室内单频）
AP6010DN（室内双频）

AP6310 SN（室内单频）

AP6510 DN（室外双频）
AP6610 DN（室外双频）

AC设备

AC6605（盒式）

S9700/S7700
（AC 插卡）

WLAN产品主要参数

编号	产品	主要参数描述
1	AP6010SN	室内放装型，单频，2×2 MIMO，内置全向天线，支持 802.11b/g/n。
2	AP6010DN	室内放装型，双频，2×2 MIMO，内置全向天线，支持 802.11a/b/g/n。
4	AP6310SN	室内分布型，单频，大功率产品，发射功率500 mw， 支持 802.11b/g/n。
5	AP6510DN	室外分布型，双频，2×2 MIMO， 支持802.11 a/b/g/n。
6	AP6610DN	室外网桥，双频，2×2 MIMO， 支持802.11 a/b/g/n，有外接电源。
7	AC6605	汇聚型盒式AC，24GE口，4Combo口，2×10GE口，可管理512 AP。
8	ACU 插卡AC	S77/97插卡式AC，可管理1024AP。

S - Single：单频；　　D - Double：双频；

N - Normal：普通型；　　E - Extened：增强型，智能天线。

附录一：802.11n AP产品竞争对比

HUAWEI

Indoor Single-band AP

AP6010SN AP6310SN

Indoor Dual-band AP

AP6010DN

Outdoor AP

AP6510DN AP6610DN

CISCO

Aironet 1040/1140/1130

Aironet 1200 Series

Aironet 1550 Series

H3C HEWLETT PACKARD

WA261x Series

WA262x Series

WA2200X Series/WA2600X Series

附录二：盒式AC产品竞争对比

HUAWEI

Box AC

AC6605

CISCO

2000/2100/2500 Series

4100/4400 Series WLC

5500 Series

Flex 7500 Series

H3C HEWLETT PACKARD

WX3008/3012/3024

WX5002/5004

WX6103

附录三：插卡式AC产品竞争对比

Chassis AC

ACU for S9700/9300/S7700

CISCO

WiSM for Catalyst 6500/7500

WiSM2 for Catalyst 6500

ISM-300/SM-700/SM-900 for ISR G2

Wireless LAN Controller Modules for 2800/3800/3700 Router

H3C HEWLETT PACKARD

LSWM1WCM10/20 for S5800

LSQM1WCMB0 for 7500E

LSRM1WCM2A1 for 9500E

附录四：Why win Cisco？

端到端融合解决方案

华为提供从路由器-BRAS-交换机-AC-AP端到端的解决方案，业务融合为客户提供精确的用户管理、策略控制及计费认证的领先解决方案，部署高品质有线无线网络；

Cisco无线WLAN网管没有和数通产品网管融合，且WLAN网管多语言支持差（不支持中文）。

基于用户组的精细化策略控制

华为基于用户组的用户管理和策略下发，精确控制用户访问策略，节省AP的ACL资源，部署简单，实现跨区域的真正的任意地点接入；

Cisco的WLAN用户策略下发方式访问控制粒度弱，不能实现同一用户组内二层隔离，用户管理方面不占据优势。

附录五： Why win H3C？

基于用户组的精细化策略控制

华为基于用户组的用户管理和策略下发，精确控制用户访问策略，节省AP的ACL资源，部署简单，实现跨区域的真正的任意地点接入；

H3C具有用户模版概念（user-profile），管理用户授权策略，但针对每个用户下发，**无法实现资源共享。**

用户接入性能

华为AP单用户转发能力较强，各款型号AP性能均衡，每用户平均带宽比H3C产品高30%；H3C不同型号AP性能差别较大，多种产品转发能力不足；802.11b/g/n等多模终端同时接入时，H3C增强型AP几乎无流量。

射频性能

华为AP发射功率强劲，信号覆盖强，近距离（<10m）吞吐量非常高；

H3C普通室内型AP2620-AGN信号功率弱，上行吞吐量不到正常的一半。

绿色低碳

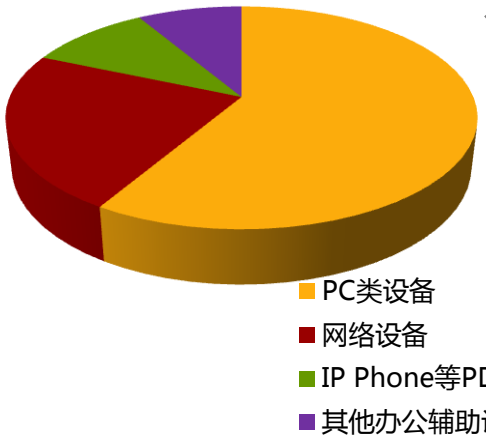
华为在产品的生命周期中，从设计、开发、生产、交付的整个过程贯穿“绿色低碳”的理念；H3C盒式AC的自身功耗与每AP管理功耗较大。

子目录

4 园区网业务解决方案

减少无效耗能，提高设备能效

企业园区网耗能分布



时间分布

- 一般企业一年大概250个工作日，每个工作日8小时工作时间，员工多在这段时间内为企业创造价值，此段时间内耗能为有效耗能8x250/24/265≈22%
- 由于员工不及时关闭PC、IP phone等引起的耗能；以及网络设备空转的耗能为无效耗能多集中于剩下的78%时间内

地域（部门）差异

- 不同业务部门耗能习惯不同。比如测试部PC机可能在非工作时间也需要保持开启；而大多数部门员工下班后PC、IP Phone为了节能的目的应该及时关闭。

类型区别

- 网络设备保持7x24小时的运转
- 服务器多保持7x24小时的运转
- PC、IP phone等终端设备随员工上下班状态改变而改变
- 摄像头多保持7x24小时运转

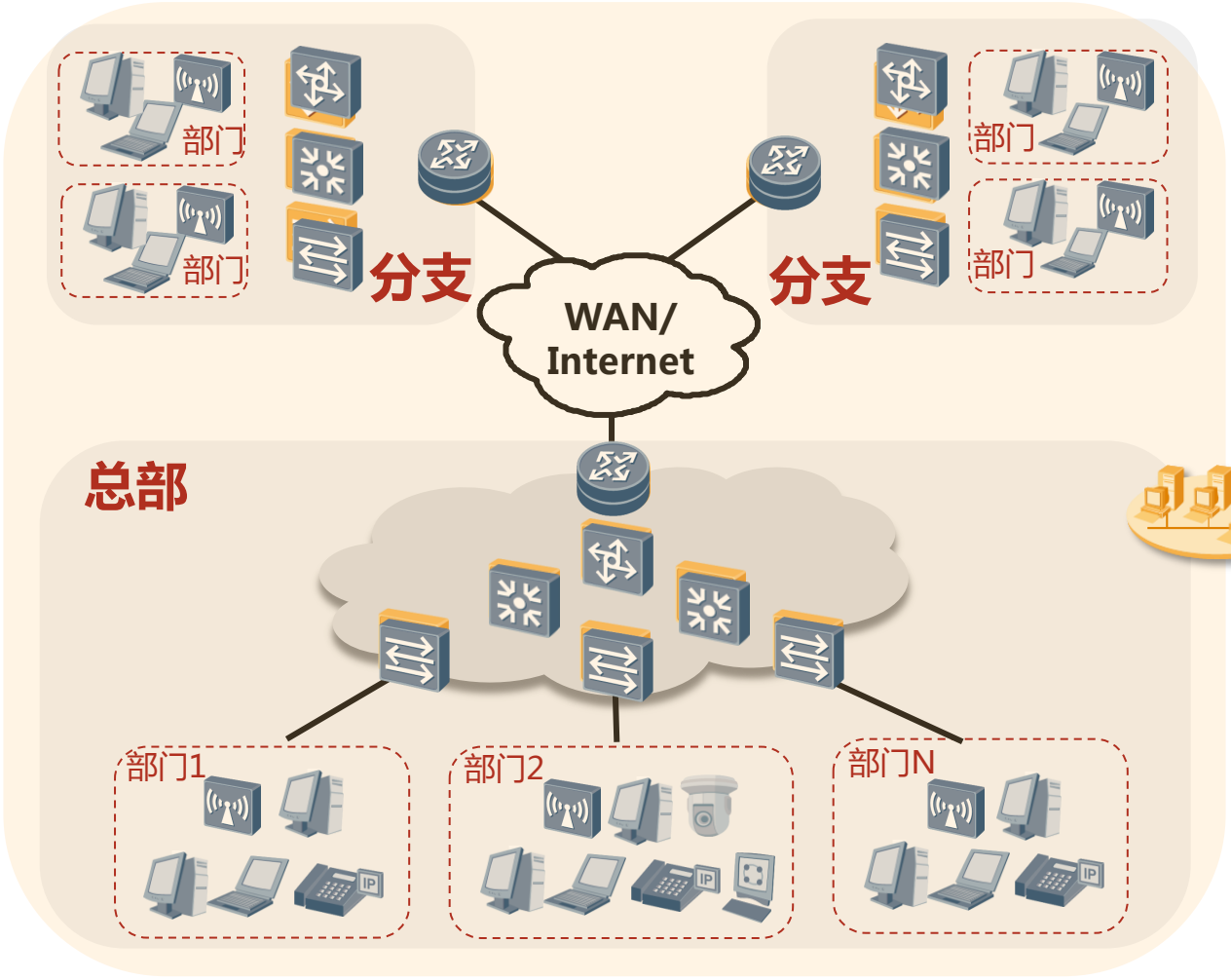
设备角度

- 降低设备工作时耗能、提高设备能效比的需求
- 设备自动识别忙闲状态，动态调节自身耗能需求
- 设备空闲端口自动休眠的需求

管理角度

- 可视化管理需求
- 统一管理需求
- 分时控制需求
- 分类控制需求
- 分域控制需求

企业园区网绿色节能解决方案



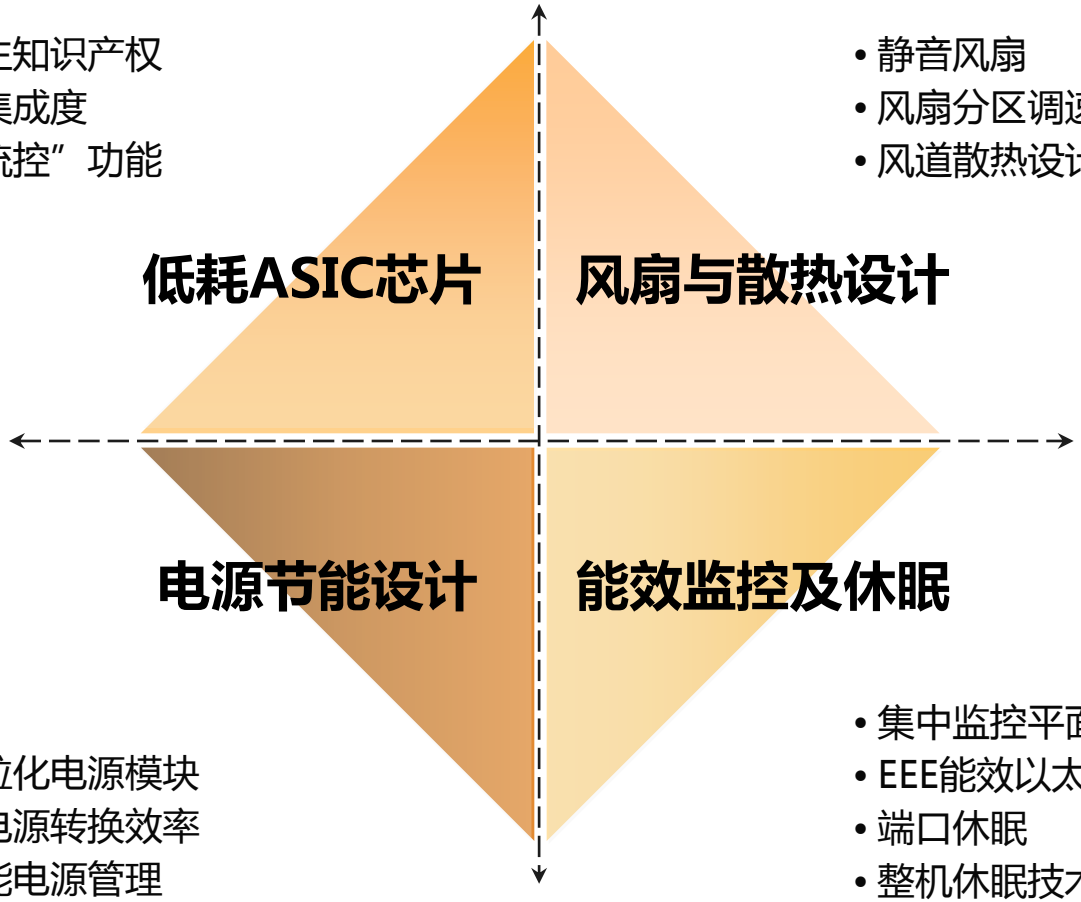
绿色设备

- 绿色节能工艺
- 高能效比
- 动态调整能耗
- 智能休眠技术

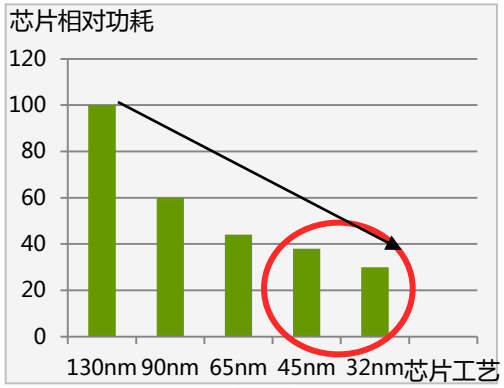
人工能耗管控

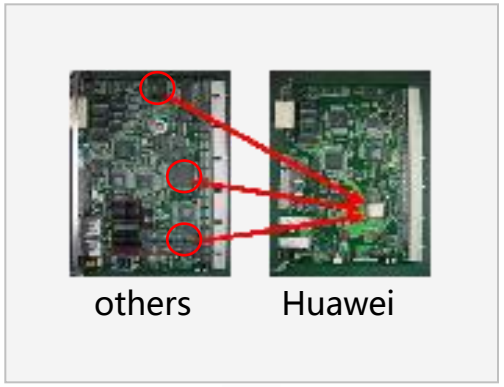
- 灵活分组管理
- 按需、定时控制
- 减少无效耗能

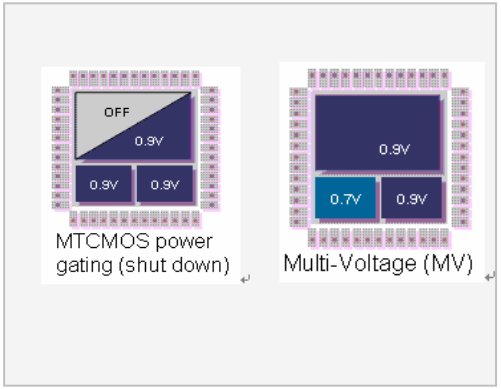
设备节能关键技术


• 自主知识产权
• 高集成度
• “流控”功能
• 静音风扇
• 风扇分区调速
• 风道散热设计
低耗ASIC芯片
风扇与散热设计
电源节能设计
能效监控及休眠
• 颗粒化电源模块
• 高电源转换效率
• 智能电源管理
• 集中监控平面
• EEE能效以太网
• 端口休眠
• 整机休眠技术

低耗ASIC芯片







- 自主研发的ASIC芯片
- 体积小功耗低
- 芯片工艺业界领先

体积减小、低功耗特性

集成度提高，功耗降低达30%

集成度提高

- 芯片分区供电
- 无业务功能关闭
- 按流量动态调整功率

“流控”功能设计

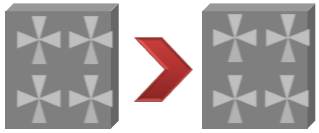
风扇与散热设计

风扇部件

无风扇

- 设备自然散热设计，“零”能耗散热
- 适用于设备功耗较小的盒式设备

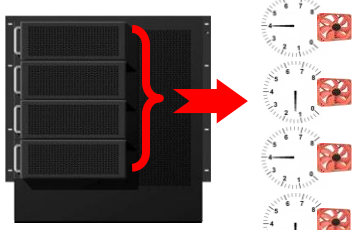
OR



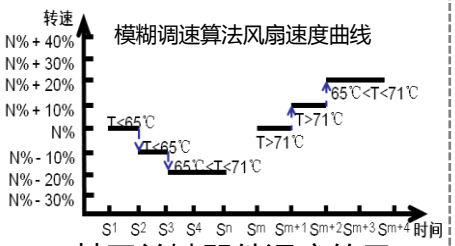
静音调速风扇

- 风扇频率可变
- 降低中心转轴摩擦系数，达到静音效果

风扇分区调速



- 根据环境温度、单板配置自动分区
- 每个分区可以独立调速与控制



- 基于关键器件温度的风扇调速策略
- 依据线卡负载和位置灵活调速

风扇设计

风道设计

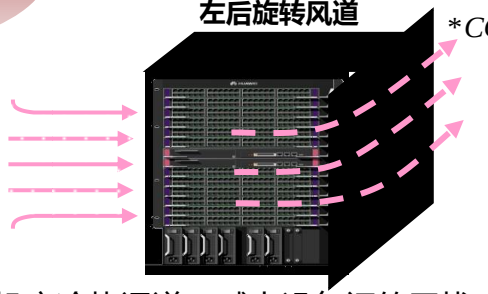
旋转风道设计

传统的左右风道

- 存在扰流现象（入口温升3～5℃）
- 受侧壁阻挡增加25%出风阻力，COP*值低 (大约10-20)
- 采用直径小转速高的低效率风扇，槽位散热能力有限，噪声大，可靠性低，无法支持单风扇失效
- 侧面几乎不能走线，一般只能120到150根双绞线

散热系统功耗占总功耗5%～10%

左后旋转风道



$$*COP = \frac{\text{整机功耗}}{\text{散热功耗}}$$

- 优化机房冷热通道，减少设备间的干扰
- 减少系统回流，提高散热效率，COP 高(大于 33)
- 可以选用直径大转速低的高效率风扇，而且风扇数量减少30%以上，噪音降低 5~10dB，支持单风扇失效
- 优化走线空间，支持1,200根双绞线出线

散热系统功耗占总功耗3%以下

本页适用于数据中心主推12800；

风扇与散热设计

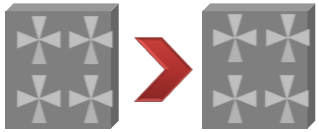
风扇设计

风扇部件

无风扇

- 设备自然散热设计，“零”能耗散热
- 适用于设备功耗较小的盒式设备

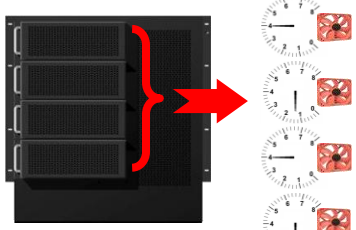
OR



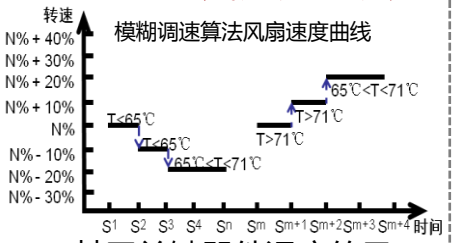
静音调速风扇

- 风扇频率可变
- 降低中心转轴摩擦系数，达到静音效果

风扇分区调速



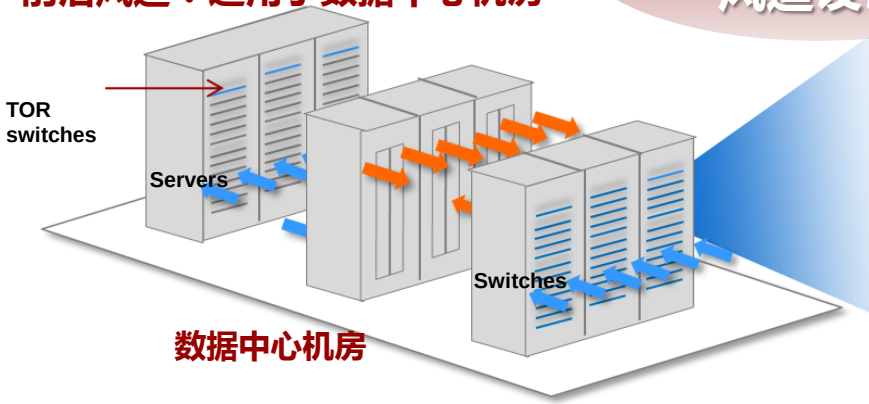
- 根据环境温度、单板配置自动分区
- 每个分区可以独立调速与控制



- 基于关键器件温度的风扇调速策略
- 依据线卡负载和位置灵活调速

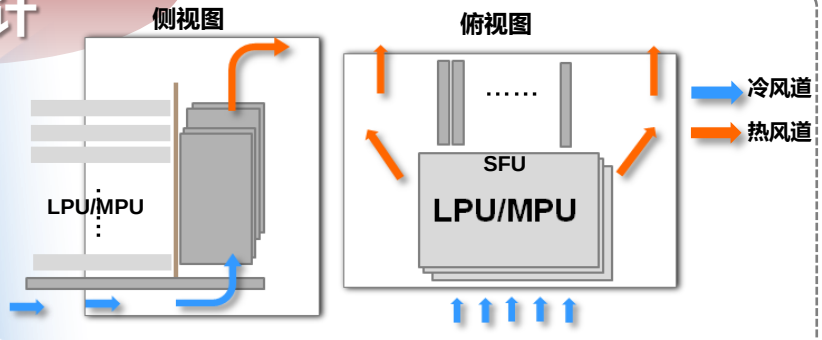
风道设计

前后风道：适用于数据中心机房



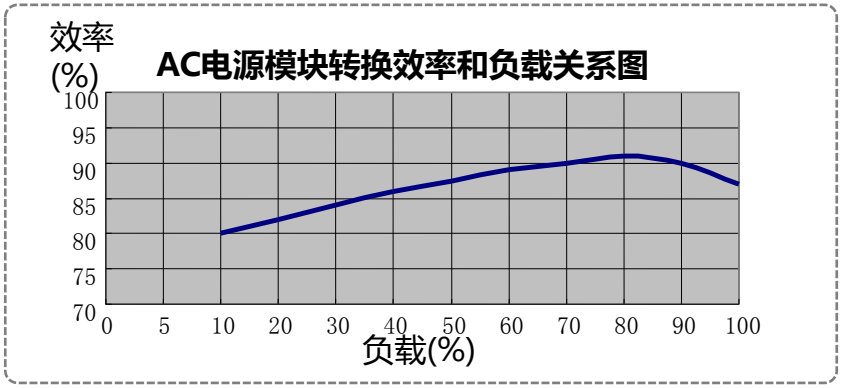
- 严格的冷热风道隔离，迎合数据中心机房风道设计，有效的降低散热功耗

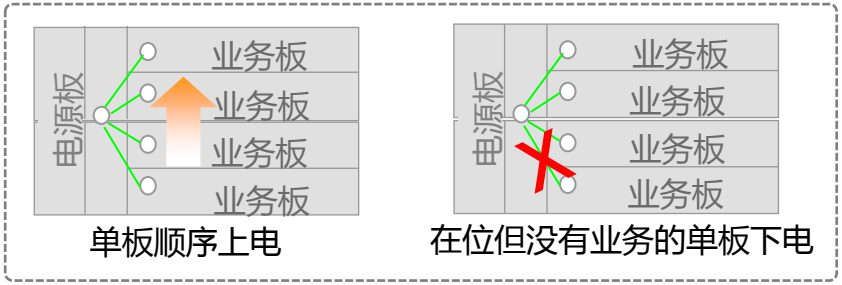
CloudEngine12800风道设计



- 风道无迂回，达到最高散热效率
- 单板无风道叠加，分区散热

电源节能设计





颗粒化电源提高电源转换效率

电源转换损耗约占通信设备30%的能耗;电源的转换效率和负载有直接关系

- 小功率颗粒化电源模块设计，搭配出400W-800W-1200W-1600W-2400W等功率等级的电源系统，提高电源转换效率5~10%
- 支持N+1、N+N的电源模块配置，提高系统的可靠性和电源的利用率

PoE供电

- 功率灵活选择：支持250W、500W、800W和2200W多种POE电源
- 智能冗余：支持1+1、2+2、3+1、4+0多种模式冗余
- PoE供电：支持802.3af（ 44～57V DC， 13W）和802.3at（ 50～57V DC，30W）标准，单端口供电能力高达30W，满足大功率供电需求（如无线AP支持802.11ac）

智能电源管理

- 监测：自测发热量、工作时间和负载响应情况
- 控制：单板顺序上电(降低单板同时上电带来的电源冲击，提高设备寿命，降低电磁辐射)；控制单板下电，隔离故障/空闲单板

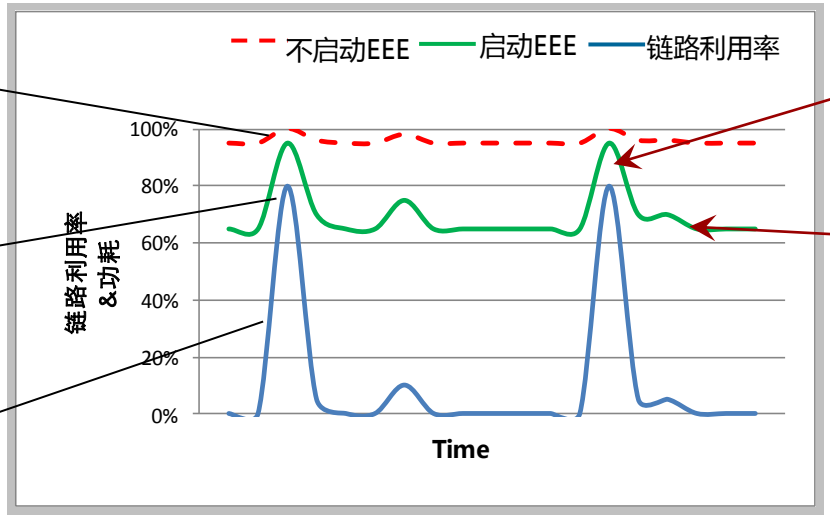
能效以太网技术

能效以太网，英文名称：Energy Efficient Ethernet (EEE) ，是美国电气和电子工程师协会2010年通过的IEEE802.3az标准，这个标准给全部以太网BASE-T收发器(100M、1G和10G)和背板物理层增加低耗电闲置(LPI)模式。

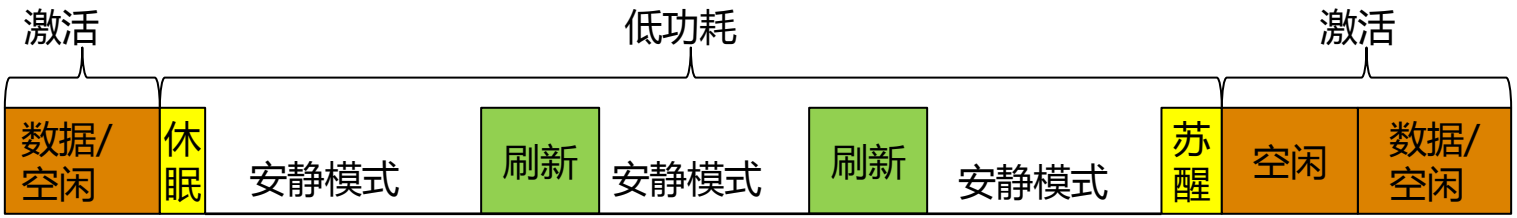
传统的以太网技术，功耗始终保持在高点（即使链路流量较低时）

能效以太网技术提供了一个低功耗状态（链路流量较低时）以达到节能目的

典型的以太网链路利用率曲线（在两个突发流量峰值点间会存在一段链路流量较低的状态）



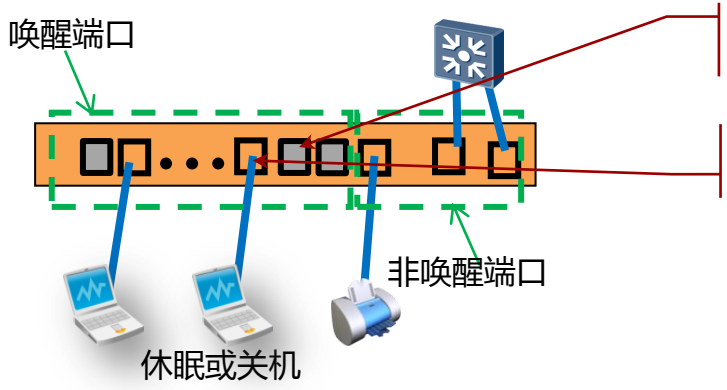
- 链路流量高，端口为全速运行模式，功耗高
- 链路流量较低时，端口为低功率闲置模式
- 端口状态根据流量快速倒换



华为交换机支持IEEE802.3az标准，端口能耗降低30%

休眠功能设计

整机休眠技术专利：
休眠与智能唤醒专利
(PCT/CN2011/083763)



空闲端口直接进入端口休眠

↓

端口无流量进入端口休眠

↓

所有唤醒端口无流量，进入整机休眠状态

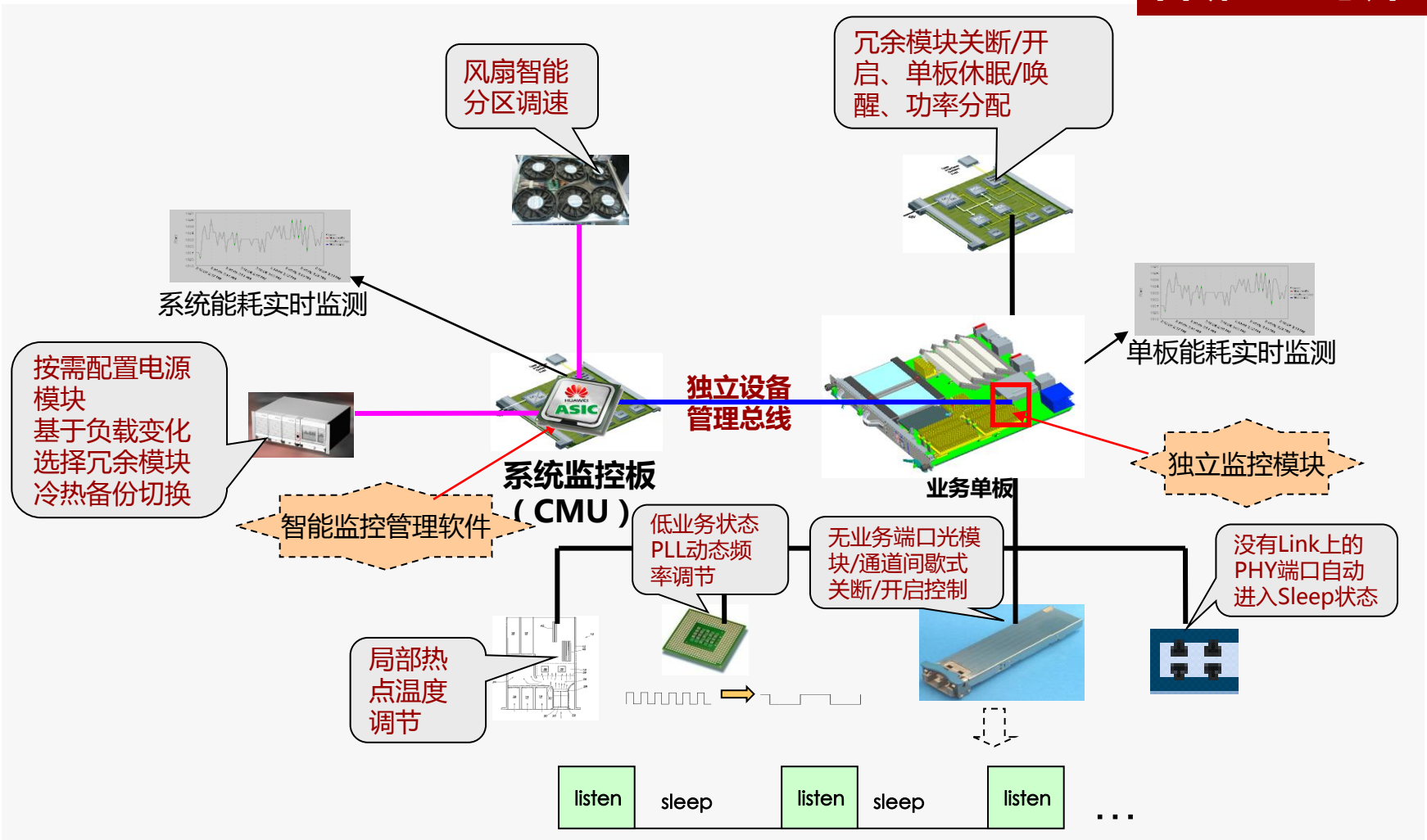
- 精细化节能，端口&芯片双重休眠
- 相比业界同等产品，单设备能够多节省 **69%**的电力

精细化休眠模式设计

标准节能模式	出厂模式，设备运行过程默认启用的节能技术，对运维、场景无特殊要求，适合在网络核心、业务繁忙场景启用；
基本节能模式	对相关未用器件启用关断、休眠操作，主要影响未配置业务、用户的，或用户不在线情况下的启动速度；
深度节能模式	对相关未用器件启用关断、休眠操作，对正常业务启动动态能耗调节，根据业务情况自动调整，在接入或某些场景下对性能、反应时间允许范围内的场景下使用；
整机休眠模式	指设备的最低功耗工作状态，设备除CPU工作外其外涉芯片都进入到节能模式；设备不提供业务能力，但可以定时唤醒和用户有输入唤醒命令方式唤醒快速响应后进入到正常支持业务模式。

本页适用于华为框式交换机节能技术CMU板使用华为自研ASIC芯片

CMU集中监控板设计

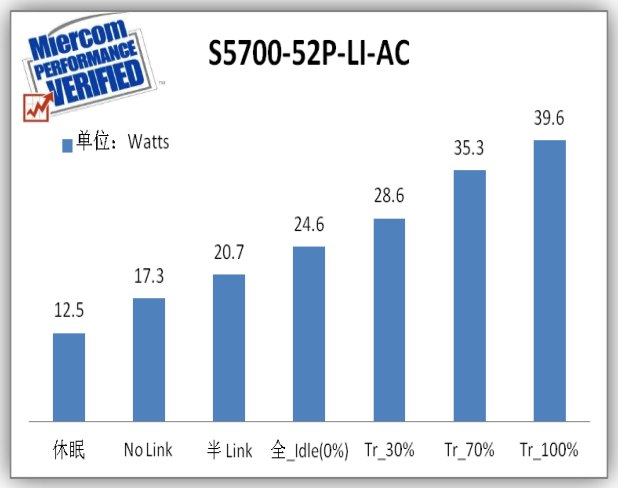


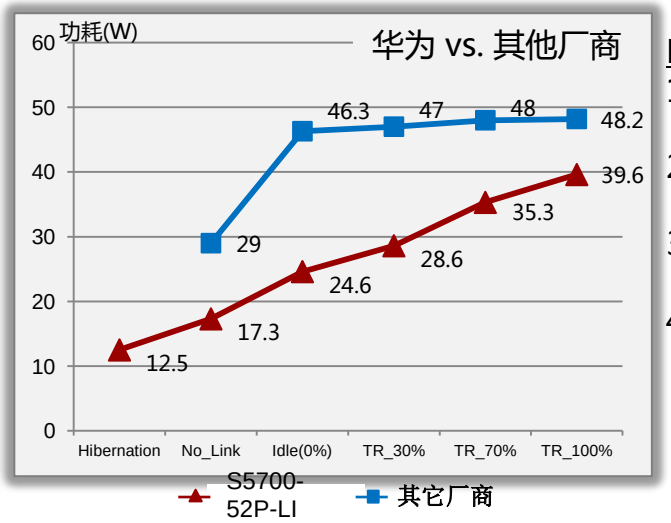
*CMU (Centralize Monitor Unit，集中监控平面)

Page 163

仅5700-LI支持

节能案例





Miercom第三方认识结果：

1. S5700-LI满负荷功耗比业界节能18%
2. 无流量时较其他厂商设备节能47%
3. 典型流量时较其他厂商设备节能39%
4. 休眠情况下，功耗又降低到12.5W, 较业界节能50%以上

客户案例：

工作时段	小时数	华为节能交换机		业界普通交换机	
空闲时段	108小时/周	休眠12.6W/时	一周耗电量：3076W	29W/时	一周耗电量：5952W
工作时段（30%流量）	60小时*/周	典型工作 28.6W/时		47W/时	

*按照一般的上班时间和设置一定的余量，上班时间为早7点-晚7点，其他时间和周末时间为休眠时间

经权威机构验证，华为交换机设备，相比业界同等产品，单设备能够多节省69%的电力

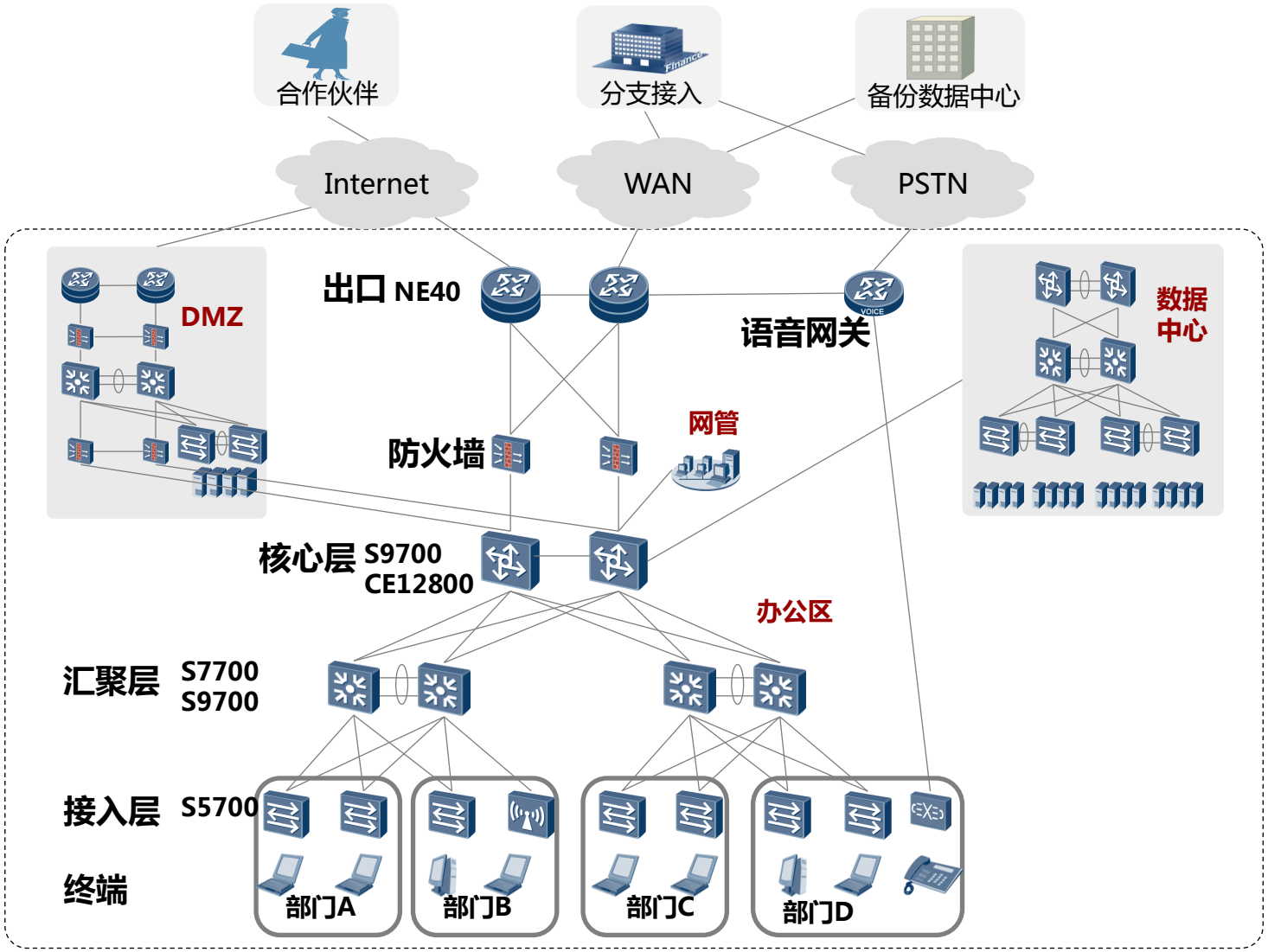
设备节能技术总结

节能技术		使用场景	节能价值
低耗ASIC芯片	自主研发	框式交换机S97、S93、S77，CMU集中监控板中控芯片	配合智能设备管理系统充分利用芯片的低功耗特性，在提升系统性能的同时还大大降低了整机功耗
风扇与散热设计	无风扇	端口较少的盒式交换机S37、S27、S57（部分）	自然散热
	静音风扇	盒式交换机S67、S57(部分)	减小噪声污染
	智能调速分区风扇	框式交换机S97、S93、S77	1、相比传统的交换机（无论是否有单板，都会全速运转），大大的降低了系统的功耗，降低系统的噪声4-6db， 2、风扇本身同时降低功耗50%以上
	旋转风道	S93、S77、S97框式交换机，适用于普通机房	左后风道，适合于将机柜面朝面、背朝背放置，形成冷热通道，再加上简单的机房通道隔离方法即可大大改善冷热气流混合交叉的问题。分析和实验数据表明，大约能节省空调耗电15%以上
	前后风道	CloudEngine12800，适用于数据中心机房	1、严格的冷热风道隔离，迎合数据中心机房风道设计，有效的降低散热功耗 2、风道没有迂回，达到最高散热效率 3、单板无风道叠加，分区散热
电源节能设计	颗粒化电源	交换机电源模块、PoE电源模块	1、提高电源转换效率 2、初始的板卡配置需要扩充时，直接添加相应需求的电源模块，避免出现电源更换过程中的故障风险
能效监控及休眠	EEE	S97、S93、S77、S57	2010节能最新标准，端口能效提升30%
	CMU集中监控板	框式交换机S97、S93、S77	配合智能设备管理系统，实现按流量动态调整功率、风扇及电源管理
	整机休眠	接入交换机，仅S5700-LI支持	精细化节能，深度休眠，相比业界同等产品，单设备能够多节省69%的电力

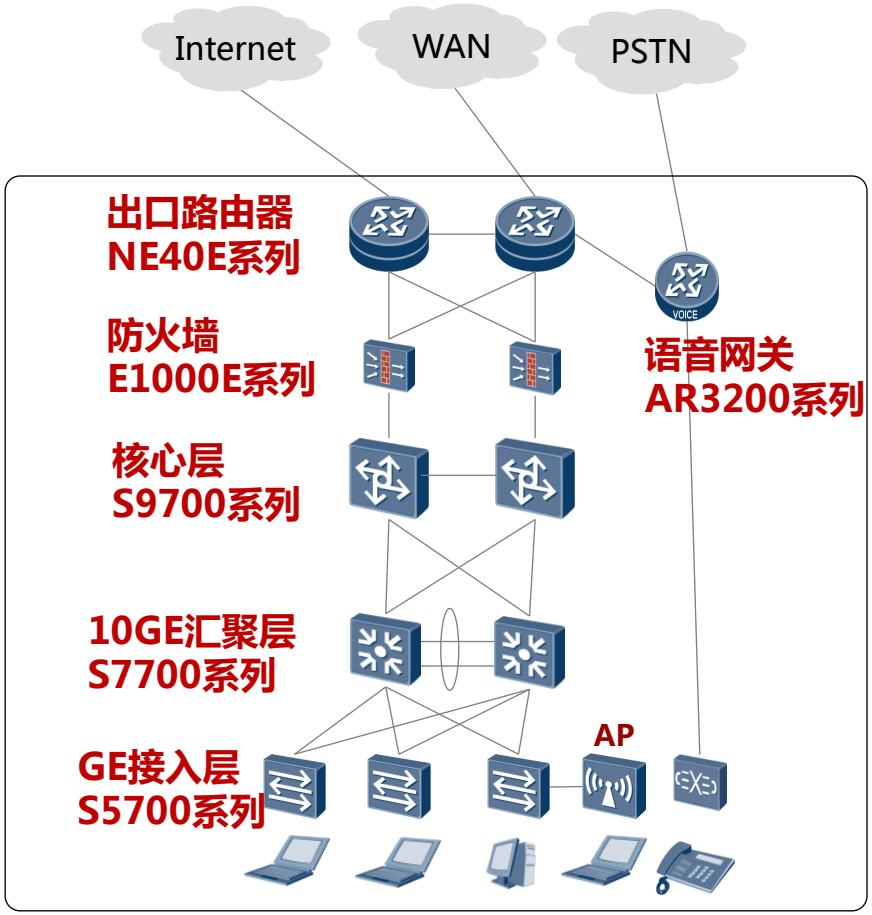
子目录

4 园区网业务解决方案

园区网全景图


合作伙伴
分支接入
备份数据中心
Internet
WAN
PSTN
DMZ
出口 NE40
语音网关
数据中心
网管
防火墙
核心层 S9700
CE12800
办公区
汇聚层 S7700
S9700
接入层 S5700
终端
部门A
部门B
部门C
部门D

大中型园区总图(大于800信息点)



接入层

S5700 iStack GE接入，主推24GE下行、10GE上行。POE实现AP接入。高配HI、中配EI、低配 SI/LI。

汇聚层

S7700 CSS集群，万兆汇聚，高配12口线速万兆单板，低配40口万兆单板。

核心层

S9700 CSS集群，集成AC功能。

出口

采用NE40系列。

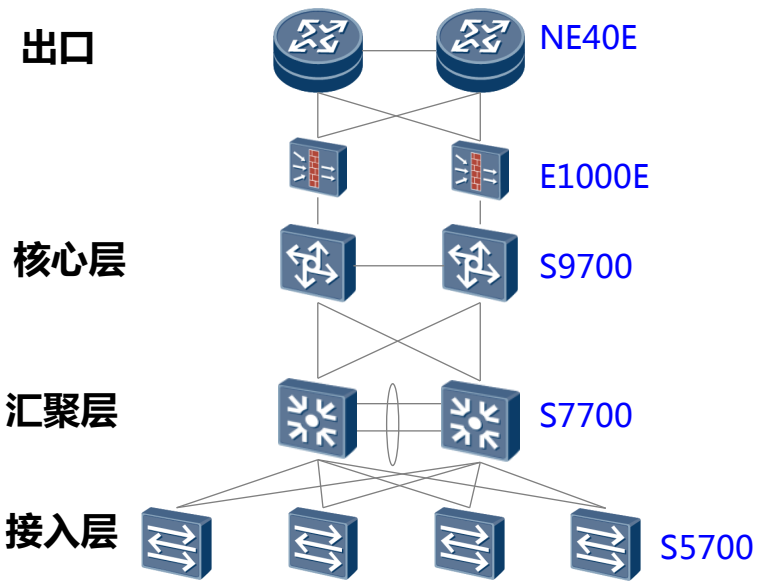
语音网关

推荐AR3260(大于10K用户）或AR2240（200-1000用户）

防火墙：

E1000E系列，采用口字型或旁挂接入。

大中型园区规模计算（高配1200信息点为例）



园区规模	1200信息点
核心交换机	S9700: 2台，每台2*16*10GE
汇聚交换机	S7706 :4 台，每台4*12*10GE 收敛比：1:2
接入交换机	S5700：50 台，每台 24GE+2*10GE 收敛比：1:1.2

范围：大于880信息节点

接入层：

1200信息点，采用S5700配置24 * 1GE（下行）+ 2*10GE(上行)，2台为一组。1200/（24*2）= 25组，共需要50台S5700设备。收敛比为：1：1.2

汇聚层：

50台S5700共需100个10GE端口双归上行，按收敛比1：2计算，需150/(12*10GE) = 13 个12*10GE单板。

则配置4台4*12*10GE S7706设备。

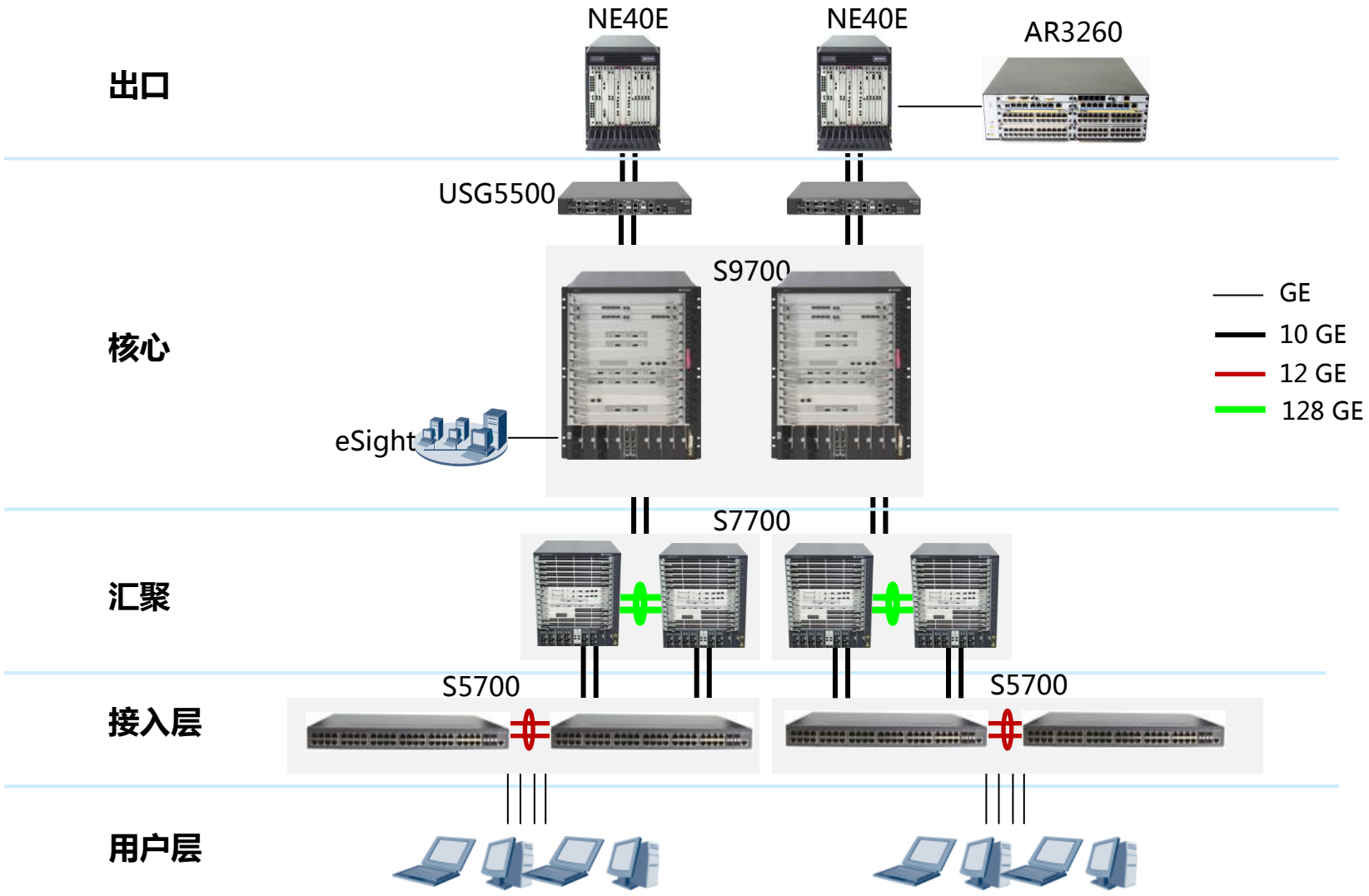
核心层：

4台S7706设备共需50个10GE端口上连核心层。需要S9700配置2*16*10GE线卡2台一组，另外2*10G接入出口防火墙。出口带宽为20GE。

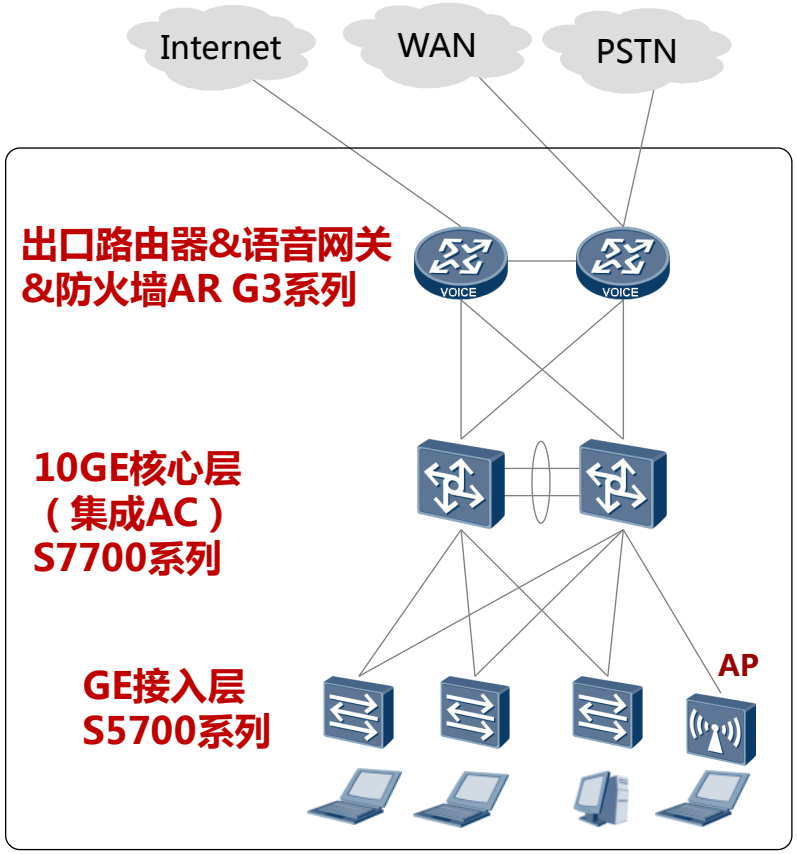
出口：

2台NE40设备，4*10GE下行连入防火墙

大中型网络组件产品全景图



小型园区总图（小于800信息点）



接入层

S5700 iStack GE接入,主推24*GE下行、2*10GE上行配置。高配HI/EI、中配 EI、低配 SI/LI。

POE交换机实现AP接入。

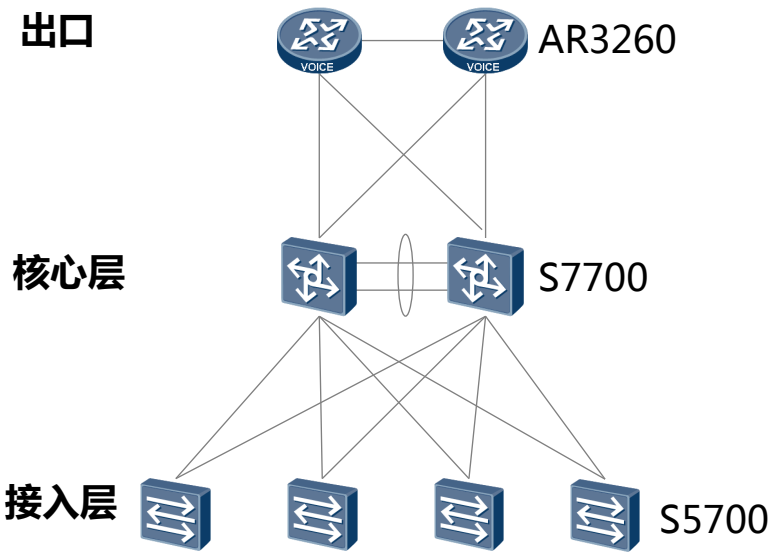
核心层

S7700 CSS部署，集成AC功能，上行GE接入出口。高配限速12口10GE万兆单板，低配高密40口10GE万兆接入。

出口

AR3260并集成防火墙和语音网关。

小型园区规模计算（ 400信息点为例）



园区规模	400信息点
出口路由器	AR3260: 2台
核心交换机	S7706 :2 台 每台2*12*10GE 每台1*24GE
接入交换机	S5700：18 台 每台24GE+2*10GE 收敛比：1:2.4

范围

小于880信息节点

接入层

400信息点；采用S5700配置1*24GE（下行） + 2*10GE(上行)，2台为一组。

400/（24*2）= 9组，共需要18台S5700设备。收敛比为：1：1.2

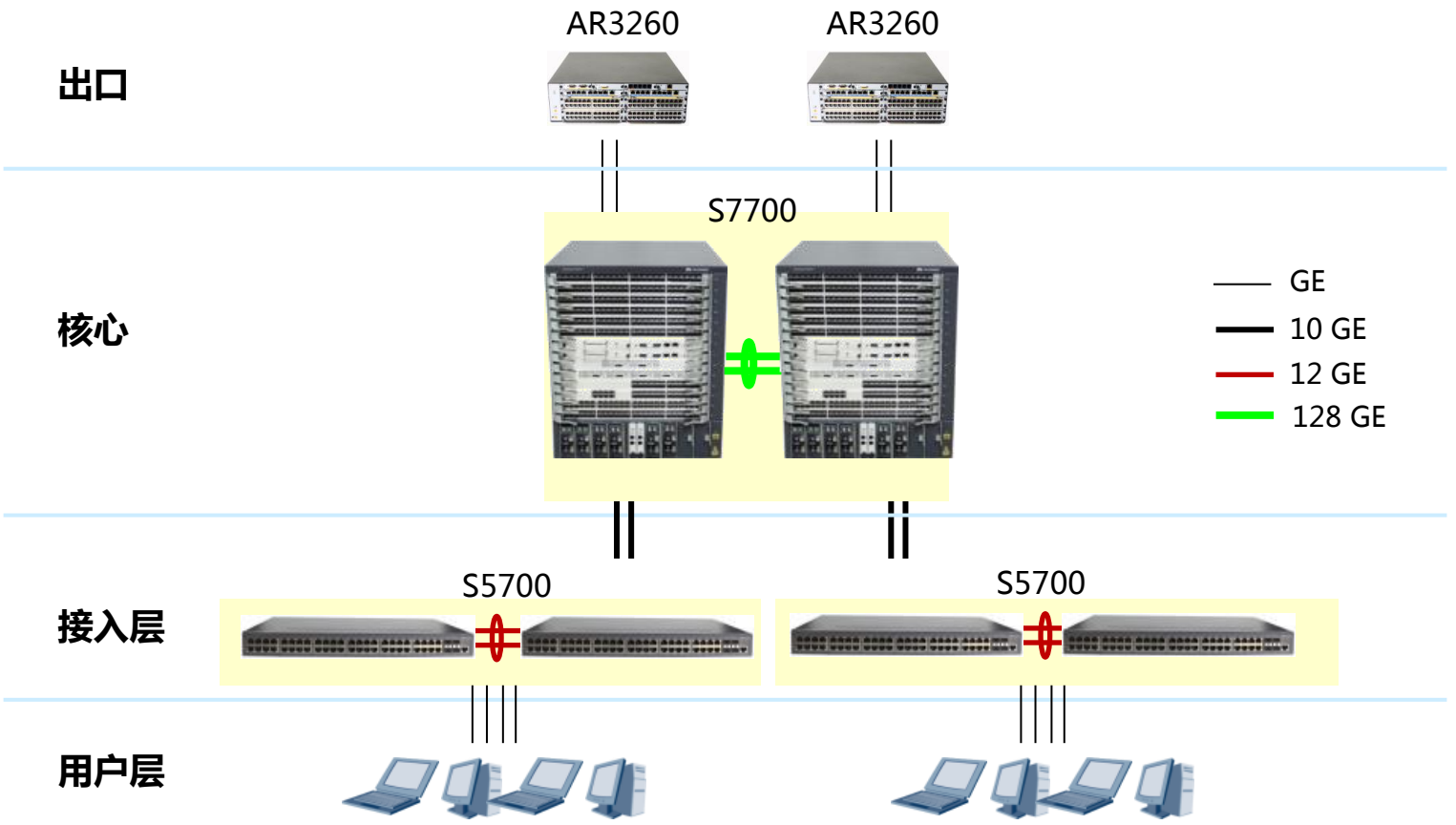
核心层

18台S5700需要36个10GE端口双归上行连接核心层，采用S7706配置2*12*10GE和1*24GE，36/（2*12）= 2台，2台一组，共48接口，其中36万兆接口下行接入层，4个GE接口上行出口路由器。

出口

2台AR3260设备，2*GE下行连入核心层，出口带宽4GE。

小型网络组件产品全景图

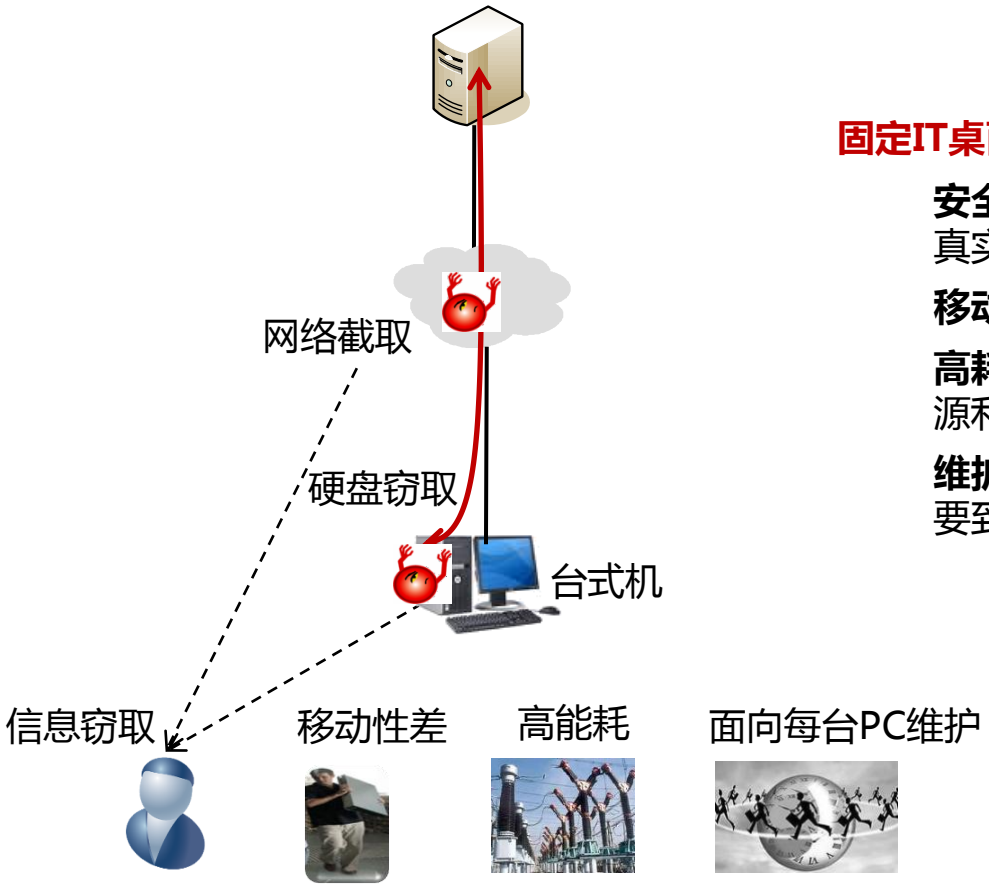


子目录

4 园区网业务解决方案

目录

固定IT桌面—高耗能、维护成本高、移动安全性差



固定IT桌面不足

安全性差：保存本地易泄露和毁坏，真实数据网络传输易被窃取。

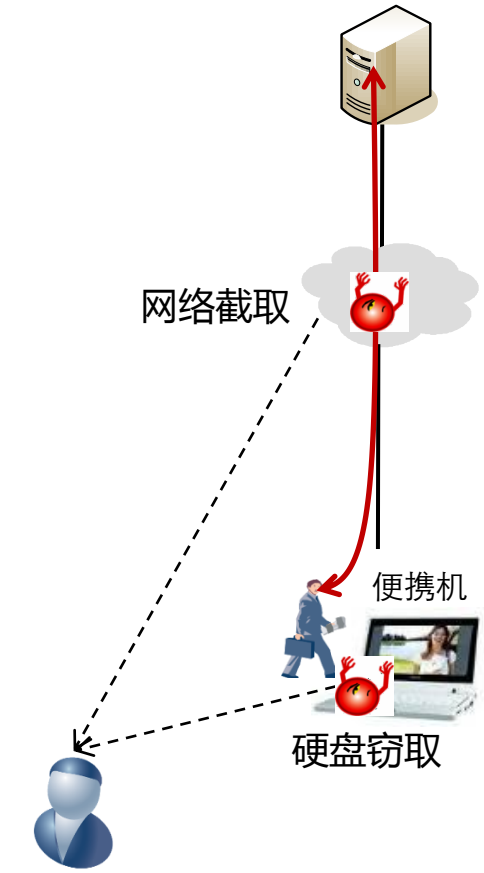
移动性差：用户难以随地访问桌面

高耗能：一台桌面配备一台PC，资源利用不充分和高能耗、高排放。

维护成本高：每次软硬件故障或升级要到特定用户，人力维护成本高。

Page 176

手提便携—存储数据易丢失、信息易被截断



每台设备维护

手提改进：

移动性：主机和显示终端合为一体，容易携带，随地接入进行办公，包括远程出差等。

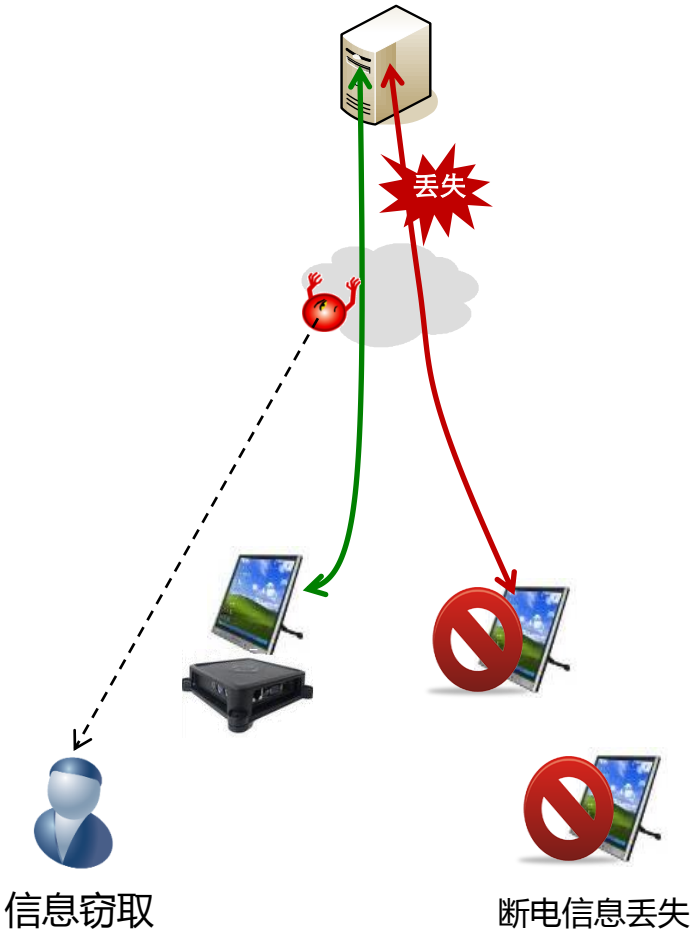
仍有不足：

安全性差：保存本地易泄露和毁坏，真实数据网络传输易被窃取。

维护成本高：每次软硬件故障或升级要到特定用户，人力维护成本高

Page 177

无盘工作站—断电数据丢失、信息易被截断



无盘工作站改进：

安全性：集中存储数据，数据不易毁坏丢失或被窃取。

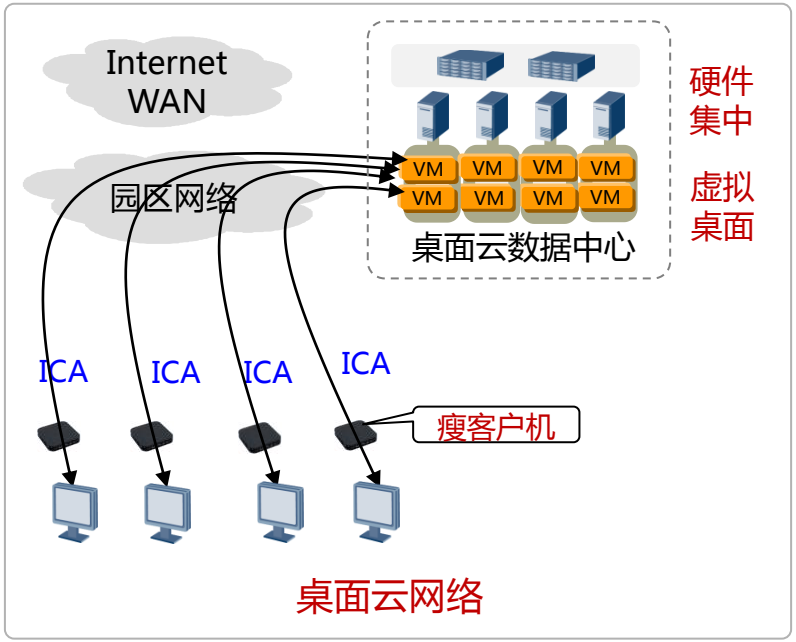
仍有不足：

安全性：真实数据仍然通过网络传输，易被窃取

断电：终端断电之后，当前工作界面数据丢失。

Page 178

桌面云—安全、移动和高效



桌面云优势

安全：远程托管，数据隔离；

集中管理存储，不易丢失，

网络不传输真实数据，不易窃取，

构建多层次安全体系，分布式控制。

灵活：只要有网络的地方，就可以随时随地的访问桌面。

高效：操作系统与硬件解耦，简化终端设备；

构建共享资源池，统一管理；

集中部署，灾难恢复快。

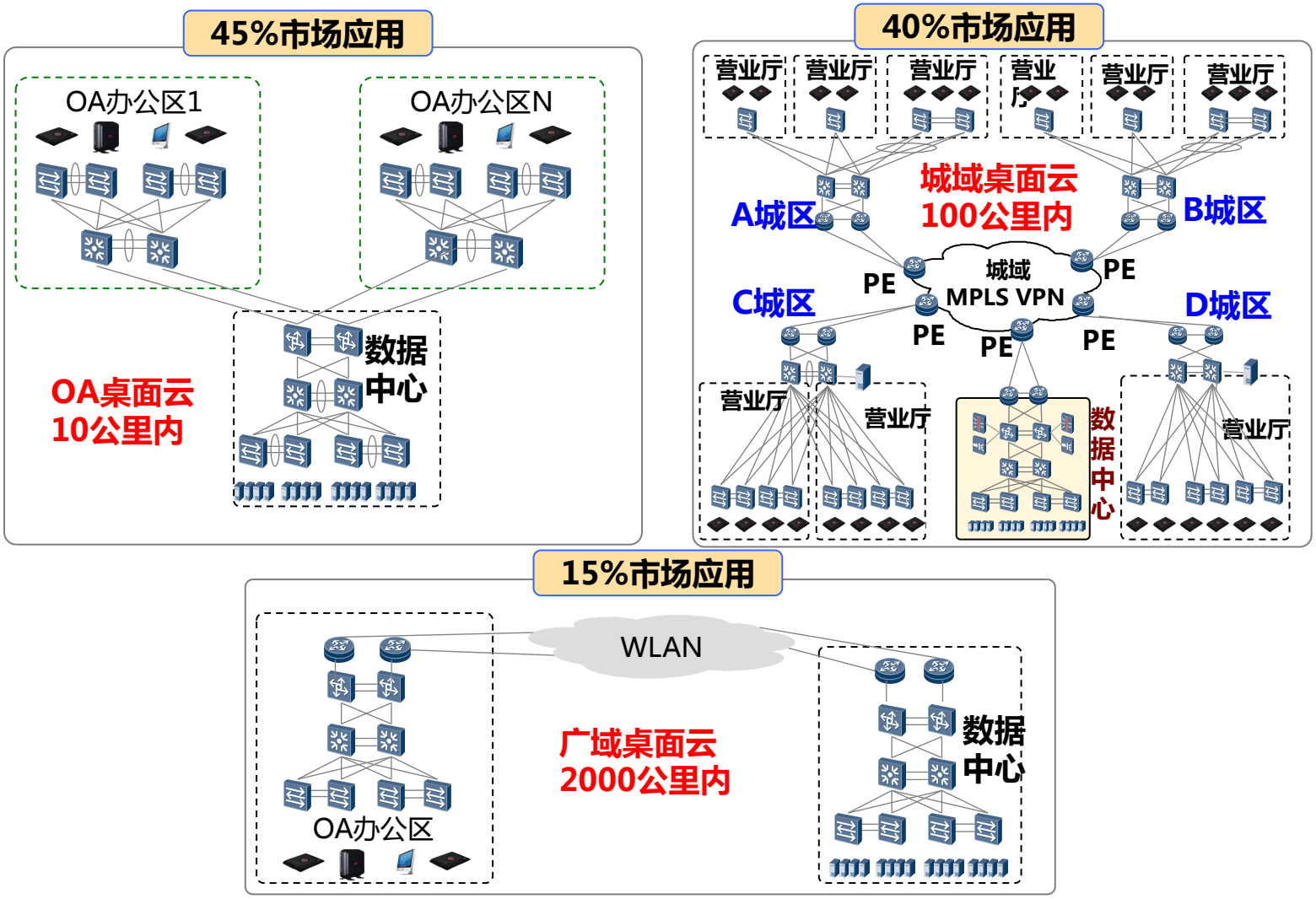
终端设备大为简化：仅需要瘦客户机、键盘、鼠标、显示器;

桌面显示数据的传输由显示器连接线变更为园区承载网络;

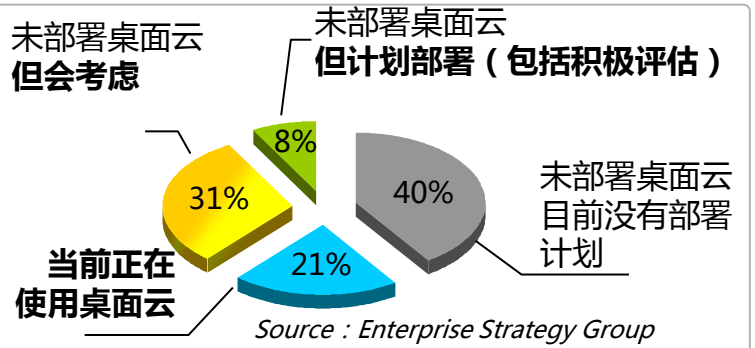
用户界面使用远程协议（例如ICA）传输到用户的终端设备上。

注：ICA： Independent Computing Architecture，终端与虚拟机之间的传输协议。

桌面云三大应用场景


45%市场应用
OA办公区1
OA办公区N
数据中心
OA桌面云
10公里内
40%市场应用
营业厅
城域桌面云
100公里内
A城区
B城区
C城区
D城区
PE
城域
MPLS VPN
数据中心
15%市场应用
WLAN
OA办公区
广域桌面云
2000公里内
数据中心

云计算时代，桌面云已是大势所趋



Source：Enterprise Strategy Group

52%大型企业和48%中型企业

计划采用桌面云服务

Acronis®

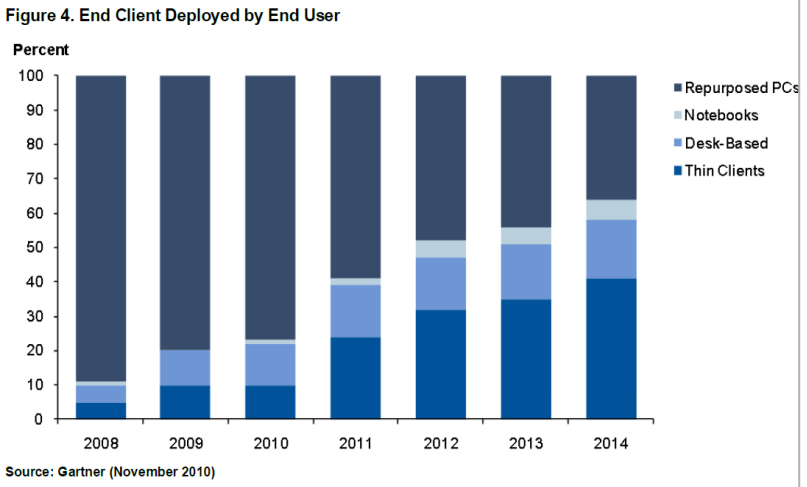
45000人体验全球最大桌面云

从2009年开始，华为开始在上海研究所部署桌面云。到目前为止，华为在全球各大研究所及海外分支机构部署45000用户规模的桌面云。

2012年中小企业将更多采用虚拟化应用

根据一份近期由 Acronis 进行的调查指出，在2012年，全球中小企业将比大型企业更快速地采用服务器虚拟化应用。但此调查也指出中小企业……

源于：http://cloud.chinabyte.com/nl/20120223/



Gartner认为绝大多数VDI用户是从台式机用户迁移过来的。基于这个认识，Gartner预测在2014年VDI将达**7千万**用户。

传统桌面架构正在向桌面云架构迁移

Page 181

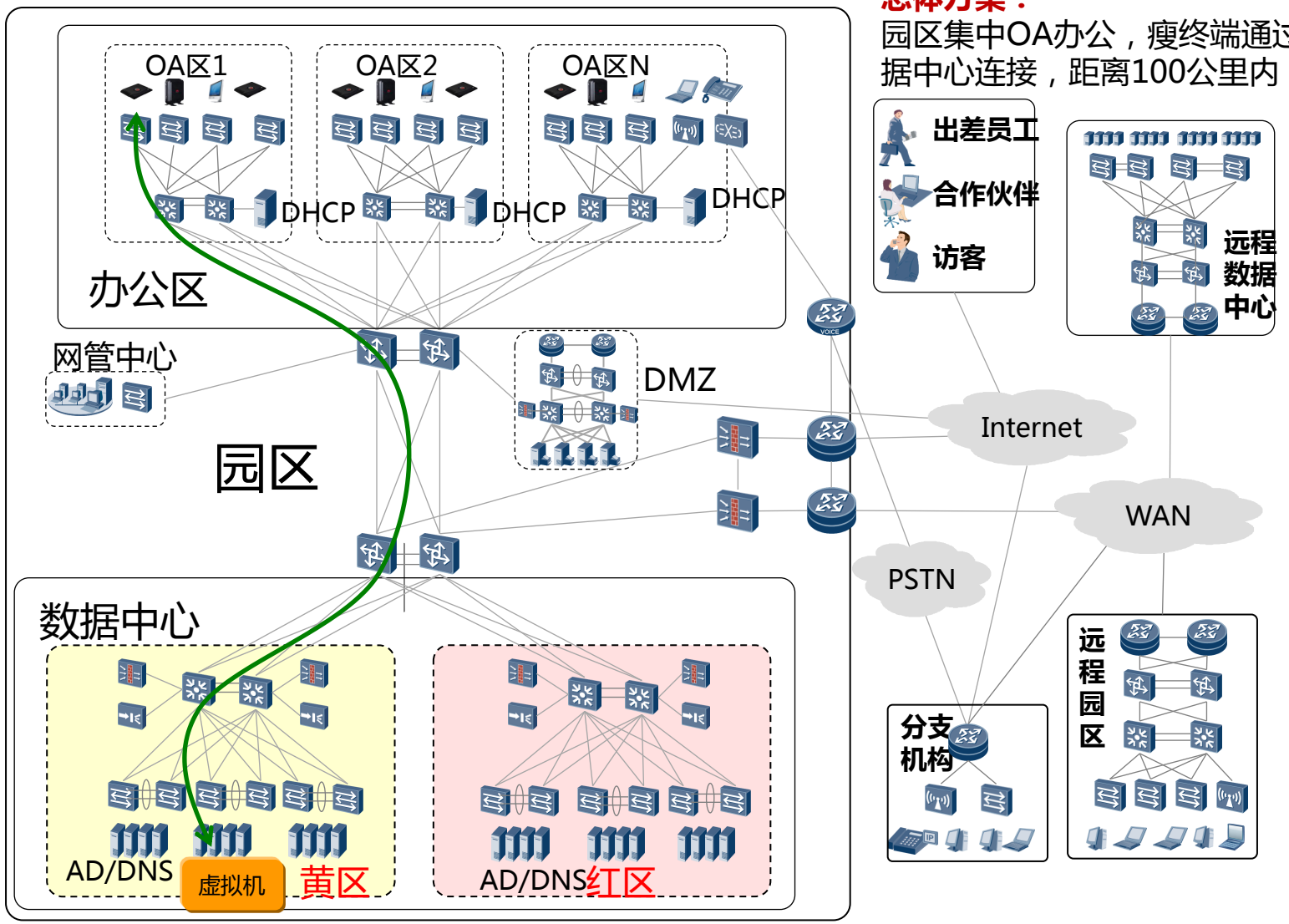
OA集中办公桌面云方案

- 总体组网
- 常见办公应用场景
- 办公区组网设计
  - 办公区接入层设计
  - 办公区三层路由设计
  - 网络规模设计和产品选型
- 数据中心网络设计
  - 三层网络平面设计
  - 云流量分布和模型分析
  - 网络规模设计和产品选型
- 网络带宽和质量设计
  - 网络带宽设计
  - 网络质量设计—时延、抖动、丢包率
  - 网络质量监控设计
- QoS和可靠性设计
  - QoS部署设计
  - 可靠性设计
- 网络安全、终端接入和运维管理设计
  - 网络安全设计
  - 终端接入设计
  - 运维管理设计
- 成功案例

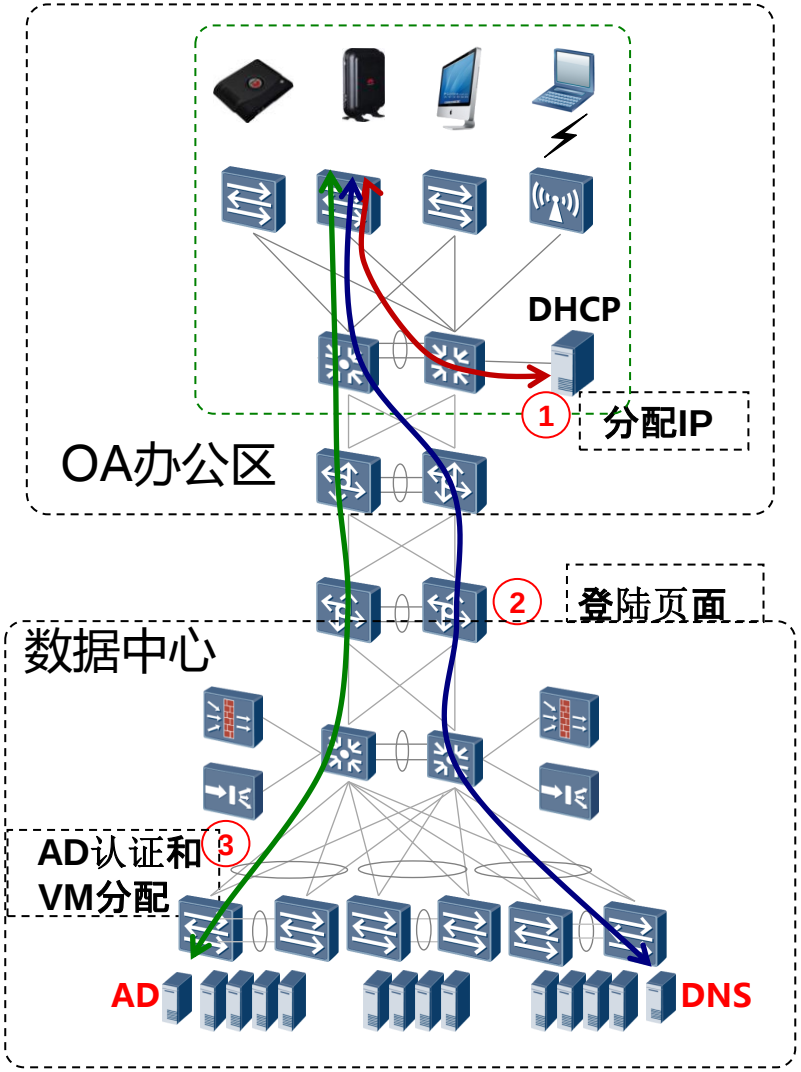
OA集中办公总体方案

总体方案：

园区集中OA办公，瘦终端通过园区网络和数据中心连接，距离100公里内



办公应用场景—终端接入



终端接入过程

1、终端从DHCP服务器获取IP地址。

2、访问DNS服务器解析获得域名IP，并打开登陆页面。

3、输入用户名/密码，AD服务器认证。

4、AD认证通过，云管理服务器分配VM，并将VM服务器IP发给终端，建立ICA通道。

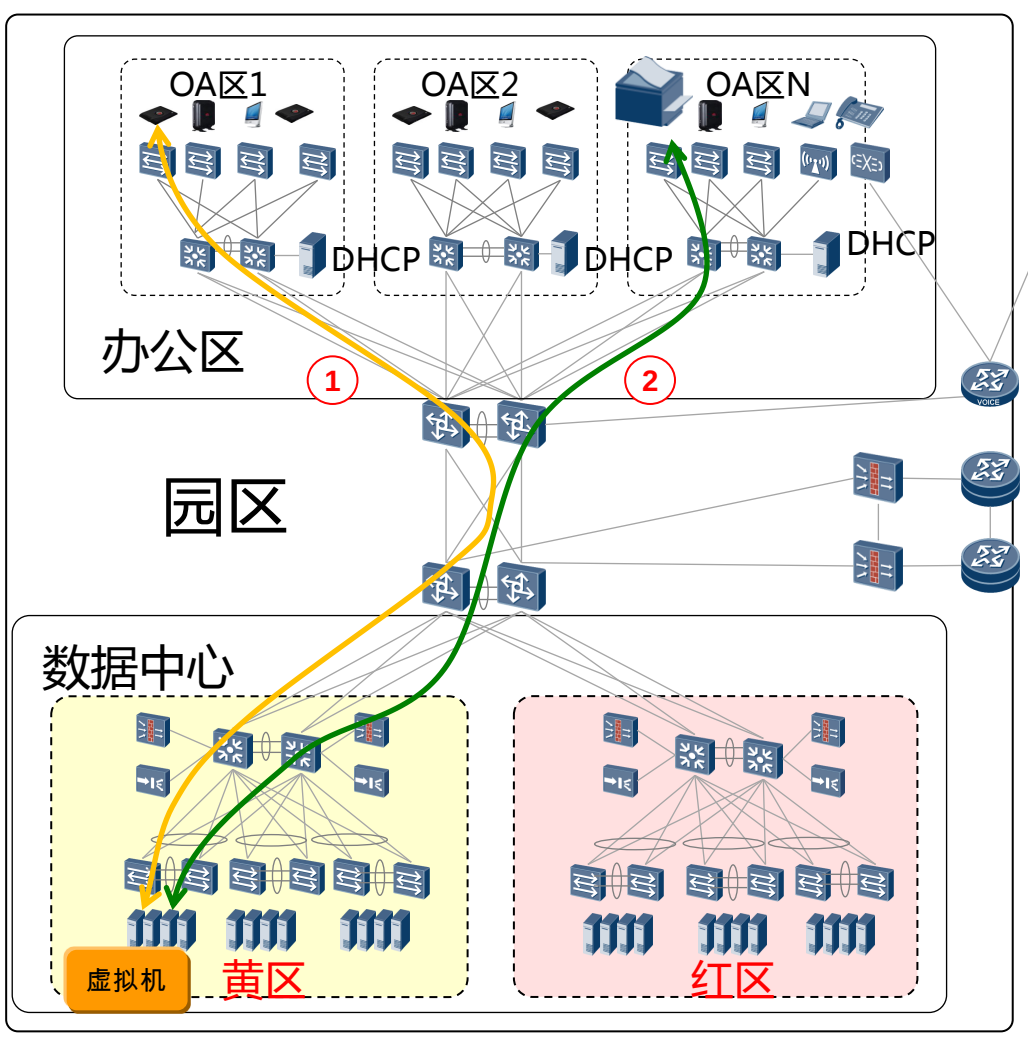
服务器位置：

DHCP：部署在汇聚三层网关

AD：部署在本地数据中心

DNS：部署在本地或总部数据中心

办公应用场景—桌面操作、打印



桌面操作业务流：

键盘、鼠标的操作信息传递给虚拟机；

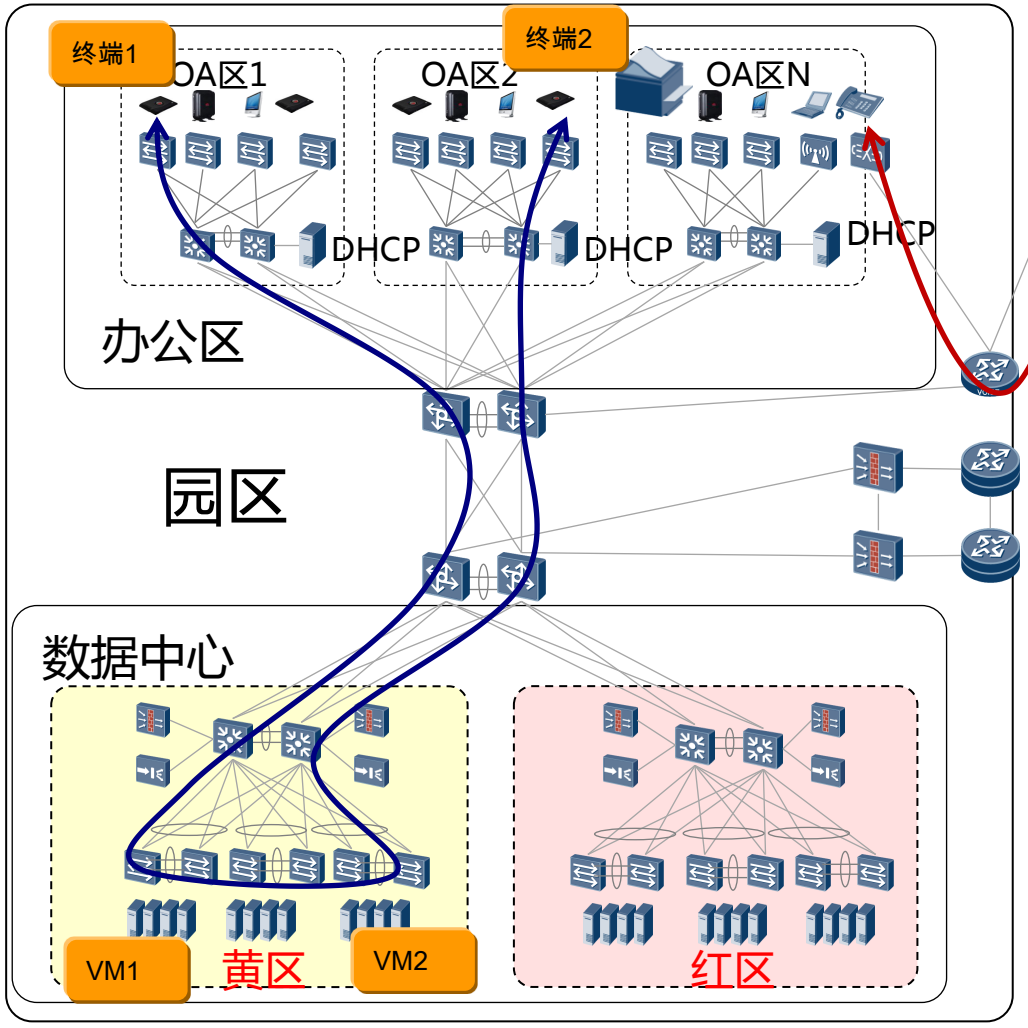
虚拟机向终端发送ICA消息，终端显示操作结果。

打印业务流：

键盘、鼠标的操作信息传递给虚拟机；

虚拟机VM向办公区打印机传输打印数据。

办公应用场景—电话、VOIP



电话业务

VOIP业务

电话业务：

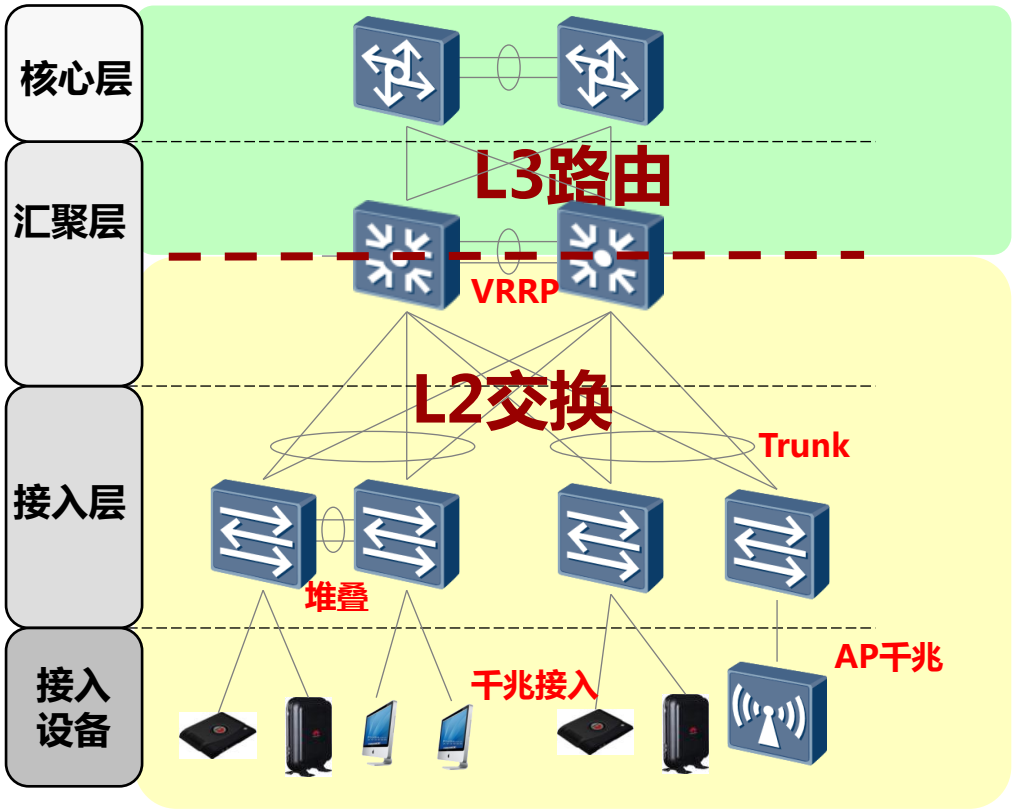
通过PSTN互连园区和分支办公。

VOIP业务（终端1到终端2场景）

终端1话筒输入语音信息，到达虚拟机VM1；

在数据中心内部，VM1传输语音信息给VM2，最后VM2把语音传输给终端2。

办公区—接入层设计



应用场景:

办公区二层网络，承载键盘鼠标操作信息和虚拟桌面显示的ICA消息。

组网部署:

S5700千兆接入，

无线AP接入S5700千兆接口，

S5700堆叠实现二层交换，

采用Trunk链路带宽复用，

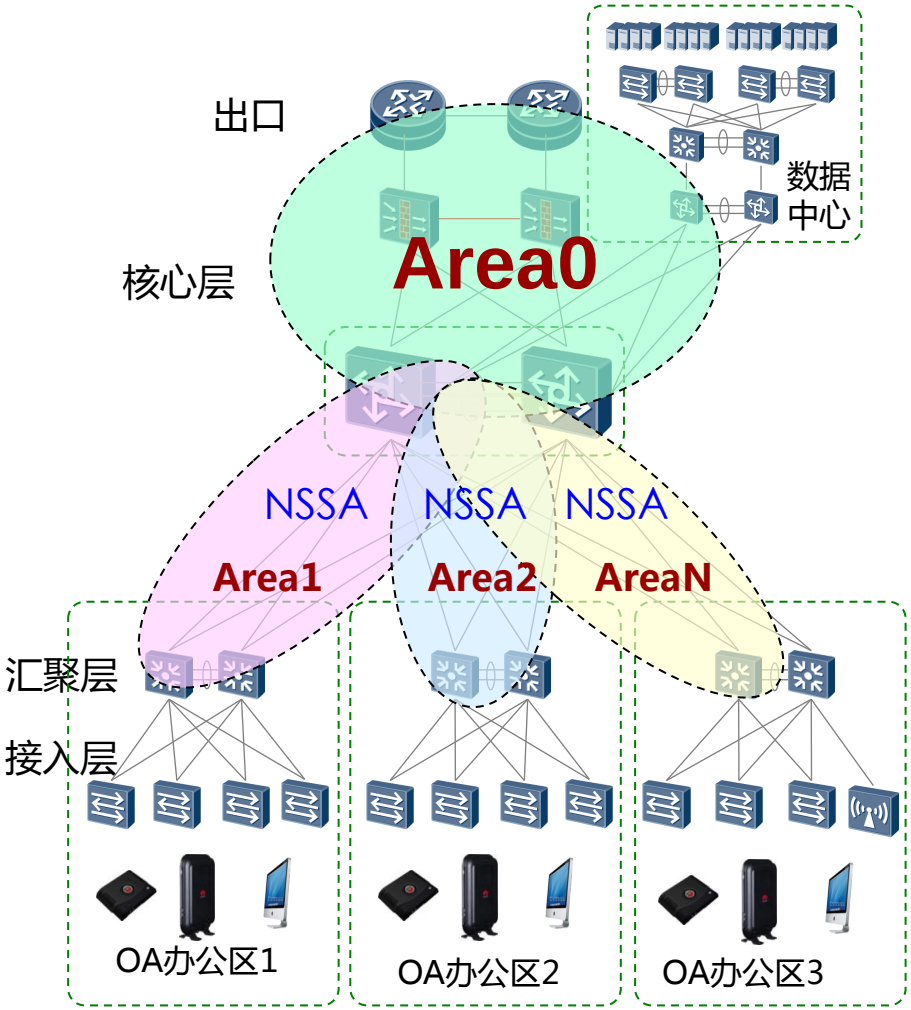
部门间不互访，无需VLAN隔离规划，

汇聚层设备不堆叠时，选用VRRP网关方案。

客户价值：

OA用户千兆带宽接入，保证足够业务带宽和体验。

办公区—三层路由设计



组网部署:

核心层和出口组成OSPF骨干Area0，汇聚和核心层组成（Area 1,2,N），分区Stub或NSSA限制路由容量，若分区数量少可全配置Area0，数据中心和园区接入OSPF骨干区。

可靠性：

汇聚和核心层交换机CSS集群，

采用ISSU无损升级技术，

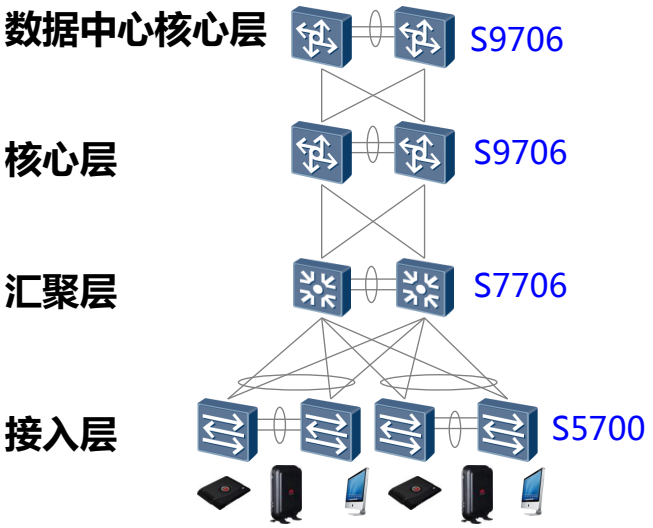
硬件BFD 10ms快速故障发现，

NSR/GR流无间断倒换，

相关产品：

汇聚层S7700，核心层S9700，出口NE40E。

办公区—网络规模设计



	5000桌面云用户
用户数量	5000,每用户需求20M
核心交换机	S9706 3*16*10GE：2台
汇聚交换机	S7706 6*12*10GE :4 台 收敛比：1:3.3
接入交换机	S5700：106 台 每台48GE+2*10GE 收敛比：1:2.4

接入层：

5000用户规模， 用户需要20M带宽，共需预留100GE带宽。

采用S5700配置48GE（下行） + 2*10GE(上行)，2台为一组。

5000/（48*2）= 53组，共需要106台S5700设备。收敛比为：1：2.4

汇聚层：

S5700 共212接口上行连入汇聚层，采用S7706配置6*12*10GE，

212/（6*12）= 3台，2组4台。

212接口连入接入层，64接口上行接入核心层。收敛比为：64:212 = 1：3.3。

核心层：

64个10GE汇聚层Trunk接口连入核心层，需要S9706配置3*16*10GE + 4*40GE 2台并为一组。

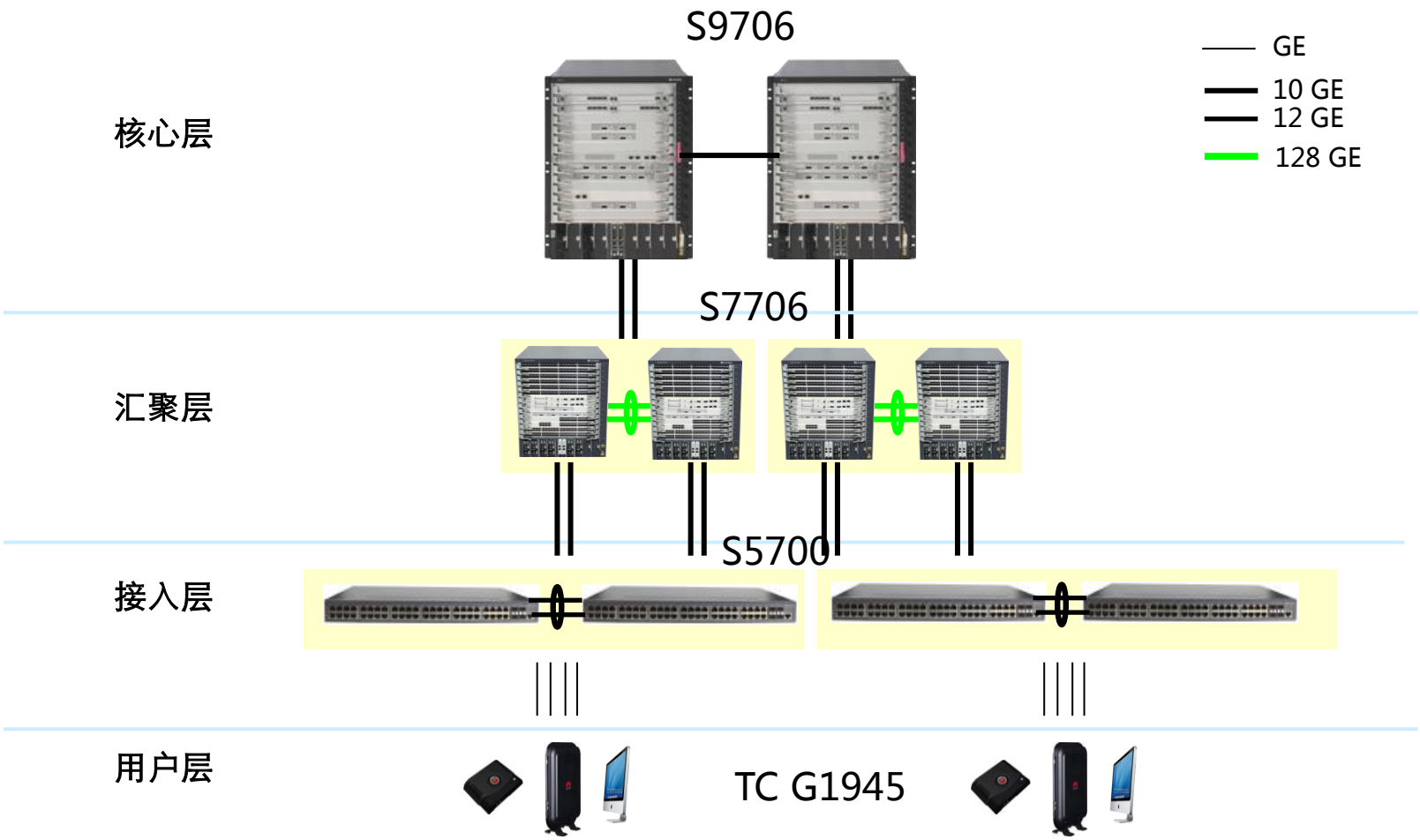
4个40GE接口连入数据中心核心层。

4个10GE接口连入园区出口

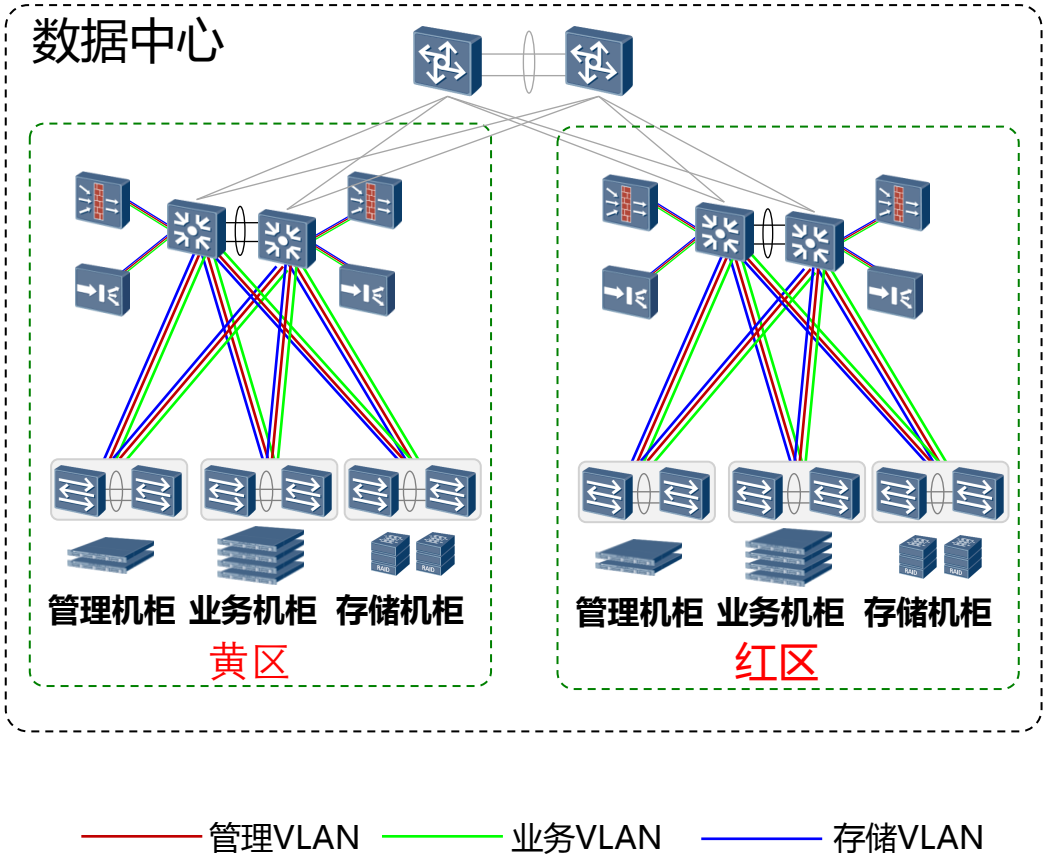
流量带宽：

接入、汇聚和核心层网络带宽预留均远远满足100GE。

办公区—产品选型5000用户



数据中心—管理、业务和存储三平面网络



应用场景：

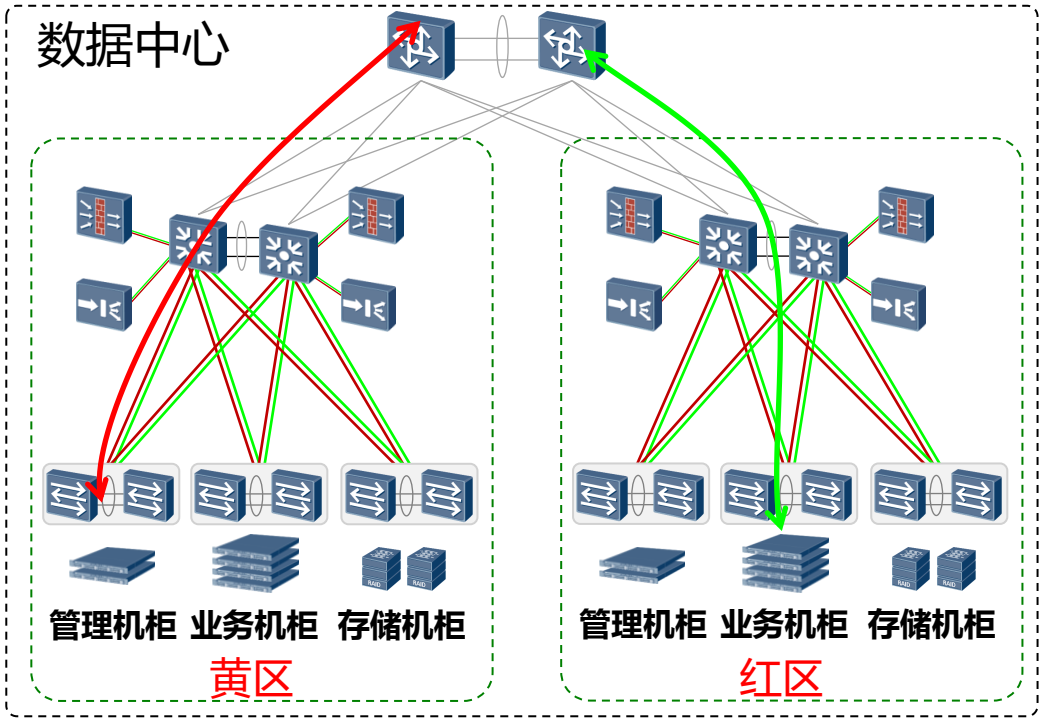
桌面云数据中心方案

组网部署：

物理机柜划分放置管理、业务和存储服务器，

虚拟VLAN划分隔离管理、业务和存储网络平面

数据中心—业务、管理网络平面



管理VLAN　业务VLAN　管理流　业务流

业务网络：用来承载用户侧TC到VM的流量。
管理网络：网管，用来承载管理系统内部的流量。
存储网络：用于承载管理服务器以及资源服务器之间的内部通讯流量。

管理、业务平面：

在整个园区网络传输，管理、业务平面与存储层面通过VLAN隔离，

防火墙过滤保证业务流安全，

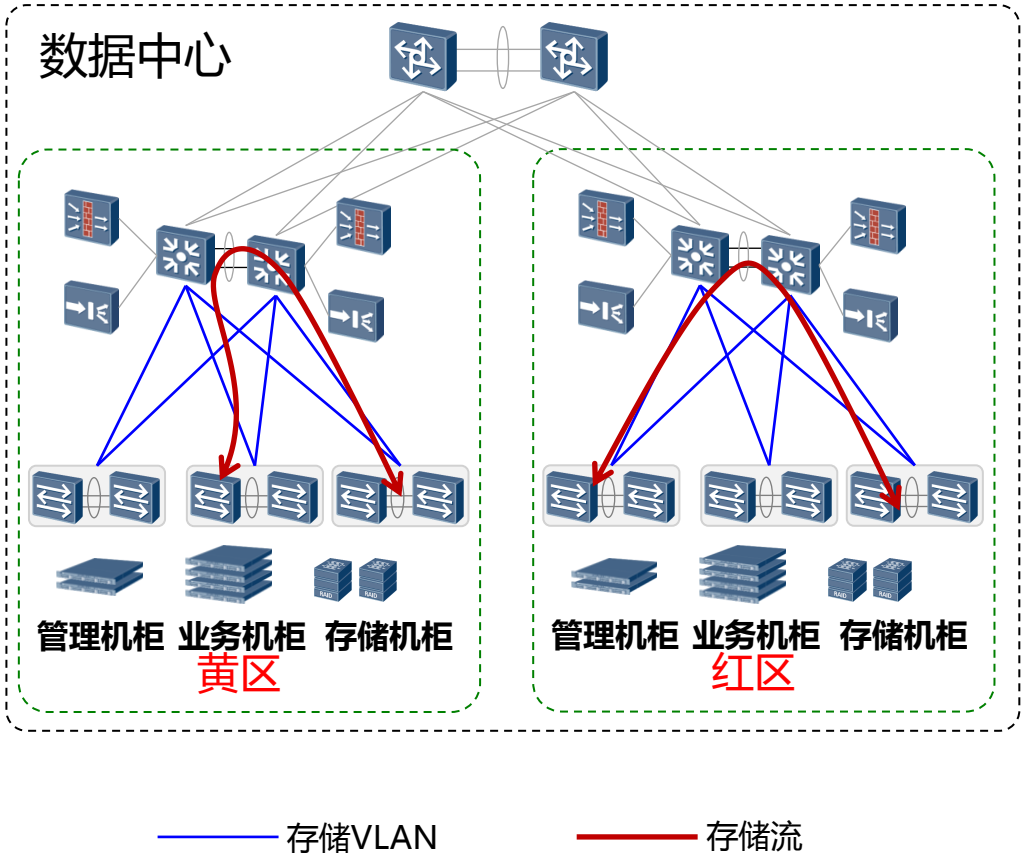
汇聚层作为VRRP网关，可部署ME60限制业务流带宽。

备注：

业务流是虚拟桌面与终端之间的ICA流量，主要在数据中心和园区纵向传输；

管理流是网络设备管理流量，在企业内部全网传输。

数据中心—存储平面

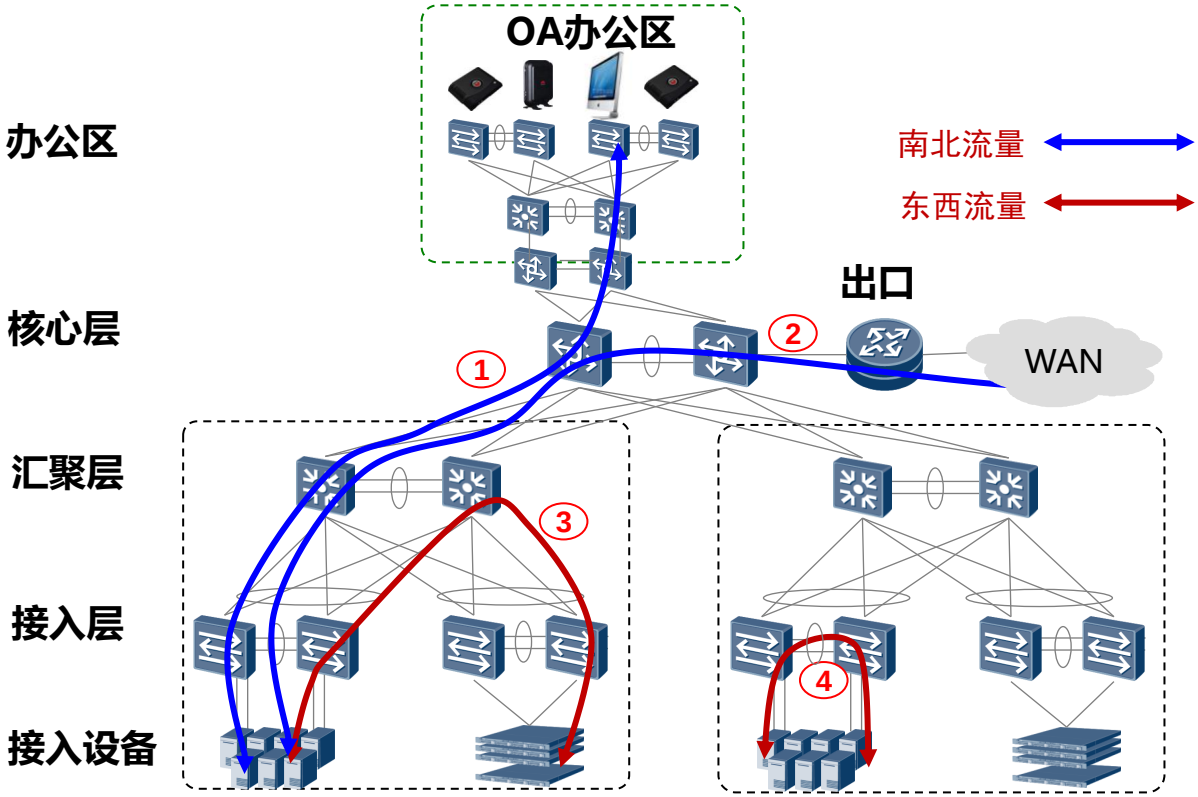


存储平面：

存储数据流主要是服务器之间内部访问流量，在二层范围内，不走三层转发；

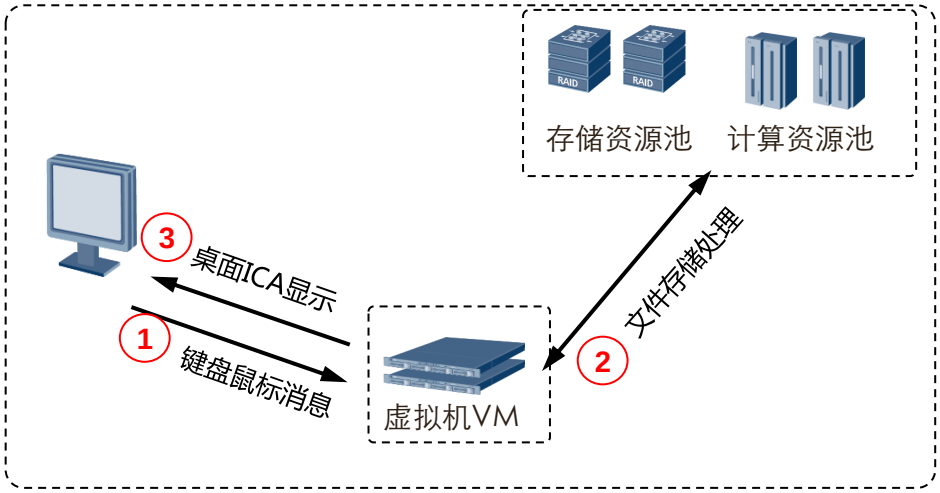
通过VLAN与管理、业务平面隔离。

数据中心—流量分布



	南北流量	东西流量
流量特点	数据中心服务器与外部通信流量	数据中心内部服务器之间流量
流量归类	键盘鼠标操作信息到虚拟机VM服务器流量；虚拟机VM屏幕显示I到终端流量。 ① 本地服务器需要访问远程数据中心或Web访问。 ②	管理和业务服务器访问存储设备流量。 ③ 服务器之间集群计算流量。 ④

数据中心—Office和播放流量模型

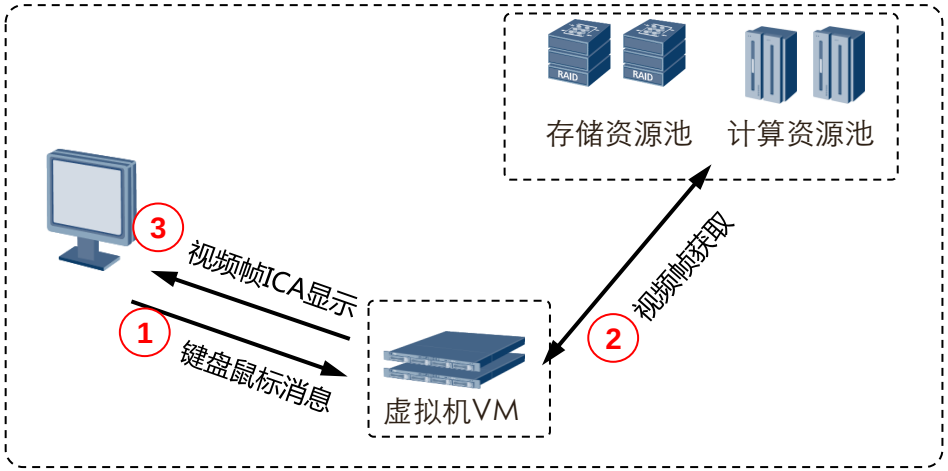


Office应用：

键盘鼠标消息→桌面虚拟机→文件存取处理→桌面虚拟机→ ICA消息桌面显示

流量分析：

虚拟机VM到终端的网络质量影响云终端显示效果，存储快慢影响文件打开速度，但不影响显示体验 。



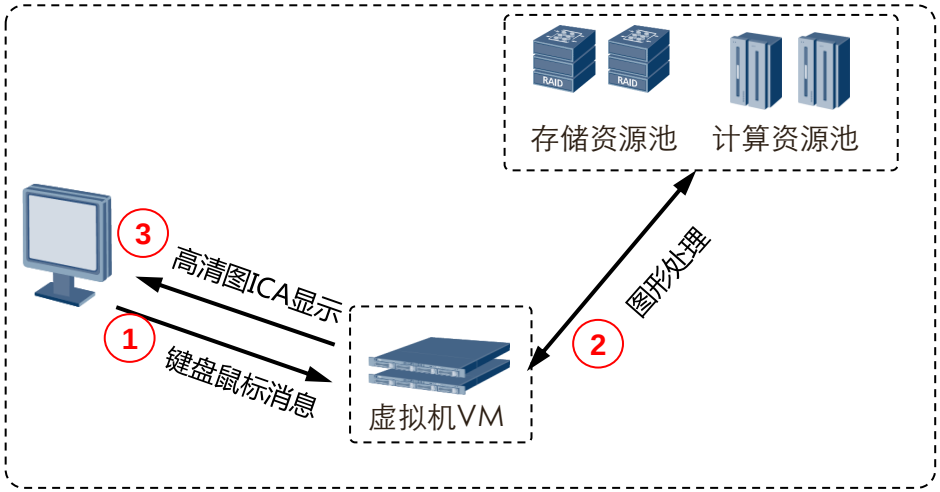
视频语音播放：

键盘鼠标消息→桌面虚拟机→从存储获取视频帧→桌面虚拟机→视频帧ICA显示

流量分析：

虚拟机VM到终端网络质量影响云终端显示效果，视频帧存储获取快慢同样影响视频播放效果。

数据中心—制图和Web流量模型

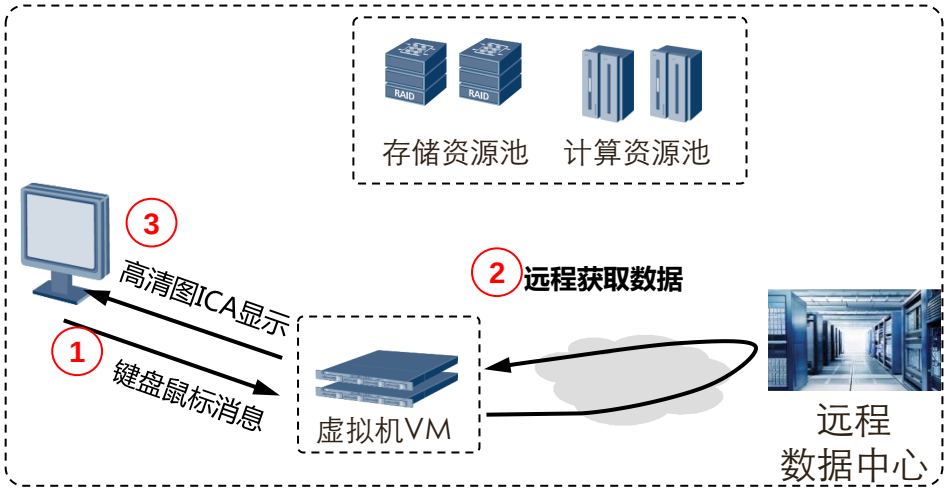


高清制图：

键盘鼠标消息→桌面虚拟机→图形计算处理→桌面虚拟机→高清图ICA显示

流量分析：

桌面虚拟机到终端网络质量影响用户体验，图形处理速度不影响显示，但高清图片差异变化导致ICA消息频繁刷新，带宽诉求高



远程Web访问：

键盘鼠标消息→桌面虚拟机→远程数据中心访问→桌面虚拟机→ICA桌面显示

流量分析：

桌面虚拟机到终端网络质量影响云终端显示效果，远程获取数据慢并不影响显示体验效果（仅下载速度慢，但显示无卡顿）。

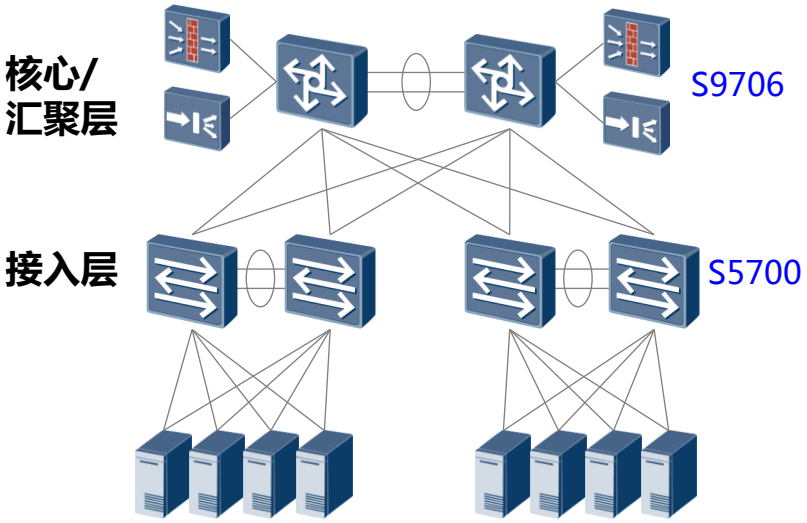
数据中心—流量模型总结

	影响显示关键环节	带宽诉求
Office应用	虚拟机到终端网络时延等影响显示效果	桌面显示变化差异小，ICA带宽需求小
视频语音播放	虚拟机到终端网络时延等影响显示效果，视频帧存取速度影响播放效果；数据中心内部处理速度慢会导致体验差。	桌面显示变化差异大，ICA带宽需求大；对数据中心存储带宽也有较高需求。
高清制图	虚拟机到终端网络时延等影响显示效果，高清图片帧差异导致ICA频繁刷新桌面	桌面显示变化差异大，ICA带宽需求大。
远程Web访问	虚拟机到终端网络时延等影响显示效果，远程获取数据慢并不影响显示体验效果	桌面显示变化差异小，ICA带宽需求小。

终端到虚拟机承载网质量直接影响桌面显示效果；

桌面显示变化差异大小直接影响ICA流带宽诉求。

数据中心—网络规模设计



	桌面云数据中心
服务器规模	小于1800台
核心/汇聚交换机	S9706 8*16*10GE：2台,
接入交换机	S5700 48GE+2*10GE：76台 收敛比1:2.4
防火墙	Eudemon 2台

接入层：

1800台服务器，每服务器主备双网卡接入，需要接入3600端口GE。

每台S5700 48GE+2*10GE端口，每两台为一组，共提供96GE双归接入能力和4*10GE上行。

3600÷96=37.5，共需要38组S5700，收敛比20GE:48GE=1:2.4。

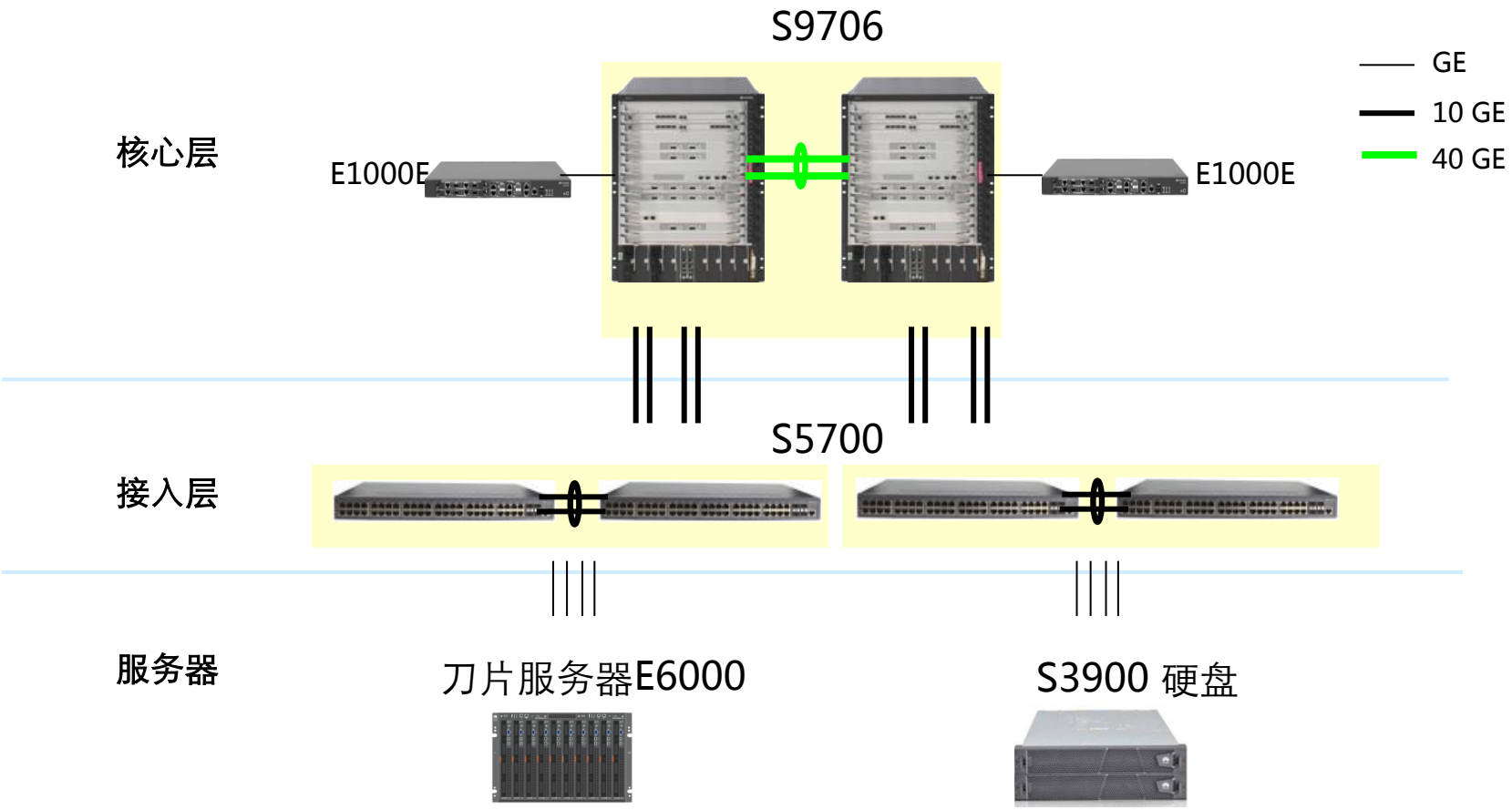
核心/汇聚层：

接入层 38*4 = 152接口连入核心/汇聚层，核心/汇聚层采用S9706配置8*16*10GE接口线卡，2台为一组，共提供256*10GE接入能力，256-152 = 104 10GE接口可用来扩容。

流量带宽：

核心层和园区核心层连接，如果根据用户计算带宽 100GE，需要采用上行4*40GE端口接入。

数据中心—产品选型


S9706
GE
10 GE
40 GE
核心层
E1000E
E1000E
S5700
接入层
服务器
刀片服务器E6000
S3900 硬盘

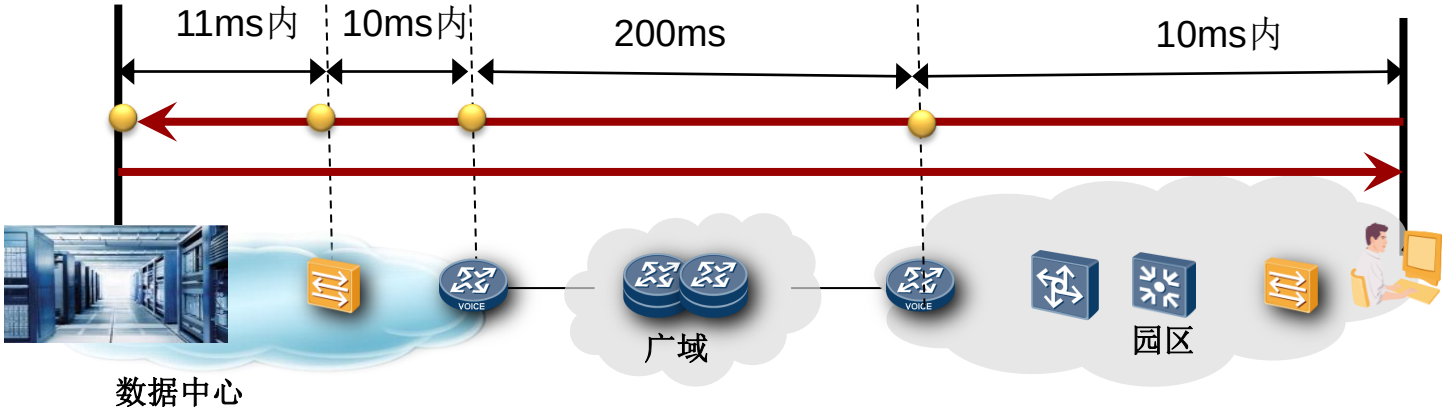
网络质量—桌面云体验网络质量要求

网络质量等级	体验效果	包丢失率	抖动(ms)	时延(ms)	带宽
良好	OA体验同传统桌面无差异，标清播放有微弱滞后感	≤0.1%	≤5	≤50	≤10M
一般	鼠标拖动有微弱滞后感，高标视图有卡顿感	≤1%	≤20	≤100	≤2M
较差	鼠标拖动有轨迹，桌面显示有顿挫感	≤5%	≤60	≤400	≤300K

Office OA日常办公应用（Word/Excel/WWW浏览）	占用50～80 Kbps
呼叫中心客服应用	100～150 Kbps
Powerpoint/图片应用	占用200～300 Kbps
标清视频	占用1～2 Mbps

往往分配足够大带宽（一般20M），避免拥堵现象造成的时延、抖动问题。

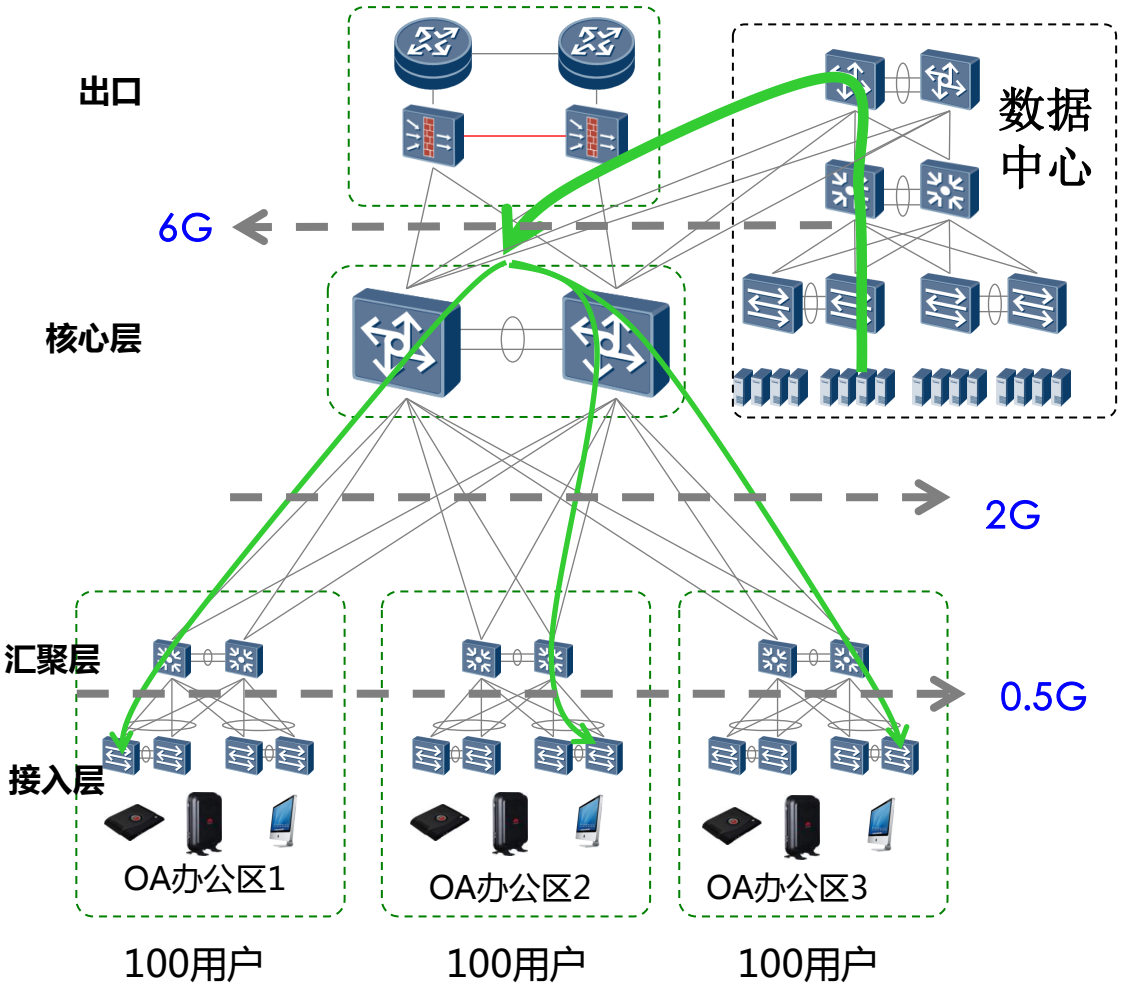
网络质量—影响质量因素



光速：30万公里折合2/3系数为20万公里；单机设备转发速度：50 μs
园区内部时延主要设备转发时延，广域时延主要是光纤距离。

时延	评估计算	其它影响因素	测量结果
园区网络	园区以太网传输时延 1.1ms 转发时延 50μs * 20(节点) = 1ms 共计双向时延 4.4ms。	园区以太网络距离误差， 存在QOS延迟调度因素等	6ms
数据中心	和服务器CPU硬件有关	虚拟机形成ICA报文处理速度	11ms
广域网络	深圳到北京租用光纤为例： 距离时延 11ms = 2200公里 / 20万公里 转发时延 50μs * 100(节点) = 5ms 共计双向时延 32ms。	光纤传输中继时延；存在QOS 延迟调度因素；	200ms

网络质量—带宽设计



举例(每户预留20M)：

接入层 25用户，带宽0.5G；汇聚层 100用户，带宽 2G；核心层300用户，带宽 6G

(3个OA办公区)；

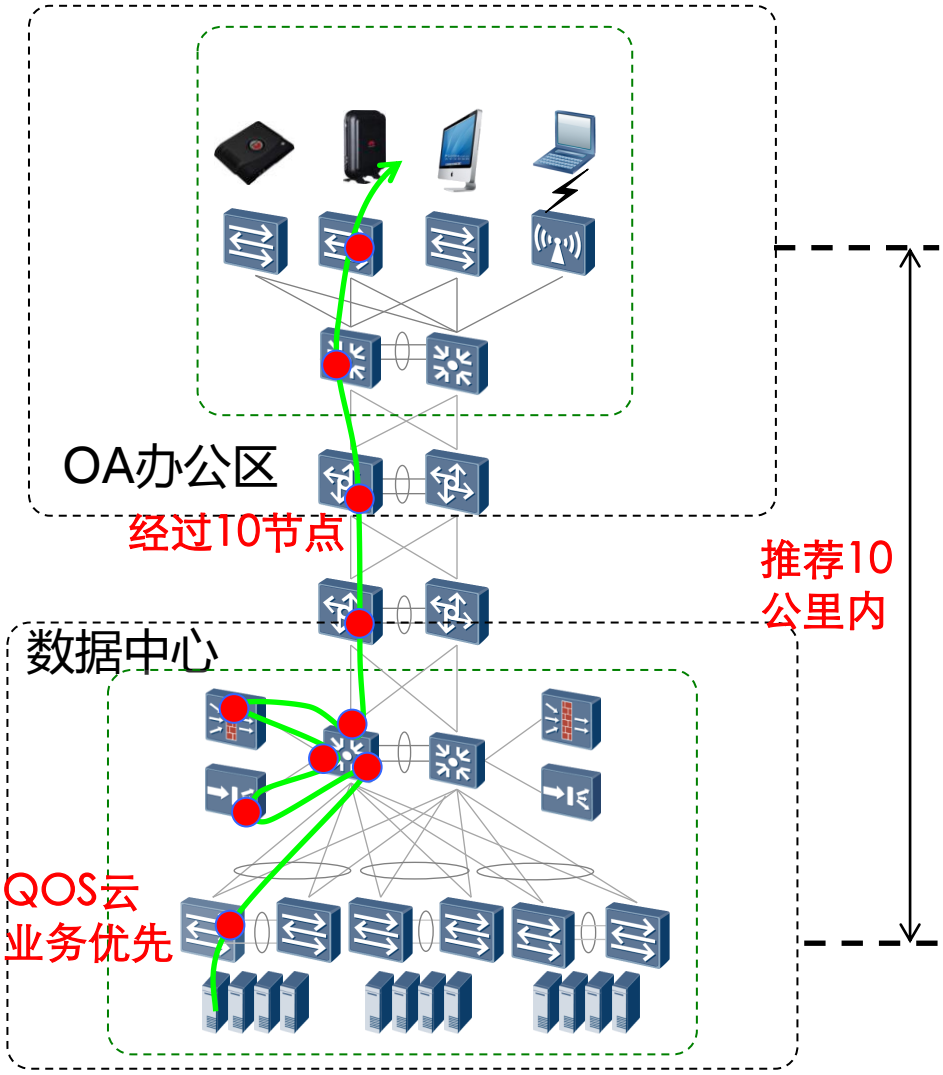
数据中心预留带宽 6G

设计原则：

用户基本同时间上线

带宽满预留；

网络质量—时延、抖动、丢包率设计



时延要求:

数据中心和办公区在10公里内。

网络设备数节点数不超15 。

QOS部署保证云业务及时调度。

双向时延目标100ms

丢包率要求:

没用户足够带宽20M，避免拥塞丢包。

QOS部署保证云业务不丢失。

丢包率目标在0.5%内。

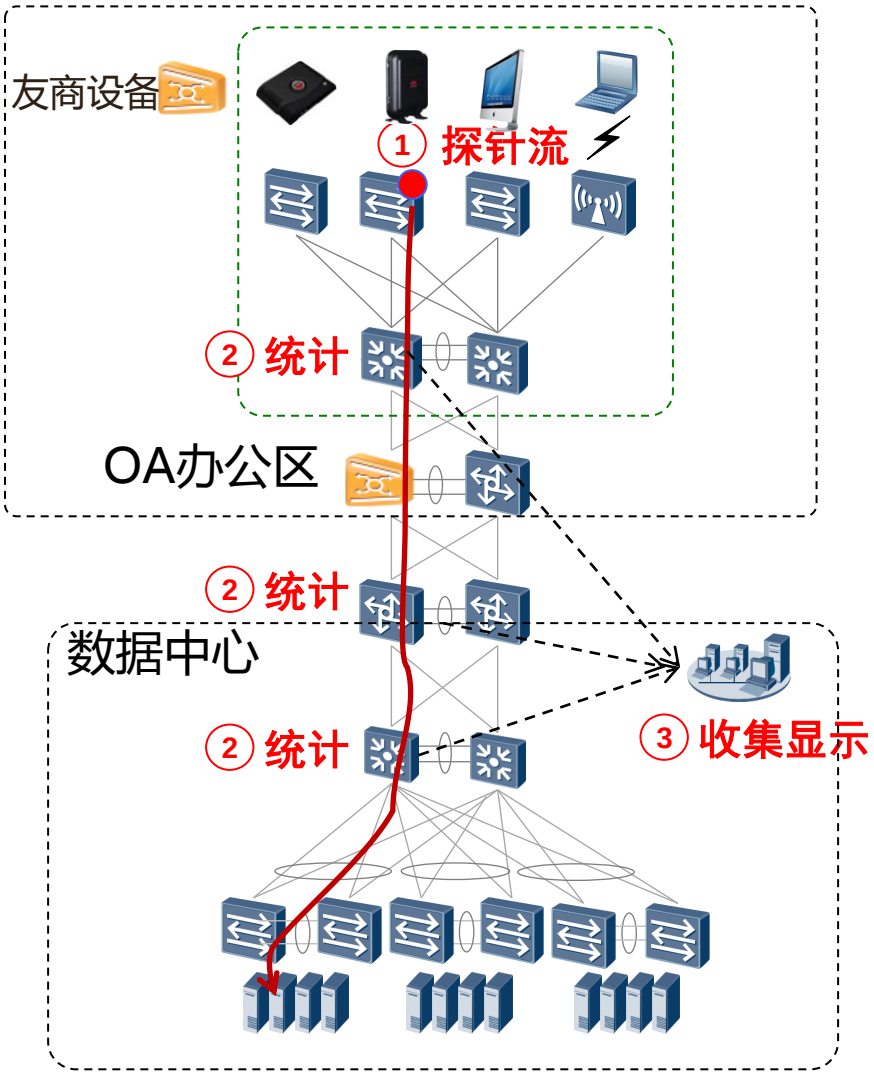
抖动要求:

网络设备数节点数不超15，

QOS部署保证云业务均匀调度，

抖动目标在20ms内。

网络质量—质量监控设计



应用场景:

部署云终端前，解决承载网时延、丢包率、抖动及QoS故障定位。

解决方案：

终端交换机发送硬件探针，

中间网络设备流量数据统计，

网管统计数据收集并分段显示，

支持多实例探测流监控，

支持友商网络互通

产品部署：

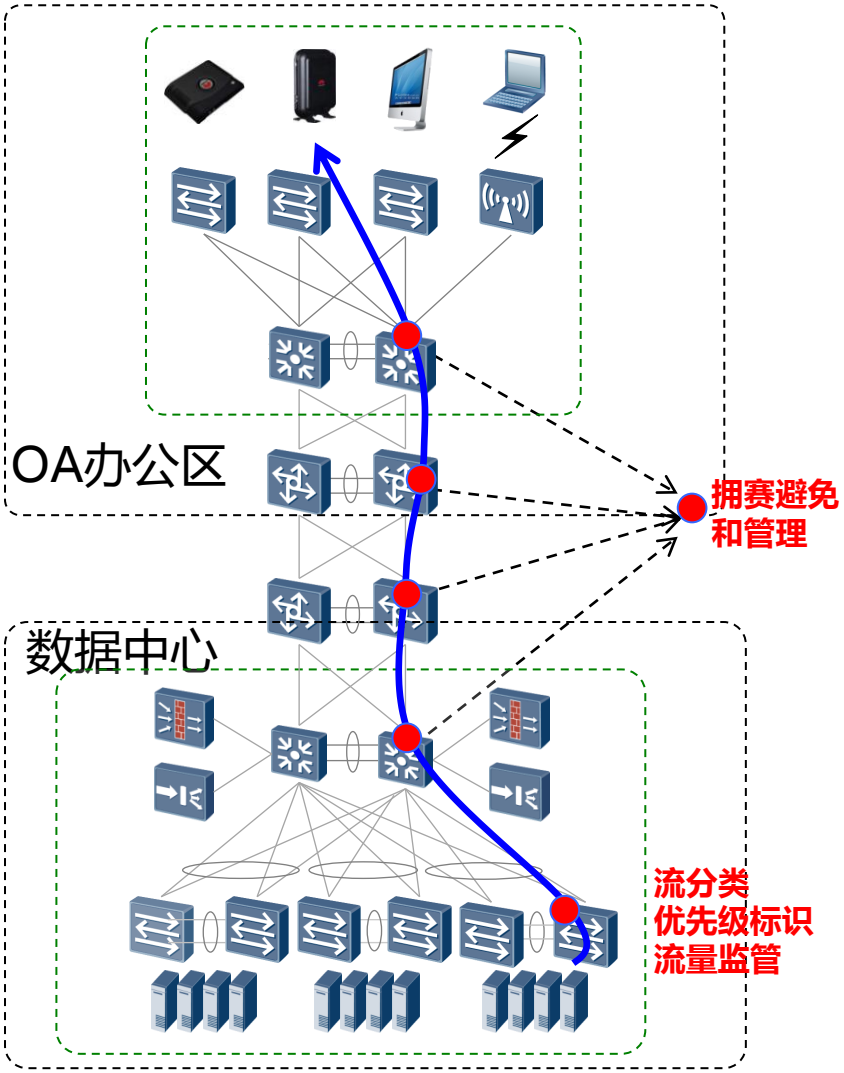
网管必选我司eSight产品；

终端交换机需要支持硬件探针如S57HI及以框式产品。

客户价值:

全路径网络分段故障可视并快速定位。

网络质量— QoS部署设计



应用场景：

园区网络多业务流，链路拥堵发生时需保证云业务优先转发。

QoS方案：

接入交换机进行流分类、优先级重标记和流量监管。

网络设备根据优先级，进行QOS拥塞避免和管理，优先保证云业务。

方案特色：

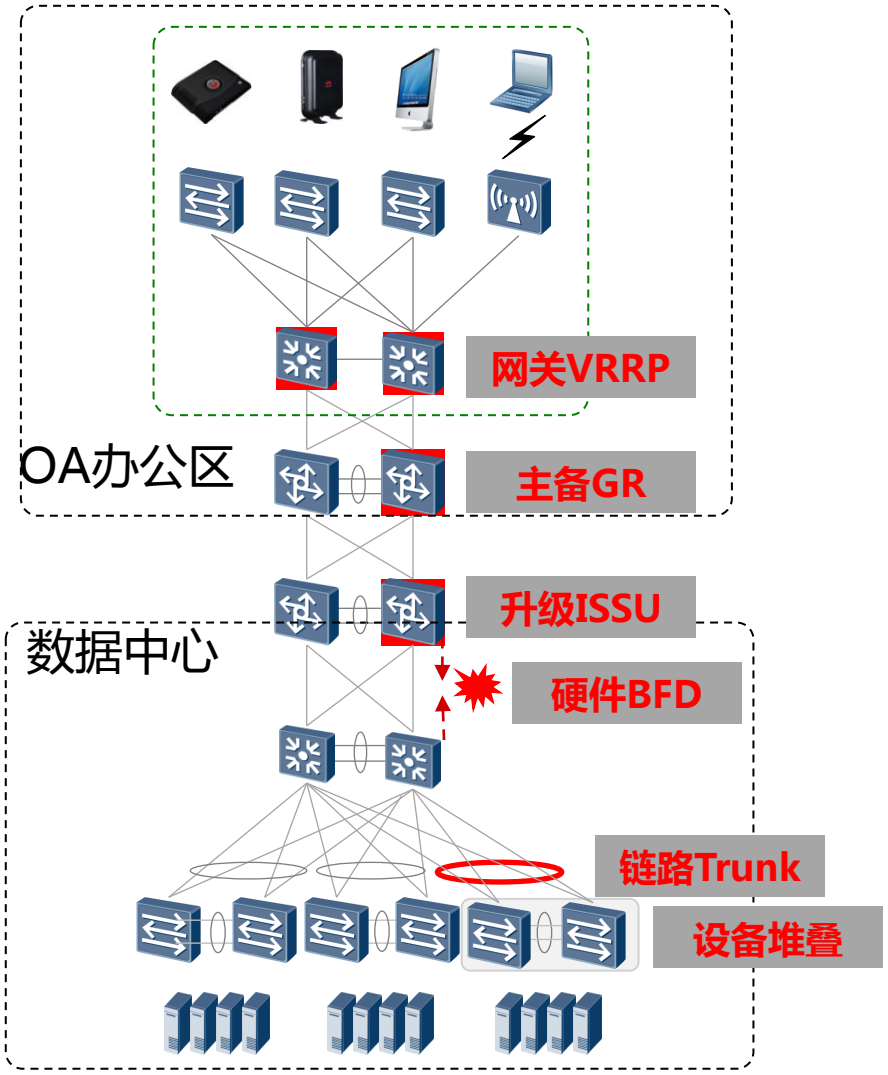
网管全路径监控DSCP状态值。

网管模板批量QoS部署云业务。

备注：

OA区一般仅有云流量，可不部署QoS

可靠性设计—故障恢复



客户场景:

网络某条链路或设备故障，需快速恢复，使用户无缝体验。

解决方案：

链路备份：链路双归，Trunk 链路绑定

设备备份：CSS/iStack，网关VRRP

主控备份：GR、NSR倒换流不中断。

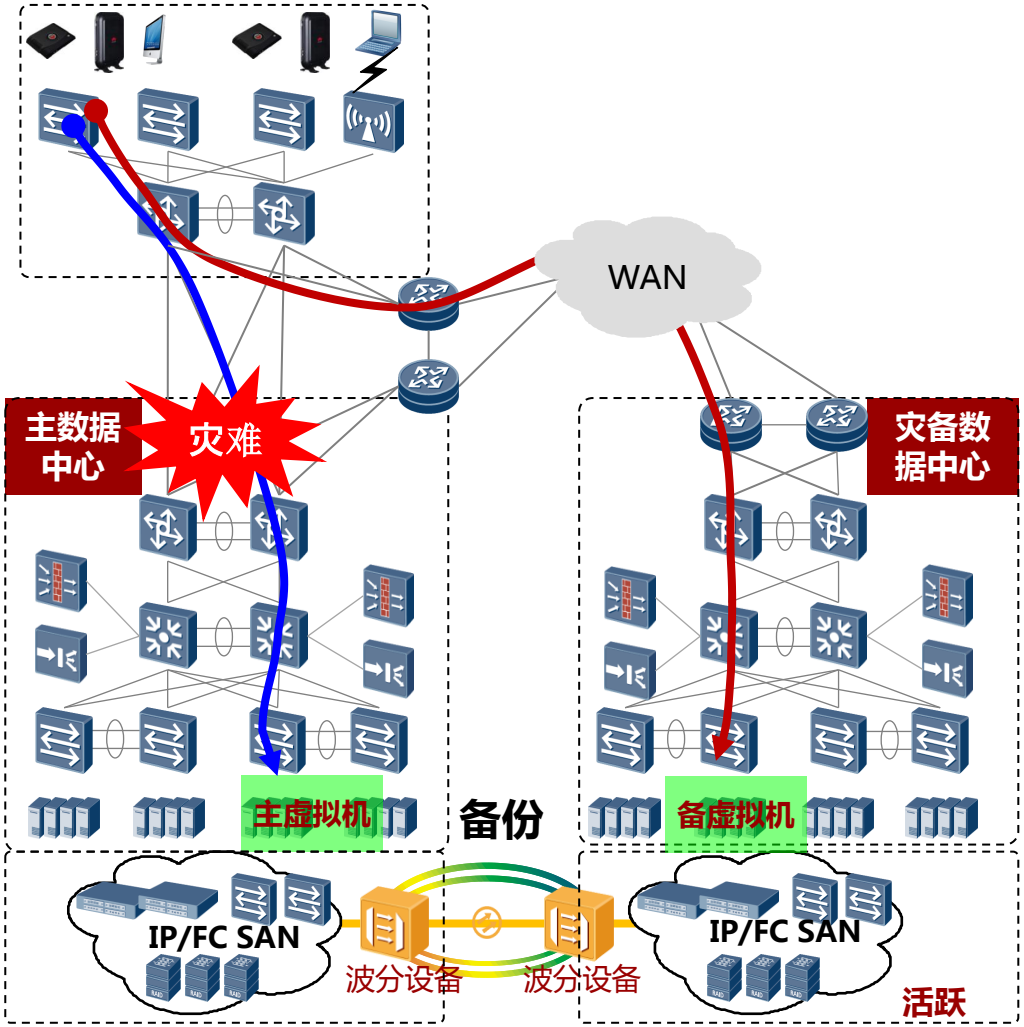
升级可靠：ISSU无损升级技术。

故障发现：硬件BFD、OAM快速故障发现

设计原则：

任何链路设备故障，均有备份快速恢复

可靠性设计—数据中心灾备



应用场景:

数据中心因物理原因如大火、地震等全网毁坏，需及时恢复OA办公

低安全:

跨越WAN夜间冷备份，

RPO、RTO目标为24小时。

高安全:

同城光专线实时热备份，DNS恢复；

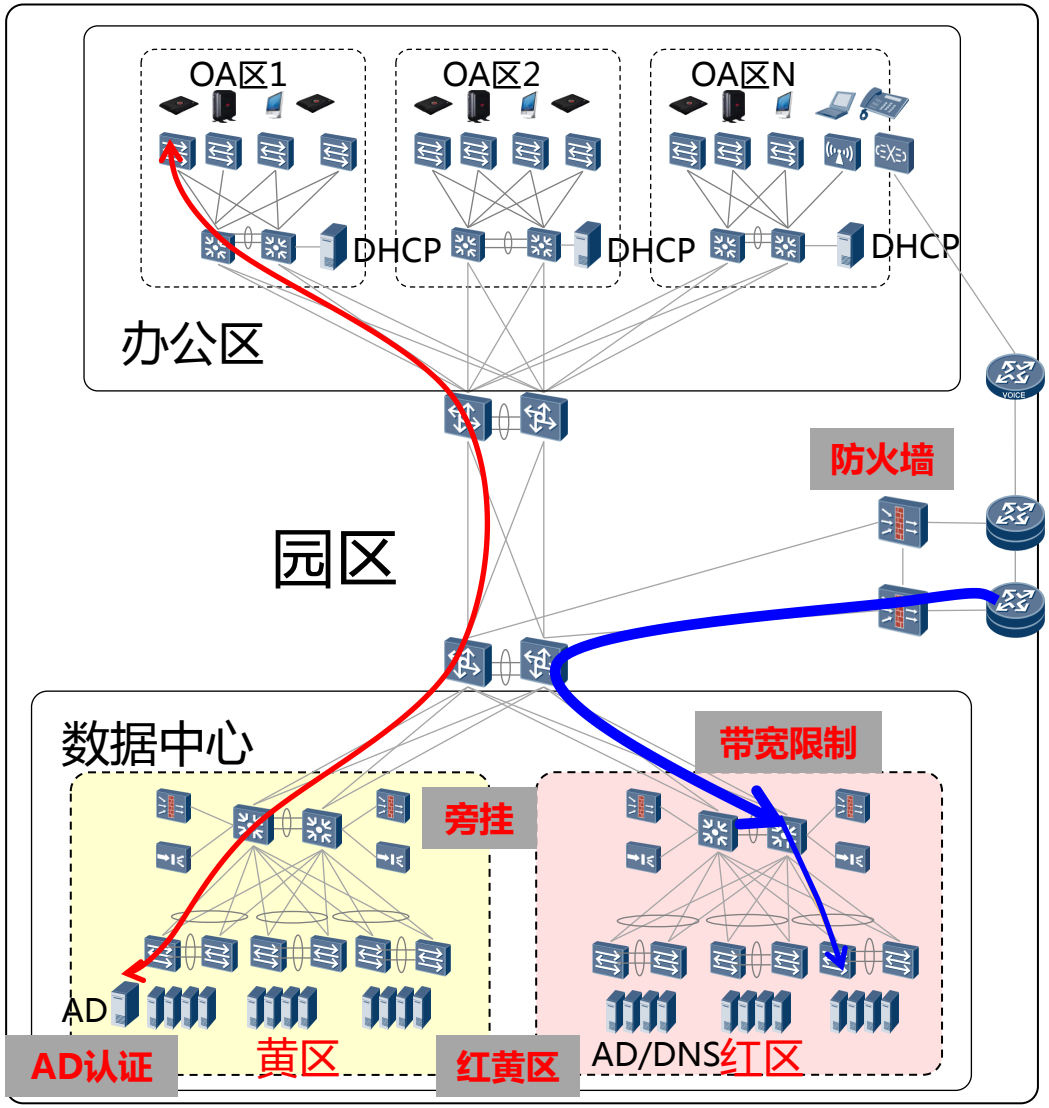
RPO目标20分钟，RTO目标2小时

备注:

RPO - 发生灾难前最后一次备份的时间点距离当前时间差；

RTO - 发生灾难后恢复物理系统环境的时间

网络安全设计



防火墙：

出口防火墙采用口字形。

数据中心汇聚防火墙旁挂，办公区仅ICA流，可不部署防火墙。

红黄区：

数据中心部署红黄区安全隔离，红黄区防火墙分别限制登陆权限，红区一般通过防火墙只有读权限，限制写权限。

AD认证：

用户名/密码AD认证，服务器部署在数据中心。

带宽限制：

数据中心汇聚层ME60限制用户带宽。

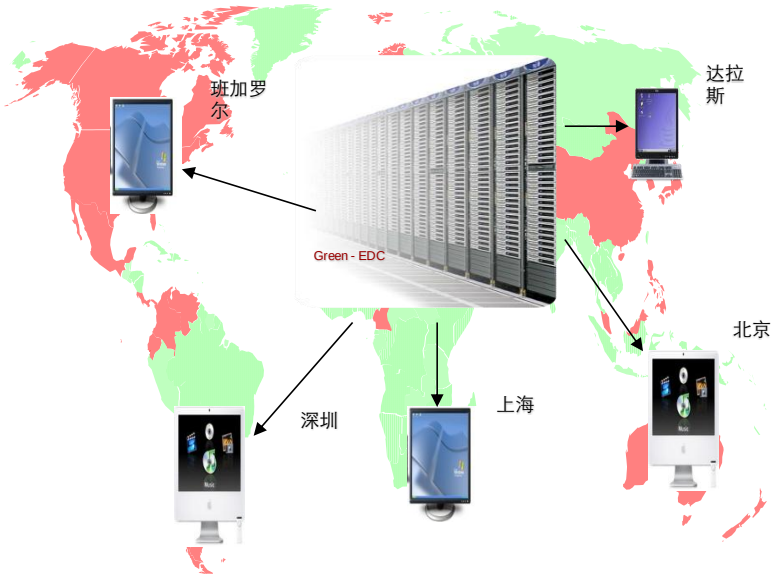
成功案例—华为虚拟桌面云计算项目

项目目的

- 降低办公系统能耗（瘦终端＋虚拟化提高服务器利用率）
- 提高IT管理维护效率（瘦终端＋服务集中部署）
- 解决研发办公信息的安全性问题（瘦终端）

项目计划

- 项目一期计划覆盖上海研究所新办公区，容量1万人，2009年11月开始交付，2010年交付完毕，目前已上线6000人
- 项目二期覆盖所有海外研究所，深圳总部各业务部门，涉及6万人，预计2011年内完成



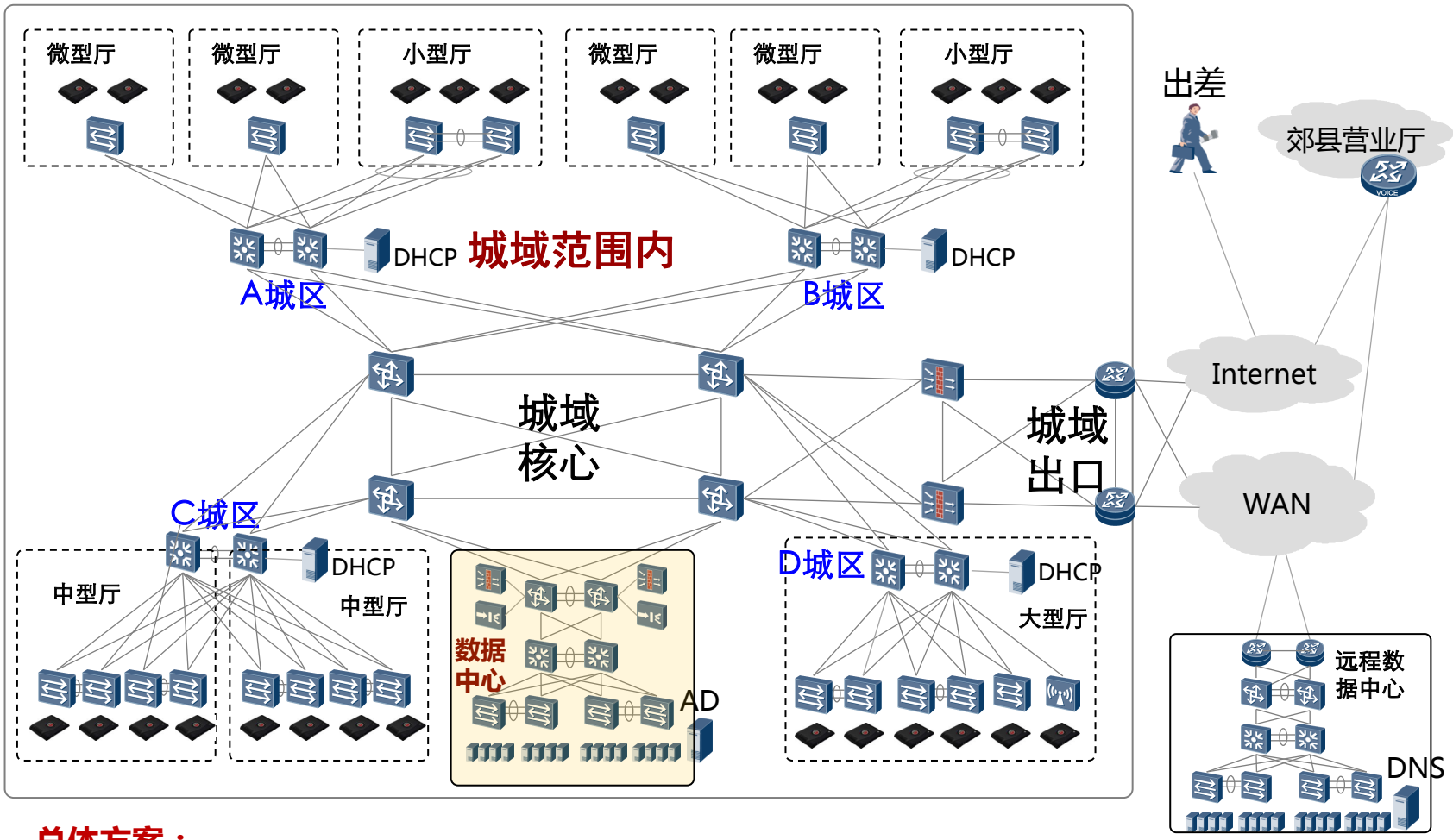
优化效果评估

	传统方式	基于云计算的NC	预期效果
服务器	57300PC ＋5730 PC	4093服务器＋57300 瘦终端	**节省40%投资**
资源利用率	<5%	>52%(NC+CI)	**提升10倍**
24小时功耗(w)	78283260	22622750	**节省71%**
业务服务器准备周期	>3个月	<3天	**减少97%**
维护效率	<100台/人	>1000台/人	**提高9倍**

城域营业厅桌面云方案

- 总体组网
- 营业分厅组网设计
- 网络部署设计
- 带宽设计
- 网络质量和监控设计
- 可靠性设计
- 产品选型设计
- 成功案例

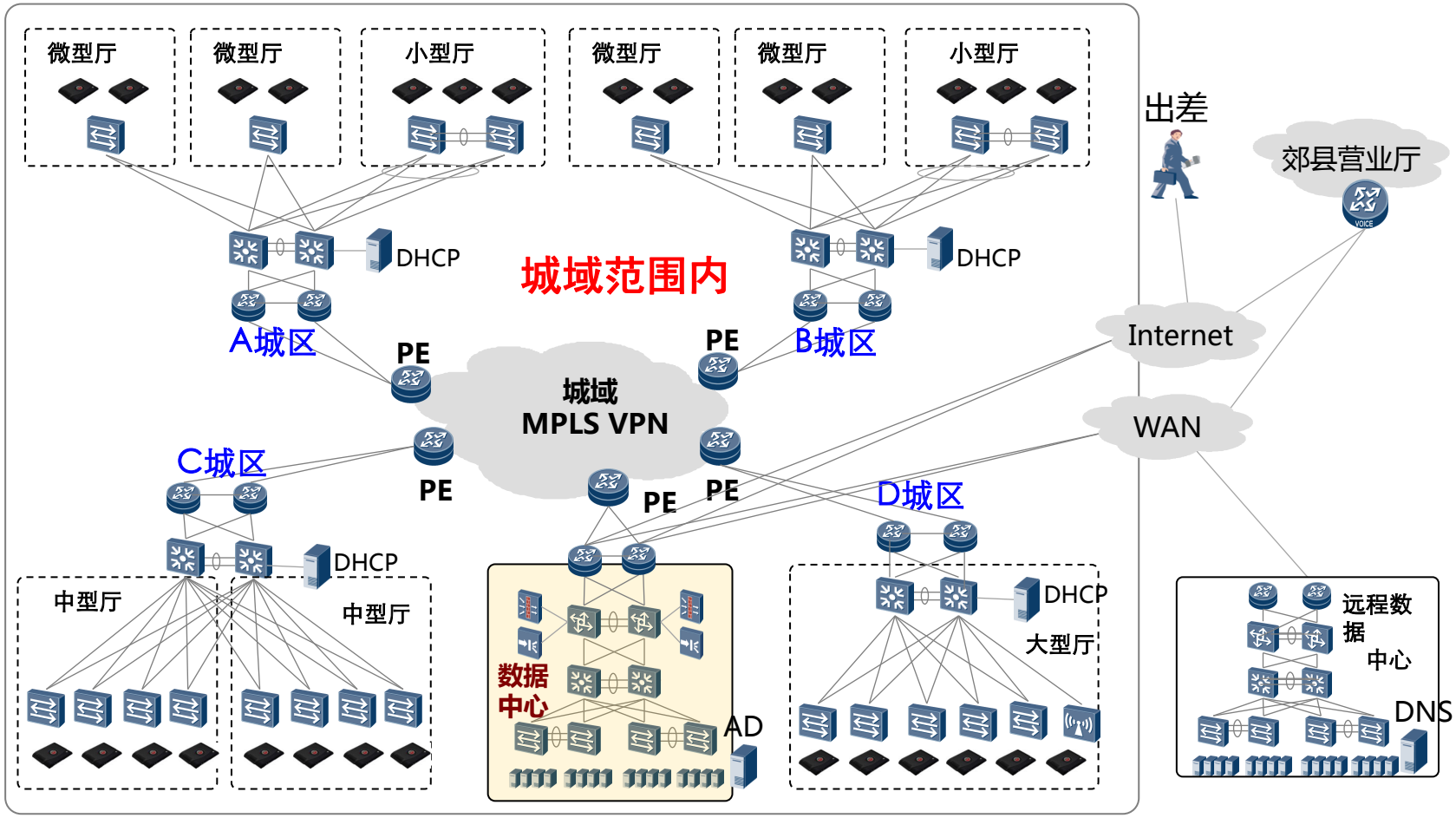
总体方案—自建城域核心（二选一）



总体方案：

城域营业厅分散办公，自建城域核心网络和数据中心。

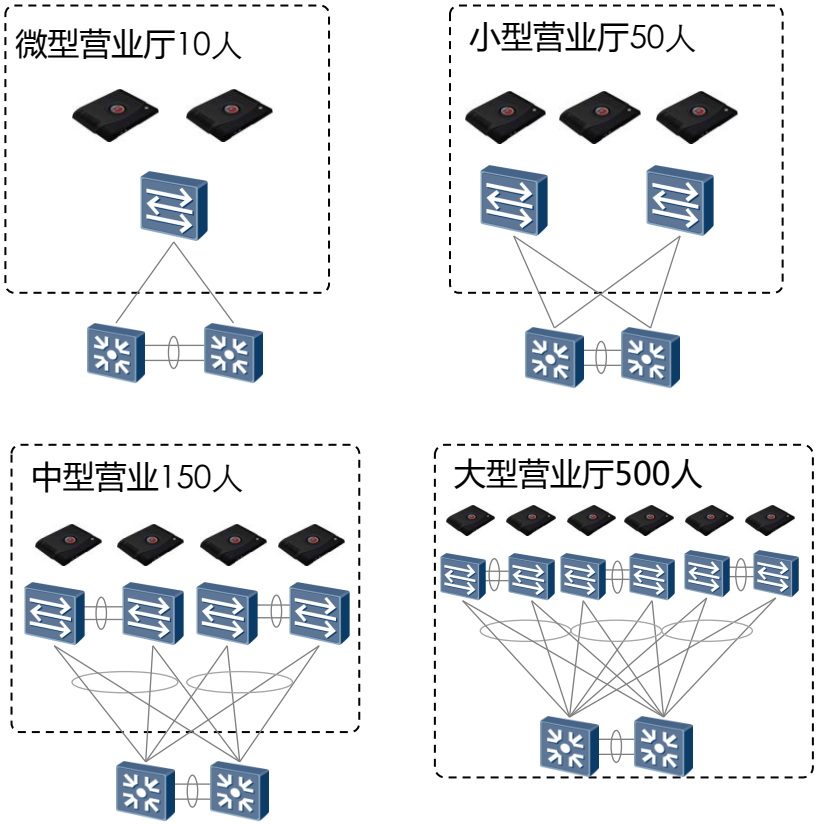
总体方案—租用MPLS VPN（二选一）



总体方案：

城域营业厅分散办公，租用运营商MPLS VPN网络和自建数据中心。

营业分厅组网设计



微型营业厅:

10人规模，一台二层交换机接入终端，双归连入城域汇聚交换机。

小型营业厅：

50人规模，两台二层交换机接入终端，双归连入城域汇聚交换机。

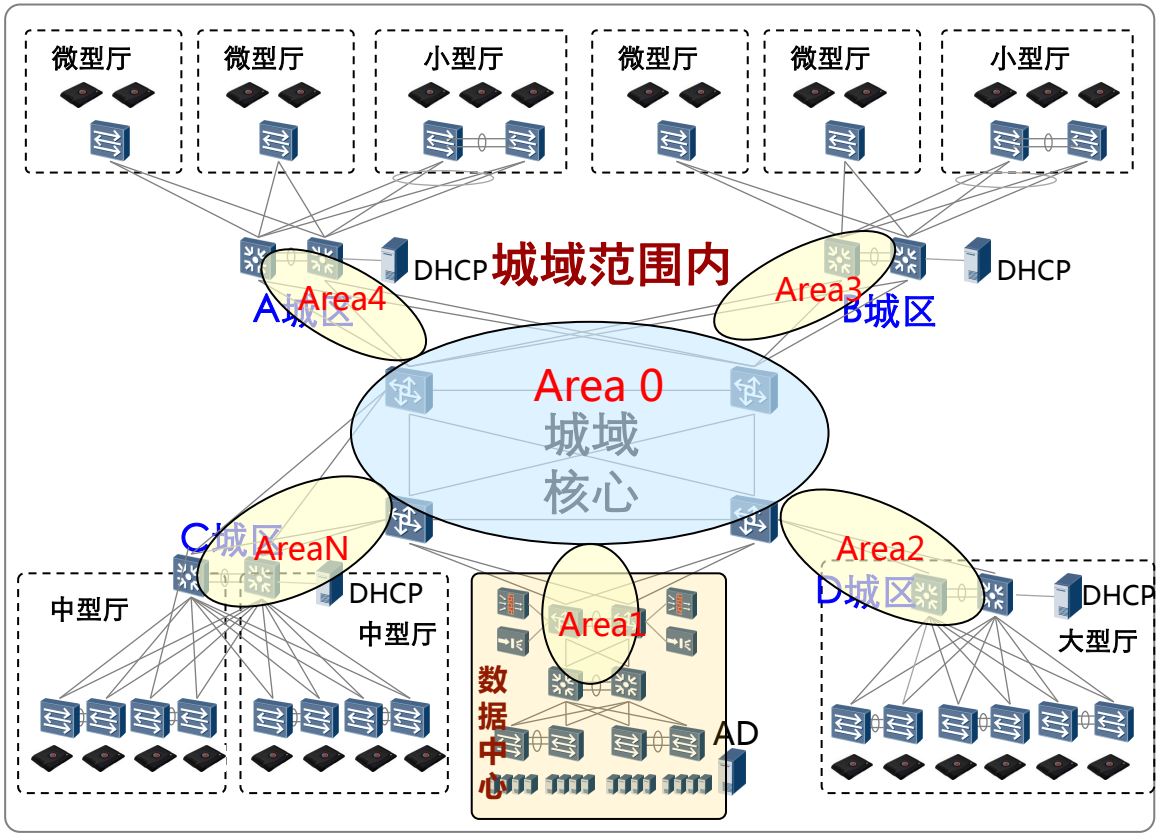
中型营业厅：

150人规模，两对二层交换机接入终端，双归连入城域汇聚交换机。

大型营业厅：

500人规模，N对堆叠二层交换机接入终端，连入营业厅内部署的一对汇聚交换机，最终接入城域核心。

网络部署—自建OSPF多区域



组网部署:

城域核心交换机和数据中心核心层形成骨干Area0。

城域汇聚层划分Area 1,2,N区域，配置NSSA或Stub。

营业厅终端二层千兆接入

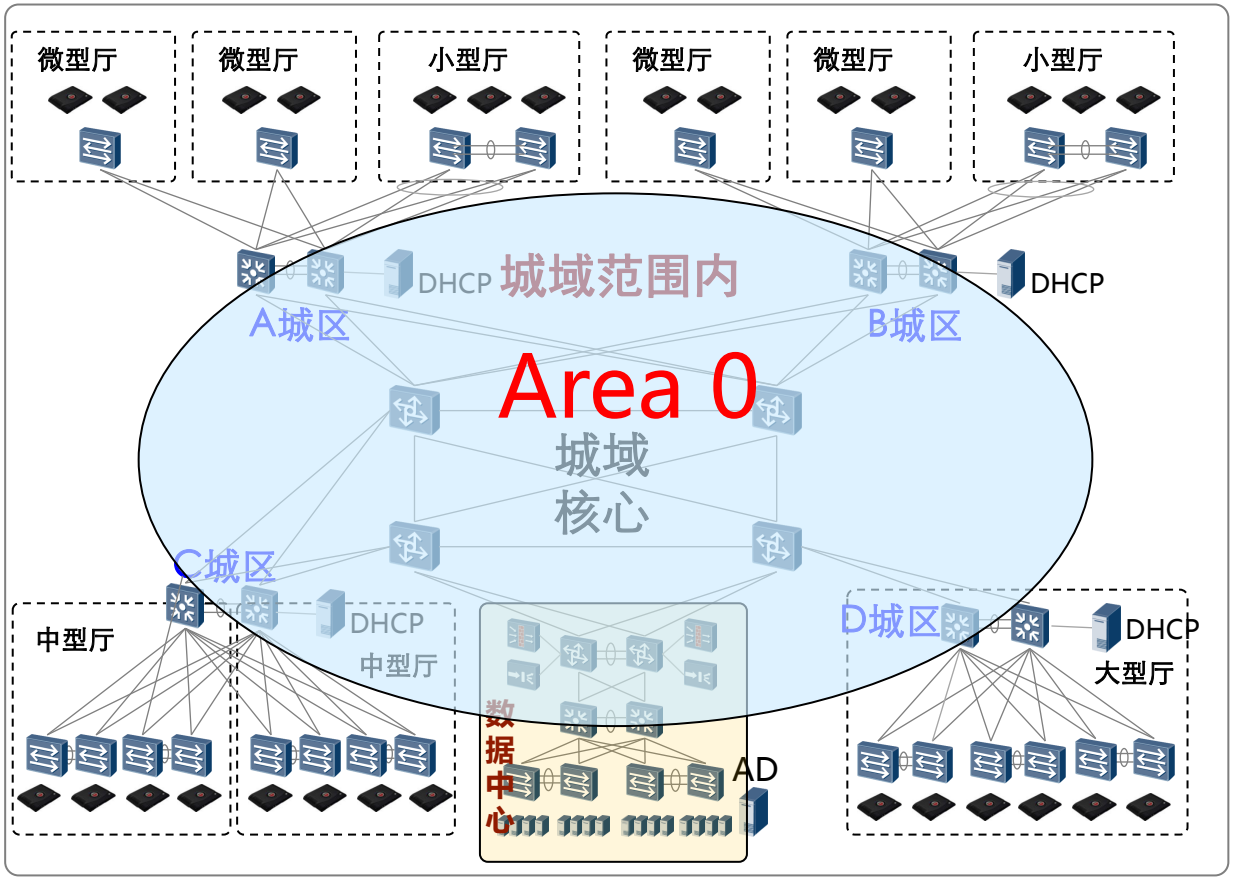
方案价值：

每个城区汇聚层拓扑改变不会全网计算。SPF计算规模大大降低。

适合场景：

适合大中型城域，汇聚节点部署较多。

网络部署—自建OSPF单区域



组网部署:

城域核心交换机、城域汇聚层设备和数据中心三层设备形成骨干Area0，不划分区域。

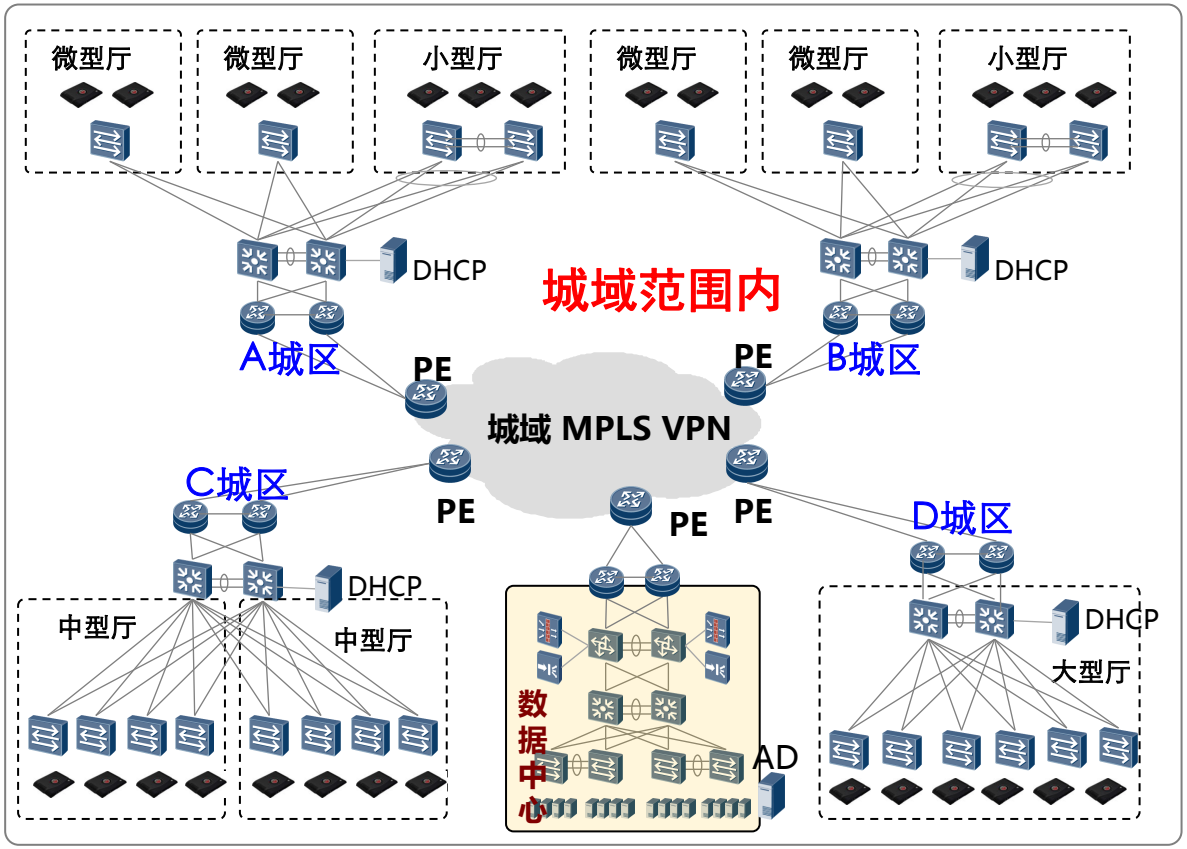
方案价值：

组网配置简单。

适合场景：

适合中小型城域网，汇聚节点部署较少。

网络部署—租用MPLS VPN（二选一）



组网部署:

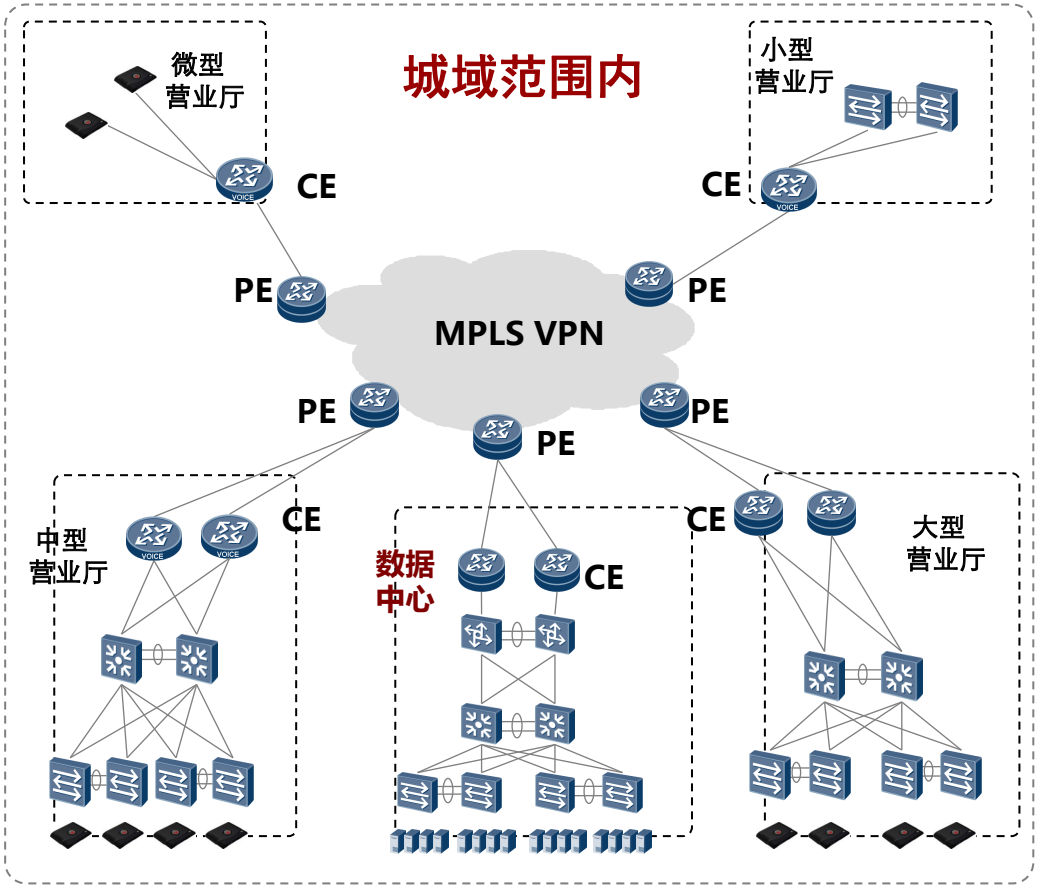
城域汇聚网络和数据中心网络，通过城域MPLS VPN互连。

NE40作为CE和运营商PE相接。

方案特点：

VPN业务隔离安全访问。

网络部署—租用MPLS VPN（二选一）



组网部署:

城域汇聚设备和数据中心通过城域MPLS VPN互连。

NE40/AR作为CE和运营商PE相接。

中小型营业厅采用AR设备作为出口，大型厅可采用NE40作为出口。

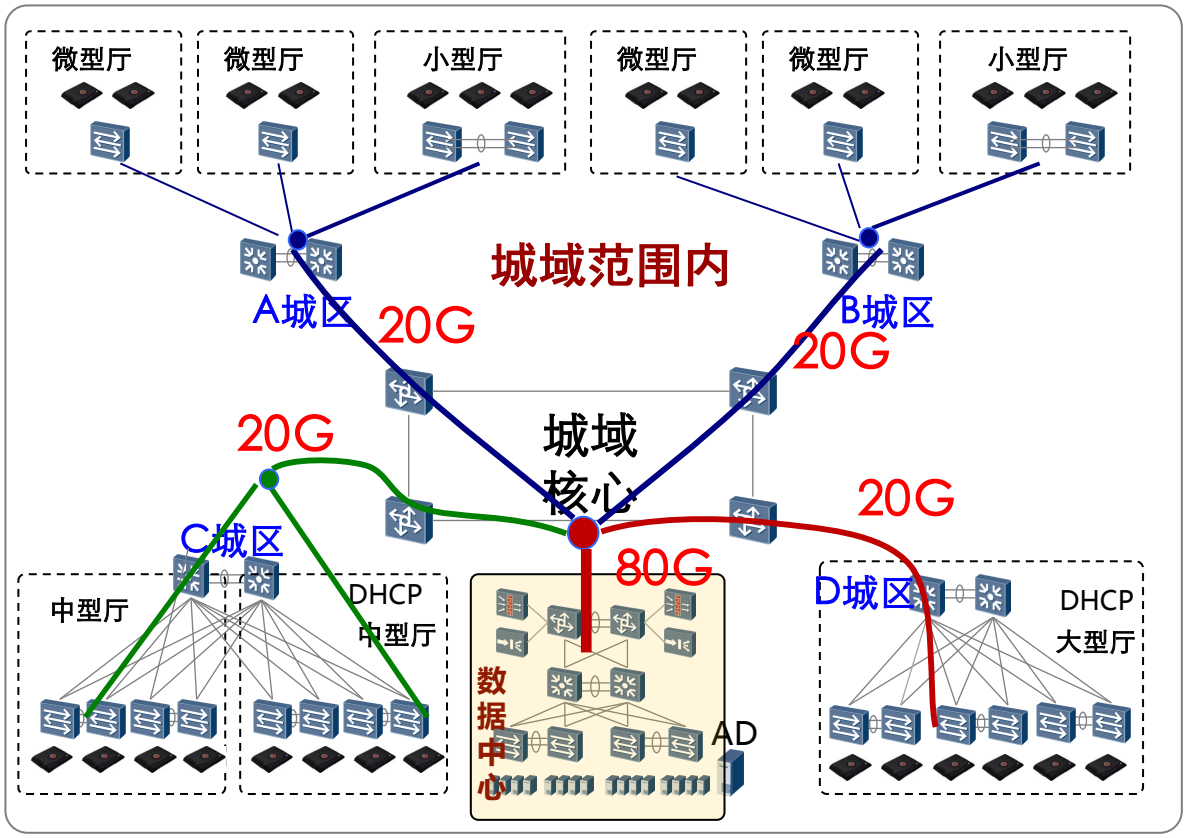
方案特点：

VPN业务隔离安全访问。

网络部署—组网对比

类型	自建OSPF多区域	自建OSPF单区域	租用MPLS VPN
组网概述	城域核心部署Area 0，城域汇聚划分子区域	城域全网部署Area 0相连	城域汇聚通过MPLS VPN互连
优点	城域汇聚层拓扑改变增量计算，可限制计算规模	组网配置简单	通过VPN业务隔离安全访问
缺点	组网配置复杂，不能业务安全隔离	城域汇聚层拓扑改变都全网计算，重复计算多	时延抖动较大，高清图像体验一般
适合场景	大中型城域营业厅	中小型城域营业厅	有安全访问隔离应用场景，如公安系统等

网络质量—带宽设计



每用户带宽20M

A、B城区：

微型厅50*10规模到汇聚，小型厅10*50到汇聚，共1000规模需20G带宽。

C城区:

中型厅2*500规模到汇聚，需要20G带宽。

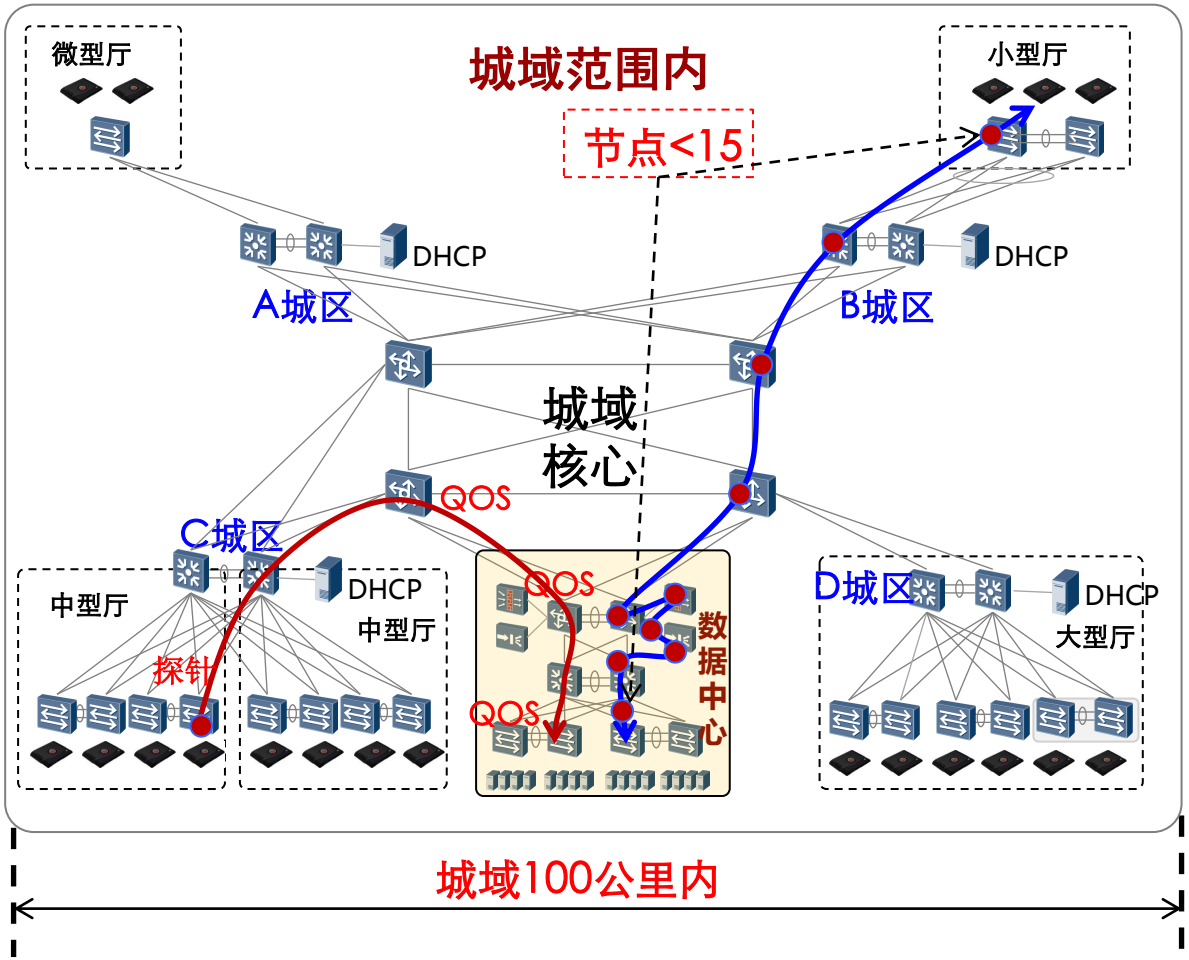
D城区:

大型厅1*1000规模到汇聚，需20G带宽。

数据中心：

20G + 20G + 20G + 20G = 80G

网络质量—时延、抖动、丢包率以及监控设计



时延、丢包率和抖动设计

城域距离小于100公里。

流经过设备节点数小于15。

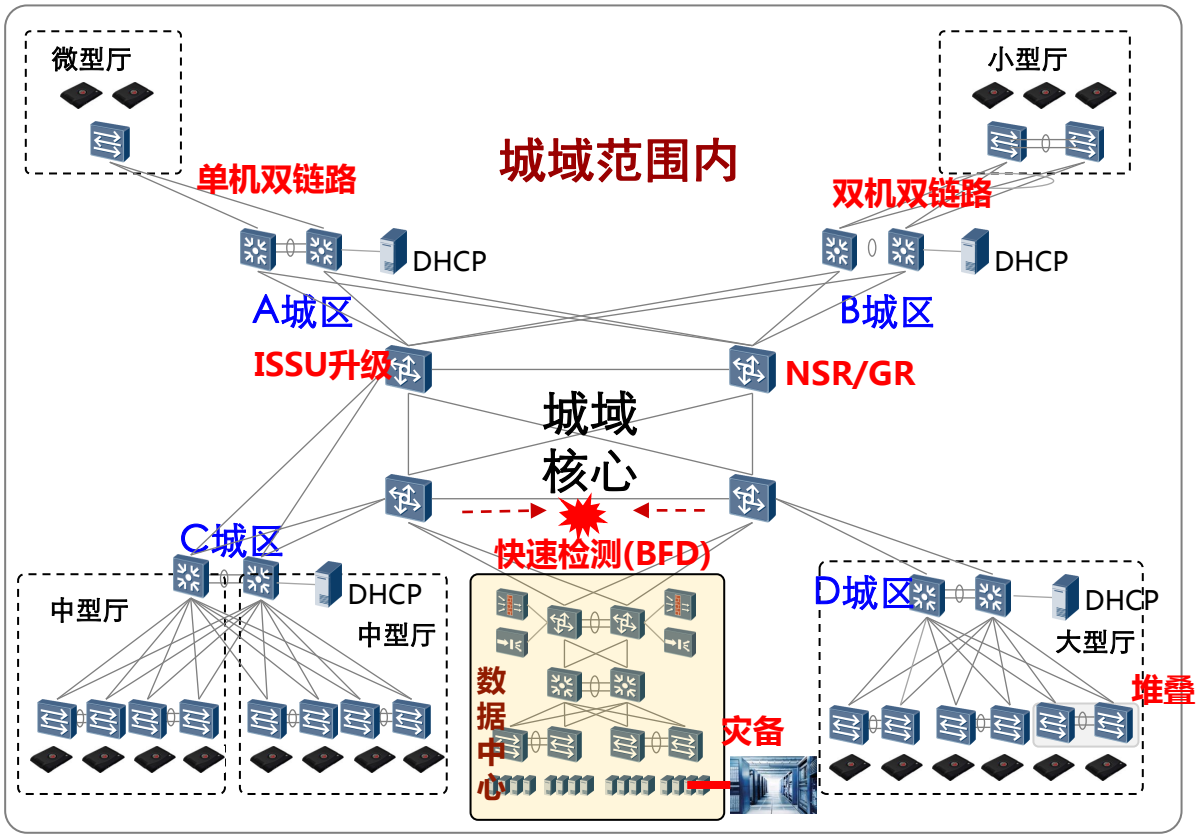
数据中心和城域核心QOS部署保证云业务。

网络监控

终端交换机发送探针，从营业厅出口到城域汇聚、核心，最后到达数据中心。路径网络设备进行数据统计。

网管收集统计并逐段显示时延、抖动质量。

可靠性设计



微型营业厅:

单台交换机，不支持双设备，仅支持双链路可靠。

其它大中小营业厅:

双设备堆叠，支持双链路双设备可靠。

数据中心：

根据业务安全系数，选择同城光纤或者异地MPLS VPN冷灾备。

城域核心：

单机NSR、GR倒换流不中断；

硬件BFD链路故障快速发现；

ISSU无损升级。

产品选型— 100个50人规模小型分厅

设备类型	部署位置	型号	单位	数量
服务器	数据中心	E6000服务器（2路6核CPU、72G内存）	台	1800
核心交换机	数据中心	S9706	台	2
接入交换机	数据中心	S5700	台	76
存储	数据中心	S3900（配置132块600G SAS硬盘）	套	50
核心交换机	城域	S9706	台	4
城域出口	城域	NE40	台	2
汇聚交换机	城域	S7706	台	6
接入交换机	营业分厅	S5700	台	200
云终端	营业分厅	TC G1945	台	5000

S9700

S7700

S5700LI/SI/EI/HI

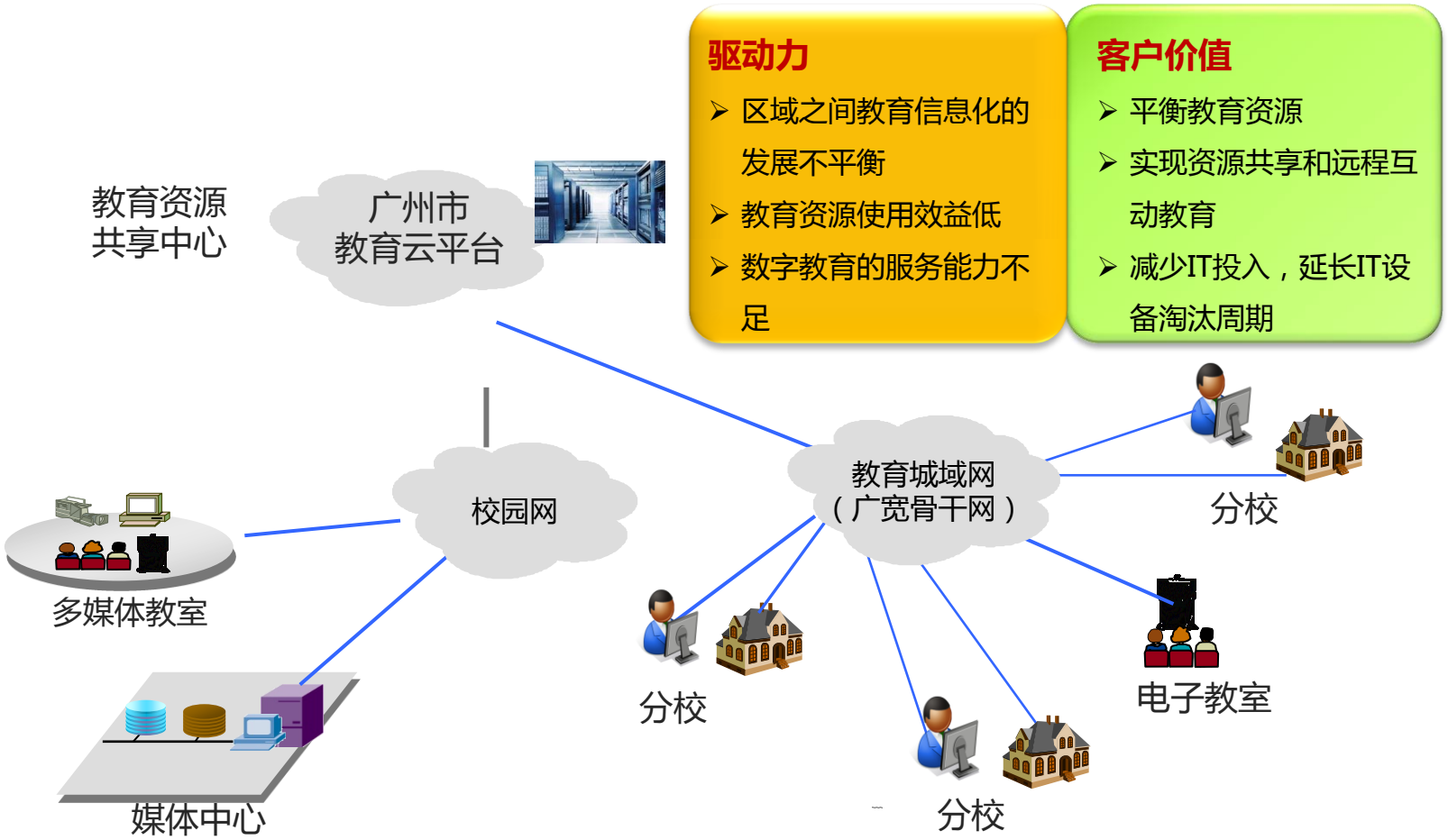
GI945

S3900

刀片服务器E6000

NE40E

成功案例—广州教育信息中心

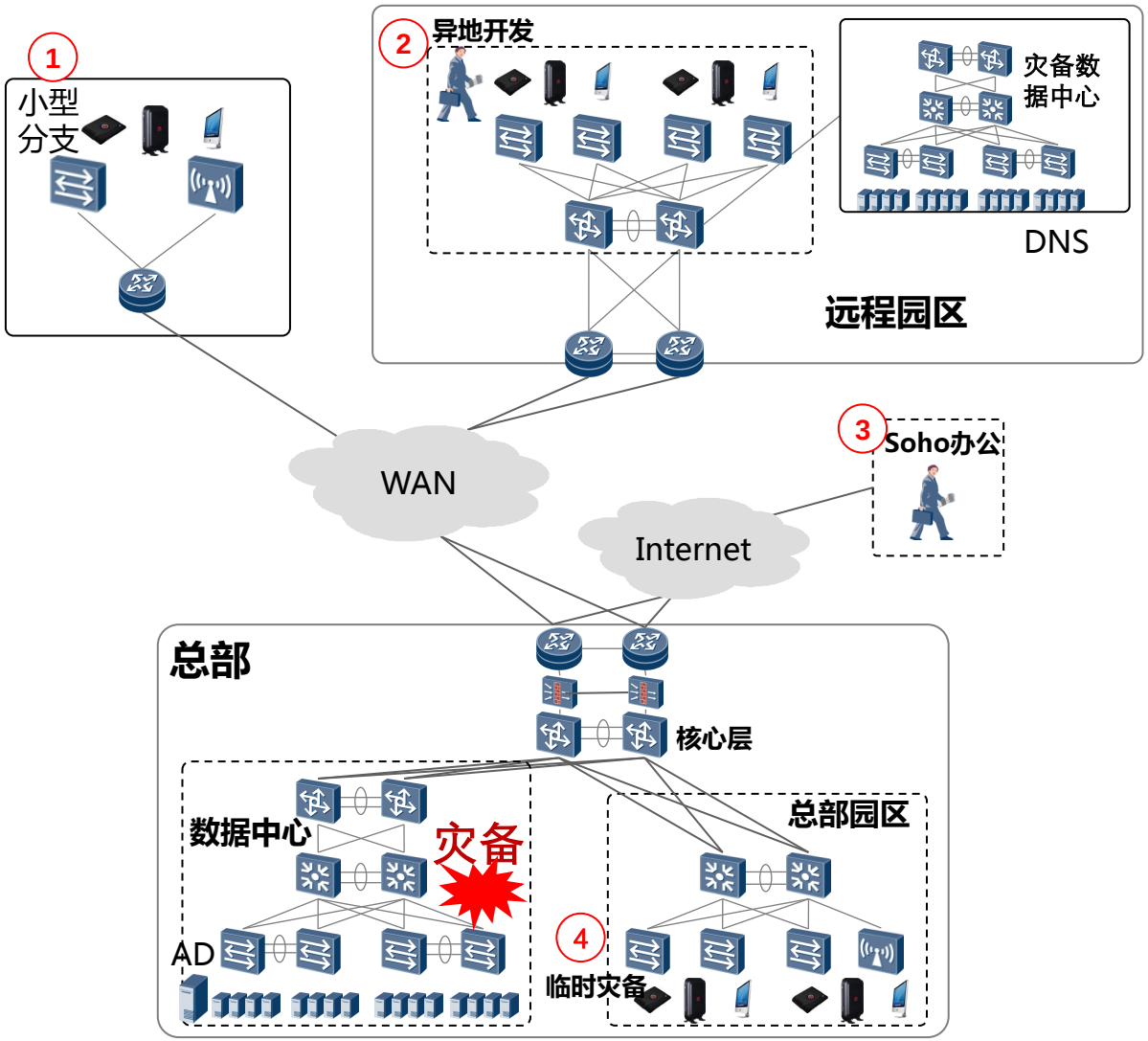


城域100公里范围内，学校部署分散，通过高速骨干网联入数据中心，完成桌面云业务承载。

广域桌面云方案

- 主要应用场景
- 流量模型设计
- 带宽设计
- 网络质量和监控设计
- 应用加速和性能路由方案设计

应用场景—广域总方案



小型分支:

一些分支，跨广域时延等质量较好网络，可访问云服务器应用桌面云。

异地开发：

出差异地园区，需要跨广域访问本部园区数据中心实现OA等桌面云应用。

Soho办公：

家里接入Internet访问数据中心应用OA办公。

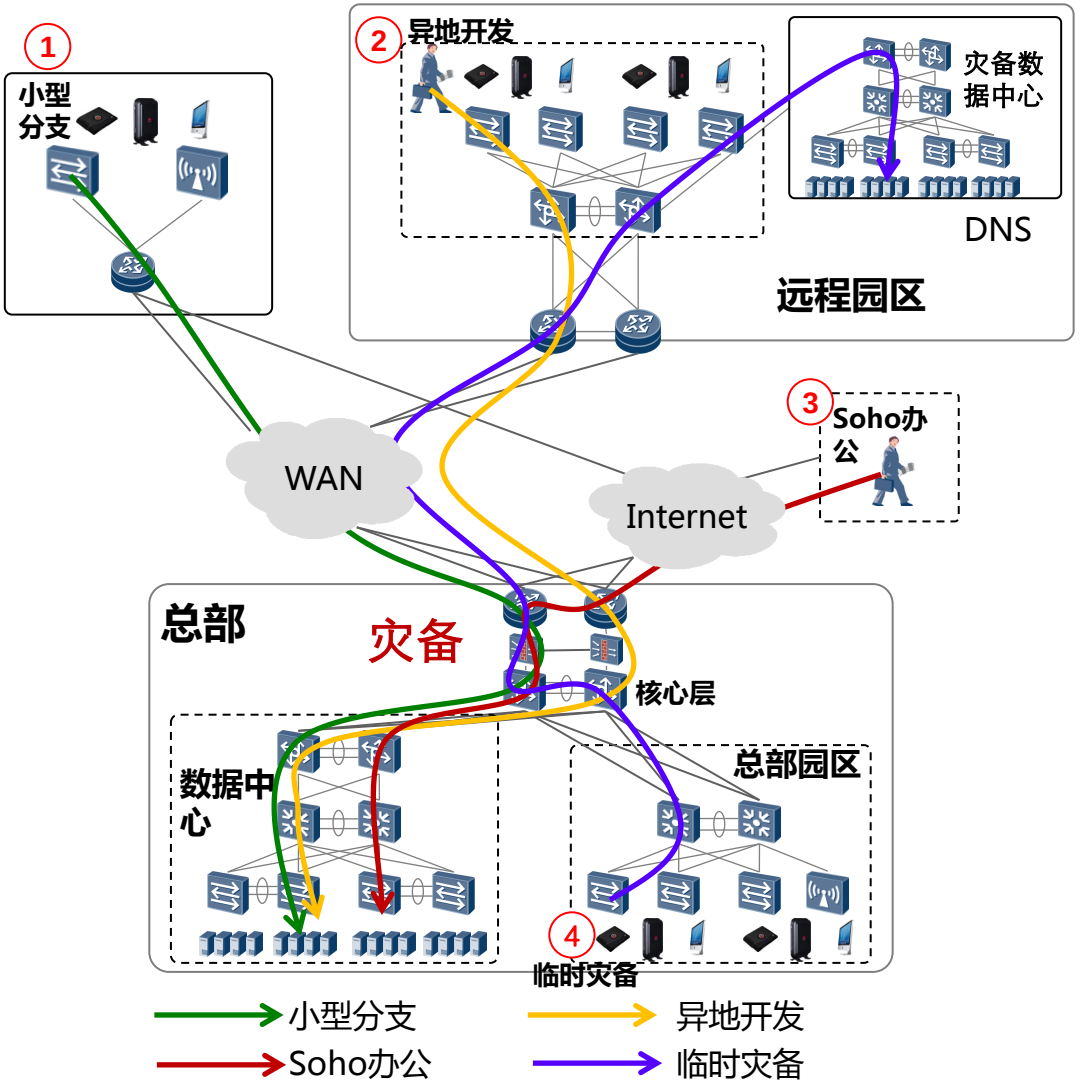
临时灾备：

本地数据中心瘫痪，远程访问灾备数据中心实现OA云办公。

应用场景—性能和业务类型

	小型分支	异地开发&灾备	Soho办公
广域接入方式	MPLS VPN/internet SSL	OTN专线、MPLS VPN	Internet 拨号接入
时延	分支距离在500公里内，MPLS VPN经过路径节点少，延迟检测100ms内;Internet SLA接入保证时延	一般大园区租用专线连接，2000公里范围时延在150ms内	通过Internet 多次中转，时延在200ms以上
带宽要求	带宽价格偏中，每用户分配5M	专线资源宝贵，每用户仅分配2M	带宽价格便宜，每用户分配10M带宽
应用类型建议	主要应用基本OA办公，含Word编辑、Excel、PPT、Notes、邮件、文档下载等；少量应用研发和图形处理	主要应用Word简单办公，可部分应用低清播放	仅应用Word等简单Office OA 办公

应用场景—广域流量模型



小型分支:

流量通过分支出口，穿越WAN或Internet广域到达园区和数据中心。

异地出差：

员工在异地园区接入，流量通过园区出口跨越WAN，到达本地园区出口和数据中心。

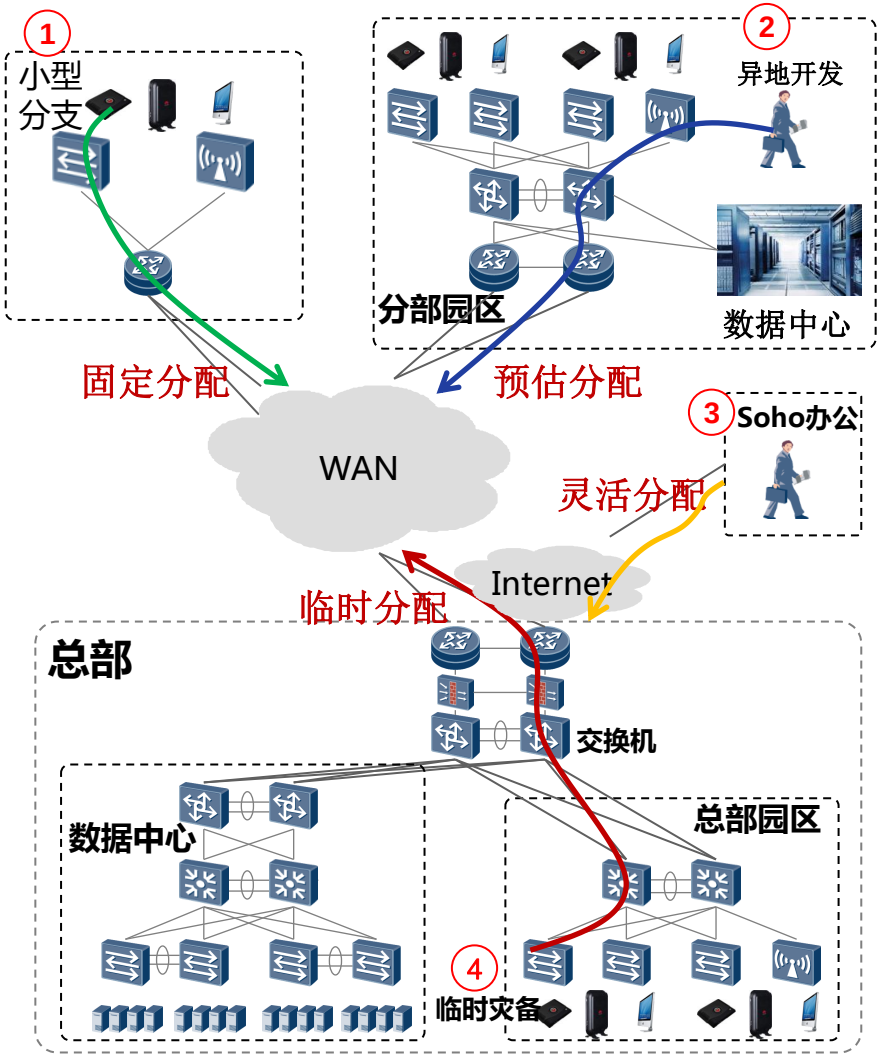
Soho办公：

家里通过Internet拨号，流量到园区出口网关，最后到达数据中心。

临时灾备：

流量通过本地园区出口，穿越WAN广域到达灾备数据。

网络质量—带宽设计



小型分支
异地开发
Soho办公
临时灾备

小型分支:

分支用户数固定，根据人数计算预留广域带宽。

异地办公：

异地办公人员动态不定，根据统计评估分配预留带宽。

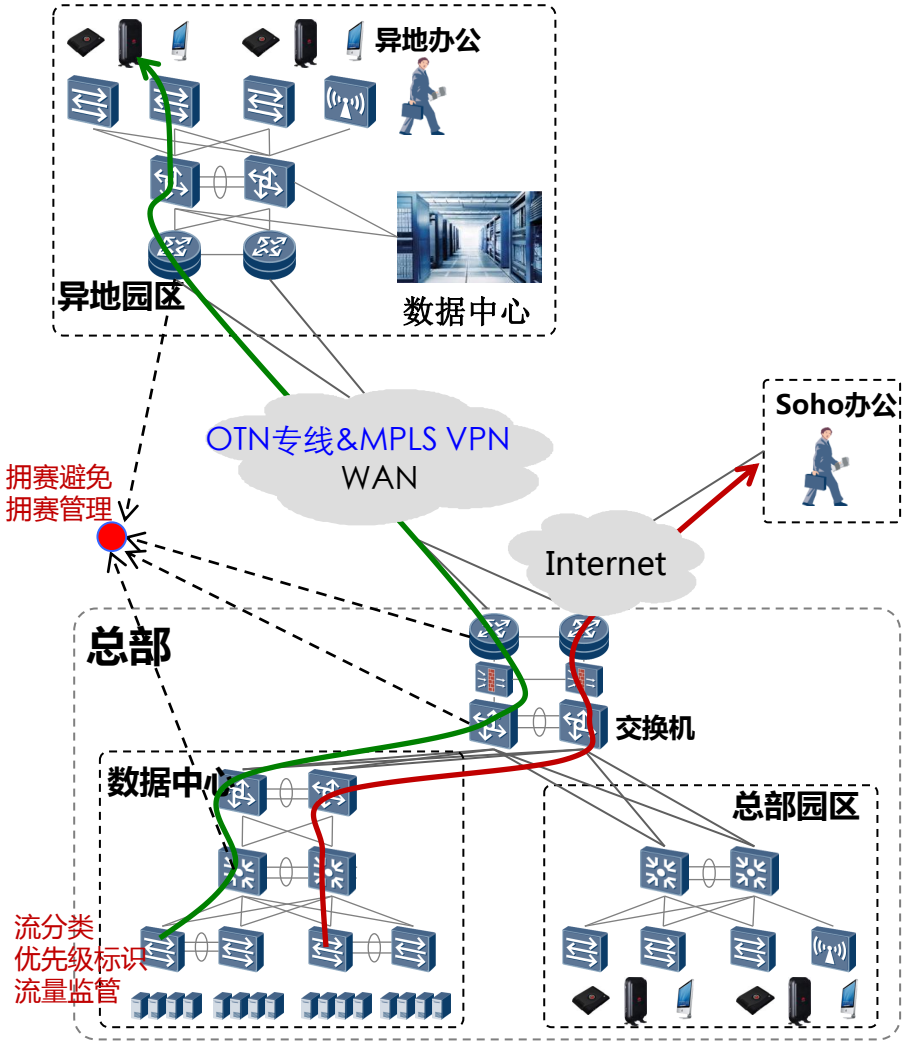
Soho办公：

根据应用业务类型灵活分配带宽，对于普通OA办公2M够用，图形应用需10M甚至更高带宽。

临时灾备：

灾备发生会有大量用户突发占用广域带宽，考虑短暂临时性，每人预留1M带宽保证普通办公应用即可。

网络质量—时延、抖动、丢包率以及监控诉求



异地园区或分支（穿越WAN）：

接入层云业务优先级级标识，路径设备拥塞避免和管理，保证云业务低时延、丢包率和抖动。

广域MPLS VPN时延高，应用普通办公业务； 短距离OTN专线时延低，可应用高清图形业务。

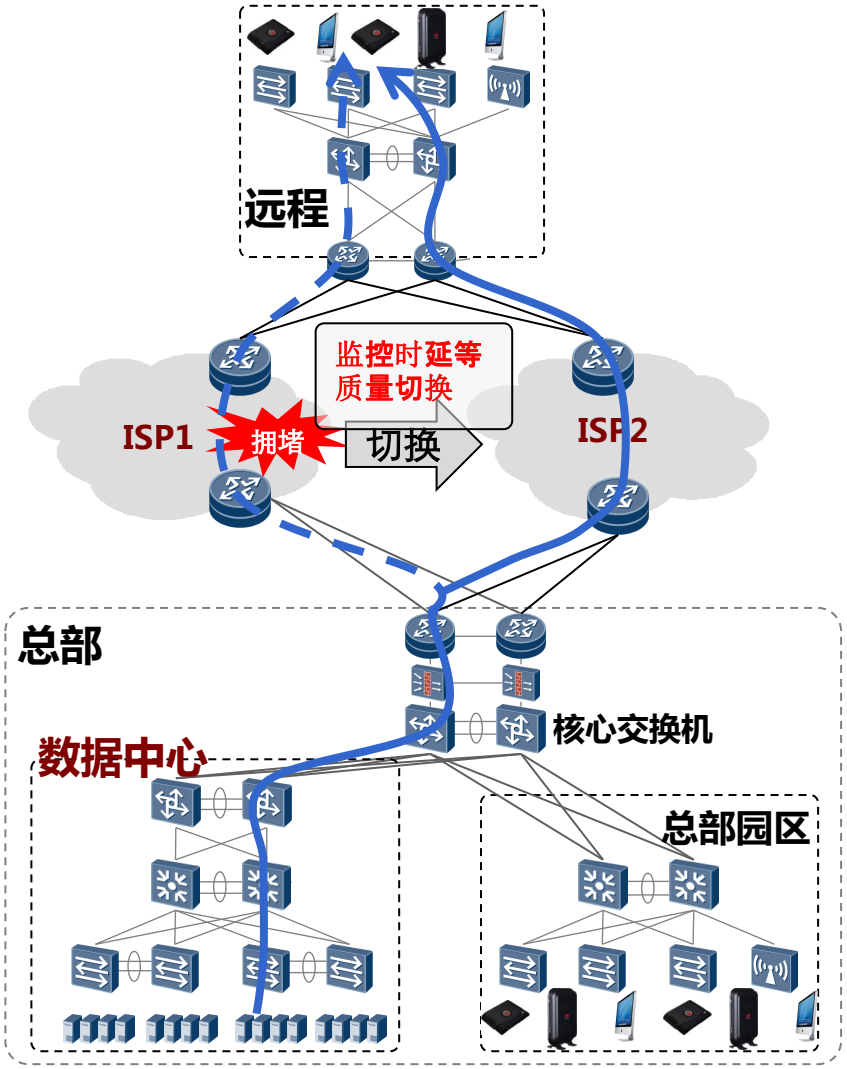
硬件探针测量和分段显示数据中心、WAN广域（黑盒）和异地园区网络质量。

Soho办公(穿越Internet)：

家中办公Internet网络质量无法保障，时延等质量会较差，建议仅应用基本OA办公业务。

硬件探针测量和分段显示数据中心到出口网络质量，Internet广域无法测量。

广域出口设计—性能路由



应用场景:

桌面云部署在分支，租用两个ISP跨广域访问数据中心，主选ISP1链路发生拥堵，造成云业务时延较长。

解决方案：

性能路由可指定云流量，实时监控时延等网络质量，如果不符合要求则智能切换ISP出口。

性能路由部署在AR出口。

竞争力—全方位解决方案

服务器、终端、承载网络全方位解决方案

华为桌面云提供端到端方案

华为桌面云提供包括终端、数据中心服务器及承载网端到端解决方案，能够满足各种桌面云应用场景（包括OA集中办公、城域营业厅和广域）。

承载网全方位技术

华为桌面云承载网络通过QOS部署、层次化可靠技术、带宽限制、网络监控、AD安全认证等全方位网络技术方案。

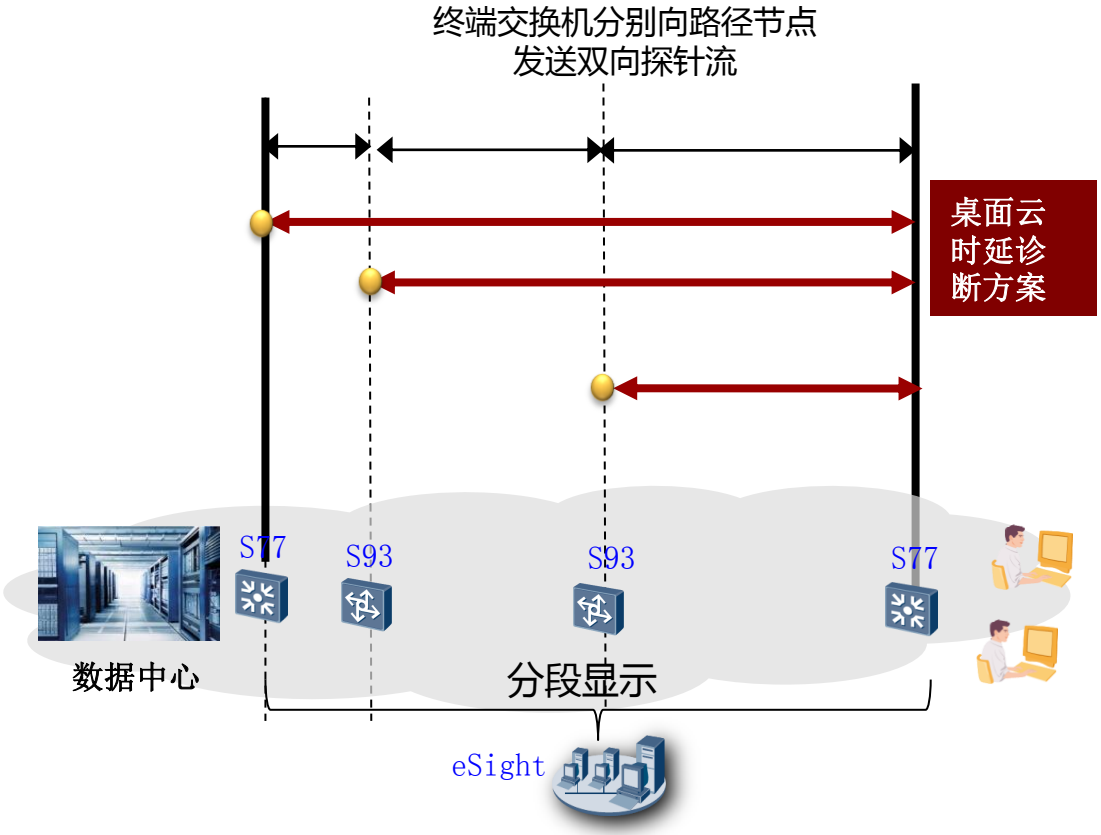
竞争力—承载网亮点

我司亮点	其它厂商情况
ME60产品汇聚层带宽限制。	Cisco、H3C均无此方案
BFD、以太OAM硬件探针发包，链路故障发现精度到3.3ms。	Cisco、H3C等软件发包，链路故障延迟发现
全路径分段显示云流量时延，抖动，丢包率质量，颗粒化管理，快速故障定位。	Cisco、H3C均无此方案

基础技术介绍

- 网络质量监控技术介绍
- QoS部署技术介绍
- 桌面云可靠性协议选择一览表
- CSS/iStack无环技术介绍

网络质量监控技术—时延



应用场景:

桌面云ICA基于TCP协议与数据中心通信，TCP属于双向协议，如果双向时延过大，给客户带来鼠标、键盘反映迟钝，桌面体验差等问题。

解决方案：

终端交换机发送TCP硬件探针进行双向时延测试，

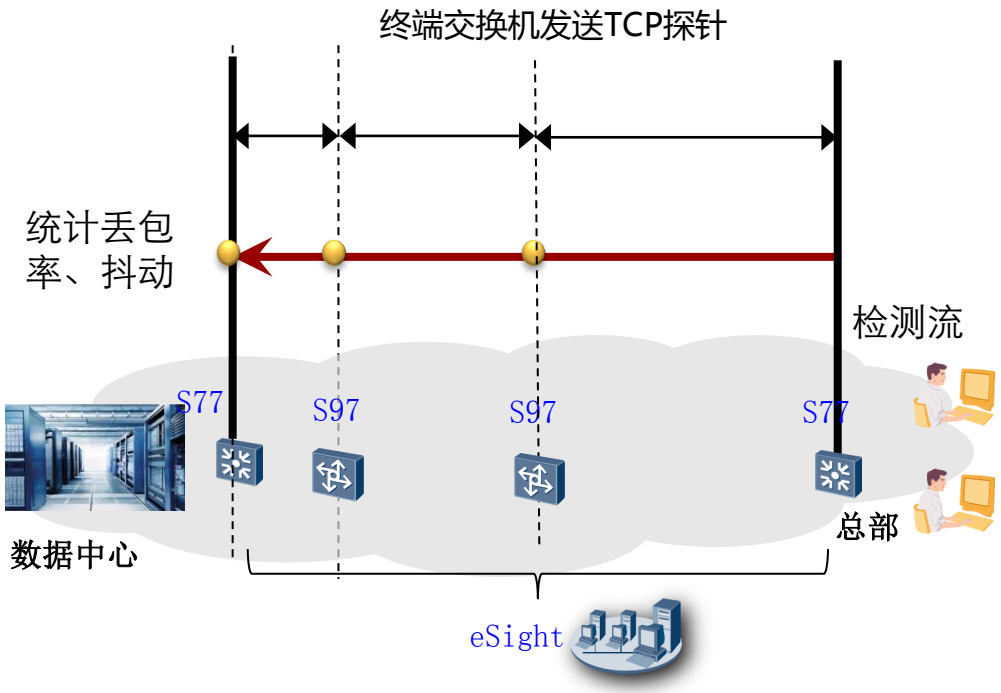
路径节点返回NQA报文，

网管时延故障分段显示。

客户价值：

全路径时延逐段故障显示，可快速修复故障。

网络质量监控技术—丢包、抖动



应用场景:

业务基于TCP协议，丢包需报文重传， 导致ICA显示卡顿。目前缺乏丢包率障定位手段。

解决方案：

终端交换机发送TCP硬件探针流，

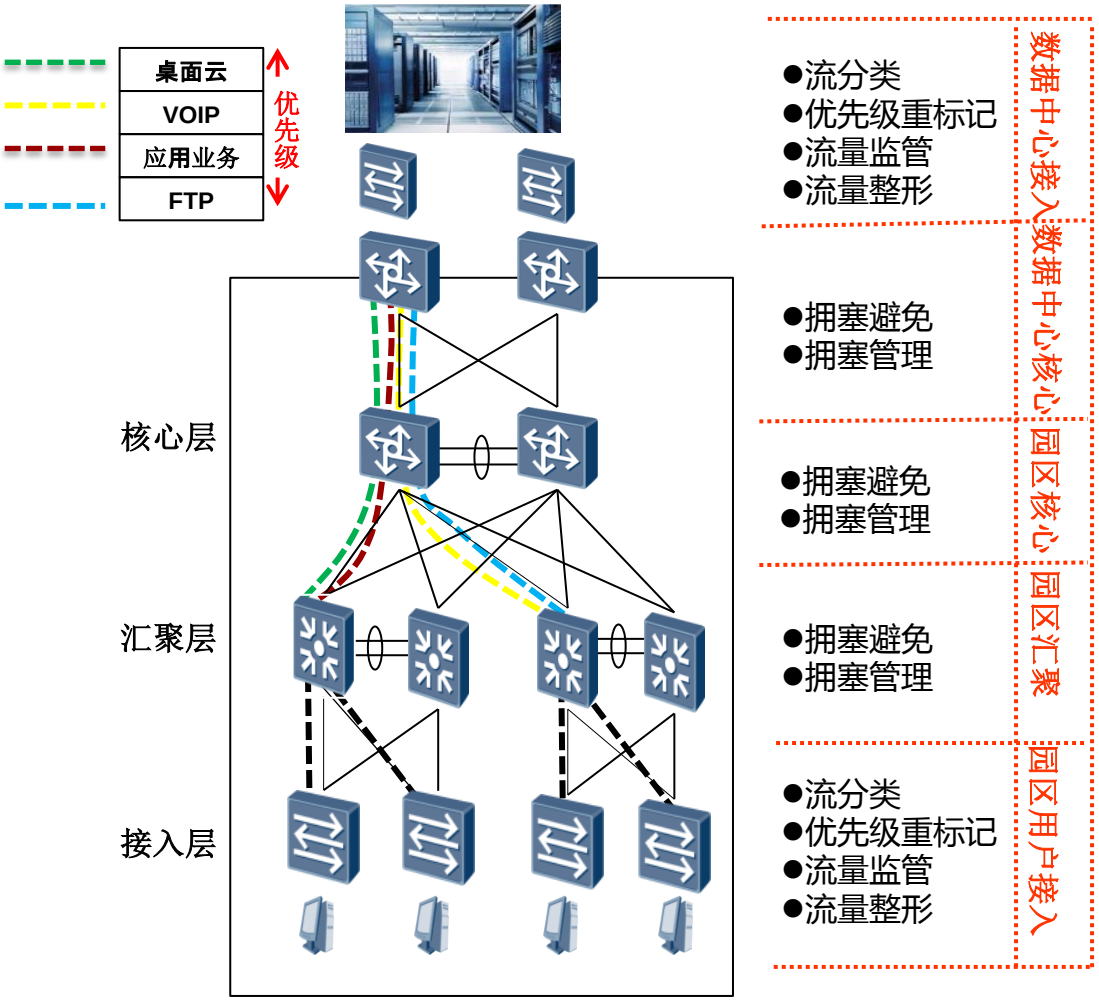
路径节点对丢包率统计，

网管收集统计并分段显示

客户价值：

全路径丢包率故障分段显示，可快速修复故障。

QoS部署技术



QoS方案描述：

园区接入交换机对业务进行流分类，并为业务流进行优先级重标记，为园区网业务流的流量策略提供依据。

园区汇聚、核心交换机依据桌面云的优先级标记，采用信任优先级标记模式进行QOS拥塞避免和管理，优先保证桌面云业务传输。

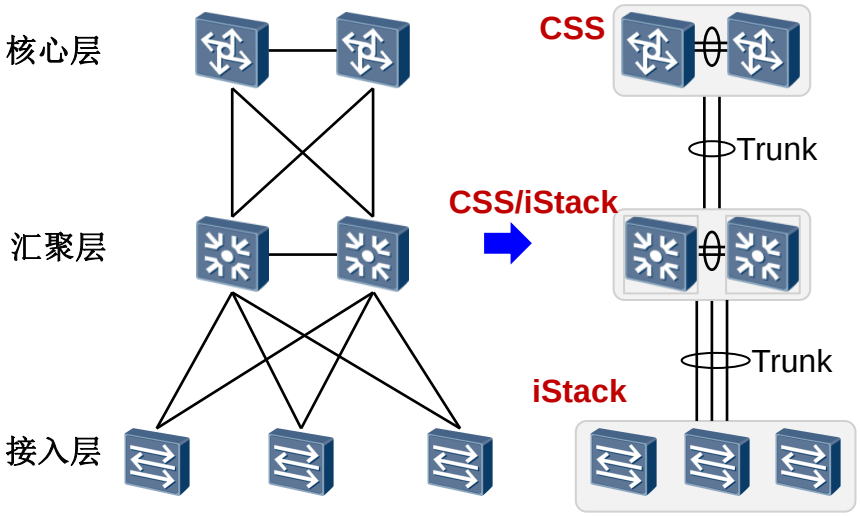
数据中心下行流量同理采用QOS策略部署。

方案特点：

网管能够全路径可视DSCP值，快速定位QoS部署实效。

网管支持模板批量部署。

CSS/iStack无环技术



高可靠的物理和逻辑拓扑

可靠性方案：

2-3台接入层堆叠，2台汇聚层集群，2台核心交换机集群。

设备可靠性保证：

采用堆叠/集群技术，一台设备故障后，另外一台设备自动接管所有业务。

链路可靠性保证：

采用Trunk技术，一条链路故障后，流量自动切换到其他绑定链路。

桌面云业务收敛：

收敛速度达到10ms内，故障发生云用户无缝体验。

桌面云可靠性协议选择

故障发生后，桌面云办公期望100ms内恢复

可靠性方案	收敛或故障发现时间	桌面云是否采用	推荐我司产品
STP/MSTP	30000ms	不采用	
CSS/Istack	10ms	可采用	S5700
RRPP	40ms	可采用	S5700
硬件以太OAM	10ms	可采用	S5700
硬件BFD	10ms	可采用	S9700/7700/5700/AR/NE系列
软件BFD	120ms	不采用	
主备倒换	60000ms	不采用	
GR/NSR	0ms	可采用	S9700/7700/AR/NE系列
IPFRR	30ms	可采用	S9700/7700/AR/NE系列
性能路由	20ms	可采用	AR/NE系列

子目录

4 园区网业务解决方案

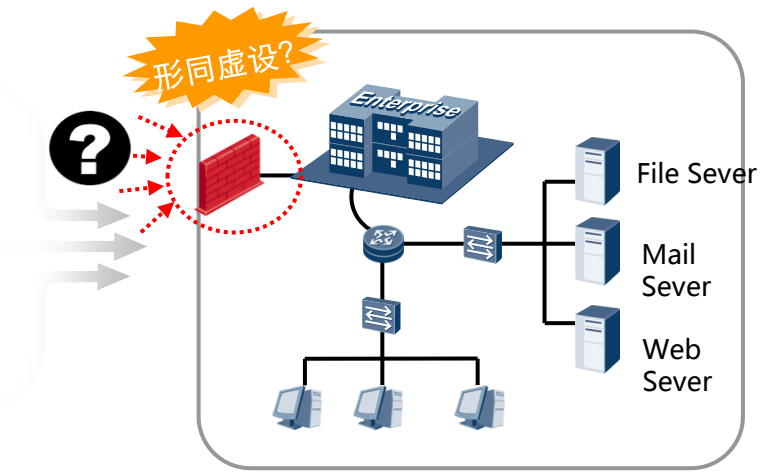
目录

绝大部分安全威胁源于内网

随着企业信息化建设的不断深入，网络安全基础设施也日渐成为企业网建设的重点。在传统的网络建设思路中，一般认为企业内网是安全的，而安全威胁主要来自外界，事实上，绝大多数威胁来自内网。

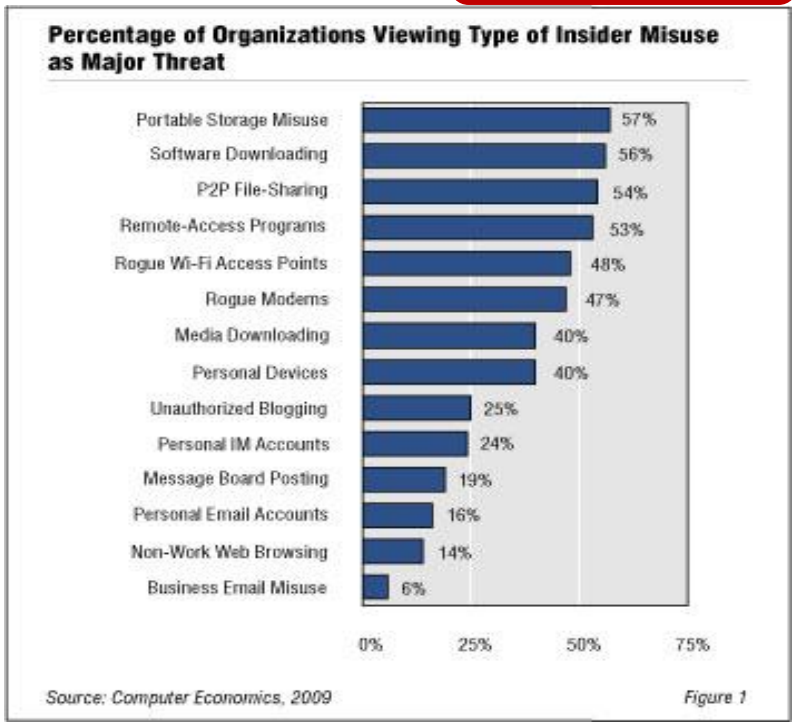
CSI COMPUTER SECURITY INSTITUTE

根据加利福尼亚州旧金山的计算机安全协会(CSI)的观点，大约60%到80%的网络滥用事件起源于内部网络。



computer economics

14种不容忽视的企业内部安全威胁



园区内网安全分析


信息泄密 引发巨额损失
无关应用 影响工作效率
腾讯QQ
证券大智慧
GW.COM.CN
单点感染 内网威胁扩散
内部员工 越权访问资源
研发
财务
市场
内网安全
危机四伏
海量终端 难以统一管理
魔兽世界
补丁加载、非法软件

园区内网安全应对方案

以用户准入控制为基础，以安全管理为辅助，结合补丁管理、软件分发、行为管控、资产管理和移动存储介质管理等组件，构建一体化的终端安全NAC解决方案。
NAC：Network Admission Control，狭义的NAC指网络准入控制方案。

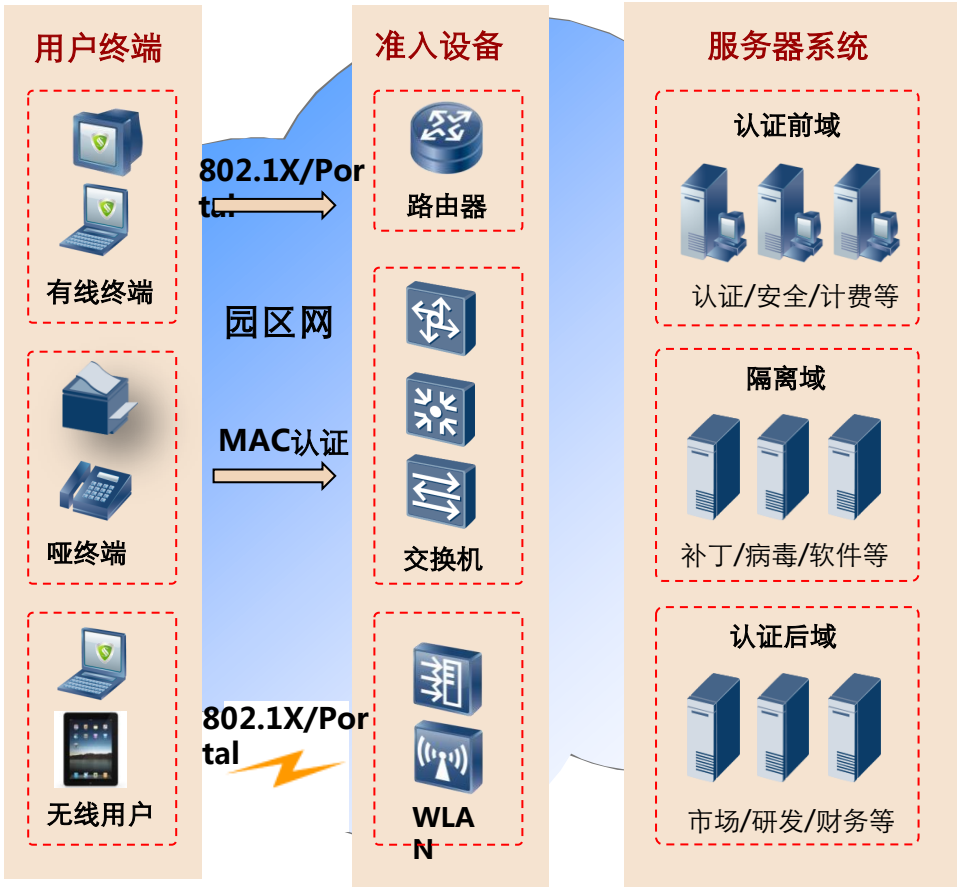
终端NAC解决方案功能组件简介

NAC组件	主要功能描述	备注
准入控制	包括用户用户接入认证、权限管理、访客管理等内容内容。支持MAC、802.1X、Portal、PPPoE等接入认证和相关统计报表。	必选
安全管理	包括终端健康检查、安全加固、自定义安全策略等内容，自定义策略可指定检查项，定制终端提示信息和违规上报信息，定制自动修复动作等策略。	可选
补丁管理	支持分布式补丁分发、断点续传，帮助内网主机及时更新OS、Office、DB、IE等系统补丁，并可和微软WSUS无缝集成。	可选
软件分发	支持分布式软件分发、断点续传，统一维护分发内容，有效分担网络流量，平衡负载，同时提供软件分发报告。	可选
行为管控	包括终端上线记录、上网行为审计、非法外联监控等，防止信息泄密。	可选
资产管理	通过客户端和资产管理服务器联动，支持资产注册、资产信息采集和资产变更告警等功能，进行企业资产生命周期管理。	可选
移动存储介质管理	通过对U盘、移动硬盘等移动存储机制进行注册、加密、读写权限控制等，对企业使用的USB移动存储介质进行安全管理	可选

NAC解决方案从功能划分来看，包括准入控制、安全管理、补丁管理、软件分发、行为管控、资产管理等组件，除准入控制为必选外，其他功能组件可按需选择。

目录

NAC安全系统架构



NAC系统框架中包括三个关键部分：用户终端、准入设备和服务器系统。

用户终端

用户终端可通过MAC、802.1X、Portal等认证方式接入网络，如果装有专用客户端，可与服务器联动做安全检查。对于不能安装客户端的设备，如打印机、IP电话等，称为哑终端。

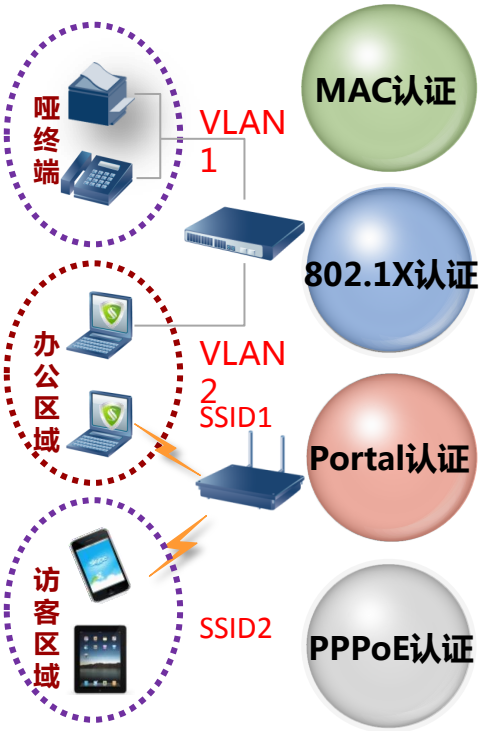
准入设备

网络准入设备是终端访问网络的控制点，基于准入了控制服务器给出的授权策略，控制用户可以访问企业内部资源（认证后域）。

服务器系统

服务器区域包括认证前域、隔离域、认证后域三部分，分别完成用户认证、软件管理、部门资源管理等功能。

用户接入认证技术



MAC认证

用户终端以MAC地址作为身份凭据到认证服务器进行认证

主要用于IP电话、打印机等哑终端设备

802.1X认证

使用EAP（Extensible Authentication Protocol）认证协议，实现客户端、设备端和认证服务器之间认证信息的交换。

需客户端支持，安全性高，园区网主推方案。

Portal认证

也称为WEB认证，用户可以通过Web认证页面，输入用户帐号信息，实现对终端用户身份的认证。

无需客户端，安全性稍低，广泛应用于园区网中。

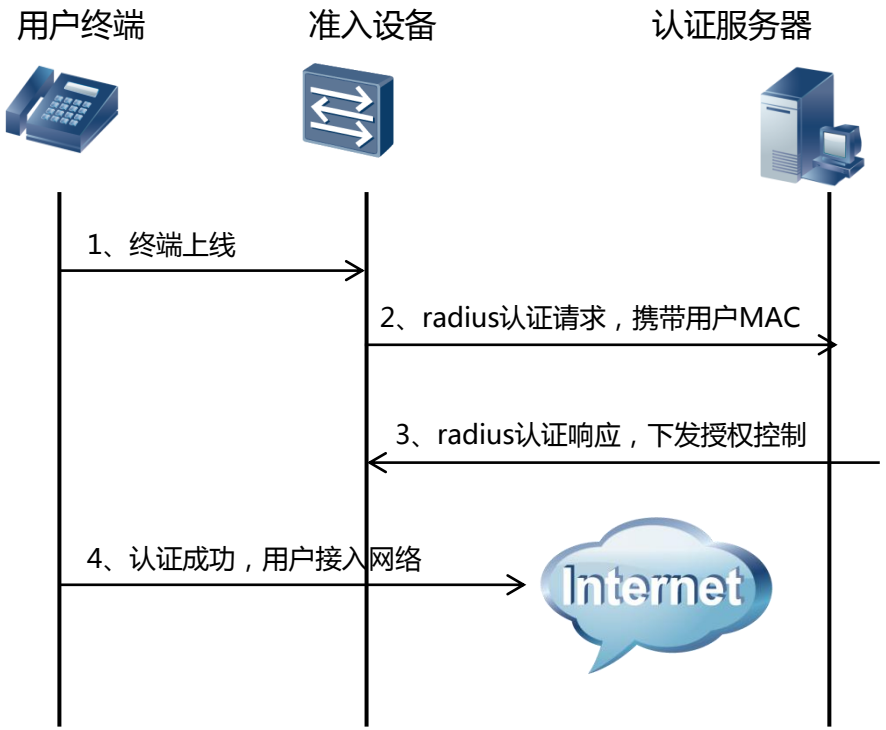
PPPoE认证

PPPoE实现广播链路上点对点通讯的协商，用户通过拨号软件输入用户信息，到远端服务器进行认证。

需客户端支持，一般用于运营商网络，企业网不推荐使用。

如上图，哑终端一般通过MAC认证接入，办公区域通过802.1X或Portal认证接入，访客区域一般通过Portal认证接入，多种认证技术保证用户终端安全接入，合法用户访问合规资源，从源头上消除安全威胁。

MAC认证流程



MAC认证介绍

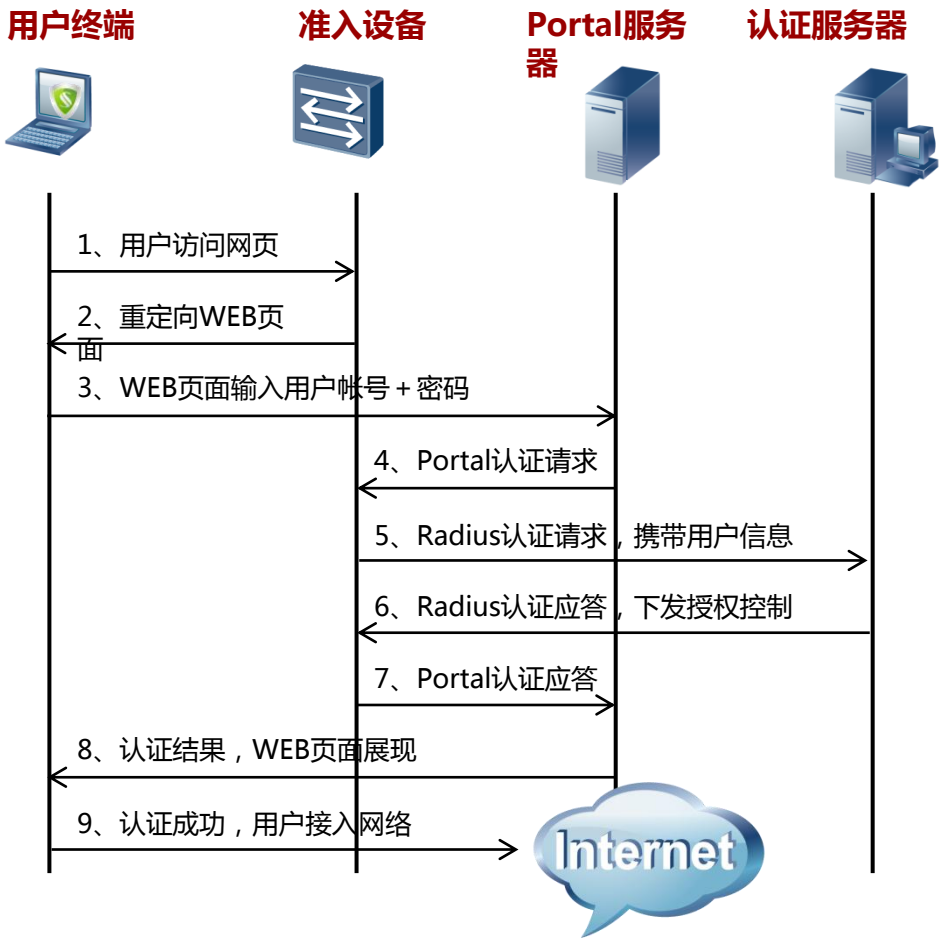
MAC认证就是以终端的MAC地址作为身份凭据到系统进行认证。启用MAC认证后，当终端接入网络时，网络准入设备提取终端MAC地址，并将该MAC地址作为用户名和密码进行认证。

应用场景

哑终端设备，如打印机、IP电话等，无法通过输入用户帐号信息的方式进行认证授权。

对某些特殊用户，希望“免认证”接入网络，用户不想通过输入用户帐号信息的方式完成认证，比如智能终端用户。

Portal认证流程



Portal认证介绍

也称为WEB认证，用户可以通过Web认证页面，输入用户帐号和密码信息，实现对终端用户身份的认证。用户访问认证页面的过程，可以采用主动访问页面和被动访问页面即强推的方式来实现。

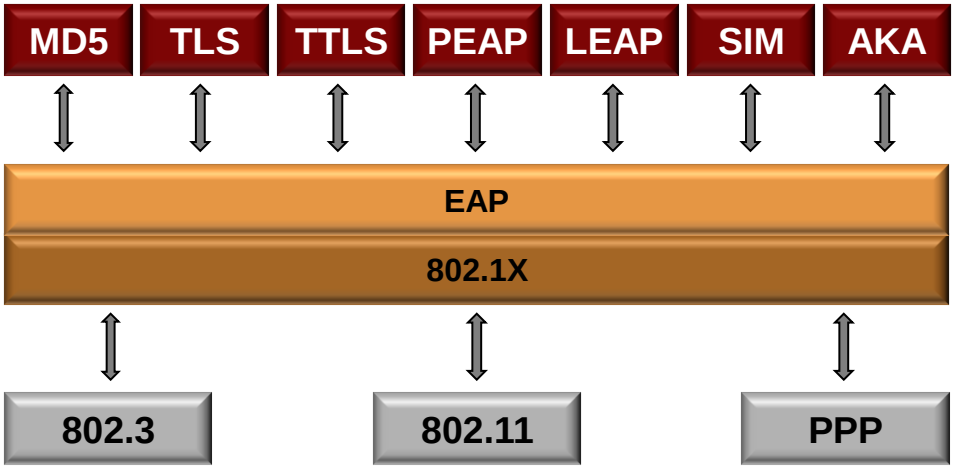
应用场景

Portal认证无需客户端支持，部署简单，广泛应用于园区网中。

用户部署NAC安全管理组件，需要客户端支持，此时可采用具有客户端的Portal认证方式。

802.1X认证简介

802.1X 协议起源于WLAN的802.11协议，用于控制无线用户的链路层接入和身份认证。经过扩展后，802.1X也可以使用以太网帧作为承载报文，可适用于以太网以及其他的有线接入方式。



EAP – Extensible Authentication Protocol
PPP – Point-to-Point Protocol

802.1X应用链路

802.1X是一种链路层认证框架，包括客户端、准入设备和认证服务器三部分。

802.1X认证类型

802.1X可承载链路层协议包括有线以太网（802.3）、无线WLAN网络（802.11）或者其他链路层协议如PPP网络等。

802.1X认证类型

802.1X认证使用EAP作为认证协议，用来传输认证信息。

目前常用认证类型有EAP-MD5、EAP-TLS、EAP-TTLS、EAP-PEAP、EAP-LEAP、EAP-SIM、EAP-AKA等。

802.1X认证类型

EAP-MD5 (Message Digest 5)

EAP-MD5使用MD5算法对用户密码和加密字（Challenge）生成消息摘要，到服务器完成用户认证过程。由于需要输入用户名和口令，本方法容易受到字典攻击，但配置简单，广泛用于园区网络。

EAP-TLS (Transport Layer Security)

EAP-TLS使用了双向认证，客户端和服务器均拥有证书并进行相互间的身份证明。EAP-TLS使用证书提高了安全性，但同时也意味着需要进行繁琐的证书管理。

EAP-TTLS (Tunneled Transport Layer Security)

EAP-TTLS是EAP-TLS的增强版本，只需要服务器端证书。TLS隧道建立后，采用用户名和密码进行认证。

EAP-PEAP (Protected Extensible Authentication Protocol)

EAP-PEAP与EAP-TTLS类似，主要指EAP-MS-CHAPv2。服务器端需要提供证书，客户端使用用户名和密码进行用户身份验证。

EAP-LEAP (Lightweight Extensible Authentication Protocol)

Cisco在2000年推出的基于Windows登录的用户名、密码认证专有技术，LEAP不需要证书。

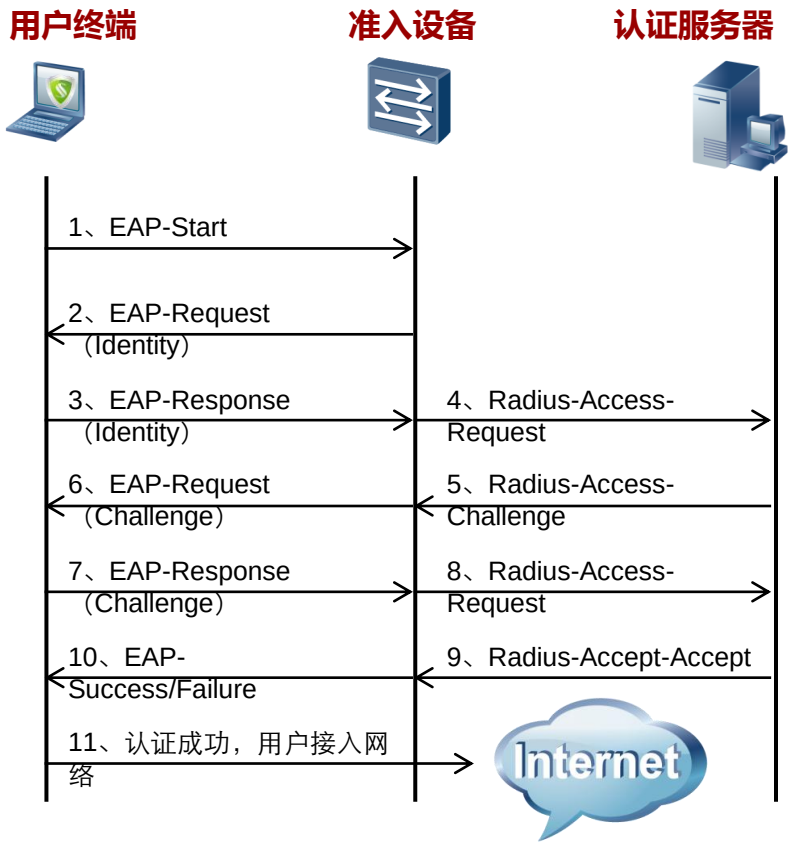
EAP-SIM (Subscriber Identity Module)

EAP-SIM认证机制提供基于GSM-SIM卡的认证和密钥分发机制，在GSM单向认证基础上，提供双向认证，一般用于运营商网络。

EAP-AKA (Authentication and Key Agreement)

EAP-AKA是用来在使用 USIM卡接入3G通信网络时，用户进行认证和密钥协商的方案，用于运营商网络。

802.1X认证流程



不同认证类型的802.1X认证流程差异较大，下面以EAP-MD5为例简要说明一下流程。

用户名上送

流程1～4，用户在客户端输入用户名和密码，其中用户名上送认证服务器处理。

生成Challenge挑战字

流程5～6，认证服务器收到用户名后，若数据库存在改用户名，则生成挑战字Challenge，并通知客户端。

用户密码上送

流程7～8，客户端使用MD5算法，使用Challenge对密码加密，并上送服务器。

认证成功授权

流程9～11，服务器收到用户密码（MD5）后，进行验证，符合要求后开放用户权限，用户接入网络。

接入认证技术比较

结合WLAN无线安全协议WEP/WPA/WPA2/WAPI等，认证技术比较如下：

认证方法	安全协议	安全性	封装开销	地址分配	客户端软件	应用场景
MAC认证	Open System	低	小	认证后分配	不需要	手持PDA、IP电话等哑终端设备
	WEP/WPA/WPA2+PSK	低	小	认证后分配	不需要	场景同上，需要维护PSK密码
Portal认证	Open System	中	小	认证前分配	不需要	中小型园区网络
	WEP/WPA/WPA2+PSK	中	小	认证前分配	不需要	场景同上，需要维护PSK密码
802.1X认证	WEP/WPA/WPA2	高	小	认证后分配	需要	大中型园区网络
PPPoE认证	Open System	低	大	认证后分配	需要	运营商市场
	WEP/WPA/WPA2+PSK	低	大	认证后分配	需要	场景同上，需要维护PSK密码

上表中，对于有线用户，则不涉及WLAN安全协议，对应Open System一行表述。

对于无线用户，当前WAPI在企业或者运营商网络应用很少，一般作为准入门槛测试。

园区网中，从从安全性和易部署性等多方面考虑，推荐有线网络采用802.1X认证，无线网络采用802.1X + WPA2的机制，访客区域Portal认证，哑终端场景MAC认证。

【相关无线WEP/WPA/WPA2等协议介绍请参见园区网WLAN专项方案】

服务器安全域划分

服务器网络资源划分为不同的逻辑安全域，系统根据终端用户身份认证和安全检查的结果，开放不同的访问权限，实现对违规终端的隔离，从而保证企业内网的整体安全性。

认证前域

终端在身份认证和安全检查通过前能够访问的网络资源，包括AAA、DHCP、DNS等服务器。

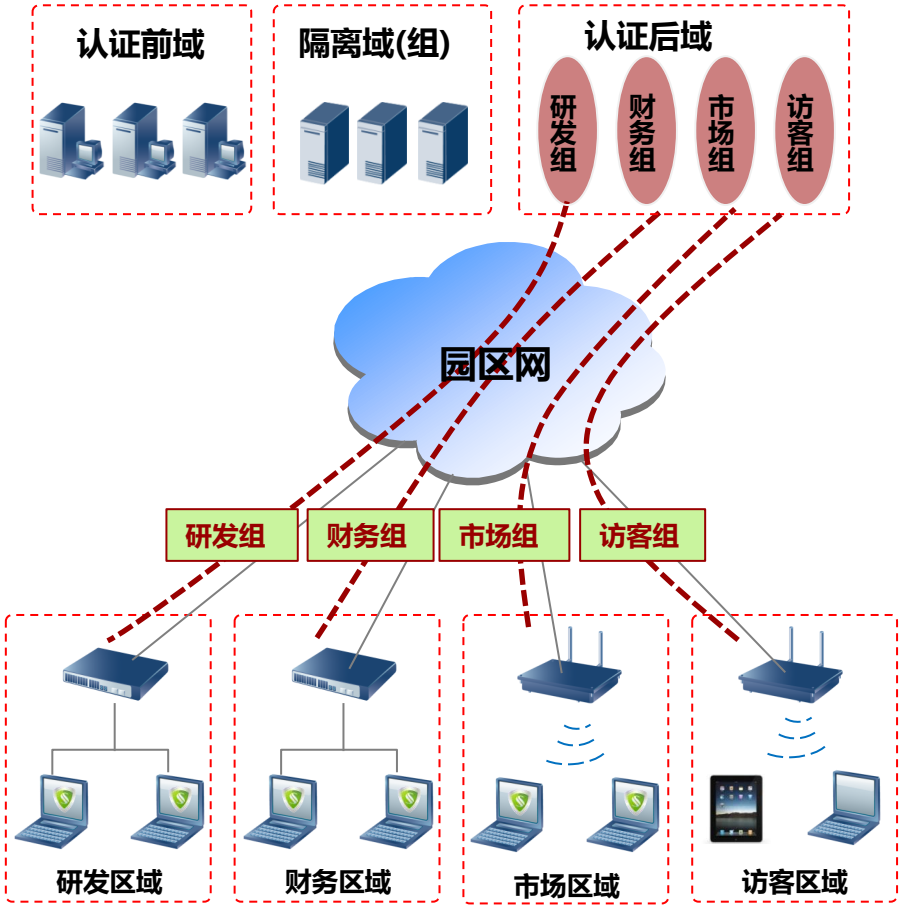
隔离域

终端已经通过身份认证，但安全检查发现违规项，此时仅能够访问隔离域进行安全修复操作。隔离域包括补丁、病毒、软件等服务器。

认证后域

终端在通过身份认证和安全检查后能够访问的网络资源。管理员可根据市场、研发、财务等划分业务服务器，不同部门的用户只能访问对应的区域服务器。

用户组基本概念



用户组概念

用户组是指具有相同角色、相同权限等属性的一组用户（终端）的集合。例如，园区网中可以划分研发组、财务组、市场组、访客组等用户组，对于不同用户组可授予不同权限。

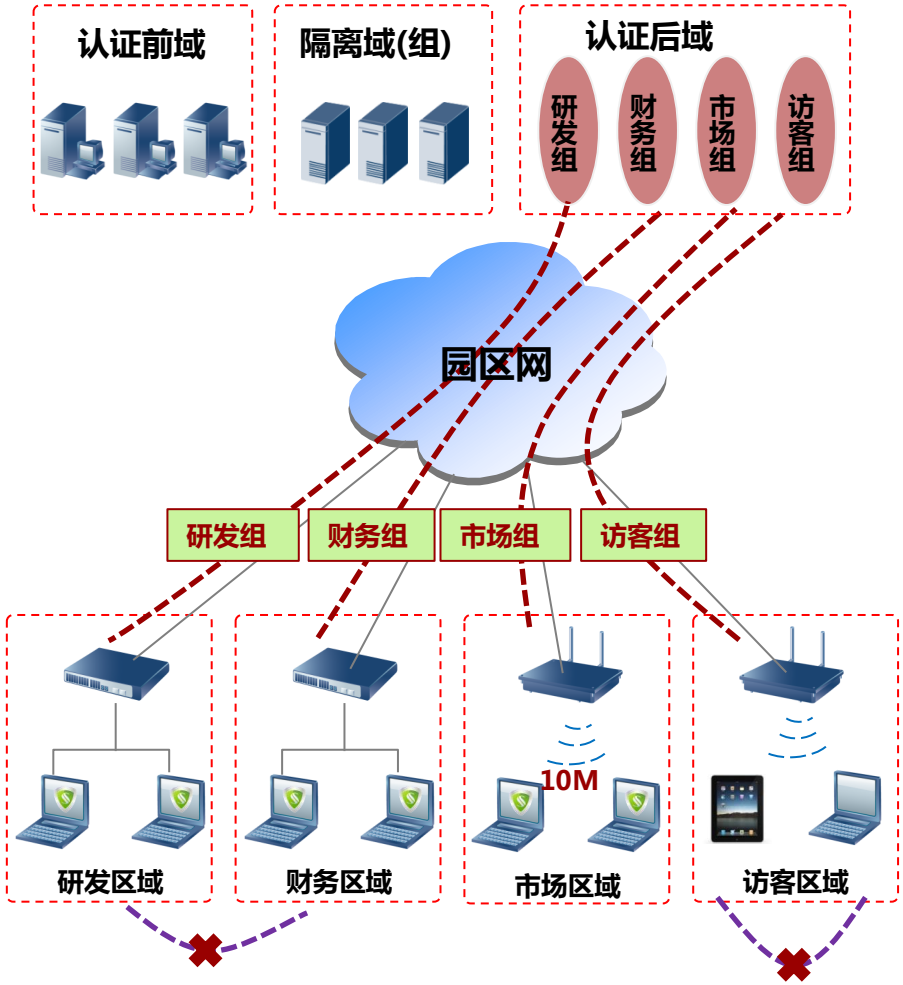
基于用户组管理用户

认证服务器基于用户组管理用户。在园区网服务器资源规划中，可以基于不同的用户组划分认证后域服务器资源。

基于用户组授权策略

在NAC方案中，认证服务器可以直接下发用户组名称到准入设备上。对于第一个用户，准入设备基于配置的用户组属性，下发安全策略，后续同一用户组用户上线，认证通过后直接加入对应用户组即可，方便NAC部署。

基于用户组的精细化策略控制



基于用户组策略部署

（1）研发组和市场组间隔离，限制研发人员和市场人员互访；

（2）市场组每用户限速10M，其他组不做限速；

（3）访客组内用户进行二层隔离，限制二层互访；

（4）各部门组需要保证较高安全，进行访问权限控制，只能访问对应特定服务器。

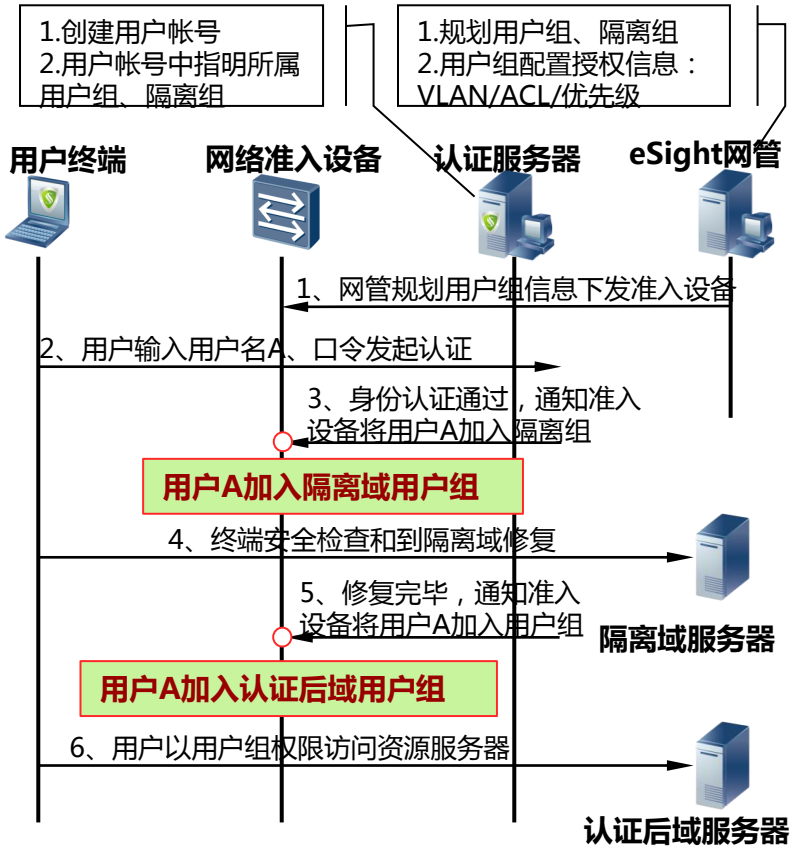
客户价值

（1）基于用户组策略控制机制 ，授权ACL基于用户组下发，多用户共享，节省ACL资源

（2）认证服务器通过下发用户组名称控制用户权限，方便NAC部署。

（3）对于无线用户授权到AP，提供业界最细粒度的用户策略控制能力。

基于用户组的策略控制流程



用户组配置

流程1。用户组需要在网络准入设备上配置，包括优先级（Remark）、授权ACL、授权VLAN等属性，可通过网管批量下发到准入设备上。

隔离组权限下发

流程2～4。用户认证通过后，认证服务器可下发隔离组权限，终端访问隔离域资源进行补丁、病毒库等软件修复。

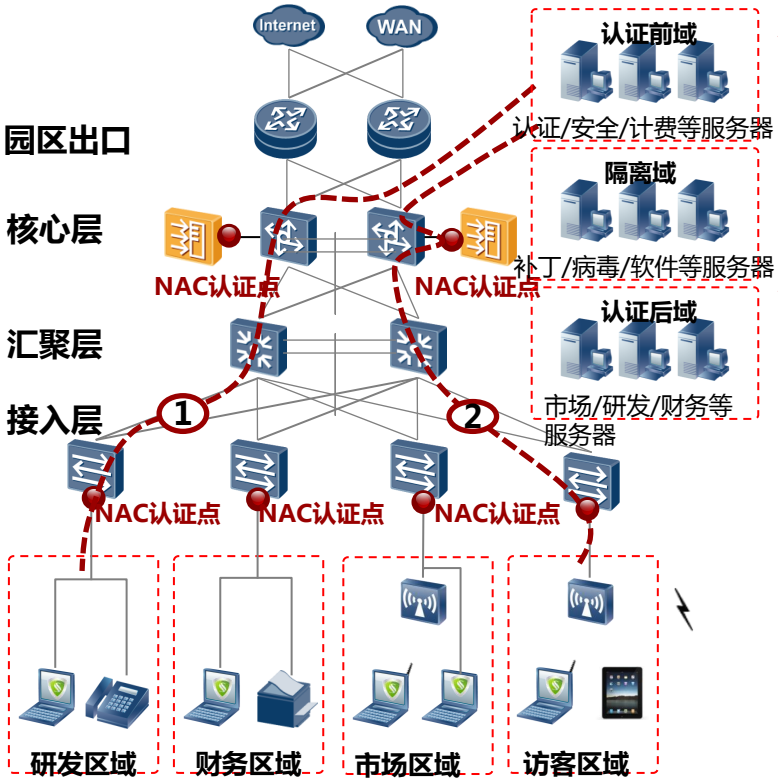
用户组权限下发

流程5～6。隔离域修复完毕，则认证服务器下发对应用户组（如研发组、市场组等）的权限，从而用户可以访问认证后域资源。

用户组可指定VLAN和Remark在2012Q4交付

目录

园区网NAC方案一：接入层802.1X认证



应用场景

本方案适于大、中、小型园区，特别是用户对于安全控制要求严格的场景，可选择在接入层部署802.1X + MAC混合认证方式。

方案部署

（1）接入层交换机启用802.1X + MAC自适应混合认证，有线用户做802.1X认证，IP电话、打印机等哑终端MAC认证。

（2）对于无线用户，AC设备启用802.1X认证，无线终端通过802.1X认证接入园区。

（3）服务器系统为TSM服务器组件，基于用户组进行用户管理和权限控制。

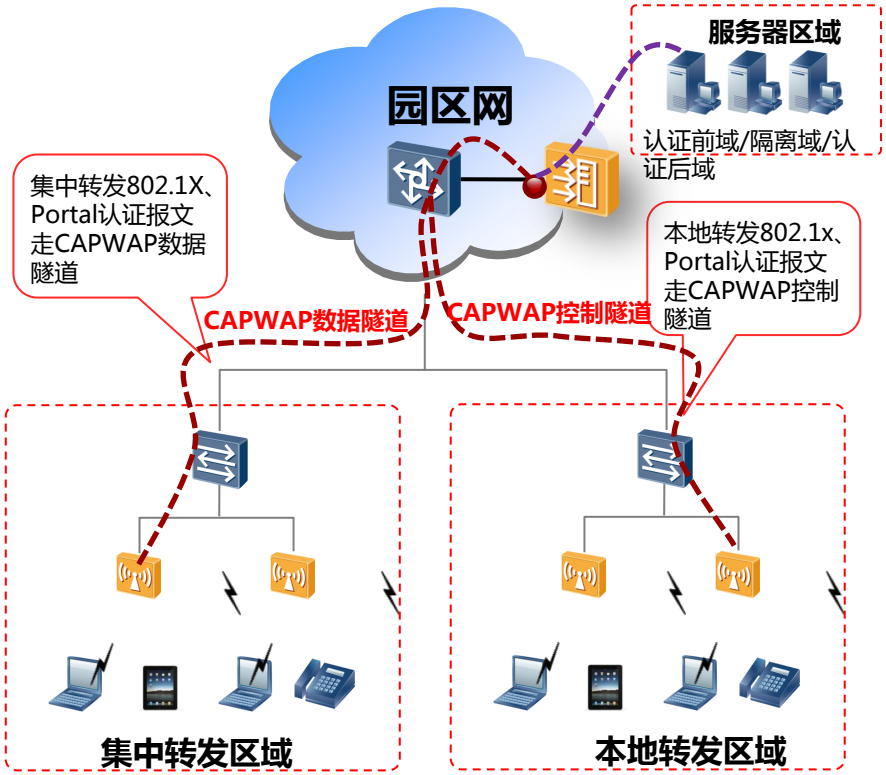
（4）接入层交换机要求为全部支持802.1X + MAC认证设备。

客户价值

（1）控制点离用户最近，内网得到最大安全保障。

（2）802.1X + MAC自适应混合认证，用户无需关注接入终端类型，方便网络部署。

无线用户AC集中认证



无线用户AC集中认证

无线用户在AC上集中认证，可以保证无线用户集中管理。

（1）授权通过AC控制隧道下发到AP，精细化控制用户访问权限。

（2）用户漫游、策略下发等由AC做到灵活控制。

两种转发场景考虑

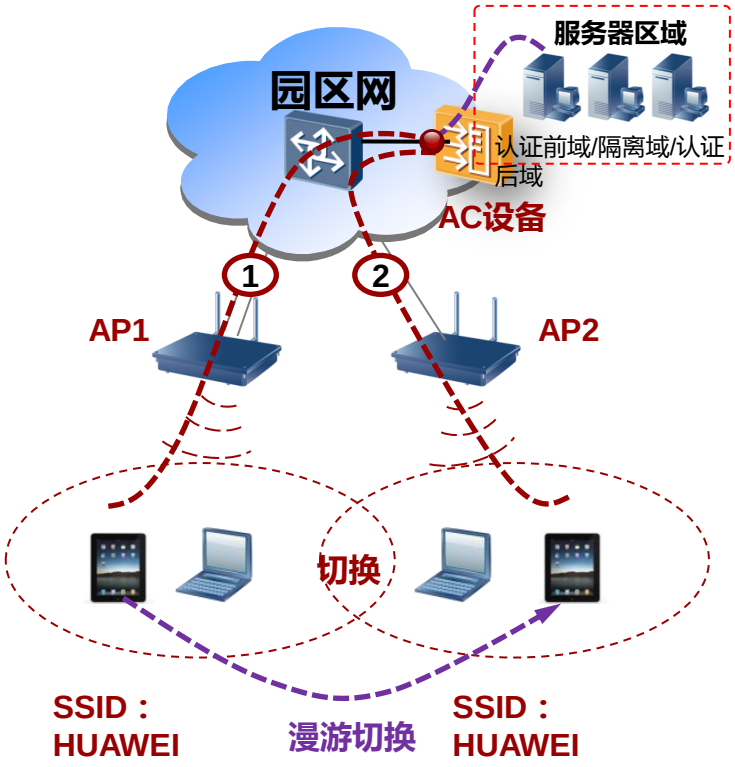
无线用户集中认证，需要保证相关认证协议能够上送AC处理。

（1）集中转发场景下，802.1X、Portal认证报文作为数据流量，通过CAPWAP数据隧道上送AC。

（2）本地转发场景下，可通过配置，让802.1X、Portal认证报文进入CAPWAP控制隧道，从而上送到AC设备，完成认证过程。

无线用户Portal本地转发场景下集中认证2012Q4交付

无线用户漫游切换：授权策略迁移



1. 解除用户和AP1间的关联，取消授权策略
2. 建立用户和AP2间的关联，完成策略迁移

漫游概念

用户在在部署了WLAN网络的场所移动时，用户终端可以从一个AP的覆盖范围移动到另一个AP的覆盖范围，用户无需重新登录和认证。

漫游过程

终端与AP1已经建立关联信息，切换到AP2流程如下：

（1）如图中的标号1 所示，终端删除用户与AP1 现有的关联，同时，由AC控制，取消在AP1上下发的策略控制。

（2）如图中的标号2 所示，客户端通过向AP2 发送关联请求，建立用户与AP2 间的关联，并由AC控制，把AP1上授权策略迁移到AP2中。

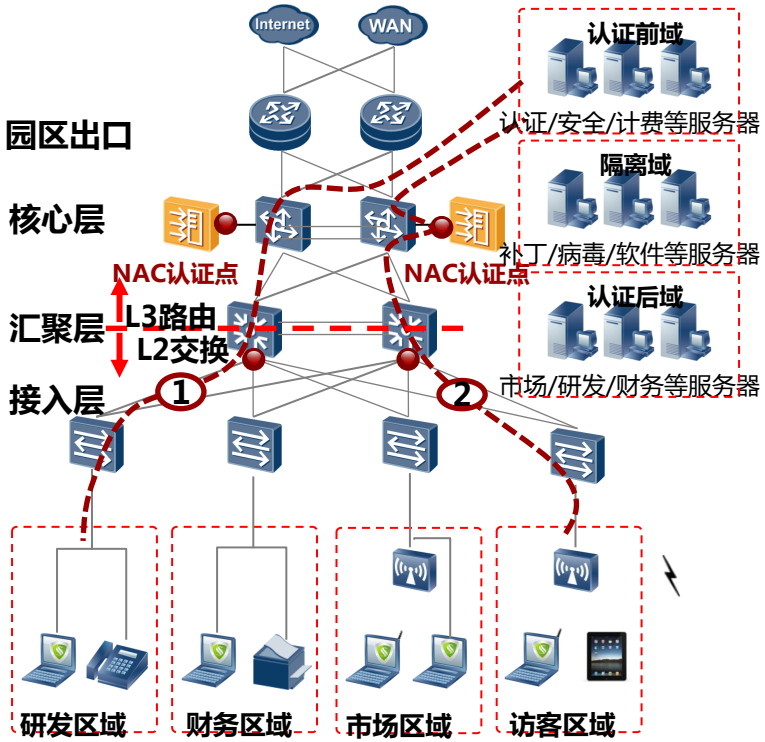
注意事项

（1）漫游切换需要保证SSID相同，即两台AP切换区域需要配置相同的SSID。

（2）漫游切换AP必须是同一个控制器AC管理，目前我司漫游性能在秒级（900ms）。

我司不支持跨AC漫游，宣传时注意

园区网NAC方案二：汇聚层802.1X认证



应用场景

本方案适于大、中、小型园区，用户对于安全控制要求较高的场景，可选择在汇聚层部署802.1X + MAC混合认证。

方案部署

（1）汇聚层交换机启用802.1X + MAC自适应混合认证，有线用户做802.1X认证，IP电话、打印机等哑终端做MAC认证。

（2）对于无线用户，AC设备启用802.1X认证，无线终端通过802.1X接入园区。

（3）服务器系统为TSM服务器组件，基于用户组进行用户管理和权限控制。

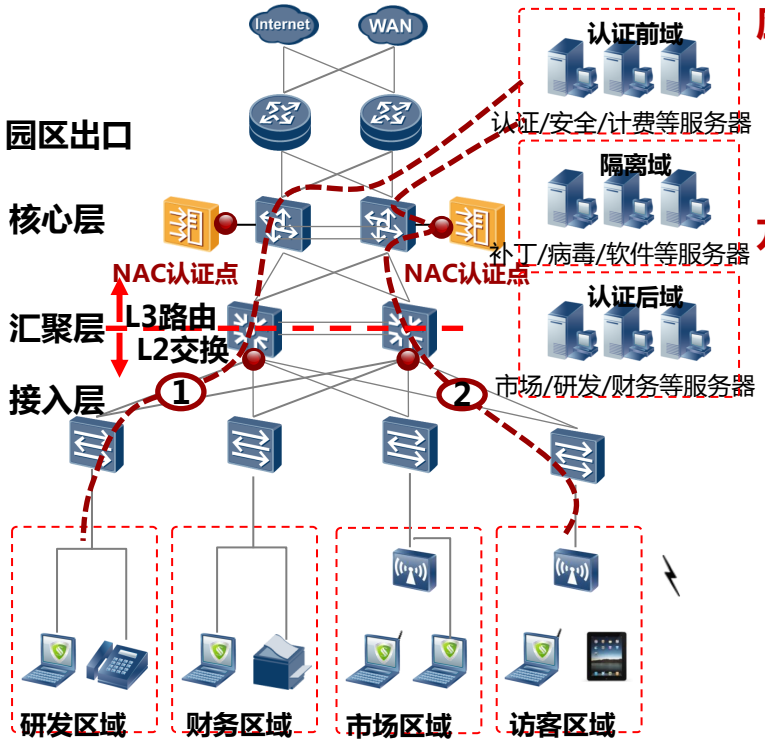
（4）园区L2/L3分界点设置在汇聚层或核心层，汇聚层交换机要求支持802.1x/MAC混合认证，对接入层交换机无特殊要求。

客户价值

（1）汇聚层部署，认证点少，方便管理维护，兼具802.1X认证安全性。

（2）802.1X + MAC自适应混合认证，用户无需关注接入终端类型，方便网络部署。

园区网NAC方案三：汇聚层Portal认证



应用场景

本方案适于大、中、小型园区，用户对于安全控制要求相对适中的场景，可选择在汇聚层部署Portal + MAC混合认证。

方案部署

（1）汇聚层交换机启用Portal + MAC自适应混合认证，有线用户做Portal认证，IP电话、打印机等哑终端做MAC认证。

（2）对于无线用户，在AC设备启用Portal认证，无线终端通过Portal认证接入园区。

（3）服务器系统为TSM服务器组件， 如果用户没有安全检查需求，则可以不部署。

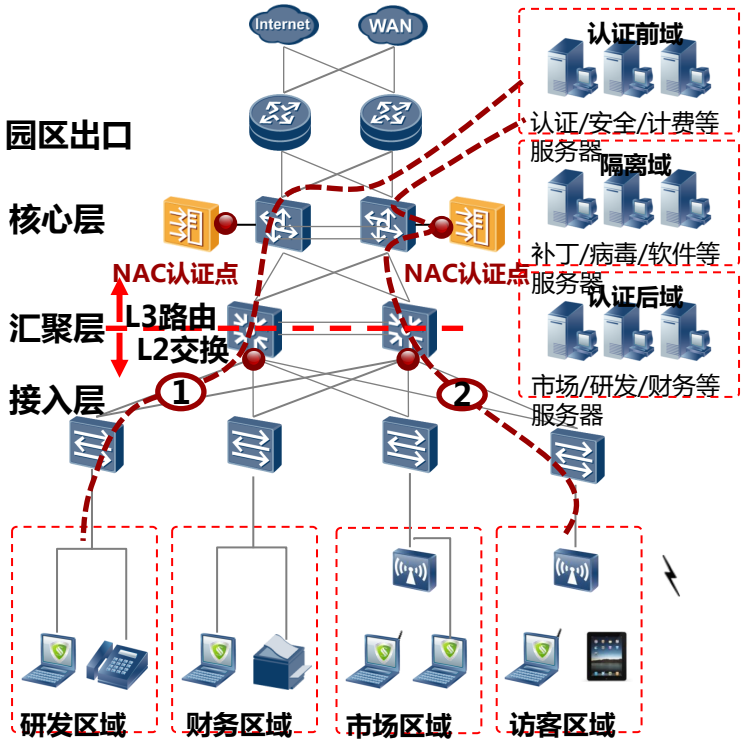
（4）园区L2/L3分界点需要设置在汇聚层或以上，汇聚层交换机要求支持802.1/MAC混合认证，接入层交换机无特殊要求。

客户价值

（1）汇聚层部署，认证点少，方便管理维护，同时客户端可按需选择。

（2）Portal + MAC自适应混合认证，用户无需关注接入终端类型，方便网络部署。

园区网NAC方案四：核心层Portal认证



应用场景

本方案适用于小型园区或大中型园区网络较为复杂的场景，对于后者，由于存在较多其他厂商设备，不适合在汇聚/接入层部署NAC认证，可选择在核心交换机上部署Portal认证。

方案部署

（1）核心层交换机启用Portal认证，有线用户做Portal认证，IP电话、打印机等哑终端通过手工配置Free Rule开放权限。

（2）对于无线用户，在AC设备启用Portal认证，无线终端通过Portal认证接入园区。

（3）服务器系统为TSM服务器组件， 如果用户没有安全检查需求，则可以不部署。

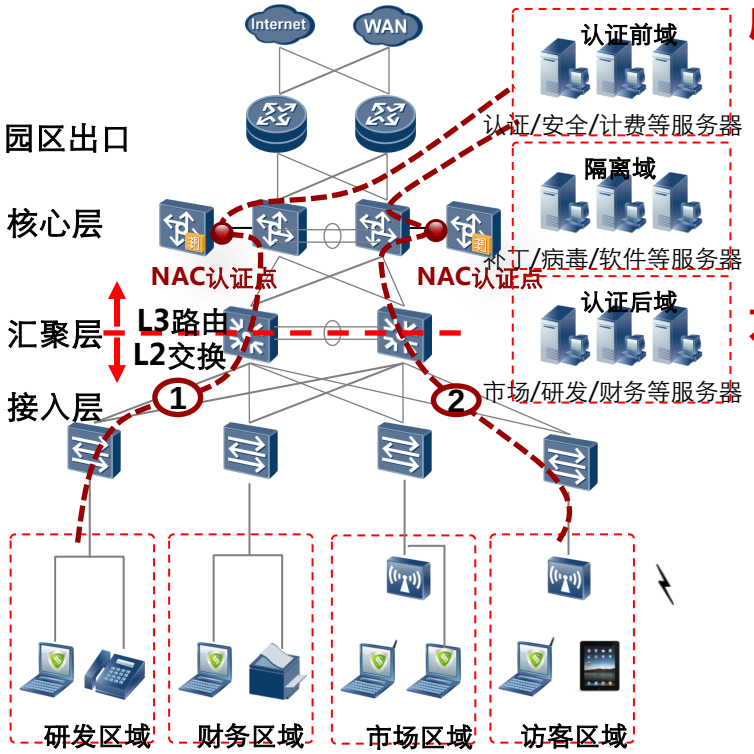
（4）核心层交换机要求全部支持Portal认证，对汇聚层、核心层其他设备无特殊要求。

客户价值

（1）小型园区部署Portal认证，认证点少，按需选择客户端，方便管理维护。

（2）多厂商设备共存时网络环境适应性好。

园区网NAC方案五：核心层旁挂Portal认证



应用场景

本方案用于网络改造场景，园区已经存量大量非我司交换机、路由器等数通设备，用户希望在既有网络基础上，部署WLAN无线网络或者终端安全NAC方案，可选择旁挂核心交换机或者SACG网关设备部署Portal认证。

方案部署

（1）核心层可旁挂具有AC插卡的核心交换机（如S77/97）或者SACG网关（中低端防火墙）设备，上行通过策略路由将用户的上行流量引流到旁挂设备进行控制，下行流量不用引流，直接按照原有交换机配置的路由进行转发。

（2）旁挂设备启用Portal认证，有线和无线用户均在旁挂设备做Portal认证， IP电话、打印机等哑终端通过配置ACL开放权限。

客户价值

（1）认证点少，用户按需选择客户端，方便管理维护。

（2）网络环境适应性好,无需改变现网拓扑、IP、VLAN等规划，保护用户既有投资。

软件防火墙实现用户二层隔离

核心层部署Portal认证方案（旁挂或者直连）控制点高，属于三层认证，无法实现用户二层隔离。我司NAC客户端（TSM Agent）集成了软件防火墙模块，可由NAC认证服务器统一制定、下发软件防火墙规格。根据此功能，用户可在主机层面实施二层用户隔离方案。

只有可信终端允许互访

当认证通过后的终端收到其他终端的访问请求时，该终端首先与其进行安全协商，检查是否为“可信”终端。只有安装了TSM 客户端且通过认证的终端才被认为是“可信”终端。基于以上机制，没有安装TSM 客户端的终端，以及安装了客户端但未通过认证的终端将被“隔离”，无法访问其他终端，即使在同一VLAN里。

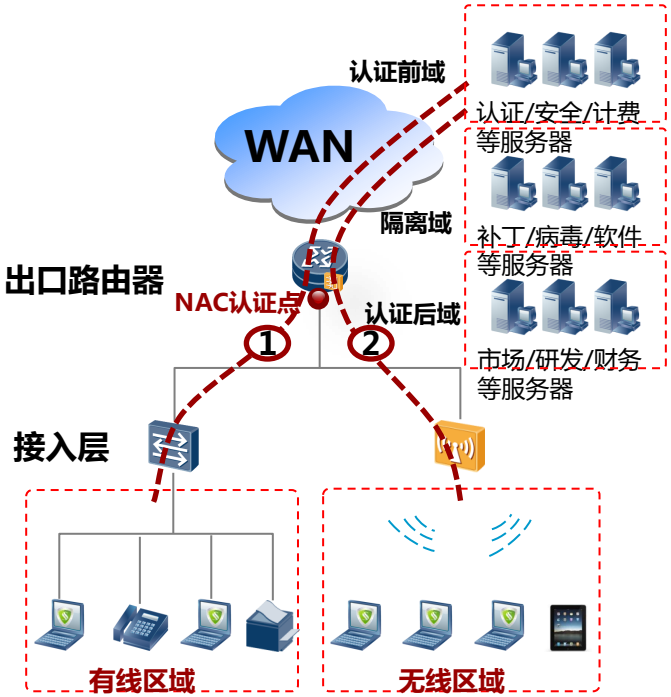
限制不同区域用户互访

客户端主机防火强支持细粒度的网络访问权限控制，管理员可在服务器上划分不同区域，通过客户端控制用户只允许在同一区域（用户组）内互访，不同区域进行隔离。

主机防火墙接入控制方式的使用限制

由于主机防火墙基于客户端实现，因此未安装客户端的终端间互访不受限制，也无法控制没有安装客户端的终端访问服务器。

园区网NAC方案六：出口网关NAC认证



应用场景

SOHO型（微小型）园区网终端规模在100以下，本方案定位于微型企业或者办事处等场景。小型分支一般在出口路由器部署802.1X + MAC或者Portal + MAC混合认证，具体可和园区网整体认证方式保持一致。

方案部署

以Portal认证为例说明如下：

出口路由器启用Portal + MAC自适应混合认证，有线用户做Portal认证，IP电话、打印机等哑终端做MAC认证。

如果需要无线接入，可采用内置AC功能的出口路由器，无线终端也通过Portal认证接入园区。

出口路由器内置Portal服务器功能，认证系统统一部署在总部园区。

客户价值

NAC认证点上移到出口路由器，控制点单一，方便管理维护。

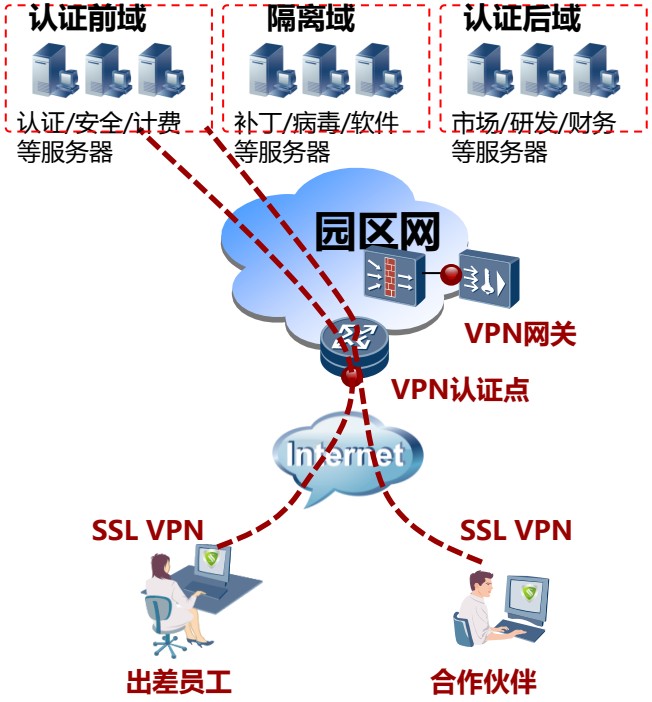
路由器内置AC功能，有线无线一体化认证。

园区网NAC部署方案对比

编号	方案名称	安全性	优点	缺点	应用场景
1	接入层802.1X认证	高	控制点在接入层，内网得到最大安全保障。	认证点多，维护较复杂。	大、中、小型园区，特别是用户对于网路安全要求严格的场景。
2	汇聚层802.1X认证	较高	认证点少，兼具802.1X认证安全性。	控制点在汇聚层，弱于接入层控制。	大、中、小型园区，特别是用户对于网络安全要求较高的场景。
3	汇聚层Portal认证	适中	认证点少，可按需选择客户端。	一般明文认证，安全性较低。	大、中、小型园区，特别是用户对于网络安全要求适中的场景。
4	核心层Portal认证	低	认证点很少，方便管理维护。	一般明文认证、安全性较低。	小型园区或者大中型园区网络环境较为复杂的场景，同时对于安全要求较低的场景。
5	核心层旁挂Portal认证	低	认证点少，无需改变现网拓扑架构。	控制点较高，旁挂设备压力相对较大。	大中型网络改造场景，园区已经存量大量非我司交换机、路由器等数通设备。
6	出口网关NAC部署	低	控制点单一，方便管理维护。	NONE，用户按需选择802.1X或者Portal认证。	小微型分支场景，认证方式和园区保持一致。

对于大、中型园区网中，一般推荐采用802.1X认证，从而获得较高的安全性和控制力度；对于中、小型园区，如果用户对内网安全要求不是很高，可以采用Portal认证部署。

远程用户接入解决方案



应用场景

本方案适于出差员工、合作伙伴等个人用户远程接入场景，一般采用SSL VPN方式接入。

方案部署

对于小型企业，远程接入用户一般在数十人，可选取出口路由器直接作为VPN网关，远程用户通过VPN接入后，可直接到认证服务器进行认证。

对于大中型企业，远程接入用户较多，可在出口防火墙旁挂VPN网关(SVN产品)，支持远程接入。

客户价值

路由器内置SSL VPN功能，用户可按需选择是否需要外挂VPN网关。

内网、外网用户一体化管理，方便运维。

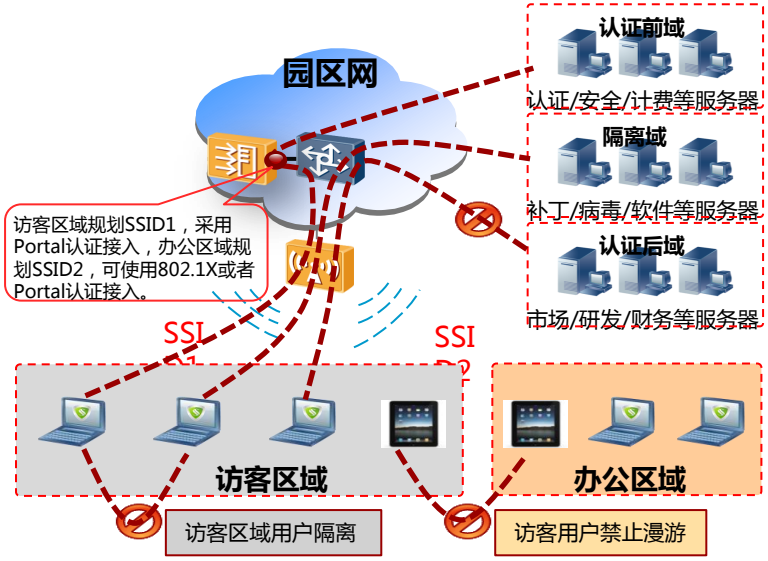
注：

AR12/22/32 SSL VPN通过License控制，License级别具有10、25、100个并发用户三级。

SVN2000/5000并发用户规格可达到1000～20000，满足远程接入需求。

外部访客管理方案

访客是指企业外部客户、合作方员工等人员，对于该类终端，其网络权限不同于内部员工，需要加以限制。在网络规划中，访客区域一般采用无线WLAN方案。



无客户端Portal认证

访客终端采用Portal无客户端方式，方便用户接入。

公共帐号管理

访客作为临时性接入，管理员会面临大量开户、销户和帐号发放的操作，可在用户管理系统中规划公共帐号，减轻管理工作量和提升客户体验。

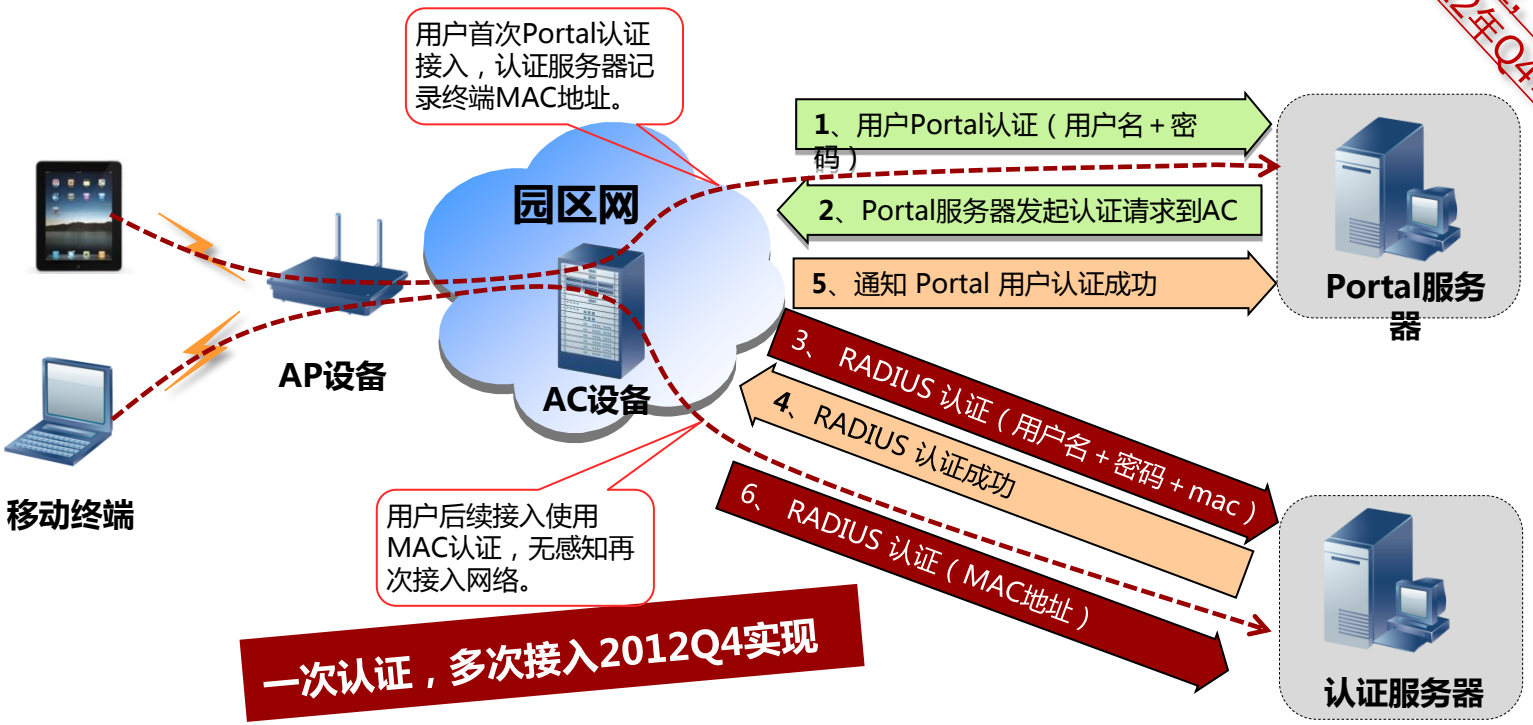
开放特定服务资源

对于访客，可只开放Internet和隔离域资源，禁止访问认证后域的企业内部资源。

用户隔离

对于无线客户，漫游存在很大安全隐患。可通过规划特定SSID，限制访客漫游到办公区域；另外，可通过二层隔离技术，限制访客之间互访。

用户一次认证，多次接入流程



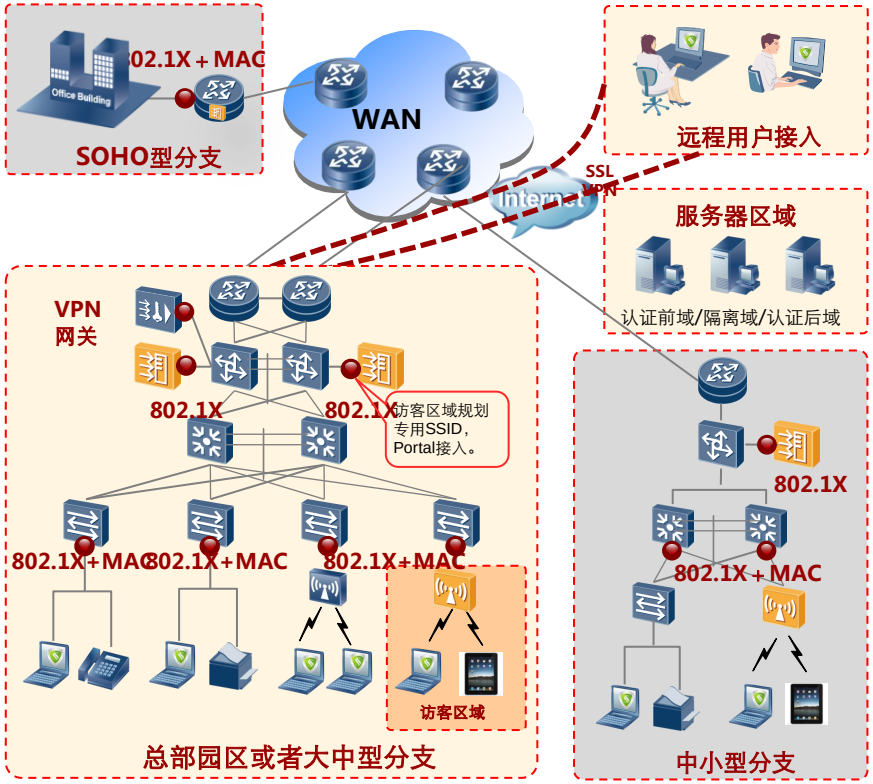
用户采用Portal + MAC自适应混合认证

首次使用Portal认证接入，并在流程3中上送终端MAC地址，Radius认证服务器记录终端信息。

用户无需认证，无感知再次接入

后续用户接入使用MAC认证，通过流程6完成认证过程，直接打开任意应用即可上网。

园区网NAC解决方案全景图



以802.1X＋MAC认证为例，给出园区网NAC部署的全景图。

部署原则

有线、无线用户，推荐采用相同认证方式，方便管理和网络维护。

部署说明

园区总部或者大中型分支安全性要求严格，采用802.1X＋MAC自适应混合认证，认证点可放在接入层。

中小型分支，如果安全要求相对较高，可把认证点规划在汇聚设备上，简化管理。

SOHO型分支或者办事处，用户接入一般在数十人，认证点可直接部署在出口路由器上。

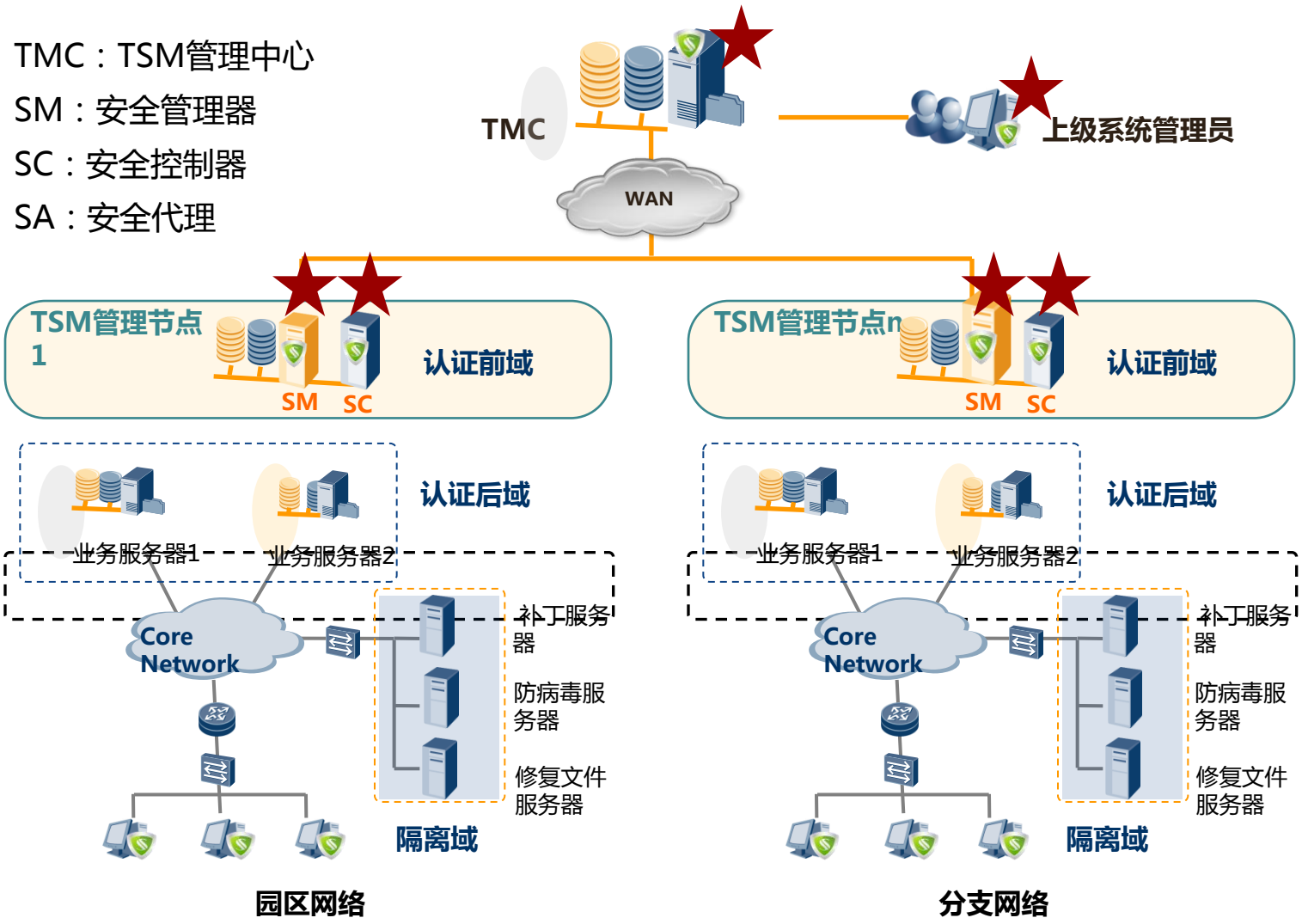
对于远程办公用户，可通过总部部署VPN网关，实现SSL VPN接入总部网络。

外部访客一般采用Portal认证无线接入。

目录

TSM终端安全管理系统部署

TMC：TSM管理中心
SM：安全管理器
SC：安全控制器
SA：安全代理



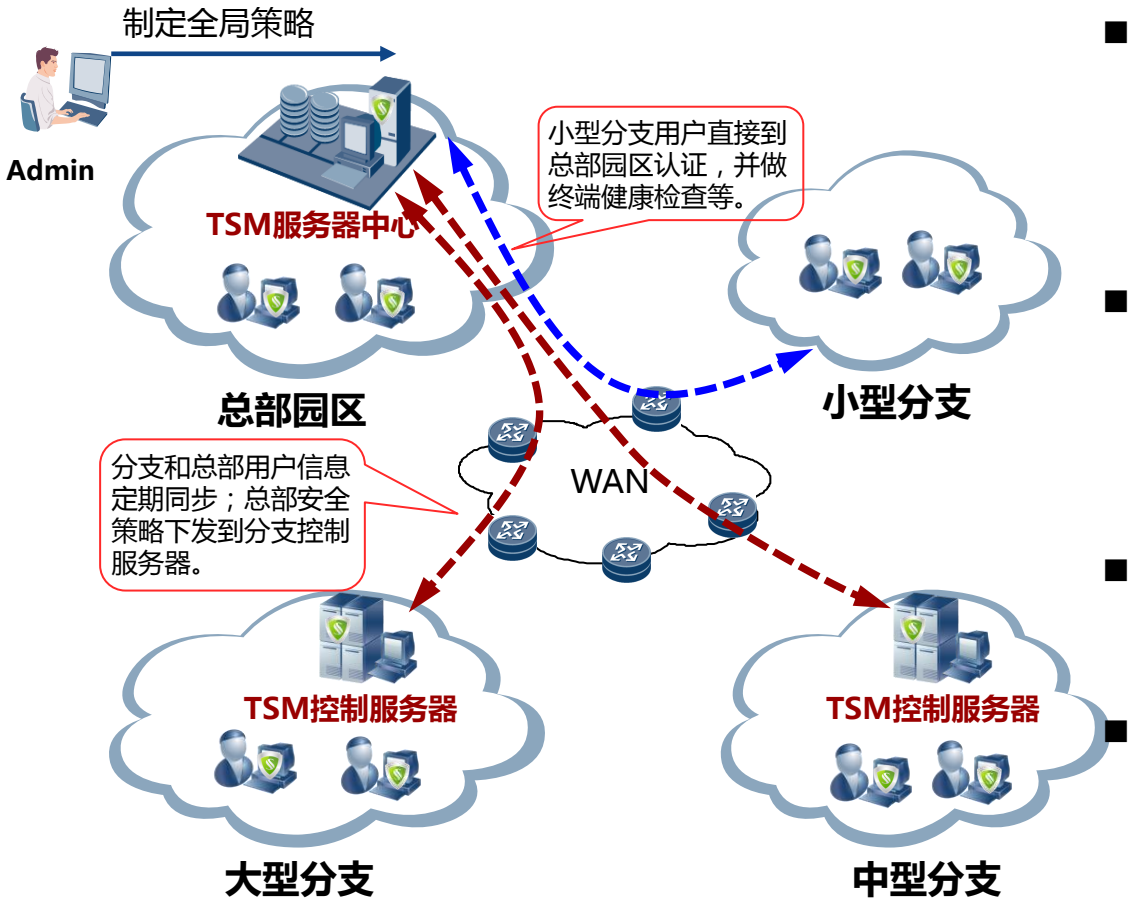
华为TSM终端安全管理系统

华为TSM系统由系统管理中心（TMC）、安全管理器（SM）、安全控制器（SC）、客户端（SA）四部分组成。

项目	组件说明	备注
TMC	软件，TSM服务器组件之一，分级式部署时作为上级的管理中心，订制总体的安全策略、补丁及软件分发任务等，下发给各个管理节点的TSM服务器，并对下级各管理节点的TSM服务器的运行状态进行实时监控。	可选
SM	软件，TSM服务器组件之一，是TSM系统的管理核心，提供各种业务功能管理，包括资产管理、软件分发、补丁管理、日志审计、终端安全策略管理、身份管理、报表等；采用B/S架构，管理员可通过WEB界面进行管理；	必选
SC	软件，TSM服务器组件之一，是TSM系统里管理策略的实施者，SC根据SM配置的数据对SA进行管理，SM决定如何做，SC协调各部件进行实施；当用户通过SA认证后，SC控制网络准入控制设备（如交换机、防火墙、wlan设备等）开放用户访问权限；	必选
SA	软件，安装在终端主机上，协助用户进行网络准入认证，并实时收集终端的安全状况上报服务器；SA对终端资源占用和系统消耗小，CPU占用率一般为 2%以内, 最大内存占用30M；	必选

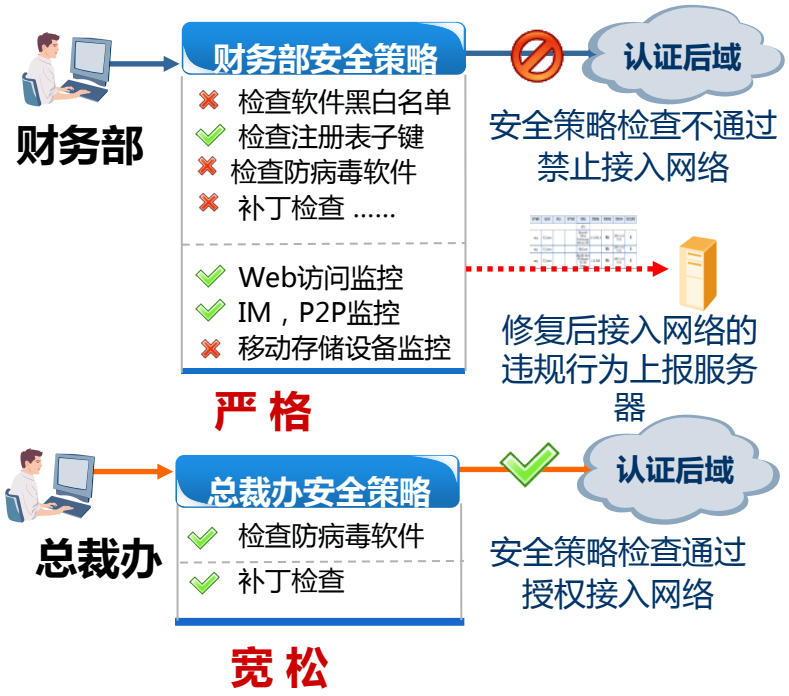
TSM服务器分布式部署,满足超大规模组网

对于存在大、中型分支的园区网络，需要部署多套TSM系统，可采取分布式部署。



- 总部园区TSM服务器作为TSM的管理中心，负责制定总体的安全策略，下发给各个分支TSM控制服务器，并且对分支TSM服务器实施情况进行监控。
- 大、中型分支部署独立的TSM控制服务器，定时同步总部TSM中心的用户信息，完成本分支用户身份认证、安全策略下发和软件下发等任务。
- 小型分支不部署单独TSM服务器，用户上线时直接到总部TSM服务器进行认证。
- 分布式补丁和软件分发发TSM系统支持分布式补丁和软件分发，有效分担网络流量，平衡负载。

终端安全管理：丰富的策略管理



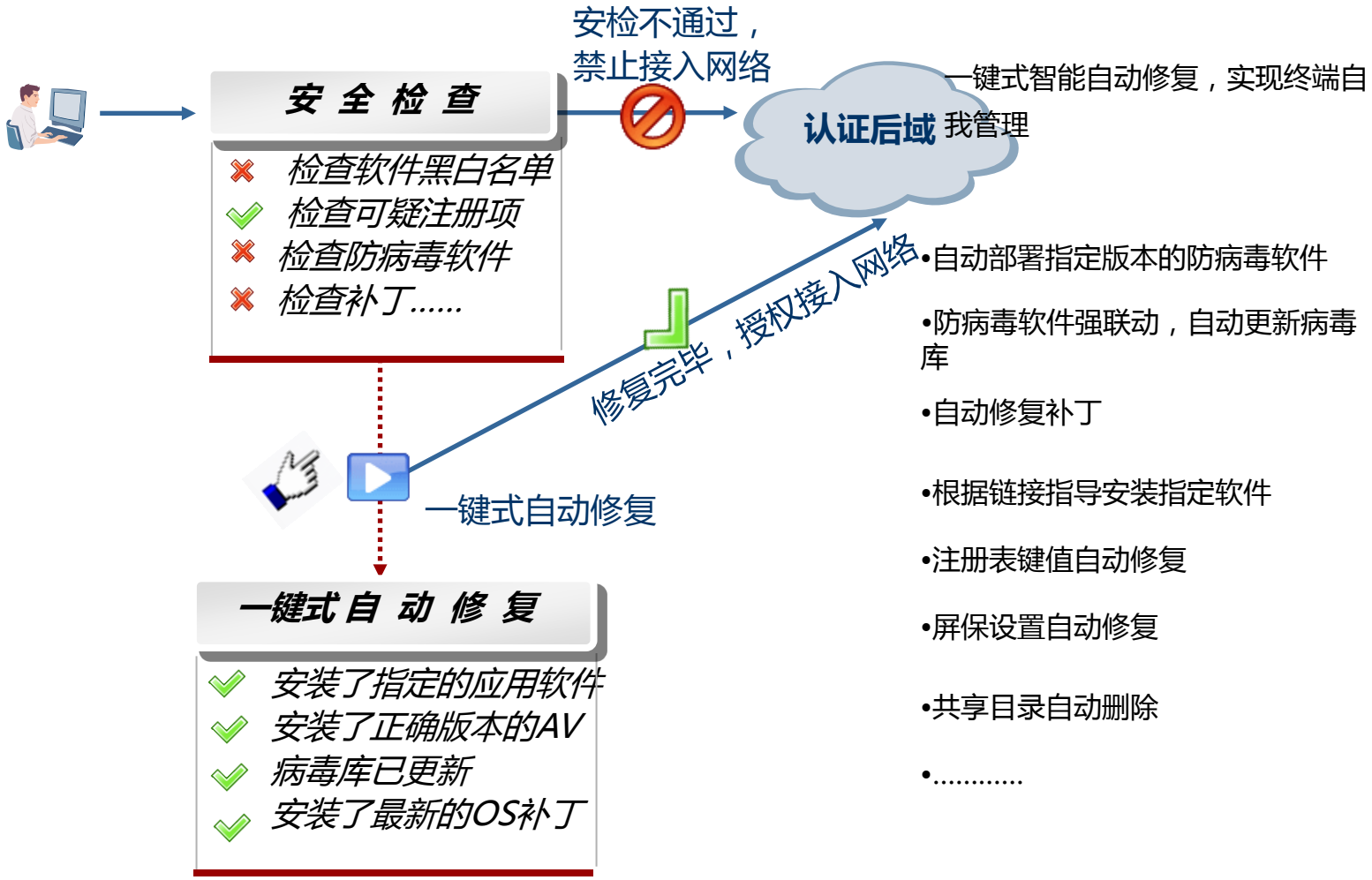
业界最丰富的安全策略，强制企业IT策略遵从

主动评估终端安全状态，强制终端策略遵从，自动发现终端漏洞，消除已知、未知威胁

量体裁衣，基于用户组的动态策略控制

基于用户或者用户组（部门）自定义不同安全规则，针对不同点控制点采取不同策略

终端安全管理：一键式智能自动修复



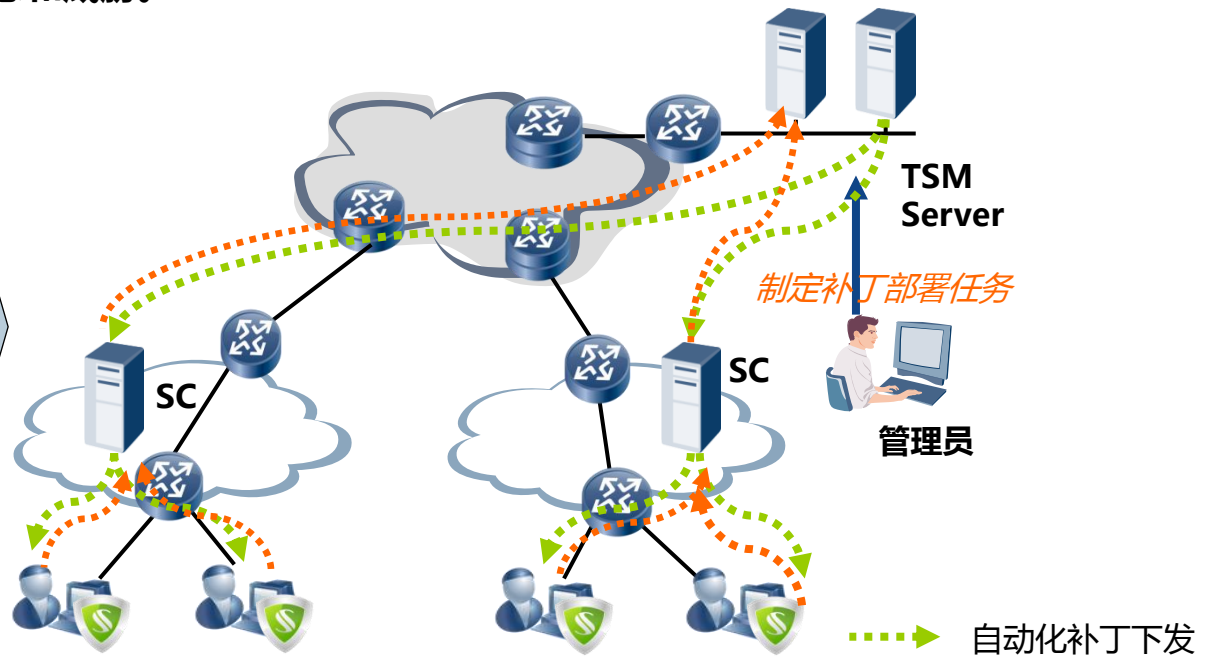
强大的补丁管理功能

自动修复系统漏洞，帮助内网的用户主机及时更新操作系统、Office、数据库、IE补丁,避免因为系统漏洞带来的安全隐患和威胁。

1 自动化补丁检查

2 智能化补丁下发

支持PULL和PUSH方式
基于用户群组分组分发
支持分布式补丁分发
断点续传，确保安装任务完成
可选择闲时分发补丁



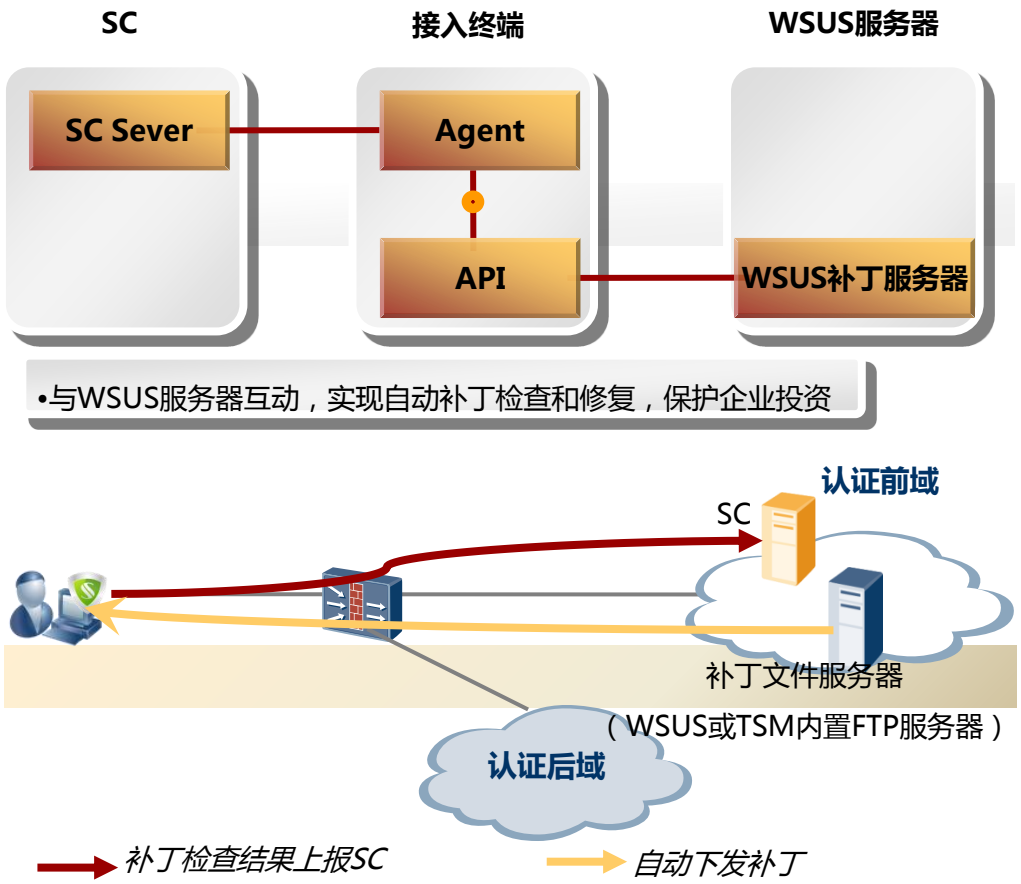
3 补丁安装

多种安装策略：自动/手动静默
支持补丁卸载

4 补丁安装统计

基于设备的统计
基于补丁的统计

一站式专业补丁管理



业界领先的补丁管理系统，免日常维护实现补丁自动修复

准确
- 依权威数据源定位漏洞
- 按照补丁、终端精准展示

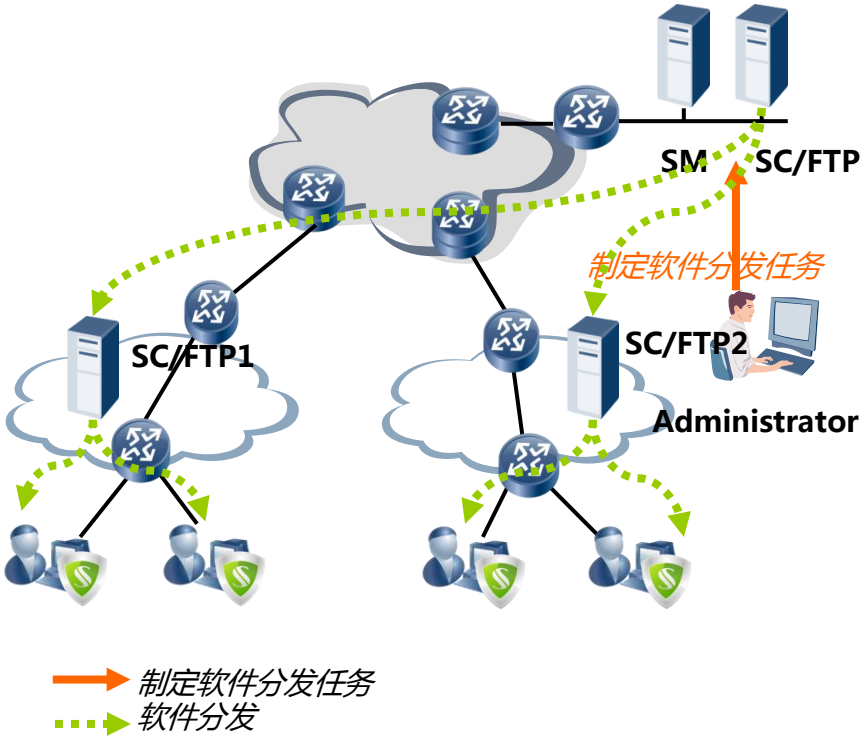
高效
- 主动扫描、快速评估
- 自动下载自动更新
- 最低带宽占用
- 主动管理，持续更新

可控
- 自动验证补丁
- 自动忽略异常补丁
- 分时分批修复漏洞

安全
- 强制在隔离区内修复
- 有效隔离安全威胁

便捷的软件分发管理

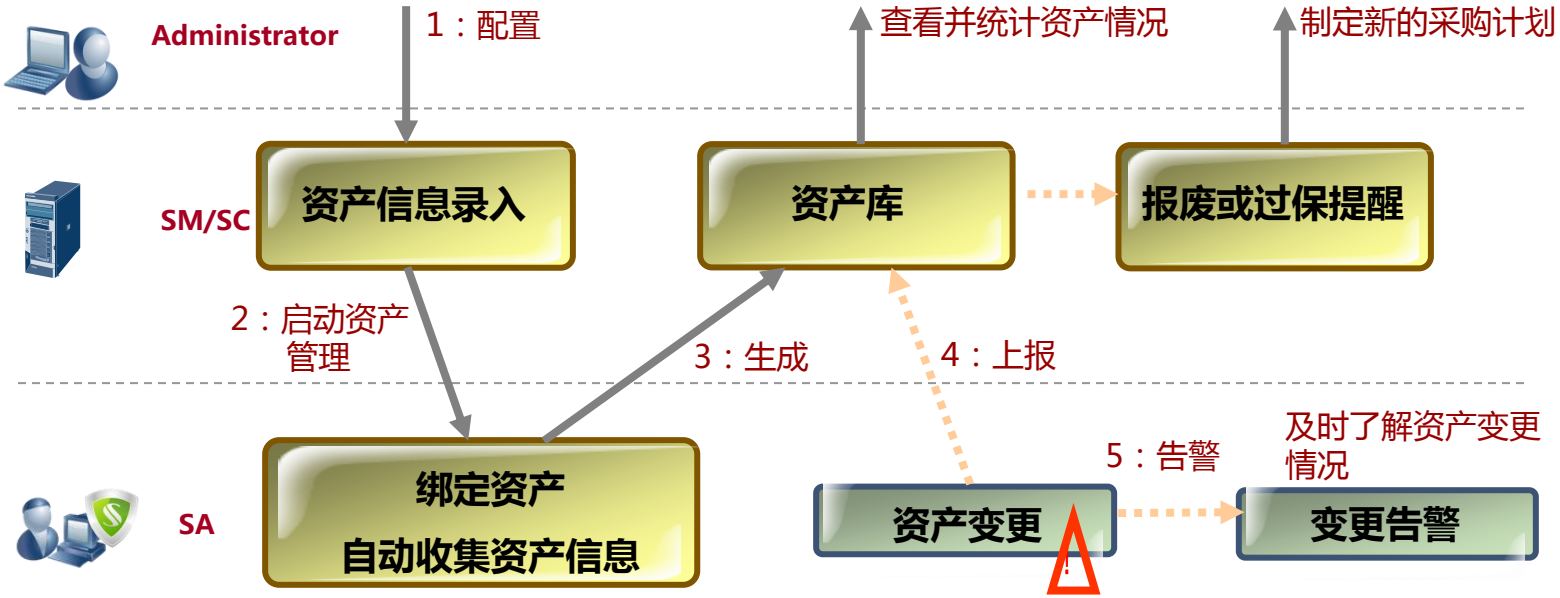
软件自动化部署 ，简易终端信息化维护工作，提高部署效率。



- 支持分布式软件分发，有效分担网络流量，平衡负载
- 多种安全策略灵活选择：自动、手动和静默安装
- 支持配置分发软件参数，带参数执行
- 支持按部门、按操作系统进行软件分发
- 支持断点续传以及文件完整性校验(MD5)

IT资产生命周期管理

资产生命周期管理流程



资产生命周期管理的好处

降低成本

- 减低采购支出，节约IT预算
- 提高设备利用率，减少资产流失
- 降低资产总拥有成本（TCO）

减少风险

- 减低设备导致的信息安全风险
- 减少法律风险，快速应付审计

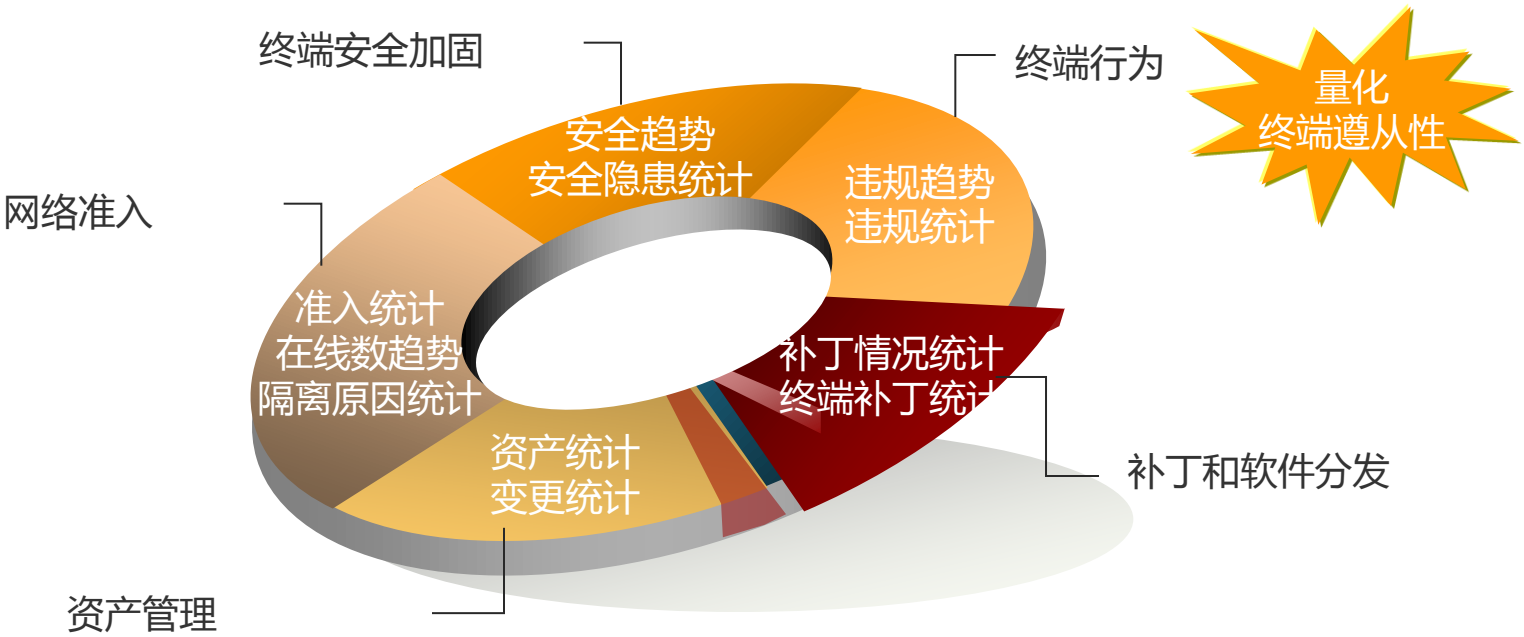
提高效率

- 全面掌控IT资产
- 辅助采购、管理层投资决策
- 提高IT运维效率

实时的网络行为管理


可区分管理
外来介质；
拷出加密
移动存储
USB
USB移动硬盘
数码相机
各类Flash Disk
智能手机
USB MP3/4
文件操作审计
增加、删除、编辑、复制、重命名操作监控
监控指定文件的指定操作
控制各类 IM、P2P软件
腾讯QQ
msn
BitTorrent
BitComet
信息泄密防护
准入控制和网络接入审查
杜绝访客、不合规终端、无权用户非法访问
设备接入审计
新设备接入告警
网络程序、网络流量控制和审计
基于协议的监控
基于端口的监控
基于网络程序的监控
外设接口管理
1394接口
红外
蓝牙
串口/并口
软驱
Printer
SD卡
MMC卡
控制各种非法外联行为
ADSL拨号
ISDN拨号
Modem拨号
同时使用内外网
VPN拨号
非法Proxy服务器、非法上网路径

可定制报表，满足个性化需求



多维度展示	可扩展报表	升级服务
趋势、TopN；饼图、柱状图 违规等级：严重、一般 简单报表：基于用户或策略 组合报表：按照模板，提供基于策略、维度、范围、时段的组合展示	预置常用报表模板 免升级导入新的报表模板	可到升级网站下载适用报表模板 导入系统使用

NAC解决方案竞争力分析

项目	HUAWEI	CISCO	H3C
用户管理	基于用户组（user-group）管理用户和授权策略，方便整网NAC部署，节省用户资源。	基于角色（role）管理用户和授权策略，类似于用户组，但对于无线用户，**无法做到同一用户组内用户相互隔离。**	具有用户模版概念（user-profile），管理用户授权策略，但针对每个用户下发，**无法实现资源共享。**
准入控制	支持MAC、Portal、802.1x等多种准入控制方案，对网络环境适应性好，特别是软件防火前功能，有效实现了用户主机层面的二层隔离。	支持MAC、Portal(WLAN场景)、802.1X、SNMP等多种准入控制方案，但SNMP方案对网络设备有依赖，需要专用NAC设备，中间多次切换设备配置，实时性差，对网络设备负载影响较大。	支持MAC、Portal、802.1x等多种准入控制方案，但其准入控制方案主要配套其网络设备，软件防火墙不能做横向隔离，仅能作简单的软件ACL控制。
安全管理	（1）多维度策略管理，可基于用户、时间、部门实施控制；支持基于位置的策略自适应（基于IP地址族），实现不同网关区域的差异化控制。 （2）安全策略可通过网站安全中心，用户自己下载策略，支持策略自定义。	（1）管理维度单一，基于用户、部门等配置，不支持基于位置的策略自适应控制； （2）安全策略没有安全中心下载机制，不支持策略自定义。	（1）管理维度单一，基于用户、部门等配置，不支持基于位置的策略自适应控制； （2）安全策略没有安全中心下载机制，不支持策略自定义。
补丁管理	支持完整的补丁管理方案，包括补丁下载、验证、分发、统计等功能；支持与WSUS联动。	依赖于WSUS联动，无独立补丁管理功能。	依赖于WSUS联动，无独立补丁管理功能。
病毒管理	支持强联动，和江民、金山等厂商合作，可主动实施病毒查杀和修复，其他厂商弱联动。	无强联动机制，只有弱联动机制。	支持强联动，和江民、金山、**瑞星**等厂商合作，其他厂商弱联动。

NAC解决方案竞争力分析

项目	HUAWEI	CISCO	H3C
软件分发	支持多种文件格式的软件下发，可自动运行。	无。	支持多种文件格式的软件下发，可自动运行。
行为监管	支持外设管控、非法外联、网络监控等功能。	无，只有进程和服务监控。	仅简单的外设管控、网络监控等功能。
资产管理	提供资产生命周期管理，支持硬件资产、软件资产、BOIS信息记录。	无，只能通过第三方集成，客户端不统一	提供资产注册管理，支持硬件资产、软件资产等，不支持提取BOIS信息。
BYOD方案	规划在移动办公版本，预期在2013Q2方能提供。	在ISE中提出BYOD方案，通过集成第三方MDM软件，实现智能终端的桌面安全方案。	当前不支持。

总体而言，华为NAC解决方案和Cisco、HP相比较优势明显，特别在用户组管理、安全管理、补丁管理、行为监管等领域。

BYOD方案（Bring Your Owen Device）从当前各厂家支持来看，Cisco、Aruba已经实现，H3C、ZTE等大部份厂家没有实现，我司当前暂不支持，预期在2013Q2正式推出。

Why win Cisco ?

无法精确实现用户隔离

Cisco基于角色（role）管理用户和授权策略，类似于用户组，但对于无线用户，无法做到同一用户组内用户相互隔离。

Cisco没有主机软件防火墙机制，需要通过VLAN隔离才能防止终端之间的交叉感染，不能做到非授信用户访问横向隔离。

整体方案复杂，集成多家厂商设备

多业务集成是终端安全管理的有效措施！但Cisco缺乏办公行为管理、网络防护、信息泄密防护、资产管理等，需要第三方服务器配合，难以被国内和中小企业用户认可。

准入控制方案对网络环境的适应性差

Cisco的准入控制技术过于复杂、环境要求苛刻，主推的OOB/ISE方式严重依赖于自身的路由和交换设备；准入控制方案成熟度较差，其IB方式只支持三层的准入控制，无法做到二层的互访控制；OOB方式通过SNMP协议动态修改交换机设备的vlan等网络配置，需要专用NAC设备，中间多次切换设备配置，准入控制效果无法实时生效，且会加重交换/路由器的负载负担，影响网络的稳定性。

不支持安全策略动态扩展

动态扩展是终端安全的高级要求！但Cisco不支持动态扩展策略和报表，不支持基于位置的策略自适应（基于IP地址族）。

不支持服务器分级管理

分级管理是终端安全系统全球或大规模部署的必要要求！但是Cisco不支持分级管理，所有管理员均登录一个系统进行管理，只能在总部管理服务器集中管理。

Why win H3C ?

用户授权不支持资源共享

H3C具有用户模版概念（user-profile），管理用户授权策略，但针对每个用户下发，无法实现资源共享，这会导致在汇聚层、核心层部署时存在ACL资源瓶颈。

无法精确实现用户隔离

H3C主机软件防火墙机制只能做简单的软件ACL控制，不能做到非授信用户访问横向隔离。

服务器平台和客户端操作性差

虽然通过iMC统一平台实现所有功能模块化管理，但易用性不好。用户配置公共参数多，操作繁琐，完成一个操作任务需要多切换多页面（如IP地址、时间段）。

客户端采用“新建拨号链接”方式由客户端自己手工添加完成，对用户技能要求高（不同认证方式需要自己完成配置）。

没有完整的补丁管理方案

H3C补丁管理功能依赖于联动微软的WSUS补丁服务器，无独立补丁管理功能，包括补丁下载、验证、分发、统计等功能。

不支持安全策略动态扩展

H3C不支持基于位置的策略自适应（基于IP地址族），安全策略没有安全中心下载机制，不支持策略自定义。

只有简单的行为管控能力

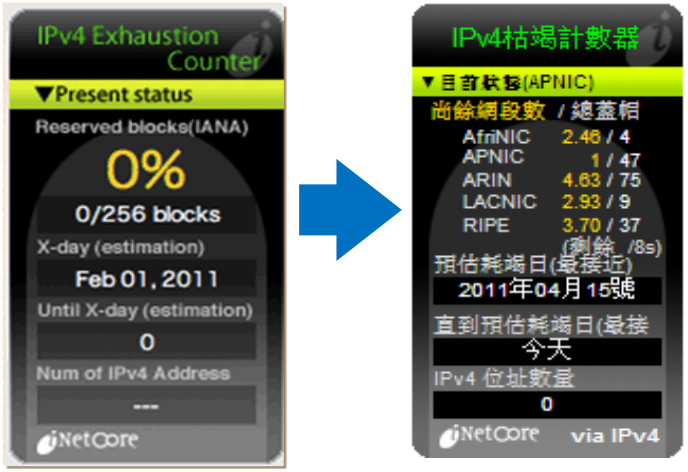
H3C仅有简单的外设管控、网络监控等功能，没有USB管理、非法外联（上网proxy、3G、WiFi等）监控。

子目录

4 园区网业务解决方案

目录

IPv4的夕照，IPv6的朝阳



2010.02　　2011.02

全球IPv4地址枯竭是必须面对的现实问题

全球IPv4地址的可用数目不足以为每一台互联网终端设备配置全球唯一的IP地址；

有限的IPv4地址资源与网络业务规模无限的发展需求之间的矛盾，已经上升为Internet发展中的主要矛盾；

IPv6是解决地址问题的根本解决方案

IPv6是128位地址结构，具备近乎无限的地址空间；

IPv6支持分层次编址和路由聚合，可以大大精简路由表项；

IPv6可以彻底解决地址不足问题，但不能向下兼容IPv4，因此需要平滑演进方案

IPv6与IPv4地址空间比较

如果1个IPv4地址 = 1克
所有IPv4地址相当于上海金茂大厦重量的2/3

IPv4地址空间为2^{32}= 4,294,967,296
IPv6地址空间为
2^{128}=340,282,366,920,938,463,463,374,607,431,768,211,456 (340万亿万亿万亿)

相当于宇宙中每个基本粒子可分配到4000万亿个地址

那么对于IPv6所有地址……
将会是 1000,000,000 地球的重量

IPv6地址格式

128位的IPv6地址被分为8组，形式如 X:X:X:X:X:X:X:X

每组的16位用4个十六进制字符（0～9，A～F）来表示组和组之间用冒号（:）隔开；

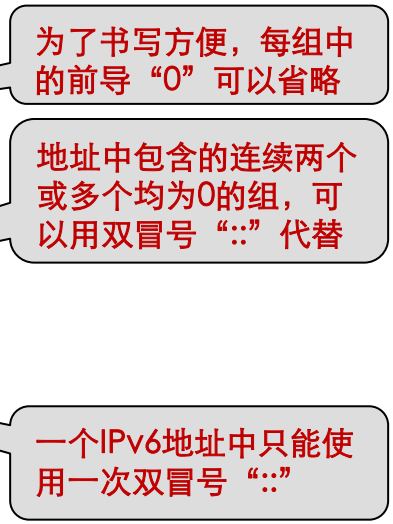
其中每个“X”代表一组十六进制数值。

示例：

2001:0000:130F:0000:0000:09C0:876A:130B

2001:0:130F:0:0:9C0:876A:130B

2001:0:130F::9C0:876A:130B



IPv6单播和任播地址格式

单播和任播地址包含两个部分：

- 64位网络前缀：路由前缀（routing prefix）+子网标识（subnet id）
- 64位接口标识（Interface identifier）

48位（或更多）	16位（或更少）	64位
routing prefix	subnet id	interface identifier

路由前缀长度可变，一个更长的路由前缀意味着更少的子网。64位的接口标识可以通过接口的MAC地址自动生成（EUI-64格式）/通过DHCPv6服务器获得/自动随机生成/手工指定。

链路本地地址（Link-local address）格式

10位	54位	64位
prefix	zeroes	interface identifier

前缀（prefix）为二进制值1111111010（FE80::/10），链路本地地址可用于邻居发现协议和无状态自动配置进程中链路本地上节点之间的通信。使用链路本地地址作为源或目的地址的数据包不会被转发到其他链路上。

组播地址格式

组播地址格式

8位	4位	4位	112位
prefix	flag	scope	group ID

前缀（prefix）为二进制11111111(FF::/8)。标志（flag）有4位。范围（Scope）有4位，用来限定地址有效范围。组ID（group ID）长度为112位，用以标识组播组，目前建议仅使用其中的最低32位组ID，其余80位保留。

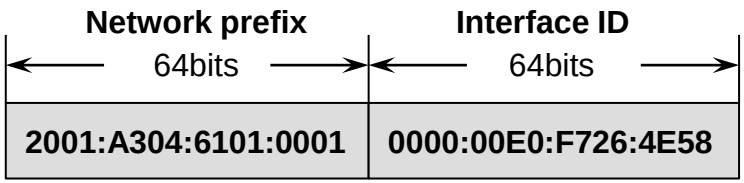
被请求节点组播地址（Solicited-Node multicast address）格式

8位	4位	4位	79位	9位	24位
prefix	flag	scope	zeroes	ones	unicast address

通过将单播或任播地址的低24位添加到ff02:0:0:0:0:1:ff00::/104来生成被请求节点组播地址。

被请求节点组播地址是一种特殊用途的地址，主要用于在邻居协议中获取邻居节点的链路层地址。节点或路由器对于接口上配置的每个单播和任播地址，都将自动启用一个对应的被请求节点组播地址，并加入相应的被请求节点组播组。

IPv6地址结构



MAC
0012:3400:ABCD
Binary
00000000 00010010 00110100
00000000 10101011 11001101

Insert 0xFFFE:
00000000 00010010 00110100 11111111
11111110 00000000 10101011 11001101

Set U/L Bit:
000000<u>1</u>0 00010010 00110100 11111111
11111110 00000000 10101011 11001101

EUI-64:
0212:34ff:fe00:abcd

网络前缀：

n比特，相当于IPv4的网络ID

接口标识：

128-n比特，相当于IPv4的主机ID

2001:A304:6101:1::E0:F726:4E58 /64

IEEE EUI-64格式的接口标识符

64位接口标识符（Interface ID）用来唯一标识链路上的特定接口。

这个地址从接口的链路层地址（如MAC地址）变化而来

IPv6地址中的接口标识符是64位，而MAC地址是48位，因此需要在MAC地址的中间位置插入0xFFFE (1111 1111 1111 1110b)

将U/L位（从高位开始的第7位）设置为“1”，得到EUI-64格式的接口ID。

IPv6地址分类

单播地址（Unicast address）

唯一标识一个接口，类似于IPv4的单播地址。发送到单播地址的数据包将被传输到此地址所标识的唯一接口。

任播地址（Anycast address）

用来标识一组接口（通常这组接口属于不同的节点）。发送到任播地址的数据包被传输给此地址所标识的一组接口中距离源节点最近的一个接口（最“近”的一个，是指根据路由协议的距离度量）。任播地址没有独立的地址空间，它们可使用任何单播地址的格式。

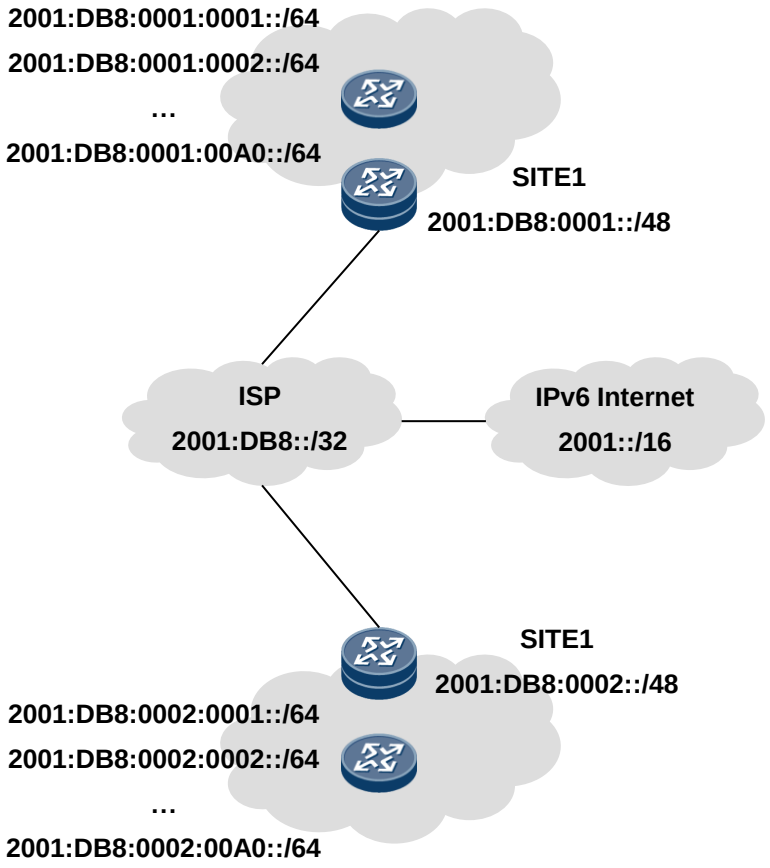
组播地址（Multicast address）

用来标识属于不同节点的一组接口，类似IPv4的组播地址。发送到组播地址的数据包被传输给加入相应组播组的所有接口。

IPv6不支持广播地址。广播地址的功能由链路本地组播地址来提供，但并不推荐使用。

大部分IPv6协议使用不同的链路本地组播地址来避免影响网络中的每一个接口。

IPv6地址层次



IPv6地址长度较长

便于分层和地址段/路由聚合

分层利于路由快速查找

路由聚合可以有效缩短路由表长度

最终加快路由收敛速度

提高路由器报文转发效率

IPv6地址与IPv4地址对比

比较项目	IPv4	IPv6
地址空间	2^32（4,294,967,296）	2^128（340个1000的12次幂）
地址语法	点分十进制，32位地址每8位分成一段，每段换算成十进制数值，并用点号隔开	128位地址每16位分成一段，每个16位段换算成4位十六进制数，并用冒号隔开
	点分十进制数作为子网掩码	不使用子网掩码，仅支持前缀长度表示法
地址类型	单播、多播、广播	单播、多播、任播
路由分层	单级路由和多级路由混合	支持分级寻址和路由聚合
主机ID长度	可变	固定64bit
等价地址	Internet地址A/B/C/D/E类	IPv6中无此概念
	多播地址（224.0.0.0/4）	IPv6多播地址（FF00::/8）
	广播地址	IPv6中无此概念
	未指定的地址0.0.0.0	未指定的地址是::
	环回地址：127.0.0.1	环回地址是::1
	公共IP地址	全球单播地址
	私有IP地址（10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16）	唯一本地（FD00::/8）或者站点本地地址(FEC0::/10)（不推荐）
	APIPA地址（169.254.0.0/16）	链路本地地址（FE80::/64）
	文本表示：点分十进制表示法	文本表示：前导零压缩/十六进制冒号表示
	前缀表示：子网掩码或者是前缀长度表示法	前缀表示：只支持前缀长度的表示法

IPv6报文结构与IPv4对比（1）

比较项目	IPv4	IPv6
报头字段	版本	相同字段，但是版本号不同
	Internet报头长度	已从IPv6中删除。IPv6不包括报头长度字段，因为IPv6报头总是40字节的固定长度。每个扩展报头或者是固定长度或者标识了自己的长度。
	服务类型	由IPv6的通信流类别字段取代
	总长度	由IPv6的有效负载长度字段取代，这个字段仅表示有效负载的长度。
	标识符	已从IPv6中删除。片段信息并不包含在IPv6报头中。而是包括在片段扩展报头中。
	标签	
	片段偏移	
	生存时间	由IPv6的跳限制字段取代
	协议	由IPv6的下一个报头字段取代
	报头校验和	已从IPv6中删除。链路层有对整个IPv6数据包做比特层面的错误检测的校验和。
	源地址	保持不变，除了IPv6的地址是128比特长。
	目的地址	保持不变，除了IPv6的地址是128比特长。
	选项	已从IPv6中删除。IPv6扩展报头取代了IPv4选项。

IPv6报文结构与IPv4对比（2）

比较项目	IPv4	IPv6
报头字段数目	12（包括选项）	8
必须由中间路由器处理的字段数目	6	4
报头选项的处理	IPv4报头包含了所有的选项，因此，每个中间路由器都必须检查他们是否存在，如果存在，则进行处理，这会降低IPv4数据包转发过程的效率。	IPv6中，发送和转发选项被移至扩展报头中。中间路由器必须处理的唯一一个扩展报头就是逐跳选项扩展报头。这加快了IPv6报头的处理速度并提高了转发效率。
片段字段	片段标签组合了片段标签和片段偏移字段后得到的16位中的高3位。	用于片段标签的是组合了片段标签和片段偏移字段后得到的16位中的低3位。
	标识字段是16位长。	标识字段是32位长，没有不要拆分（DF）的标签，因为IPv6路由器绝不执行拆分操作。

IPv6报文结构与基本报头

报文结构

基本信息

IPv6基本报头含8个字段

总长度为40个字节

与IPv4包头对比

6个域或被删除或置于扩展报头中；

头长/标识符/标志/报头偏移/校验和/选项

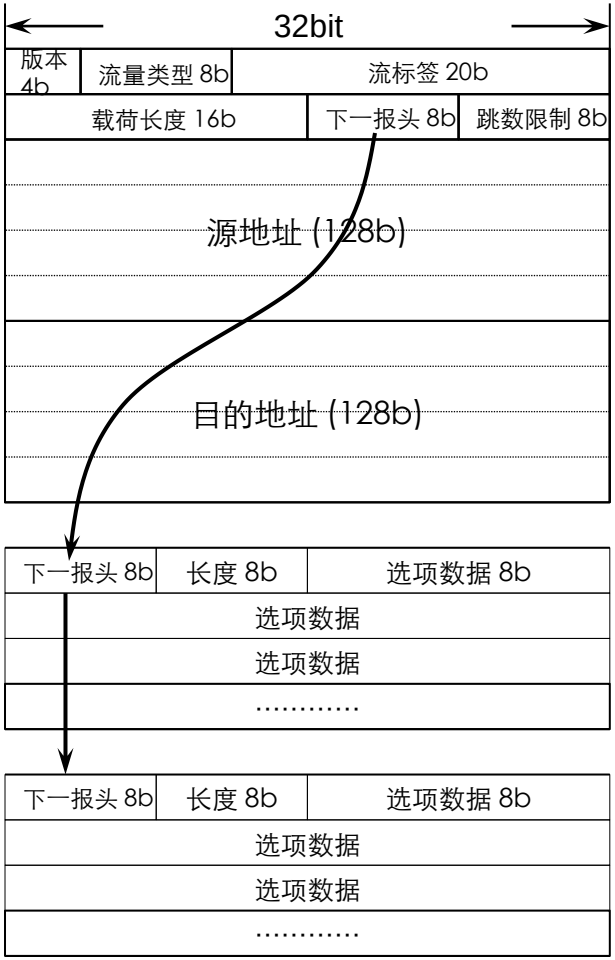
3个域名称/功能类型被改变功能

服务类型/协议类型/生存时间

新增加1个域

流标签

IPv6扩展报头



扩展包头设计

IPv6扩展报头是可能跟在基本IPv6报头后面的可选报头

将所有可选字段移出IPv6报头，置于扩展头中

提升路由器处理数据报的效率，对转发性能有正面影响

IPv6邻居发现协议

邻居发现ND（Neighbor Discovery），确定邻居节点之间关系的一组消息和进程

邻居发现协议替代了IPv4的ARP和ICMP路由器发现

IPv6邻居发现协议主要包括以下功能：

地址冲突检测功能

确定IPv6地址是否可用的一种探测机制

邻居发现功能

类似IPv4中的ARP，主要实现对邻居地址的解析和邻居可达性的探测

路由器发现功能

用来定位邻居路由设备，同时学习和地址自动配置有关的前缀和配置参数

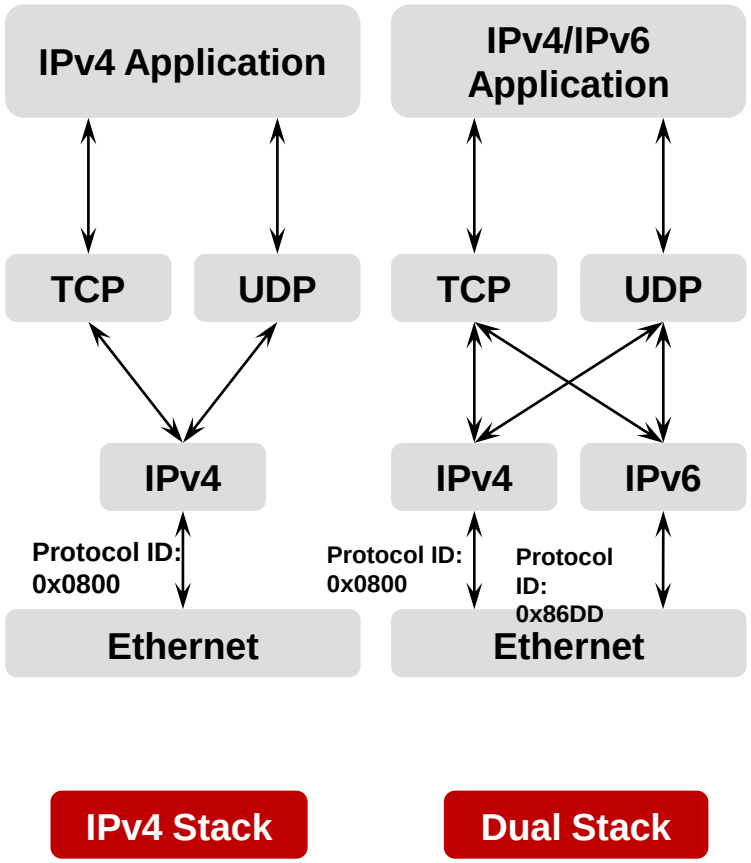
地址自动配置功能

路由设备通过使用路由器通告报文和针对每一前缀的标记通知主机如何进行地址自动配置

重定向功能

用来通知主机去往目的地的理想下一跳IPv6地址

IPv4/IPv6双栈技术总览



双协议栈节点(Dual Stack)

IPv6节点兼容IPv4的最直接有效的办法就是保留一个完整的IPv4协议栈，这样的节点即为双栈节点；

双协议栈特点：

以太网等多种链路协议支持双协议栈；

根据三层报文类型确定IPv4/IPv6报文；

IPv4报文0x0800/IPv6报文0x86DD；

多种应用支持双栈，如DNS/FTP/Telnet；

上层应用在传输层可选用TCP或UDP，但优先选择IPv6协议栈；

IPv4不足与IPv6的改进

IPv4的不足

IPv4地址空间不足

IPv4地址空间约43亿，在移动互联网/物联网技术发达的今天难以满足用户需求；

不能有效聚合路由

IPv4发展初期的分配规划问题，造成IPv4地址分配不连续；

这导致路由聚合困难，路由表日益增大，占用存储空间，降低处理效率；

不易进行自动配置和重新编址

由于IPv4地址只有32比特，并且地址分配不均衡，导致在网络扩容或重新部署时，经常需要重新分配IP地址。

不能解决日益突出的安全问题

IPv4协议没有针对安全性的设计，固有的框架结构不能支持端到端的安全。

IPv6的改进

近乎无限的地址空间

提供约 3.4×10^{38} 个地址，可为所有网络设备提供一个全球唯一的地址；

层次化地址设计

IPv6的地址空间采用了层次化的地址结构，利于路由快速查找；

同时，路由聚合可精简路由表的大小，提高路由设备的处理效率；

地址可自动配置

IPv6支持有状态和无状态地址配置；

内置安全性

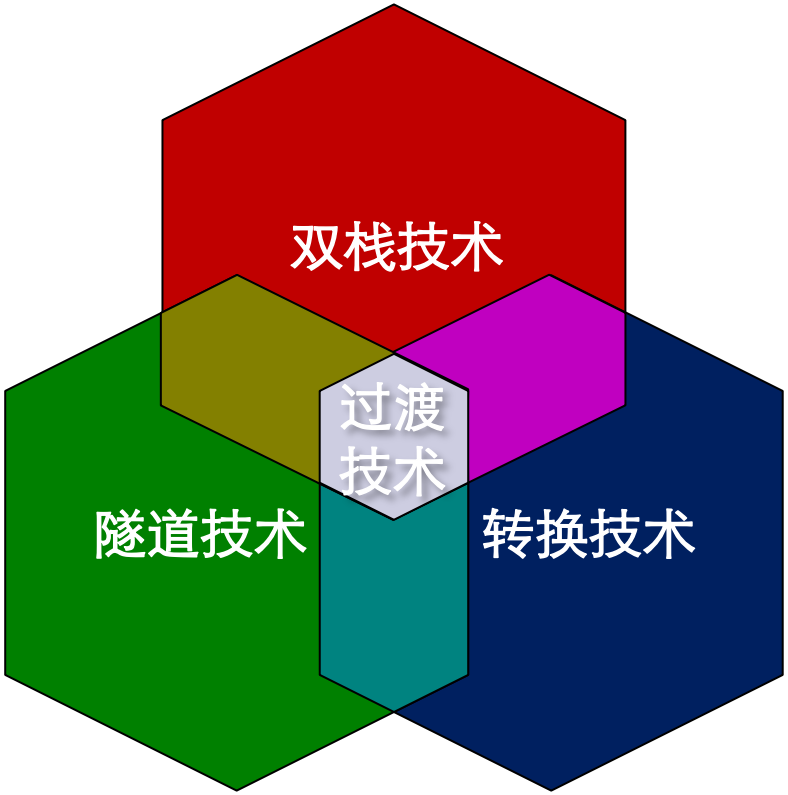
IPv6报文包含一个与IPSec特性相关的标准扩展头，可以提供端到端的安全特性；

其他改进

QoS改进/源和目的地址选择/扩展报头

目录

业界公认的IPv6的过渡技术



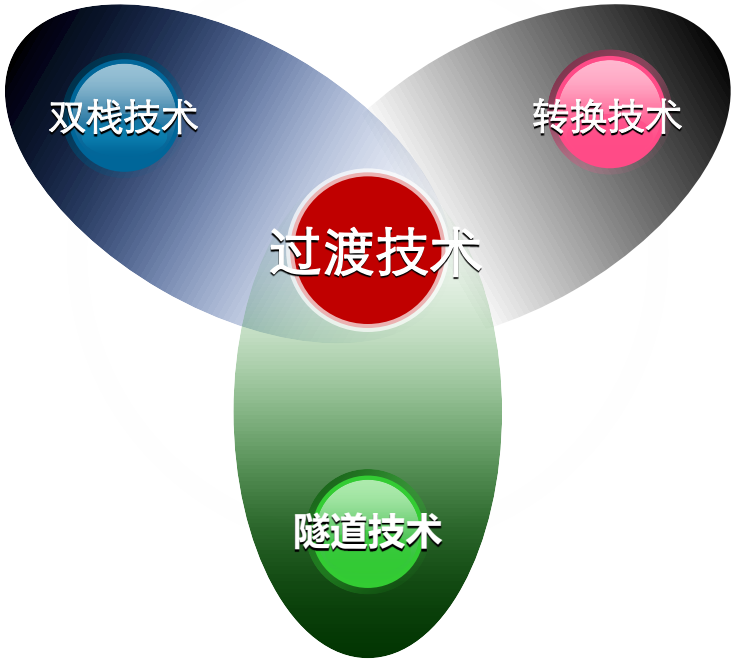
主要分为3类过渡技术；

根据具体的应用场景灵活选择相应的技术；

没有最好的过渡技术，没有任何一种技术方案可以解决所有问题。

现网部署过程中，往往是多种技术方案组合部署，应对多种应用场景。

业界常见的三种过渡技术



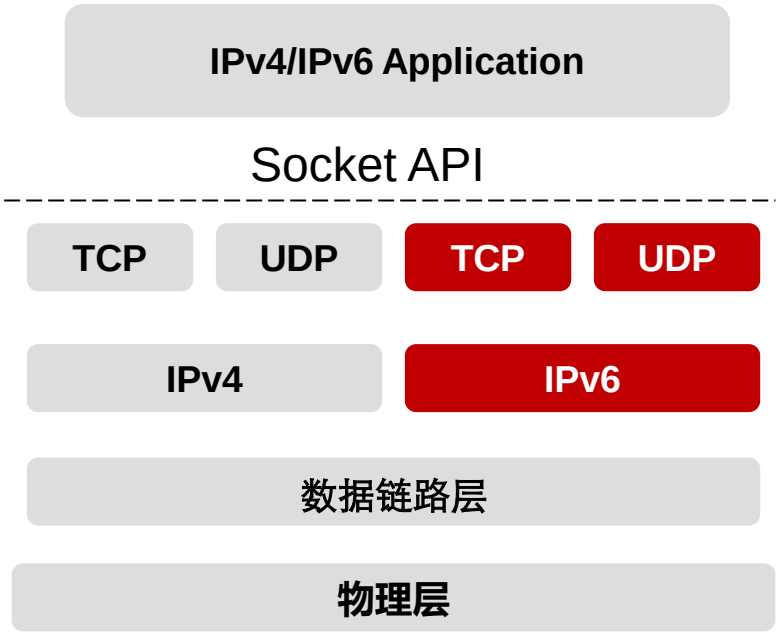
主要分为3类过渡技术；

根据具体的应用场景灵活选择相应的技术；

没有最好的过渡技术，没有任何一种技术方案可以解决所有问题。

现网部署过程中，往往是多种技术方案组合部署，应对多种应用场景。

双栈技术



双栈技术简介

在RFC4213中定义

在终端设备/网络节点上，既安装IPv4又安装IPv6的协议栈；

实现分别与IPv4或IPv6节点间的信息互通；

双栈技术实现与部署

网络节点同时支持IPv4和IPv6协议栈；

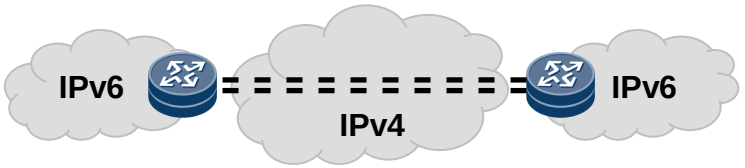
源节点根据目的节点选用不同的协议栈；

网络设备根据报文协议类型，选择不同的协议栈进行处理和转发；

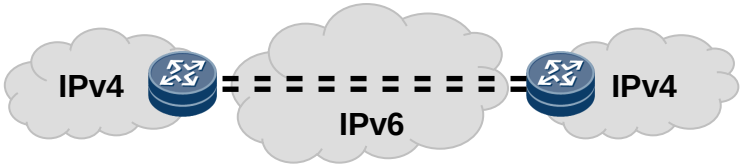
双栈技术可在单一网络节点上实现，也可以是一个双栈网络；

对于双栈网络，其中所有节点必须同时支持IPv4/IPv6协议栈，连接双栈网络的接口必须支持配置IPv4地址和IPv6地址；

隧道技术



IPv6 Over IPv4隧道



IPv4 Over IPv6隧道

隧道技术简介

将一种协议封装在另一种协议中的技术；

用于实现IPv4网络中IPv6网络孤岛之间的互联，或者IPv6网络中的IPv4网络互联；

只需要边界节点实现双栈；

隧道技术实现

应用A协议网络的边缘节点，将A协议报文封装在B协议报文中；

这个B协议报文，在B协议网络中传输到目的所在的A协议网络的边缘节点后，解封装去掉外部B协议报文头，恢复原来的A协议报文；

IPv6 Over IPv4隧道：A=IPv6, B=IPv4；

IPv4 Over IPv6隧道：A=IPv4, B=IPv6；

IPv6手工配置隧道

简介

IPv6手工配置隧道在RFC 2893中定义，源和目的地址唯一确定，提供一个点到点的连接；

应用场景

在IPv6过渡初期，为实现IPv6穿越IPv4网络互通可以使用IPv6手工配置隧道技术；

配置与实现

在一对边界节点上，手工配置隧道的源地址/目的地址，通常用于为两个IPv6网络提供连接；

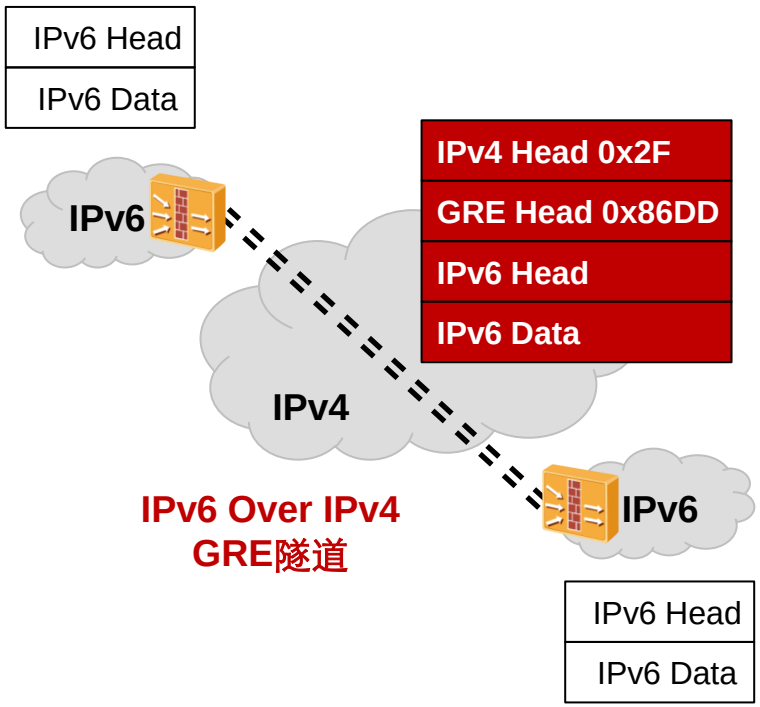
对于从IPv6侧收到的IPv6报文，根据报文目的地址查找IPv6转发表，根据隧道接口配置的隧道源端和目的端的IPv4地址进行封装，由IPv4协议栈处理。在经过IPv4网络转发到隧道对端节点后，进行解封装，并交给IPv6协议栈处理；

优势与不足

IPv6手工配置隧道技术实现简单，除边界路由器以外的其它设备没有双栈要求；

隧道需要手工配置，网络维护成本较高，只能提供点对点连接导致使用范围狭窄；

IPv6/IPv4 GRE隧道



IPv6 Over IPv4
GRE隧道

简介

GRE是通用路由封装协议(Generic Routing Encapsulation)的缩写；

由RFC2784所定义；

应用场景

两个IPv6区域之间点对点连接；

没有密文传输的需求；

配置与实现

隧道终端节点支持双栈；

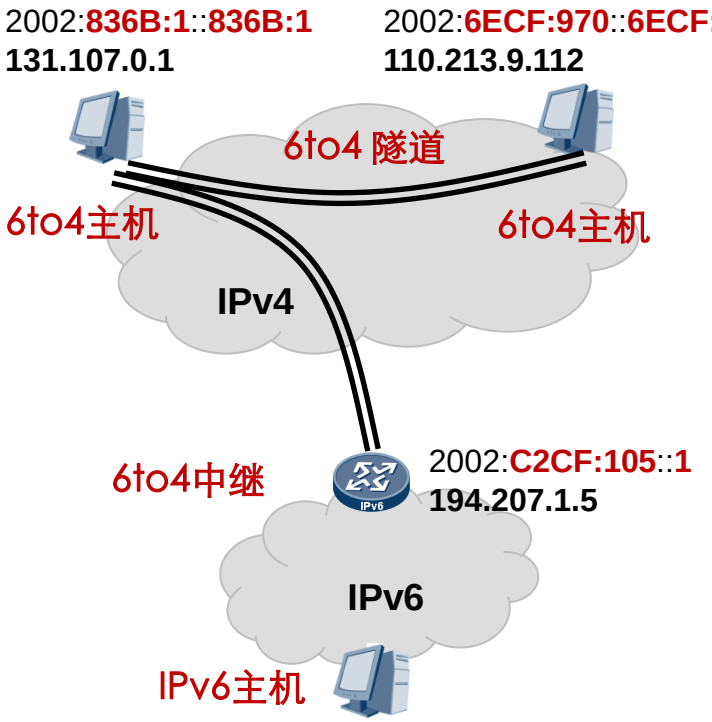
在一对终端节点手工配置隧道；

优势与不足

技术成熟，实现简单；

需要手工配置，增加网络维护成本，只能提供点到点连接；

6to4隧道



简介

6to4隧道是一种通过内嵌IPv4地址将多个IPv6孤岛通过IPv4网络互联的机制；

由RFC3056/2893等定义；

应用场景

多个IPv6孤岛之间互联；

配置与实现

48bit地址前缀 2002::[IPv4 Addr]；

16bit子网ID和64bit接口ID；

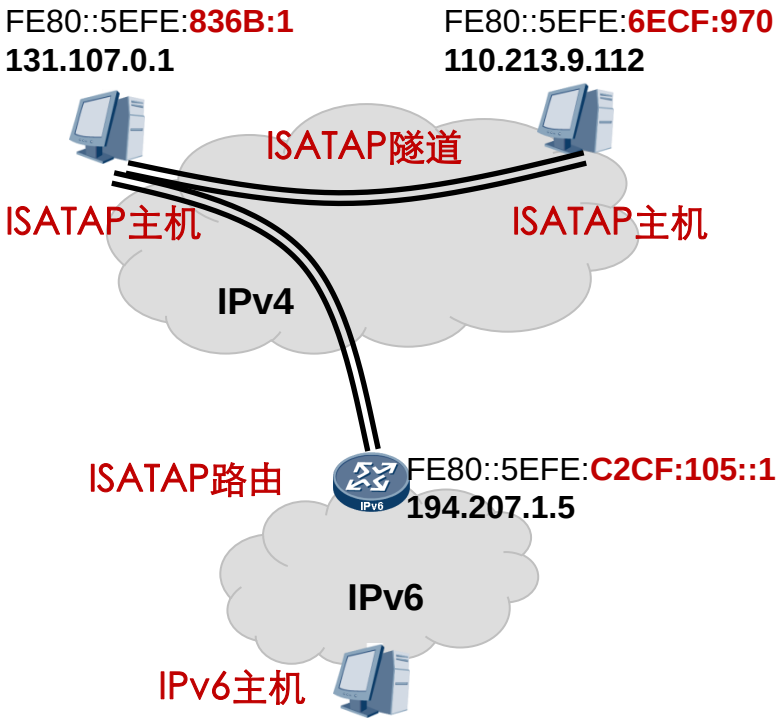
通过虚拟6to4隧道接口收发报文；

优势与不足

可点对多点，可以自动配置；

需要使用者对IPv6有一定配置经验；

ISATAP隧道



简介

ISATAP隧道通过内嵌IPv4地址，实现IPv6孤岛或主机之间的互联；

由RFC5214定义；

应用场景

孤立IPv6主机互联或接入IPv6网络；

IPv6孤岛接入IPv6网络；

配置与实现

Link-local 地址前缀 FE80::/64；

32bit子网ID 0000:5EFE;

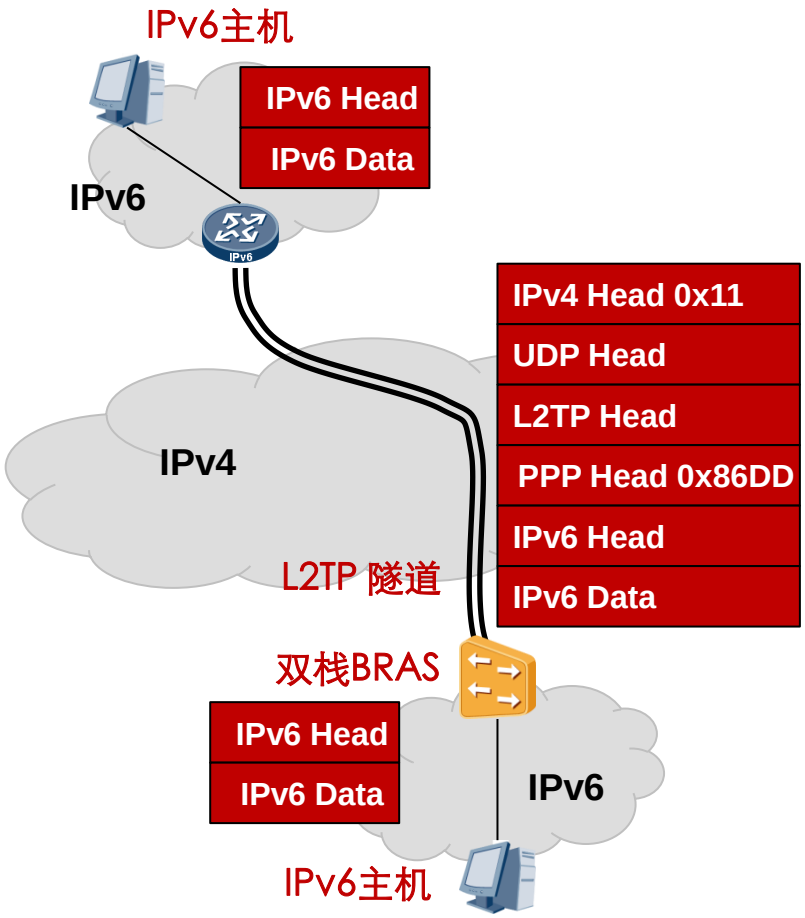
32bit IPv4地址；

优势与不足

不要求隧道端节点具备IPv4公网地址；

需要使用者对IPv6有一定配置经验；

L2TP隧道



简介

L2TP隧道是一种将PPP协议封装在UDP报文中的二层隧道技术，隧道可承载IPv6；

由RFC2661定义；

应用场景

多个IPv6孤岛之间互联；

双栈主机穿越IPv4网络访问IPv6网络；

配置与实现

BRAS支持v6/v4双栈接入，v6/v4双栈节点接入v6/v4双栈BRAS；

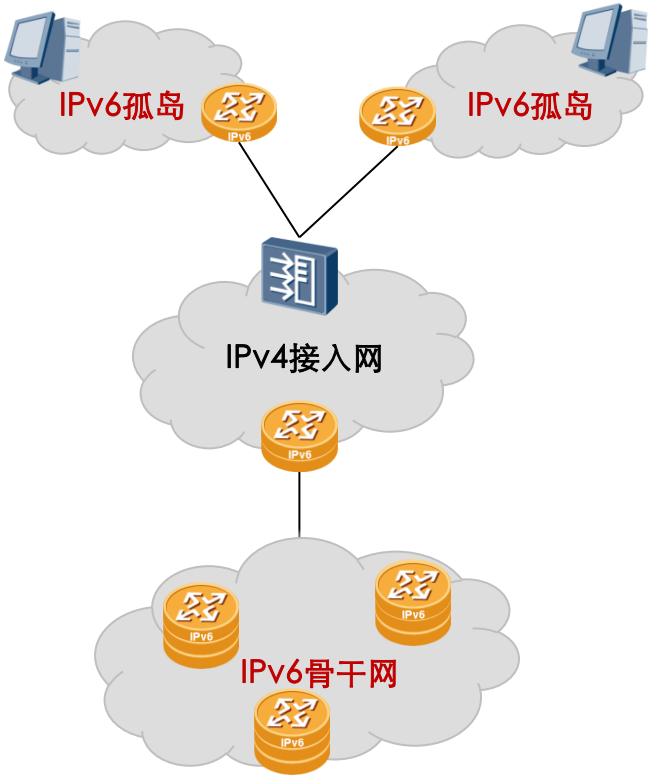
IPv6协议承载于虚拟PPP二层隧道中；

优势与不足

支持基于用户名/密码的访问控制，带宽/认证/计费等可以灵活配置

BRAS价格较高；

6RD隧道



简介

6RD是IPv6运营商在原有IPv4网络基础上，向IPv6用户提供接入服务的过渡方案；

在RFC5969中定义；

应用场景

IPv6孤岛接入IPv6骨干网；

配置与实现

IPv6孤岛的CPE支持6rd；

运营商城域边界接入服务器等保持现状；

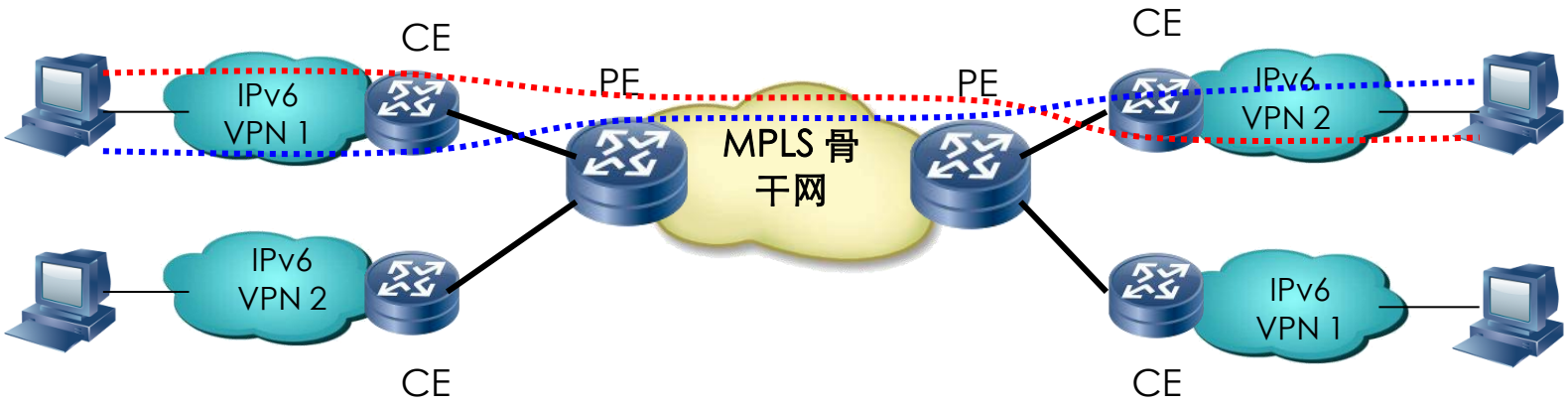
运营商集中部署6rd网关；

地址前缀由运营商分配；

优势与不足

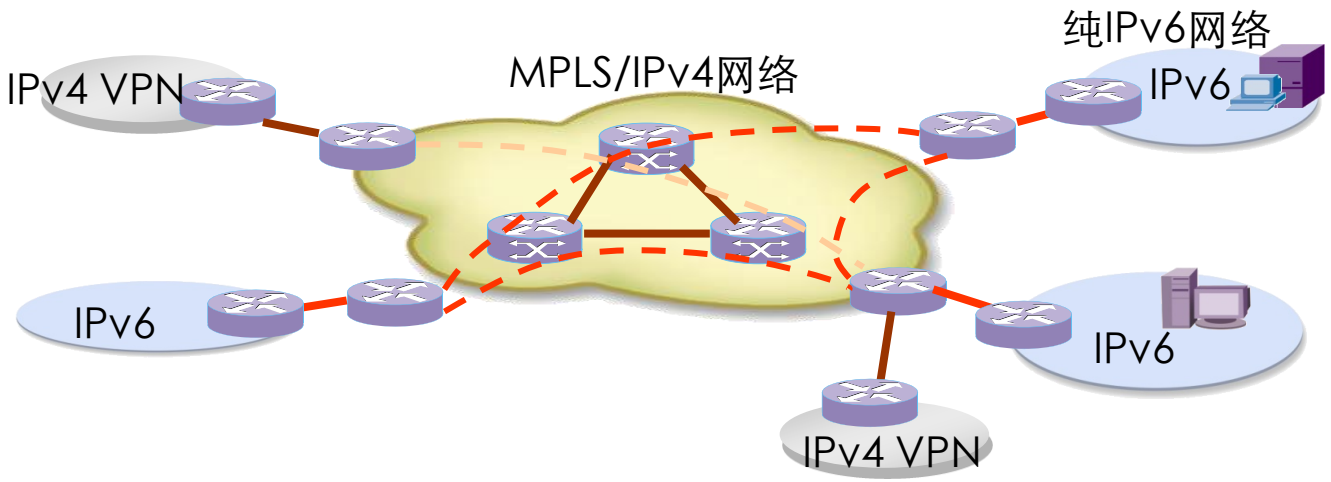
可快速部署IPv6试点；

IPv6 VPN互连的解决 - 6vPE



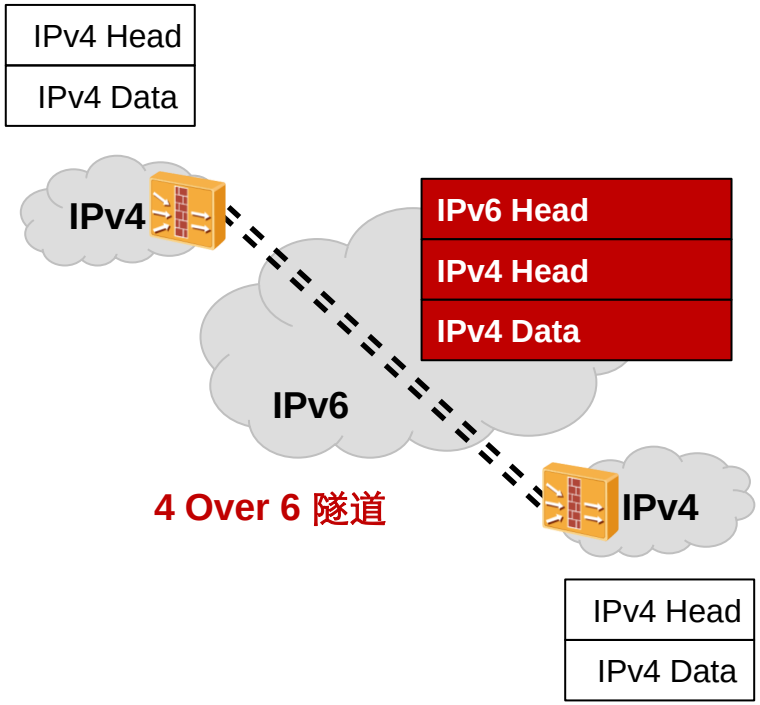
- IPv6 VPN（6VPE）：当VPN的每个站点具有IPv6能力，用IPv6地址通过某个接口或子接口链接到骨干网的边缘路由器PE，该VPN就叫做IPv6 VPN。
  - ✓ PE的控制层面完成私网IPv6路由的学习发布，以及给私网IPv6路由分配标签，转发层面支持多实例转发，其实现原理类似于IPv4 VPN。
  - ✓ 用户站点为IPv6站点，PE设备应支持IPv6、IPv4双协议栈

IPv6孤岛互连的解决 - 6PE



- 6PE：具备IPv6能力的PE
  - ✓ 在一个已经部署了MPLS的IPv4骨干网上，可以利用6PE（IPv6 Provider Edge）技术为分散用户的IPv6网络提供互连的能力
  - ✓ PE升级IPv6即可，原理同IPv4 VPN，即将IPv6看作为IPv4的一个VPN，多个IPv6孤岛属于同一VPN，利用VPN机制在PE之间建立隧道连接
  - ✓ IPv6-in-MPLS，适用于有MPLS网络的场合，通过MPLS网络连接多个IPv6 孤岛，使用MP-BGP交换IPv6可达信息
  - ✓ 可以充分利用已有MPLS或VPN网络

IPv4 over IPv6隧道



简介

4 Over 6 隧道用于连接IPv6网络中IPv4孤岛；

应用场景

IPv6演进后期，保证IPv4孤岛之间互联；

配置与实现

IPv4网络的边界防火墙/路由器支持双栈；

在一对终端节点手工配置隧道；

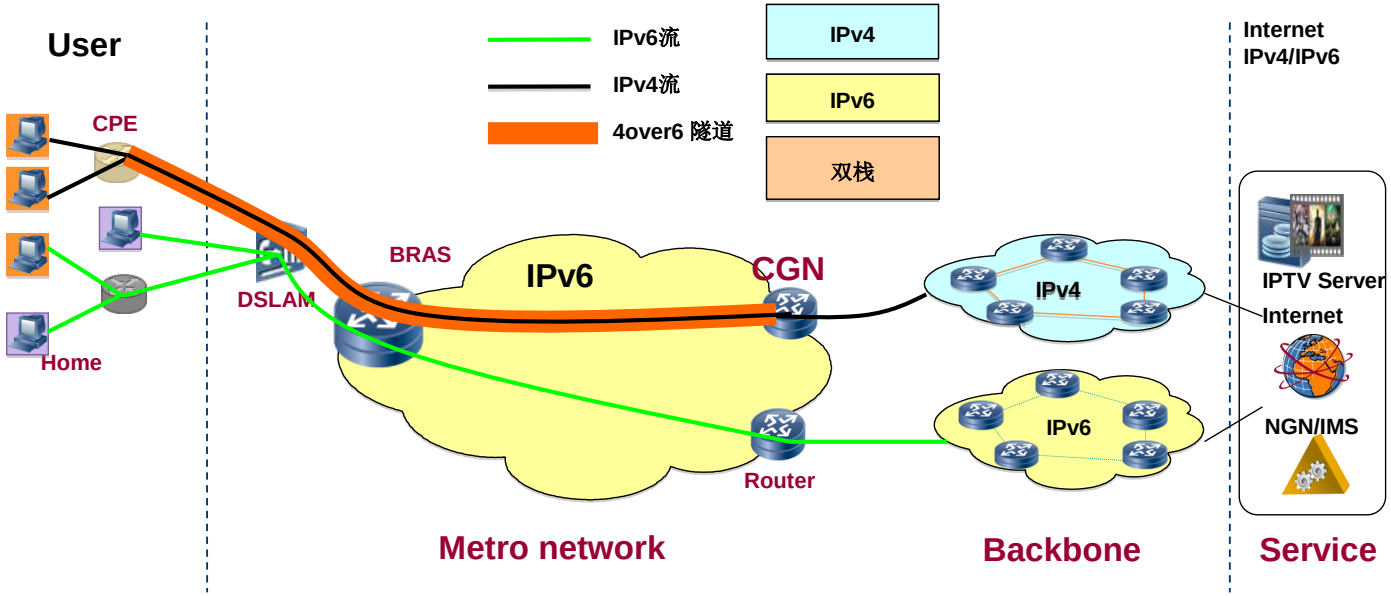
优势与不足

可以最大限度保护原有IPv4网络投资；

支持4Over6的网络设备较少；

Ds-Lite

Ds-Lite也称作轻量级双栈，有双栈主机+IPv6主机组成，DS-lite网络中只有家庭网关CPE和运营级网关CGN为双栈，其它网络节点只支持IPv6。CGN网关需要同时支持IPv4-in-IPv6 tunnel和NAT44功能。可看成IPv4 over IPv6隧道技术与NAT44的组合。家庭用户可获得IPv6和私有IPv4地址，这样IPv6报文直接穿越家庭网关进入IPv6 Internet；IPv4报文通过CPE和CGN间的IPv4-in-IPv6 tunnel 到达CGN网关，在CGN上网关实现tunnel 的解封装，并将v4私有地址转化为公网地址，发送到IPv4 Internet。



隧道技术比较

	手工配置隧道及GRE隧道	6to4	L2TP	ISATAP
关键特征	静态配置	IPv6地址内嵌IPv4公网地址；采用知名前缀	基于PPP，隧道从BRAS发起	可使用私网地址
适用场景	网络设备间的IPv6孤岛互联	IPv6孤岛互联	宽带接入	站点内终端使用
成熟度	高	高	高	高
部署情况	有部署	有部署	有部署	有部署
是否要求终端支持	和终端无关	终端已支持	和终端无关	终端已支持
主要问题	配置工作量大	可运营部署性差。路由发布有问题	对于双栈用户，v4和v6流量都要经过BRAS	只适合站点内通信

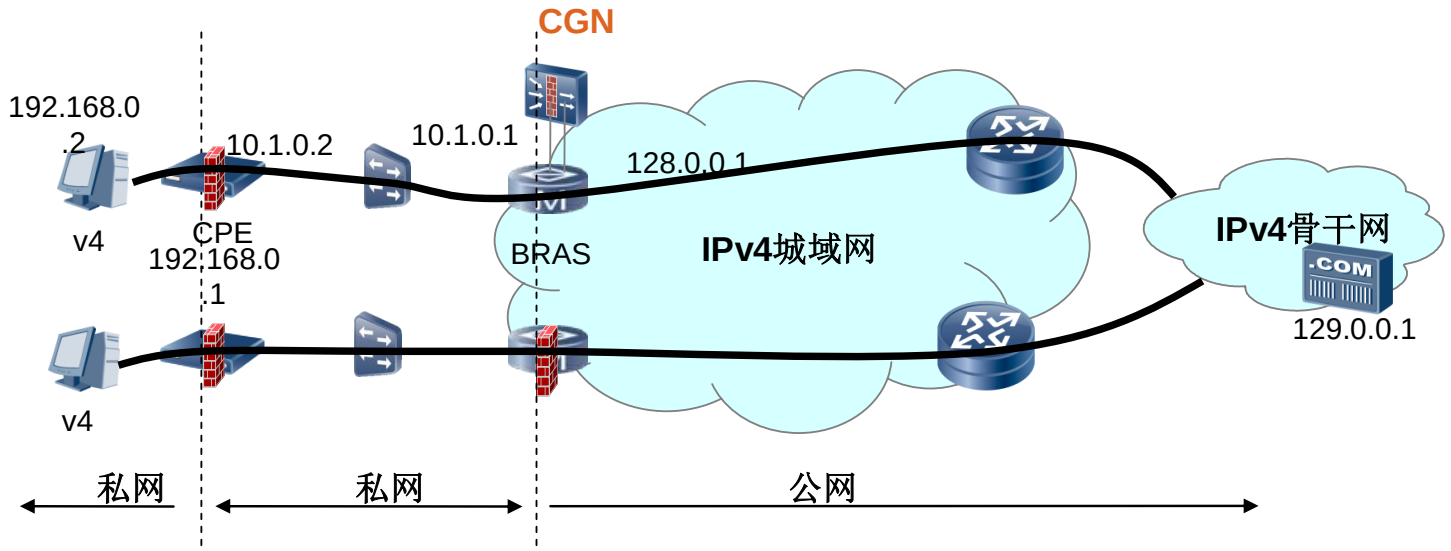
地址转换技术

转换技术		基本原理	应用场景	问题分析
网络层转换技术	NAT-PT(RFC2766)	在网络层实现IPv4与IPv6双向地址转换	早期必选的地址转换技术，目前标准被废弃	存在网络单出口，ALG等问题，目前被NAT64替代
	Stateful NAT64 (RFC6146)	剥离NAT-PT与DNS ALG的偶合，简化处理流程	只能应用于v6发起访问到v4	ALG问题仍然存在
	Stateless NAT64(IVI) (RFC6145)	通过特殊地址实现v6到v4的无状态地址转换	只能应用于特定场景下的转换	不能解决地址紧缺问题，ALG问题仍然存在
	SIIT(RFC2765)	使用特殊地址 :0:0:0:0:FFFF:w.x.y.z 或 ::FFFF:w.x.y.z，实现v6到v4的无状态地址转换	早期的无状态转换技术，目前很少应用	需要IPv4公网地址，不能缓解抵制短缺问题；需要ALG配合.
	BIS(RFC2767)	在主机或终端协议栈实现的IPv4到IPv6的地址转换	一般应用于单栈主机	网络设备不涉及
传输层转换技术	TRT(RFC3142)	在传输层IPv6的TCP/UDP与IPv4的TCP/UDP之间实现地址转换	适用于网络设备，目前很少应用	TRT转换设备实现代价很大
应用层转换技术	SOCKS64	通过SOCKS64服务器，实现IPv6 Socket与IPv4 Socket之间的转换	一般适用于双栈主机或网络设备，目前很少应用	SOCKS64代理服务器的实现代价很大
	BIA(RFC3338)	在主机Socket API实现转换	应用于双栈主机应用程序转换	网络设备不涉及
	ALG	应用层地址转换	NAT-PT及NAT64等都需要与ALG配合，实现应用层转换	对具体每一种应用协议都需要识别分析，实现代价很大，性能较低

为了缓解IPv4地址紧缺的问题，地址转换技术也是运营商网络过渡的必然选择；
地址转换技术主要包括IPv4私网地址到公网地址转换的DS-Lite, NAT44和NAT444；
IPv6地址到IPv4地址转换AFT(Address Family Translation)相关的NAT-PT和NAT64；

NAT44/NAT444

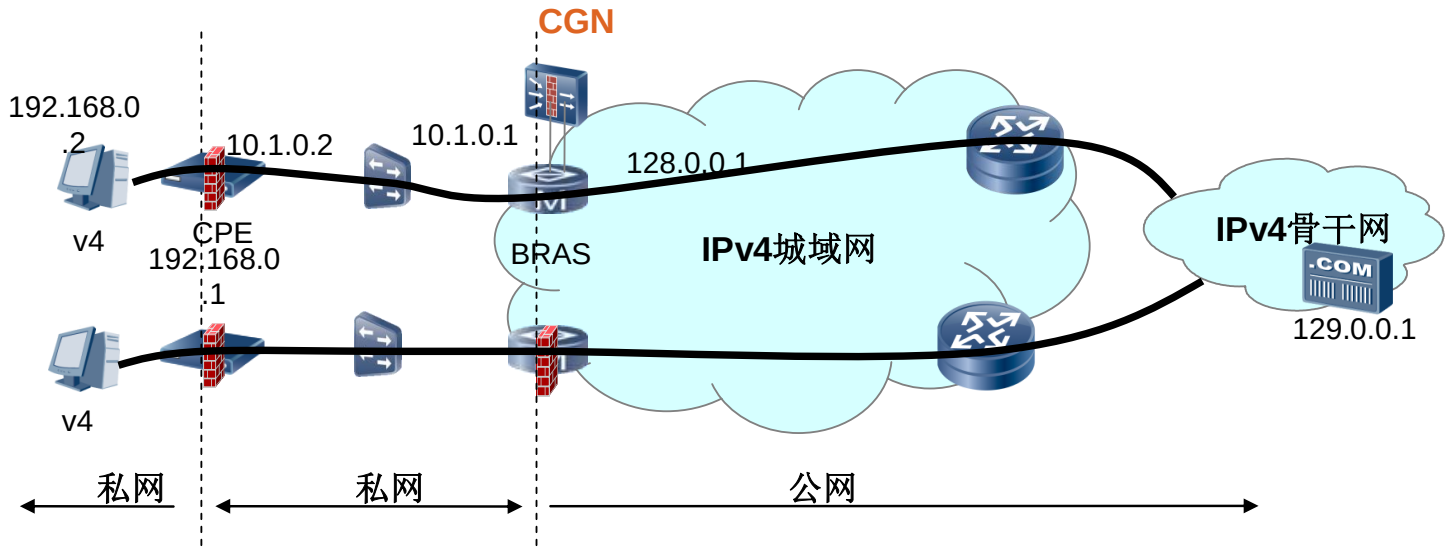
私网地址是不会出现在Internet上的，使用私网地址的主机也不能直接访问Internet。通过NAT转换，可以将私网地址转为公网地址，使私网主机能够访问Internet。只有当私网主机需要访问Internet的时候，NAT路由器才为该主机分配一个临时的合法IP地址，因此用户网络内的主机不需要都拥有合法的IP地址就可以访问Internet，这样就达到了节省IP地址的效果。



为了节省IP地址，可以选择在CPE或CGN设备作NAT44地址转换，使私网地址用户能够访问Internet，也可以选择同时在CPE和CGN作地址转换也就是NAT444。CPE NAT将用户网络私网地址转换为运营商网络私网地址，CGN NAT将运营商私网地址转换为公网地址。

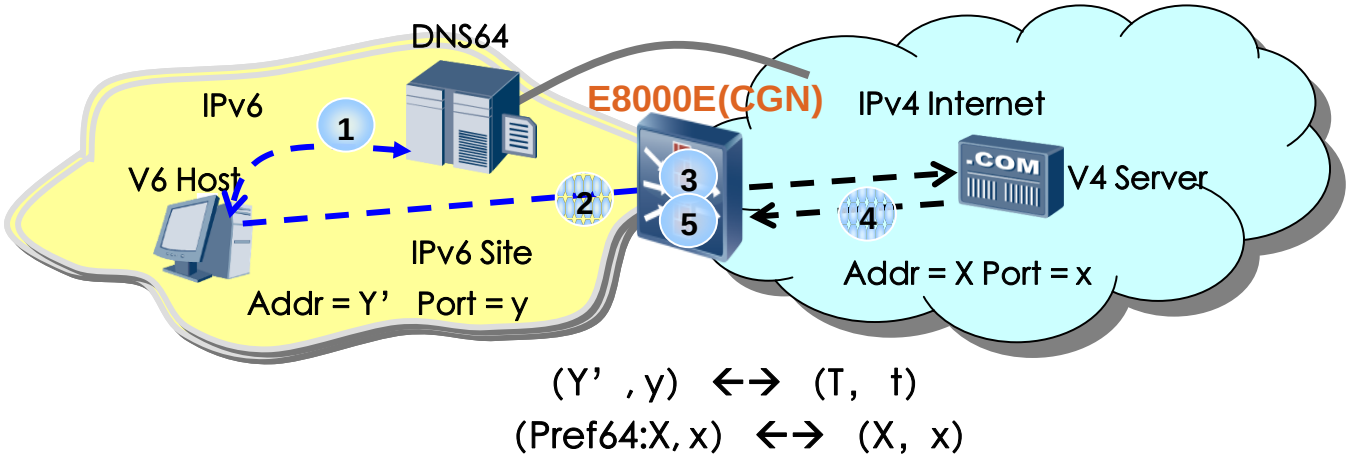
NAT44/NAT444

私网地址是不会出现在Internet上的，使用私网地址的主机也不能直接访问Internet。通过NAT转换，可以将私网地址转为公网地址，使私网主机能够访问Internet。只有当私网主机需要访问Internet的时候，NAT路由器才为该主机分配一个临时的合法IP地址，因此用户网络内的主机不需要都拥有合法的IP地址就可以访问Internet，这样就达到了节省IP地址的效果。



为了节省IP地址，可以选择在CPE或CGN设备作NAT44地址转换，使私网地址用户能够访问Internet，也可以选择同时在CPE和CGN作地址转换也就是NAT444。CPE NAT将用户网络私网地址转换为运营商网络私网地址，CGN NAT将运营商私网地址转换为公网地址。

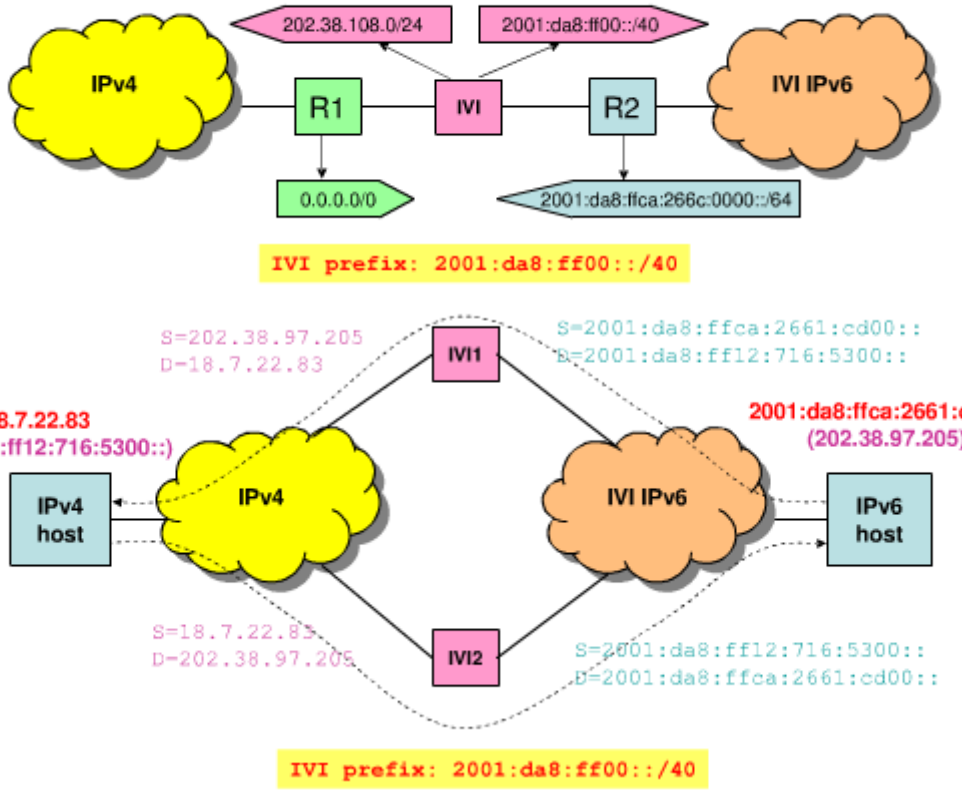
Stateful NAT64



Stateful NAT64可以说NAT-PT的简化版本。NAT64解除了和DNS ALG的耦合，降低了协议实现复杂度，可以解决NAT-PT组网中的单出口问题，但是动态NAT64只能实现IPv6 Site发起访问到IPv4 Internet。

IVI

IVI方案是由CNGI-CERNET2的研究人员清华大学李星教授提出的IPv4和IPv6的翻译技术。IVI方案的思路是把IPv6集中在某个特定的地址，使其能与IPv4进行无状态的映射，实现IPv6和IPv4的互访并保持端到端的地址透明。这种转换对上层协议是透明的，可以在纯IPv6节点和纯IPv4节点之间建立通信，无需修改应用软件。IVI是Stateless的一种。

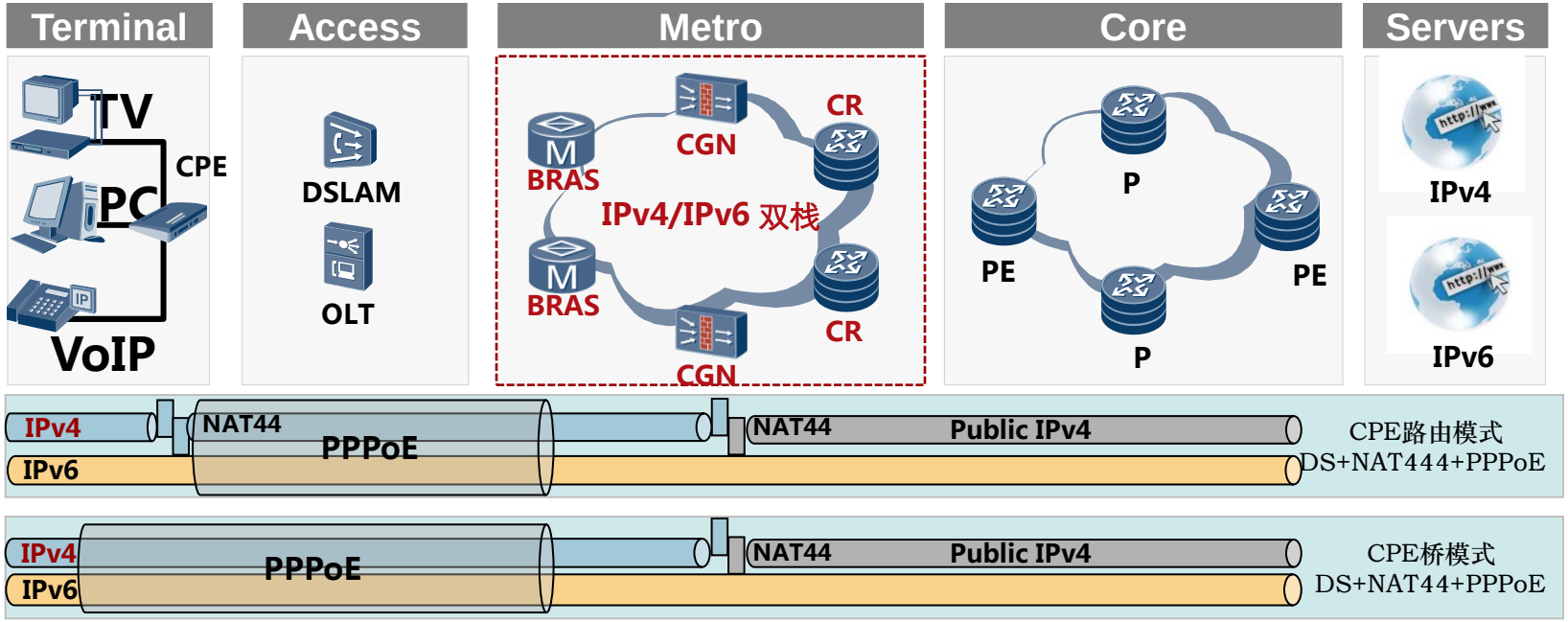


地址转换技术比较

	NATPT	NAT64	IVI
优势	能解决4访问6，虽然有缺陷	DNS-ALG单独部署	无状态，简单
存在的主要问题	拓扑限制、扩展性问题、记录优选问题、热备份情况下需要状态同步	继承NAT的相关问题	不能节省地址。对于不使用IVI地址的其它IPv6节点，还需要其它翻译技术。
适用场景	6访问4或4访问6	6访问4	6访问4或4访问6

基于主机的转换技术很少有实现；应用级的技术通常深度解析而效率低下，不能作为通用的转换技术；纯网络级转换效率较高、但难以处理报文体中携带的地址，最理想的转换应该是NAT-PT(NAT64)+常用ALG的组合部署 。

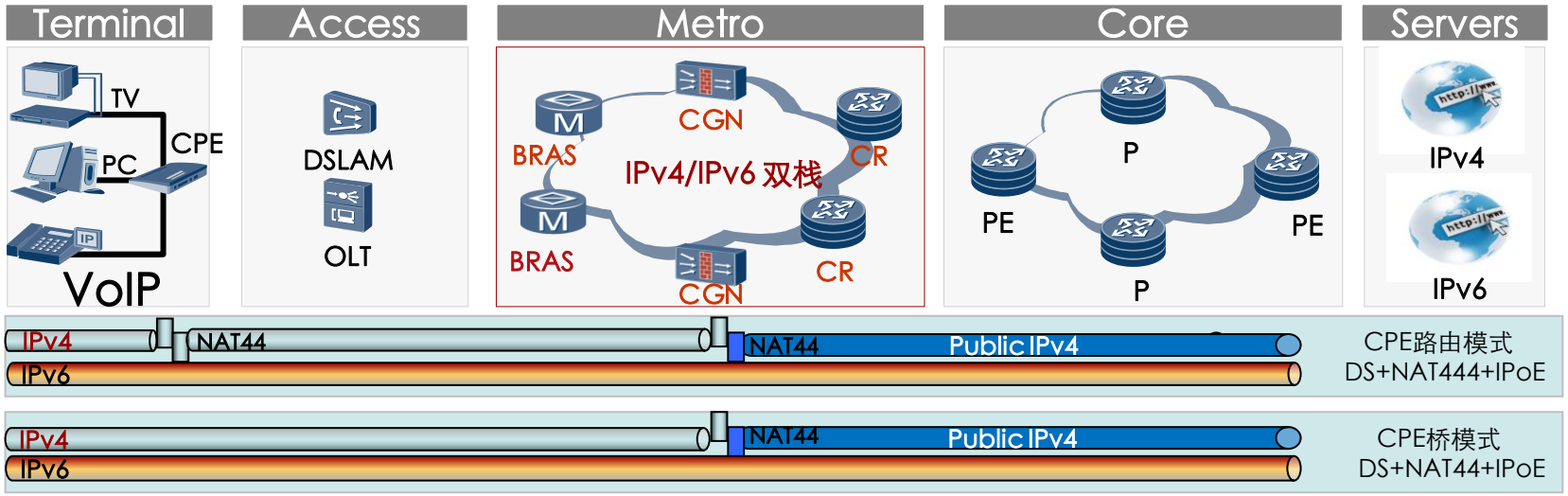
Dual Stack+NAT444+PPPoE



- BRAS和城域三层设备开启双栈，节点具有IPv4和IPv6双重地址和协议栈，提供IPv6路由和转发能力。
- 主机双栈，通过IPv4地址访问IPv4 Internet，通过IPv6地址访问IPv6 Internet。
- 主机分配IPv4私网地址，通过NAT解决IPv4地址耗尽问题。 CGN提供电信级NAT转换能力。
- IPv4、IPv6报文使用同一PPPoE逻辑链路接入，用户接入和认证方式不变。

最大限度保留用户投资，解决IPv4地址短缺，支持已有网络平滑升级到IPv6

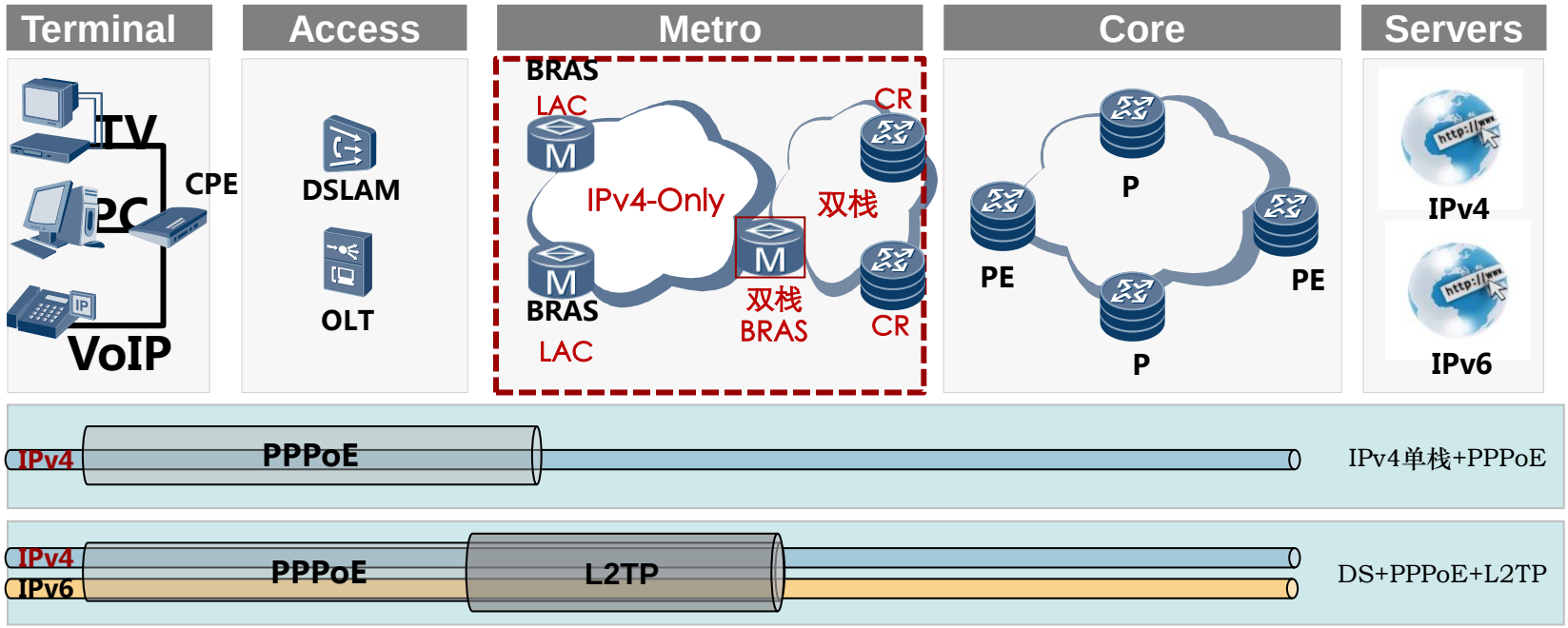
DualStack+NAT+IPoE



- BRAS和城域三层设备开启双栈，节点具有IPv4和IPv6双重地址和协议栈，提供IPv6路由和转发能力。
- 主机双栈，通过IPv4地址访问IPv4 Internet，通过IPv6地址访问IPv6 Internet。
- 主机分配IPv4私网地址，通过NAT解决IPv4地址耗尽问题。 CGN提供电信级NAT转换能力。
- IPv4、IPv6报文在BRAS上作为一个IPoE逻辑链路接入，用户接入和认证方式不变。

最大限度保留用户投资，解决IPv4地址短缺，支持已有网络平滑升级到IPv6

DualStack+L2TP



- 城域新增少量BRAS和CR设备支持双栈（或现网设备软件升级），其它大部分网络设备保持IPv4不变。
- 单栈IPv4用户接入方式不变，PPPoE报文仍在边缘BRAS(LAC)终结。
- 双栈用户，由双栈BRAS(LNS)分配IPv4和IPv6地址，通过IPv4地址访问IPv4 Internet，通过IPv6地址访问IPv6 Internet。
- 双栈用户PPP报文通过L2TP穿越IPv4三层网络，在新增双栈BRAS(LNS)终结。

初期IPv6用户量较少，且分布较稀疏时，仅在城域核心增加少量双栈BRAS，快速实现IPv6接入

基础过渡技术对比

过渡技术	技术介绍	优点	缺点
双栈 Dual Stack	同时支持IPv6和IPv4协议，应用程序根据DNS解析地址类型选择使用IPv6或IPv4协议。基础的过渡技术IPv6孤岛互连，IPv6和IPv4的互通都需要。	互通性好，实现简单，允许应用逐渐从IPv4过渡到IPv6适合大规模部署。	对每个IPv4节点都要升级，没有解决IPv4地址紧缺问题（企业使用私有地址时无此影响）。
隧道 Tunnel	主要利用IPv6报文作为IPv4的载荷或由MPLS承载。在原有IPv4的网络使IPv6孤岛互连。主要的技术有：手工隧道、6to4、6over4、BGP Tunnel、ISATAP等。主要解决IPv6孤岛互连。	将IPv4的隧道作为IPv6的虚拟链路。	额外的隧道配置，降低效率，只能实现v6-v6设备互连，适合小规模使用。
转换技术 Translation	转换过渡技术用于实现纯IPv6节点和纯IPv4节点间的互通。一般是借助中间的协议转换服务器实现IPv6网络与IPv4网络间的通信。 主要技术有：SIIT、NAT64和IVI等。	不需要升级设备。	需要投入额外的设备，效率低。存在应用层网关（ALG）问题，可扩展性差

目录

IPv6外部环境

内容可根据需要自行选择

分类	内容	备注
政府政策 （国际、国内）	美国政府	各国政府政策大力推动IPv6发展
	其他国家或地区政府	
	中国政府	
国内运营商规划 （产业链成熟）	中国电信	骨干网络及业务对IPv6的支持，厂商对运营商的支持
	中国移动	
	中国联通	
互联网协会 （论坛技术推动）	世界IPv6日 （World IPv6 Day）	世界范围的网站、运营商、CDN网络对IPv6的支持
	世界IPv6启动活动 （World IPv6 Launch）	

各国政府和地区的IPv6部署进展

区域	进展
美国	2010年发布了IPv6计划及路标，2012年将确保政府机构可以利用IPv6与外界保持通信； 2014年将实现政府机构的内部网络可以通过IPv6运作。
欧盟	欧盟IPv6路线图计划到2010年底，实现25%的企业、政府机构和家庭用户迁移至IPv6。但是这一目标未能实现，欧盟范围内的使用率约为8%。
韩国	2010年9月，韩国通信委员会召开了关于创建“下一代互联网协议（IPv6）促进计划”会议，并宣布从2011年6月开始，韩国国内的互联网、IPTV、3G等移动通信服务都将启用下一代互联网协议IPv6。韩国政府曾宣布2011年6月禁用IPv4，全面部署IPv6，然而，没有进一步消息证实韩国成功实现IPv6对IPv4的全面替代。而韩国网络服务商则计划在2013年提供IPv6服务。
中国	中国下一代互联网示范工程(CNGI)是为通过提前部署IPv6来占据Internet比例的一项五年计划。中国在北京2008奥运会时展示了CNGI和IPv6网络基础设施，通过使用IPv6来互联从安全摄像头、出租车到奥林匹克赛事摄像头的各种设备。
印度	印度政府、通信与信息技术部和通信部的IPv6部署路标及策略: 所有的主要服务提供商（至少有10,000 Internet 用户或有STM-1 带宽）在2011年12月前需要支持IPv6流量处理及提供IPv6服务. 所有的中央及州政府部门包括其PSUs应该在2012年3月前开始使用IPv6服务.
日本	2009年10月，由日本总务省、JPNIC、电信和互联网运营商协会成立“日本IPv4地址枯竭工作组”，发布《IPv6行动计划》，决定从2011年4月全面启动IPv6服务，目前已有11家ISP提供IPv6商用服务。

国家政策助推IPv6产业发展

2011年12月23日

国务院常务会议研究部署加快发展我国下一代互联网产业，确定我国IPv6发展路线时间表；

2012年2月10日

国家发改委办公厅发布《关于组织实施2012年下一代互联网技术研发、产业化和规模商用专项的通知》；

明确投入专项资金扶持四大方面：

电信运营企业公众网络IPv6升级改造及规模商用；

网站系统IPv6升级改造；

技术研发、产业化和新兴应用示范；

下一代互联网标准体系建设；

2012年3月27日

中国国家发改委、工信部等七部委联合发布了《关于下一代互联网“十二五”发展建设的意见》。

2012年5月9日

国务院常务会议研究部署推进信息化发展、保障信息安全工作，确定了加快部署下一代互联网，重点研发下一代互联网关键芯片、设备、软件和系统，推动产业化等重点工作。

关于下一代互联网“十二五”发展建设的意见

2012年3月中国国家发改委、工信部等七部委根据党中央、国务院关于从战略高度重视下一代互联网发展的精神，按照《国务院关于加快培育和发展战略性新兴产业的决定》（国发〔2010〕32 号）的统一部署，为加快推进下一 代互联网发展，联合发布了**《关于下一代互联网“十二五”发展建设的意见》**。

“十二五”期间，互联网普及率达到45%以上，推动实现三网融合，IPv6宽带接入用户数超过2500万，实现IPv4和IPv6主流业务互通，IPv6地址获取量充分满足用户需求。

“十三五”期间，基本建成世界先进水平的网络基础设施，完成向下一代互联网的平滑演进过渡。

IPv6重点任务：

- 网络信息基础设施建设
- 重点产品研发及产业化
- 网络商用及业务创新
- 网络与信息安全保障
- 理论研究与技术突破
- 标准体系与知识产权

IPv6在中国——发改委291号文件

准备期 2003~2010年	过渡期 2011-2015年	普及期 2016-2020年	提升期 2020年后
初步构建产业链 试点商用	现网规模试点 发达地区初步完成过渡	部署推广 全面普及	开创增值创新模式

十二五目标

现网规模试点：2011-2013年

- **用户**：**1000万**
- **网络**：**100%**电信骨干网,**30**个城域网,**100%**教育、科研网络
- **网站**：**TOP 100** 商业网站,**地市级**（含）以上政府公共服务网站
  100% 211校园网站、信息化系统

现网规模部署：2013-2015年

- **用户**：**10%**互联网用户，**约7000万**
- **网络**：**100%**东部城域网，**50%**中西部部城域网
- **网站**：**100 %**主要商业网站，**100%**政府公共服务网站，
  100% 校园网站、信息化系统

IPv6重点任务

网络信息基础设施建设
重点产品研发及产业化
网络商用及业务创新
网络与信息安全保障
理论研究与技术突破
标准体系与知识产权

现网商用试点阶段（2013 年底前）

阶段主要任务

开展小规模商用试点，形成成熟 商业模式， 加快推进相关研发工作，为全面部署做好准备；

网络建设与用户规模

所有CERNET/CSTNET/其他新建骨干网全部支持IPv6，域名解析基本支持IPv6；10%城域网支 持IPv6，IPv6接入用户数超过800万，制定大规模网络平滑演进方案，网页浏览互通；

业务应用与终端支持

国内排名前100位的商业网站支持IPv6，70%的中央企业和市级以上政府网站支持IPv6，重点大学网站全部支持 IPv6，运营商新业务基本支持IPv6，新增上网终端基本支持IPv6；

技术突破与知识产权

加强平滑演进等技术的研发，构建自主知识产权的标准体系，缩小与国际先进水平的差距；

网络与信息安全

在CNGI 开展网络与信息安全防护试点，建立网络信任体系，加强互联网数字证书管理；

节能降耗与产业带动

单位信息流量能耗下降8%以上，网络设备产业万元增加值能耗年均下降3%以上；新增就业岗位150 万个以上；

全面商用部署阶段（2014-2015年）

网络建设与用户规模

开展IPv6 网络大规模部署和商用，逐步停止向新用户和应用分配IPv4 地 址，组织新型网络体系架构及技术的规模 验证，为“十三五”期间产业创新发展做好准备；

网络建设与用户规模

东部发达地区所有城域网支持IPv6，中西部50%的城域网支持IPv6，全面支持IPv6域名解析；推动大规模公众网络由IPv4向IPv6平滑演进，实现IPv4和IPv6主流业务互通；互联网普及率达到45%以上，IPv6宽带接入用户数超过2500万；

业务应用与终端支持

国内排名前1000位的商业网站，70%的县级以上政府网站，70%的高校外网网站支持IPv6，新增上网终端全面支持IPv6，移动互联网业务和运营商业务，互动电视业务逐步支持IPv6，物联网、云计算等新型业务全部使用IPv6，广电企业开展的电信业务基本支持IPv6；

技术突破与知识产权

基于自主知识产权技术，建立新型下一代网络体系架构及技术试验床，开展小规模现网试验，在部分关键领域达到国际先进水平；建立适用全面商用的下一代互联网标准体系；

网络与信息安全

在公众网络中建立信息安全防护体系，完善国家数字证书管理体系，提升网络安全水平；

节能降耗与产业带动

单位信息流量能耗下降12%以上，网络设备产业万元增加值能耗年均下降4%以上；新增就业岗位150 万个以上；

《关于下一代互联网十二五发展建设的意见》

IPv6支持情况	现网商用试点阶段（2013年底前）	全面商用部署阶段（2014-2015年）
骨干网	100%	100%
城域网	约10%	东部地区100%，中西部地区约50%
Internet域名服务	基本支持	全面支持
IPv4/IPv6业务互通	网页浏览业务	主流业务
商业网站	国内访问流量排名前100位	国内访问流量排名前1000位
政府网站	约70%的中央企业及地市级以上政府外网网站系统	约70%的县级以上政府外网网站系统
电信业务	新开展的业务基本支持	既有业务逐步向IPv6迁移，广电企业开展的电信业务基本支持IPv6
新增上网固定终端和移动终端	基本支持	全面支持

运营商-中国电信

中国电信 CHINA TELECOM

Global IPv6 全球高峰会议 Summit

中国电信在2012全球IPv6暨下一代互联网高峰会议上提出“抓住机遇，全面推动我国下一代互联网发展”，中国电信将在已有工作基础上，积极响应国家发展下一代互联网的战略部署；

2013年开展IPv6网络小规模商用试点，2014年至2015年，开展大规模部署和商用2013年底发展800万用户，2015年底发展为2500万用户；

总体实施计划

拟在2010-2011年的基础上，基于有线宽带、无线宽带、IDC等重点业务，扩大规模，增加新的省市启动改造，深化已有城市扩大覆盖；

为支持CP/SP的网站改造工作，改造CP/SP集中的重点城市的大型IDC机房；

有线宽带、无线宽带：覆盖用户达到600万，力争发展IPv6接入用户300万；

第一阶段(2012)	第二阶段(2013)
以提升网络能力为主，确保网络可运营，营业可支持，用户可使用。	以扩大用户覆盖规模为主，对城域网分区域、分步骤实施改造，扩大网络覆盖，满足用户容量要求。

运营商-中国移动

在“2012全球IPv6暨下一代互联网高峰会议”上，中国移动提出“加速IPv6应用，推动移动互联网发展”

准备大范围开展IPv6试点；

已在9个省启动；

根据国家行动指南切实推进IPv6工作；

结合企业自身特点，大力推进以TDSCDMA/TD-LTE为主的IPv6移动互联网。

以发展IPv6移动用户/实现流量向IPv6迁移为目标；

从网络/终端/业务三个关键环节入手；

联合上下游单位，大力推动移动互联网IPv6的成熟。

运营商-中国联通

在“2012全球IPv6暨下一代互联网高峰会议”上，中国联通发表“IPv6发展策略及未来网络探索”的演讲，认为向IPv6迈进是必然的选择，要加快IPv6的培育，中国联通将启动IPv6规模试商用 （2013年前，300万用户规模）

联通对IPv6的培育

- 改造以双栈方式改造骨干网与城域网，构建IPv6核心网络
- 改造运营支撑体系，支持IPv6业务开展
- 改造IDC，支持IPv6应用部署
- 使用双栈或隧道技术为有IPv6业务需要的用户或应用提供IPv6接入手段
- 随着IPv6接入需求的增多，逐步实施接入网与城域网的全面IPv6化改造
- 新建的接入网和城域网要求支持IPv6
- 新的网络设备、终端设备与业务系统要求支持IPv6
- 新建IPv6安全监控体系

全球范围IPv6的发令枪

首个世界IPv6日 2011/06/08

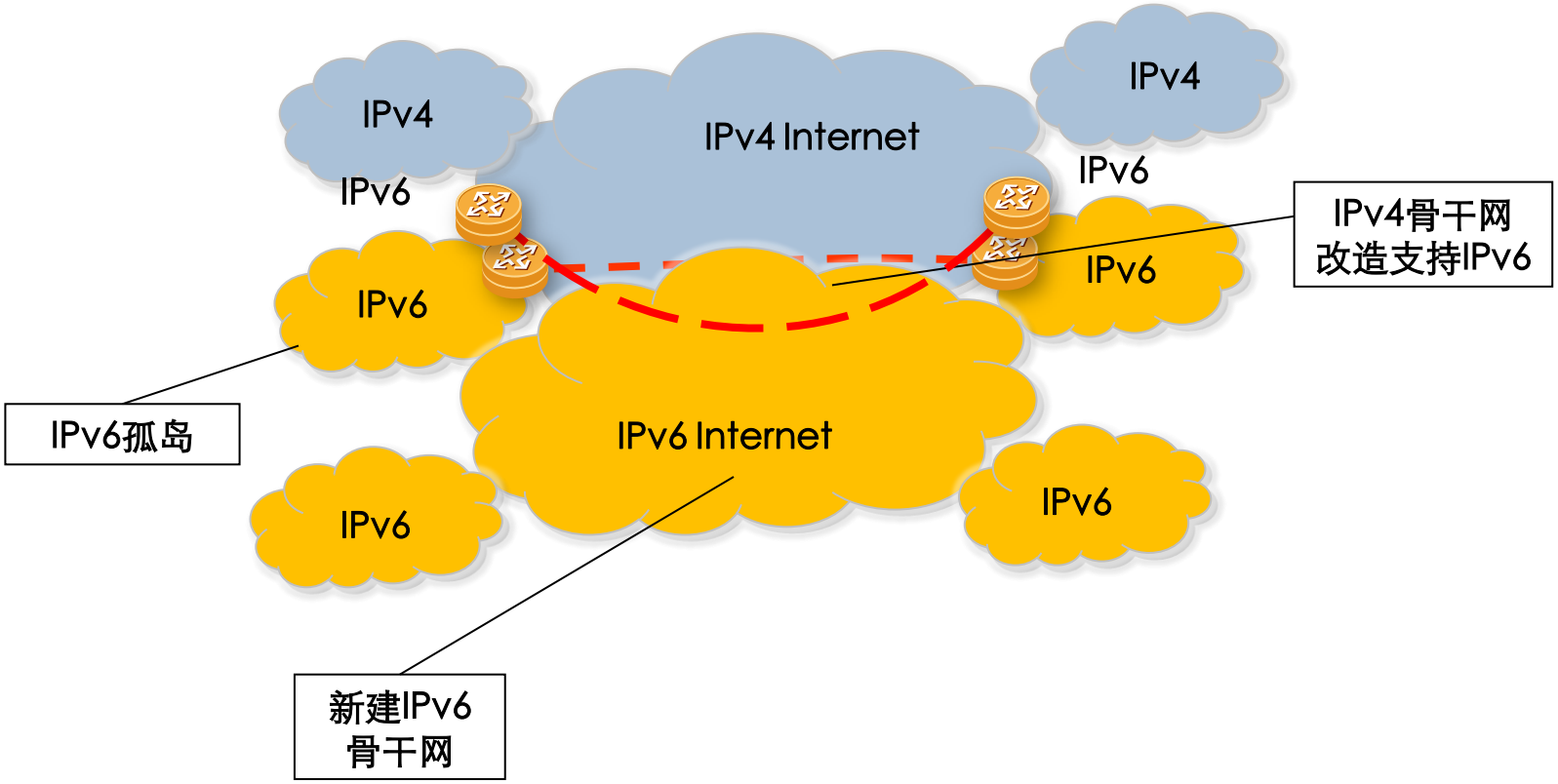
全球各大互联网服务提供商与内容提供商开通IPv6网址，进行24小时访问测试

世界IPv6启动 2012/06/06

全球IPv6演进与发展的里程碑时刻，主流网络运营商与家庭网络设备制造商开始支持IPv6

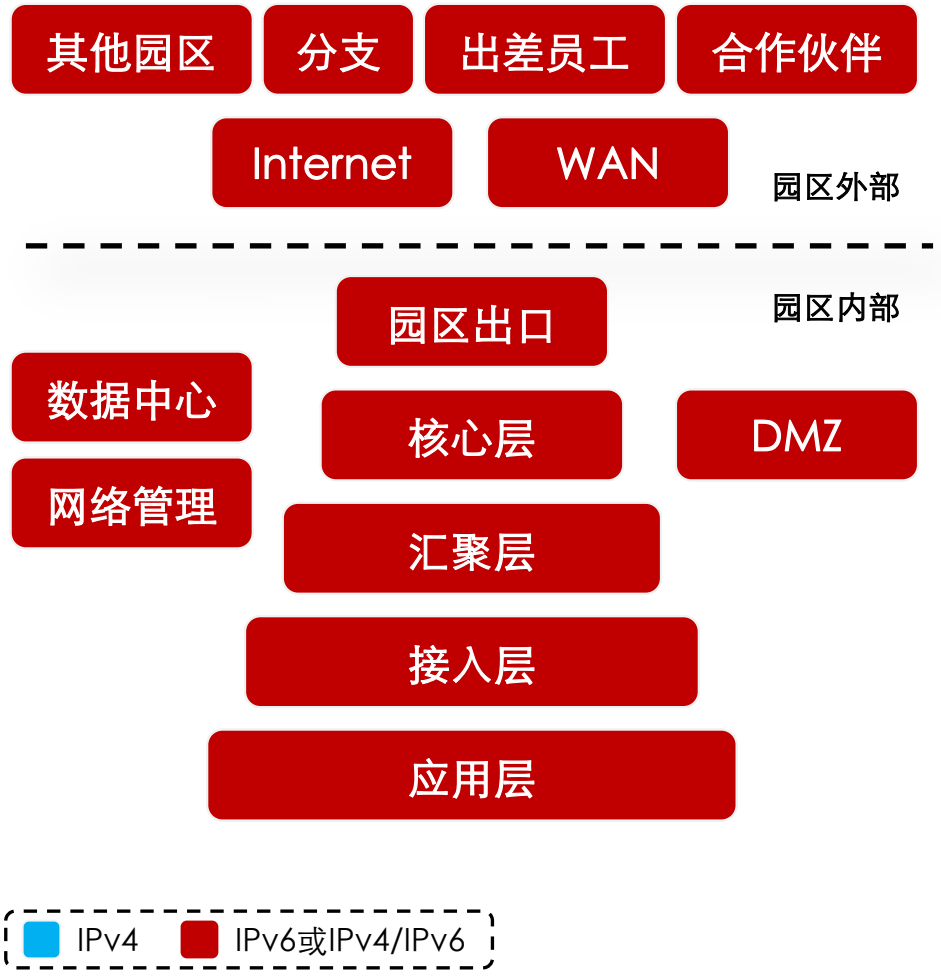
广域网IPv6演进方向

需放映



全IPv4 → 初期 → 发展期 → 演进后期 → 全IPv6

企业IPv6演进状态



①全IPv4

初始状态，互联通过IPv4实现

②初期

终端/应用层部署IPv6，接入/汇聚/核心层支持IPv6，数据中心部署IPv6业务，升级DMZ区域为提供IPv6服务做准备

升级园区出口，支持接入IPv6广域网络，对外提供IPv6服务

允许其他园区/分支/合作伙伴通过WAN或IPv6 Internet接入

允许通过IPv6远程接入

支持IPv6基础网络管理

③发展期/④演进后期

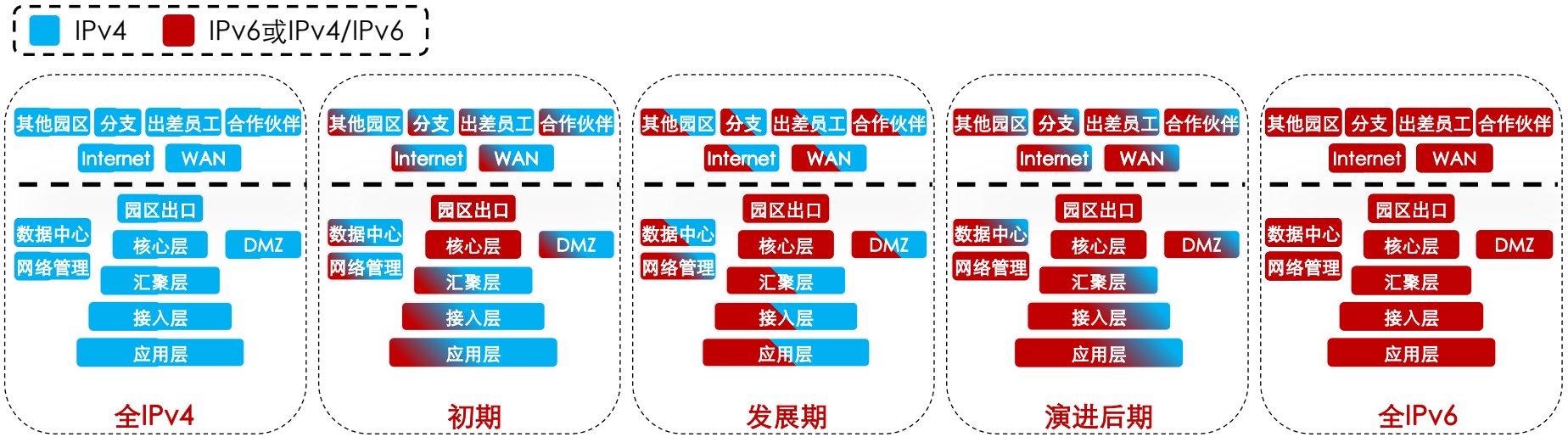
加大IPv6部署范围，业务向IPv6迁移

⑤全IPv6

终结状态，企业网络互联完全通过IPv6实现

企业IPv6演进状态

与上页二选一

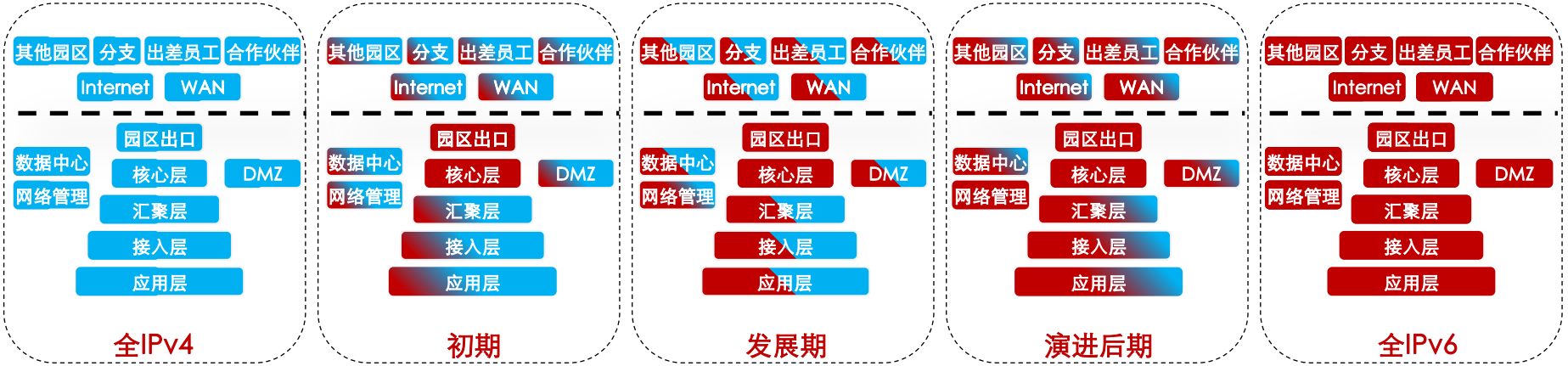


状态	应用	汇聚&接入	核心&出口	数据中心&DMZ	互联
全IPv4	IPv4	IPv4	IPv4	IPv4	IPv4
初期	**20%**应用及终端支持IPv6	**20%**设备支持	**100%**设备支持IPv6	**20%**服务及设备可支持IPv6	**20%**支持IPv6 Internet接入、分支互联、出差员工接入
发展期	**50%**支持	**50%**支持		**50%**可支持	**50%**支持
演进后期	**80%**支持	**80%**支持		**80%**可支持	**80%**支持
全IPv6	**100%**支持	**100%**支持		**100%**可支持	**100%**支持

企业IPv6演进状态

与上页二选一

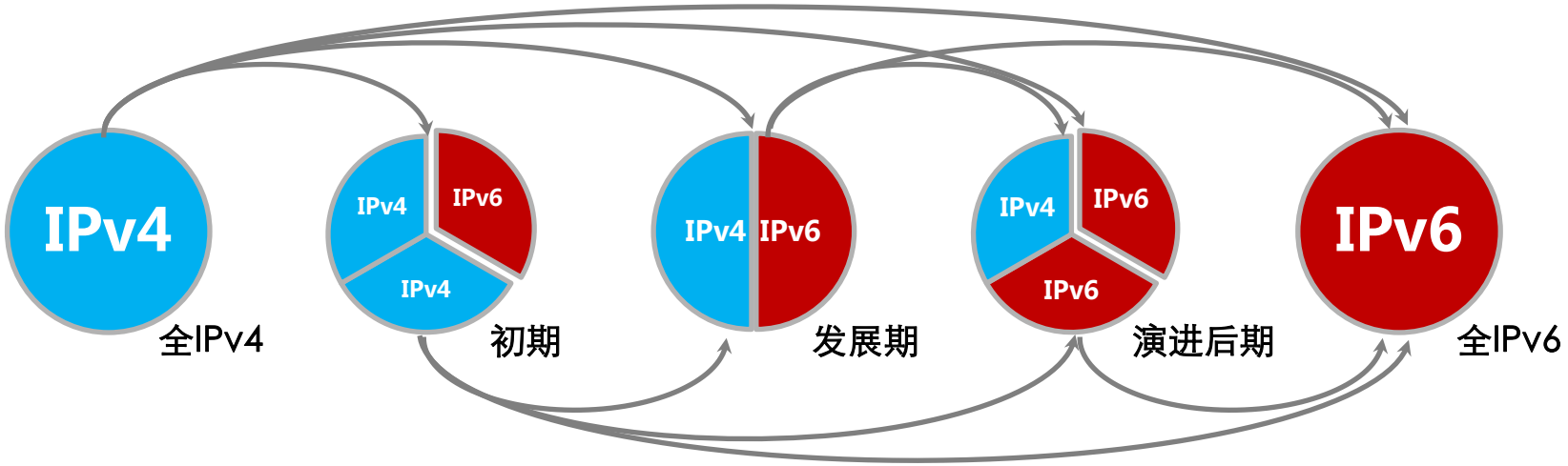
IPv4　IPv6或IPv4/IPv6



状态	应用	汇聚&接入	核心&出口	数据中心&DMZ	互联
全IPv4	IPv4	IPv4	IPv4	IPv4	IPv4
初期	**少量**应用及试点区域终端支持IPv6	**试点区域**设备支持IPv6	**所有**设备支持IPv6	**少量**服务及服务器可支持IPv6	**少量支持**IPv6 Internet接入、分支互联、出差员工接入
发展期	支持IPv6的应用及终端数量占总数的**一半**左右	**半数区域**设备支持IPv6		**半数**服务及服务器可支持IPv6	**半数支持**IPv6 Internet接入、分支互联、出差员工接入
演进后期	IPv6应用及终端占**主导**地位	**少数区域**设备不支持IPv6		**少数**服务及设备不支持IPv6	**少数不支持**IPv6 Internet接入、分支互联、出差员工接入
全IPv6	应用及终端**全部**支持IPv6	**所有区域**设备支持IPv6		**所有**服务及设备支持IPv6	**全部支持**IPv6 Internet接入、分支互联、出差员工接入

企业IPv6演进所需技术

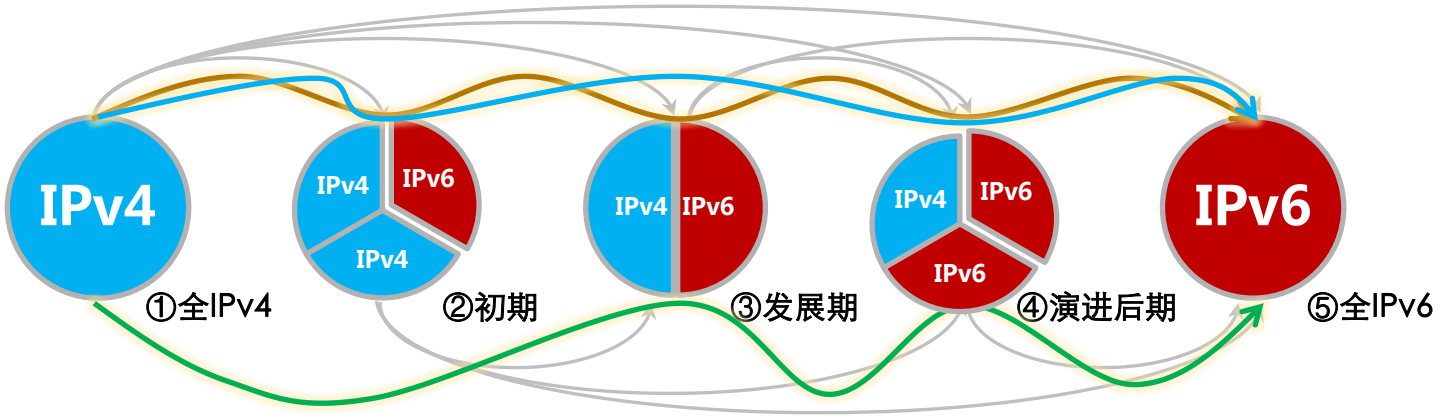
需放映



- 双栈技术
- IPv6 over IPv4等隧道技术
- ISATAP隧道
- 6PE/6vPE
- IPv4 over IPv6 隧道
- 转换技术

其中**双栈技术**为必须使用的基础技术

企业IPv6演进方案



方案	特点	演进时间	现网影响	技术成熟度	风险	
一	①-②-③-④-⑤ 平滑演进	充足	小	高	小	推荐方案
二	①-②-③-⑤ 适度演进	适中	中	中	中	
三	①-②-④-⑤ 适度演进	适中	中	中	小	推荐方案
四	①-②-⑤ 跃进演进	紧张	大	低	大	
五	①-③-④-⑤ 适度演进	适中	中	中	小	推荐方案
六	①-③-⑤ 跃进演进	紧张	大	低	中	
七	①-④-⑤ 跃进演进	紧张	大	低	大	
八	①-⑤ 跃进演进	紧张	大	低	大	

企业IPv6演进方案选择

1、方案需经历**四个以上阶段**，否则过于激进；

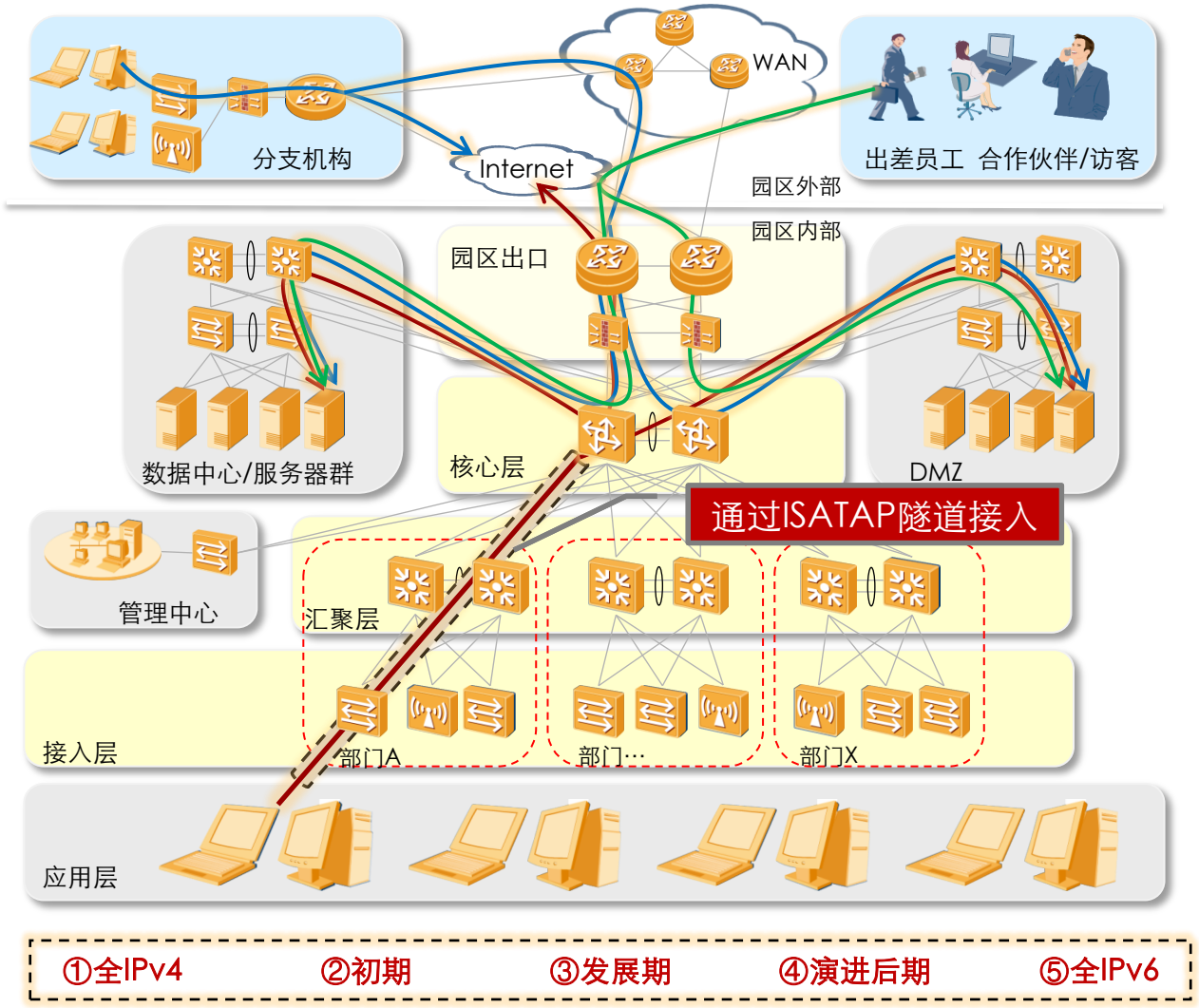
2、**演进后期**是IPv6演进的**必经阶段**，没有演进后期的方案过渡不平滑

方案**二、四、六、七和八**不满足上述要求，不推荐。

方案	特点	演进时间	现网影响	技术成熟度	风险
一	①-②-③-④-⑤ 平滑演进	经历五个阶段，演进时间充足	分五个阶段对现网进行改造，现网影响最小	演进时间充足，可充分等技术成熟后使用，技术成熟度最高	演进时间充足，对现网逐步改造，并使用成熟技术，风险小
三	①-②-④-⑤ 适度演进	经历四个阶段，演进时间适中	分四个阶段对现网进行改造，现网影响程度中等	演进时间适中，并经历漫长的演进后期阶段，技术成熟度中等	演进时间适中，使用成熟技术，风险小
五	①-③-④-⑤ 适度演进	经历四个阶段，演进时间适中	分四个阶段对现网进行改造，现网影响程度中等	演进时间适中，并经历漫长的演进后期阶段，技术成熟度中等	演进时间适中，使用成熟技术，风险小

企业IPv6演进方案一(ISATAP隧道)

需放映



全IPv4-初期-发展期-演进后期-全IPv6

适用场景： 希望逐步迁移并先部署小规模IPv6试点的企业。

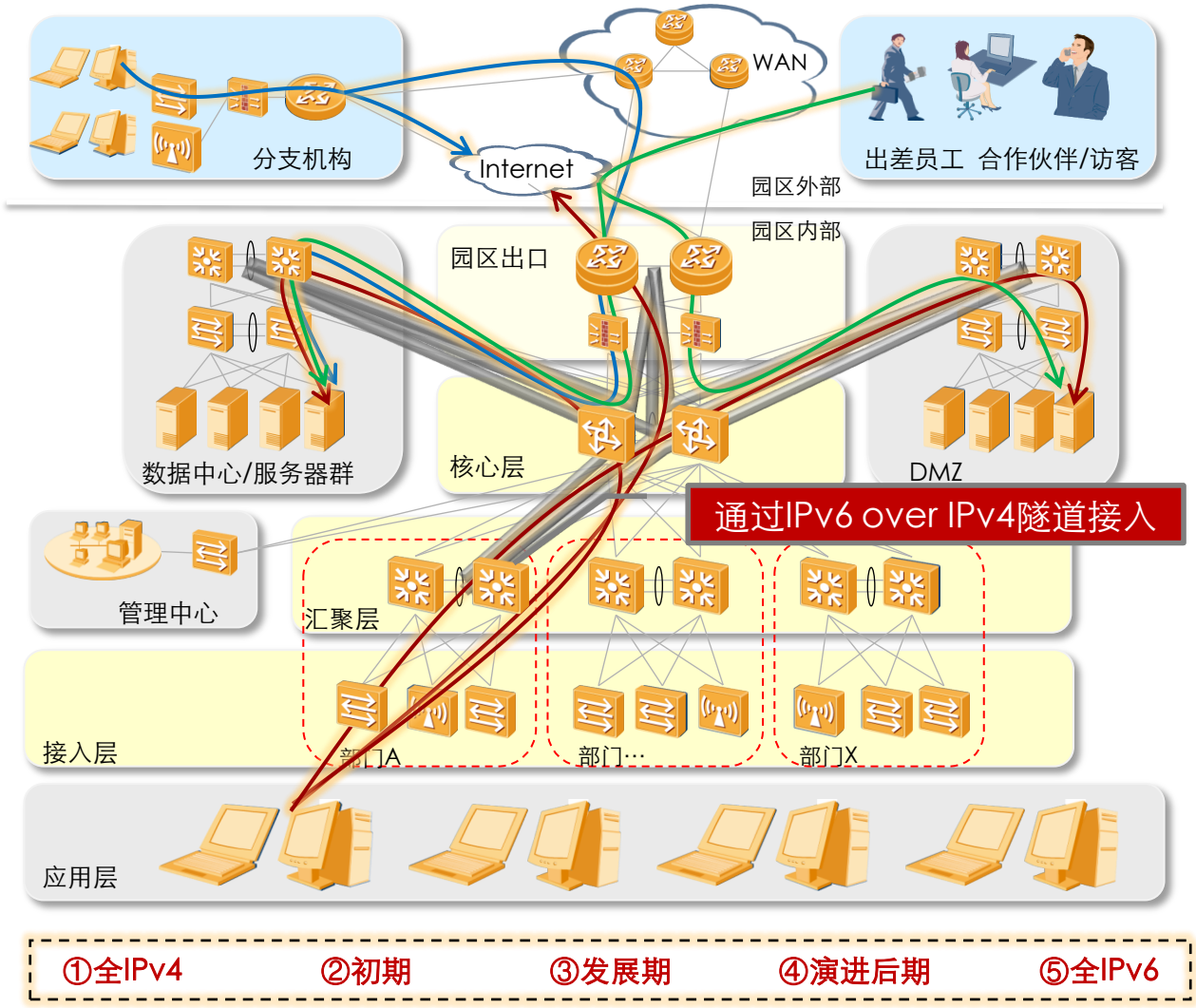
方案特点： 平滑演进，演进时间充足，逐步对现网进行改造或者新建，对现网影响小，可以在演进过程中使用更成熟的技术，风险最小，但并不能快速利用IPv6的优势。初期使用ISATAP隧道，使主机快速接入IPv6网络。

客户价值： 逐步演进，可先小规模试点使用IPv6，保护现有投资。

备选方案： 当不希望升级接入层、汇聚层设备或设备不具备IPv6能力时，可选此方案。

企业IPv6演进方案一 (IPv6 over IPv4隧道)

需放映



全IPv4-初期-发展期-演进后期-全IPv6

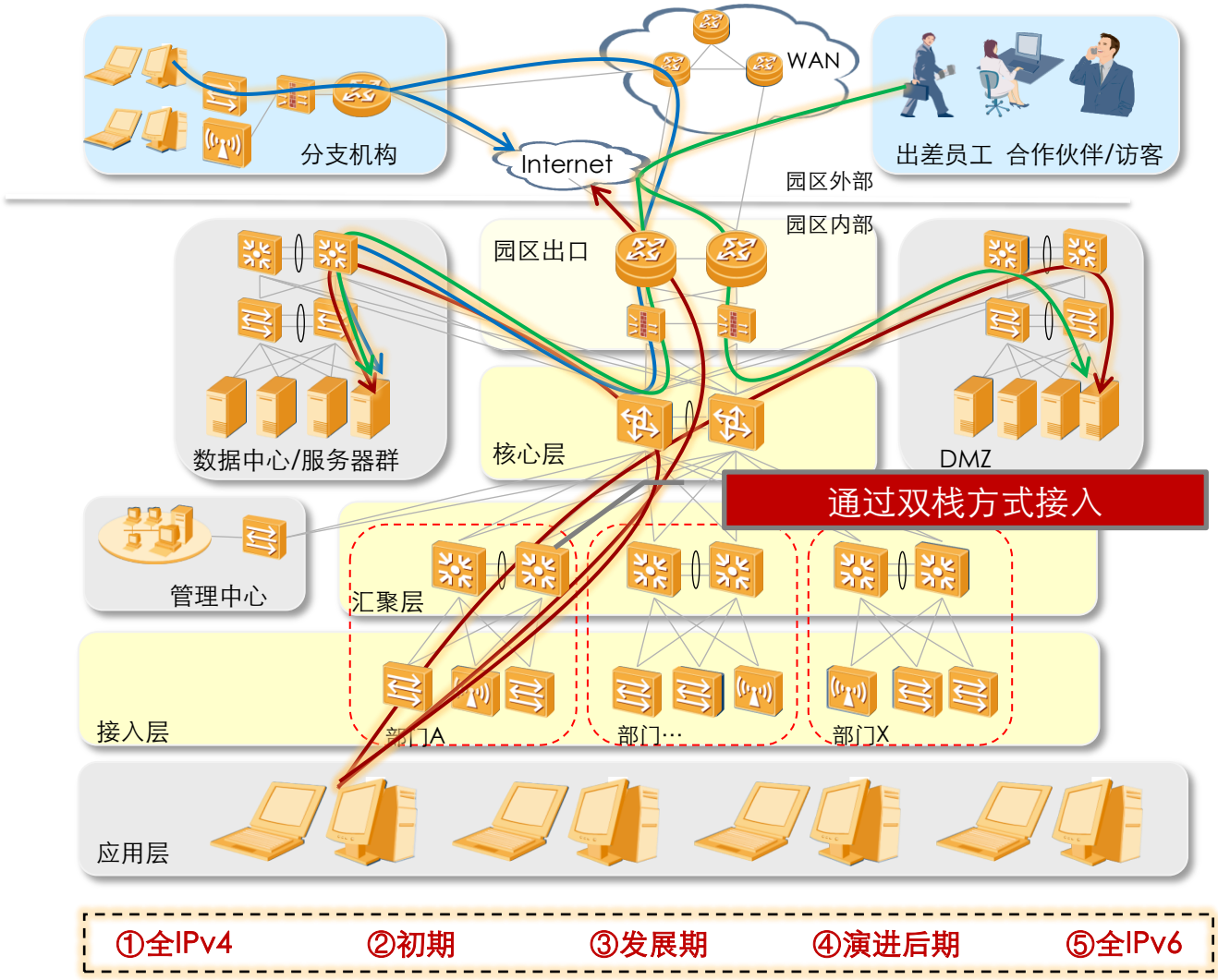
适用场景： 希望逐步迁移并先部署小规模IPv6试点的企业。

方案特点： 平滑演进，演进时间充足，逐步对现网进行改造或者新建，对现网影响小，可以在演进过程中使用更成熟的技术，风险最小，但并不能快速利用IPv6的优势及持续创新。初期使用IPv6 over IPv4隧道，可暂时避免对核心层改造。

客户价值： 逐步演进，可先小规模试点使用IPv6，保护现有投资。

备选方案： 当不希望升级核心层设备或设备不具备IPv6能力时，可选此方案。

企业IPv6演进方案一（全双栈）



全IPv4-初期-发展期-演进后期-全IPv6

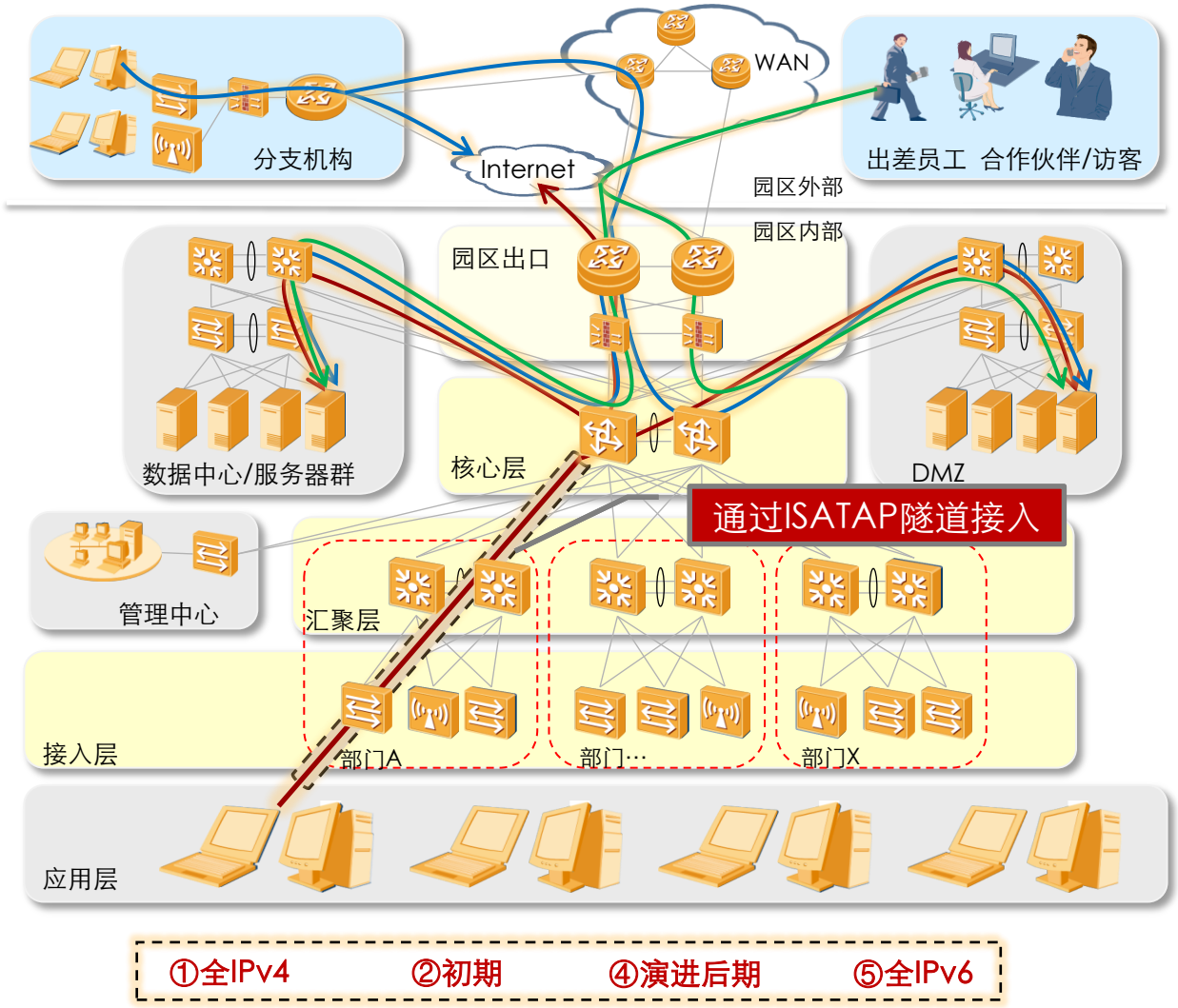
适用场景： 希望逐步迁移并先部署小规模IPv6试点的企业。

方案特点： 平滑演进，演进时间充足，逐步对现网进行改造或者新建，对现网影响小，可以在演进过程中使用更成熟的技术，风险最小，但并不能有效利用IPv6的优势及持续创新。初期使用全双栈方式引入Native IPv6接入而不是使用隧道技术，使IPv6网络结构同IPv4网络相同，结构简单，更高效、易管理维护。

客户价值： 逐步演进，可先小规模试点使用IPv6，保护现有投资。

企业IPv6演进方案三（ISATAP隧道）

需放映



全IPv4-初期-演进后期-全IPv6

适用场景： 前期部署IPv6试点，并在一段时间内对IPv6业务需求小的企业。

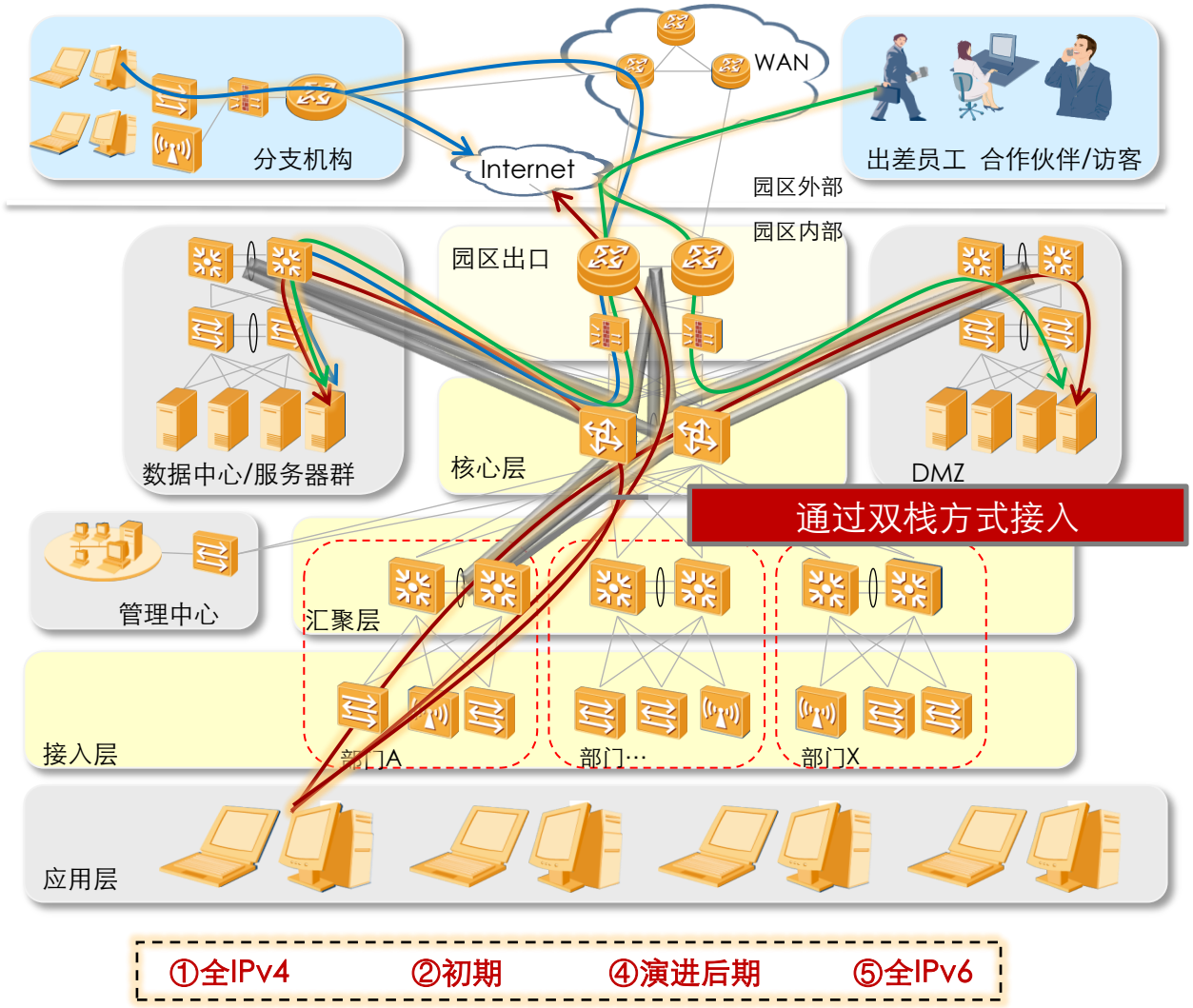
方案特点： 适度演进，演进时间较充足，从初期跃进到演进后期，对现网影响稍大，可以在演进过程中使用更成熟的技术，风险小。通过迅速演进到演进后期，可以更好的利用IPv6优势，持续创新。初期使用ISATAP隧道，使主机快速接入IPv6网络。

客户价值： 可以进行IPv6试点，并在需要时大规模部署，保持现网投资

备选方案： 当不希望升级接入层、汇聚层设备或设备不具备IPv6能力时，可选此方案。

企业IPv6演进方案三 (IPv6 over IPv4隧道)

需放映



全IPv4-初期-演进后期-全IPv6

适用场景： 前期部署IPv6试点，并在一段时间内对IPv6业务需求小的企业。

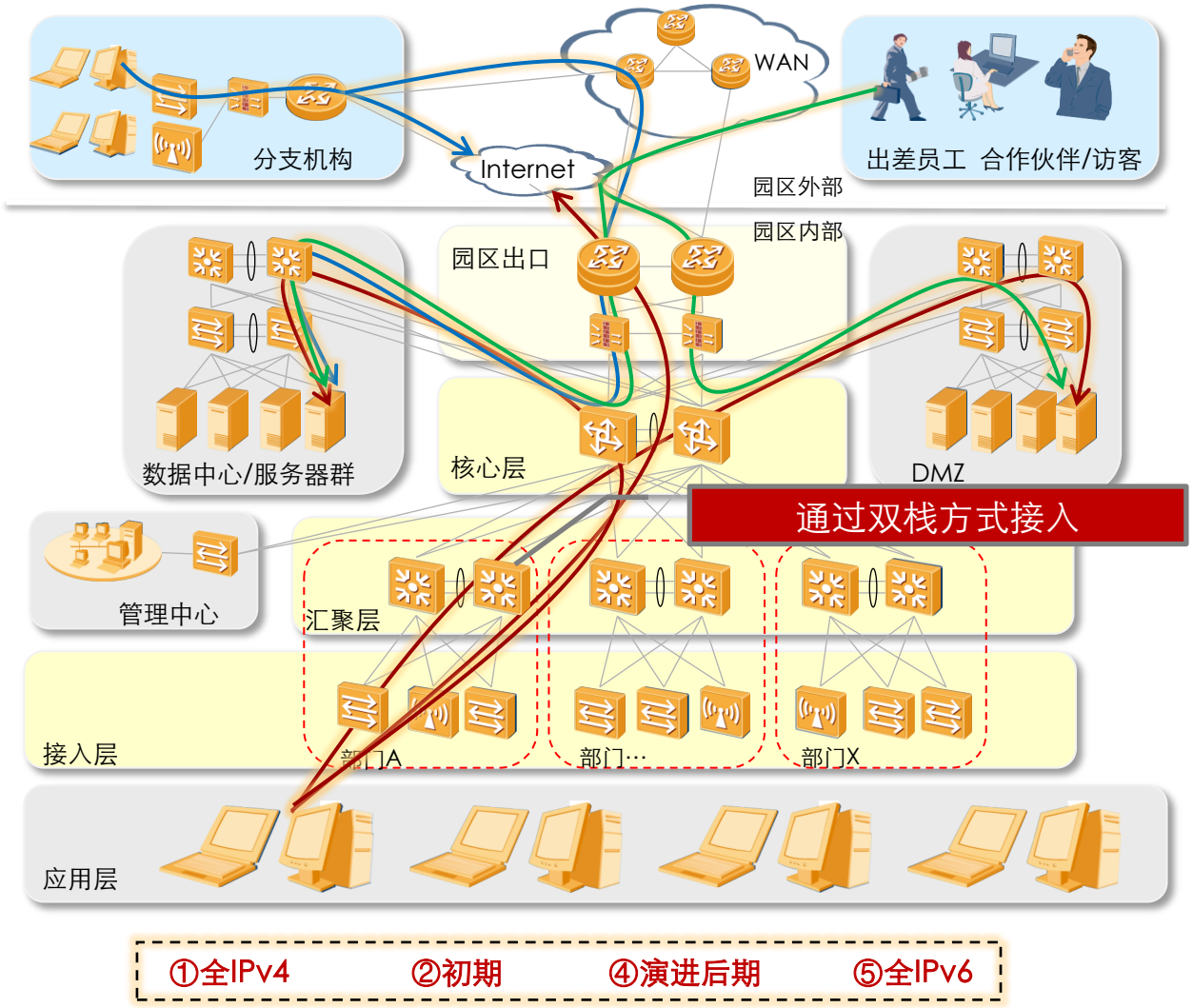
方案特点： 适度演进，演进时间较充足，从初期跃进到演进后期，对现网影响稍大，可以在演进过程中使用更成熟的技术，风险小。通过迅速演进到演进后期，可以更好的利用IPv6优势，持续创新。初期使用IPv6 over IPv4隧道，可暂时避免对核心层改造。

客户价值： 可以进行IPv6试点，并在需要时大规模部署，保持现网投资

备选方案： 当不希望升级核心层设备或设备不具备IPv6能力时，可选此方案。

企业IPv6演进方案三（全双栈）

需放映、推荐方案



全IPv4-初期-演进后期-全IPv6

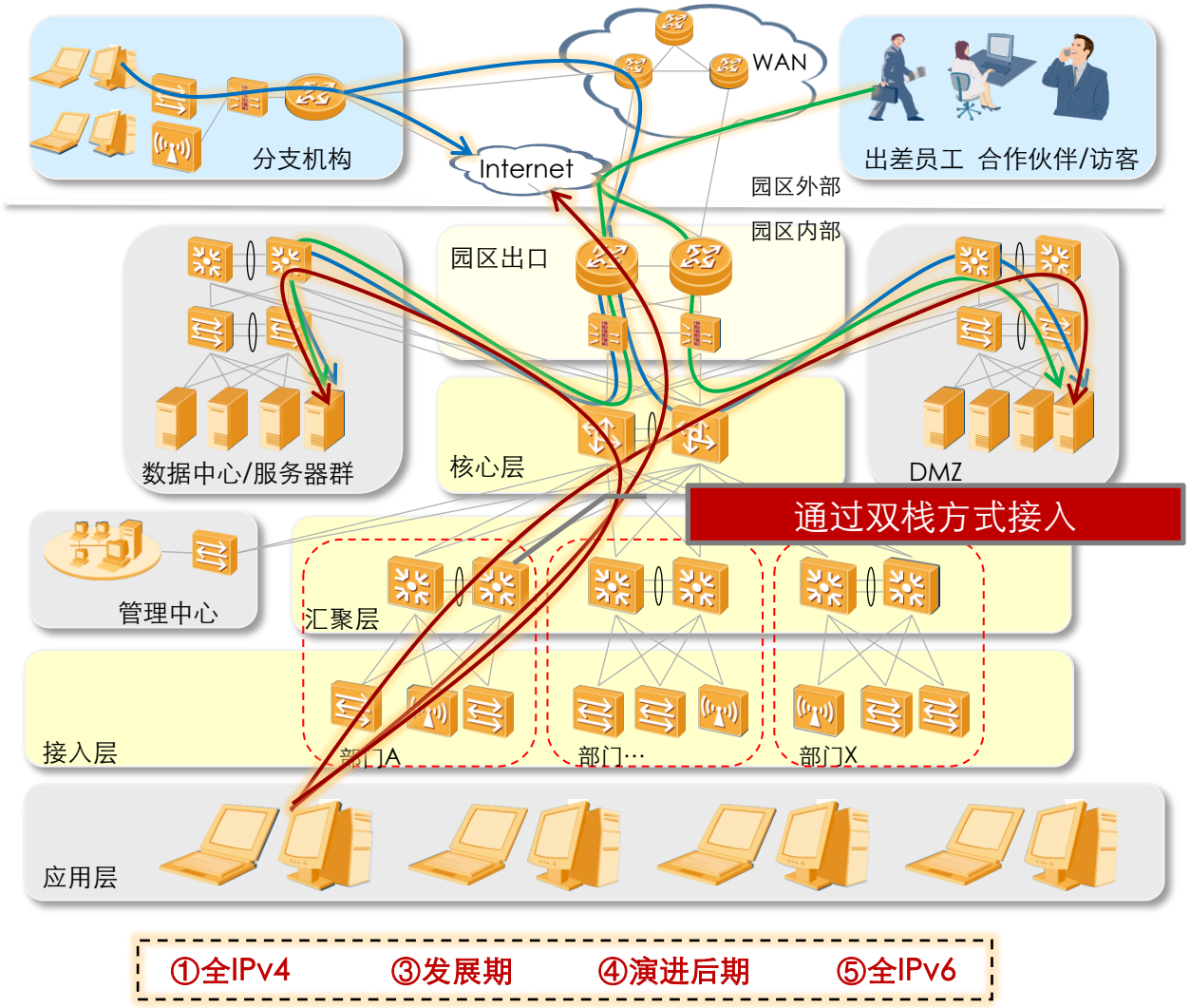
适用场景： 前期部署IPv6试点，并在一段时间内对IPv6业务需求小的企业。

方案特点： 适度演进，演进时间较充足，从初期跃进到演进后期，对现网影响稍大，可以在演进过程中使用更成熟的技术，风险小。通过迅速演进到演进后期，可以更好的利用IPv6优势，持续创新。初期使用全双栈方式引入Native IPv6接入而不是使用隧道技术，使IPv6网络结构同IPv4网络相同，结构简单，更高效、易管理维护。

客户价值： 可以进行IPv6试点，并在需要时大规模部署，保持现网投资

企业IPv6演进方案五

需放映、推荐方案



全IPv4-发展期-演进后期-全IPv6

适用场景：以Native IPv6方式逐步引入IPv6。

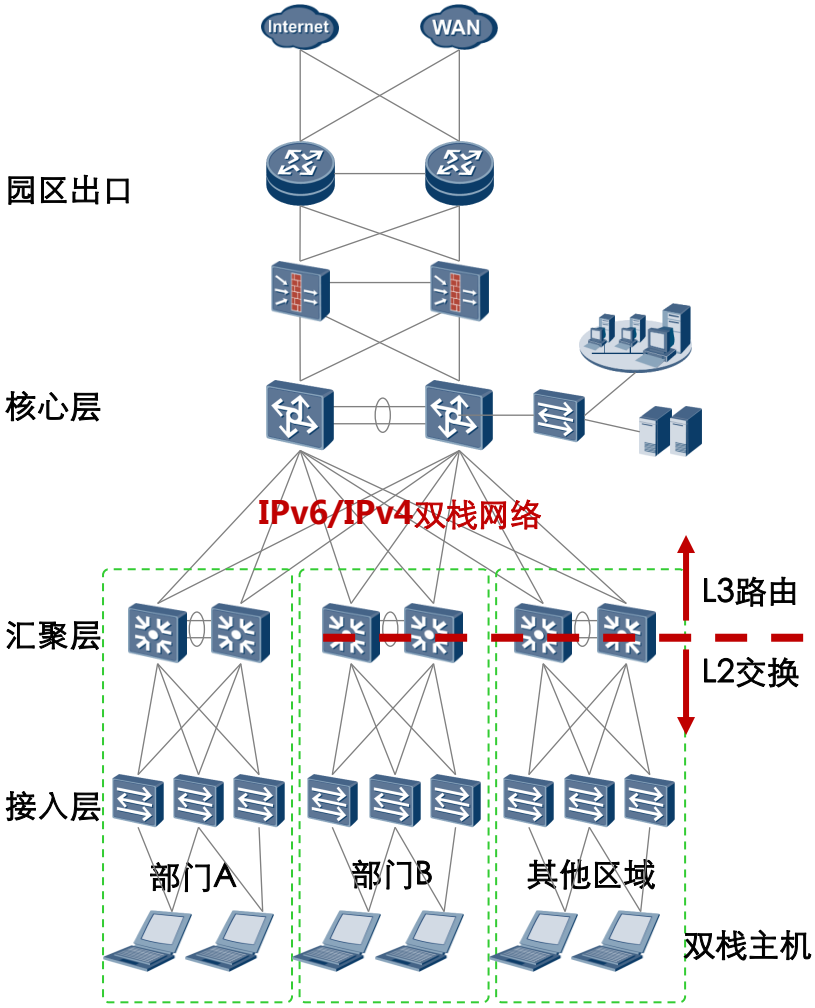
方案特点：适度演进，演进时间充足，通过越过初期的IPv6部署试点部署，全双栈方案可以规模实现Native IPv6引入，有效利用IPv6优势，持续创新。

客户价值：Native IPv6方式引入IPv6，使IPv4/IPv6网络结构保持一致，易于维护、管理，适度演进能保持企业有效维持企业业务持续性及持续创新。

目录

全双栈方案

主推方案



应用场景：

园区网升级时需要考虑对IPv6的全面支持，采用全双栈模式部署，平滑过渡到IPv6。

解决方案：

全网设备开启IPv6/IPv4双栈，网络结构相同。

汇聚、核心层设备必须支持IPv6转发，支持IPv6相关协议。

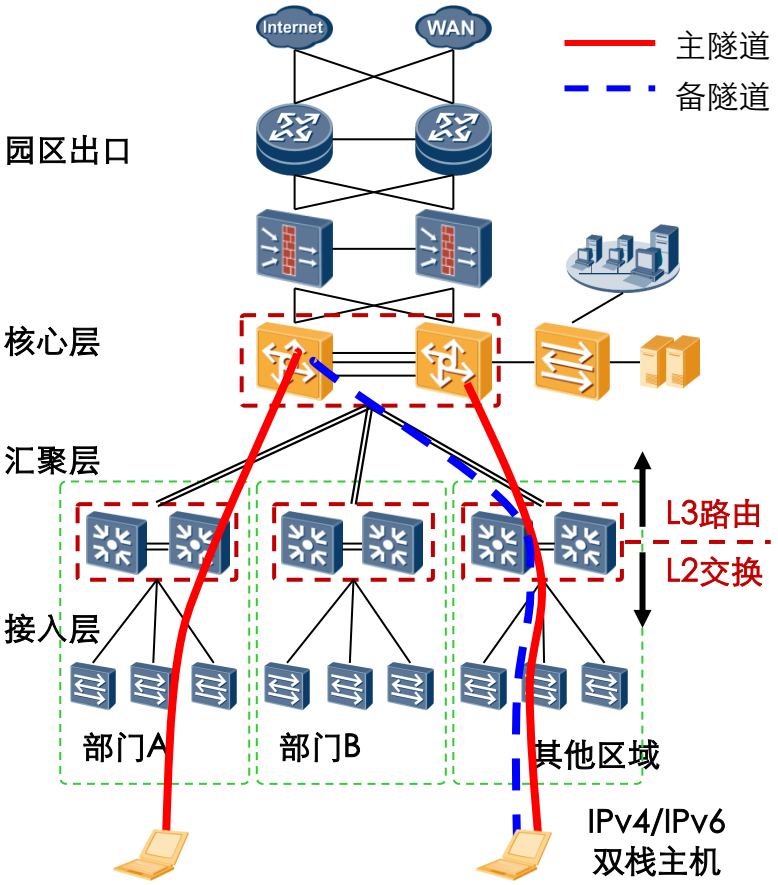
汇聚层作为L2/L3分界，要求支持VRRP6、DHCPv6 relay。

接入层交换机整体上对IPv6三层转发是不可见的，仅支持部分IPv6业务即可：如MLD snooping，IPv6管理（telent/SSH/SNMP）。

客户价值：

Native方式引入IPv6，平滑过渡，有利于未来全面改造为纯IPv6网络。

ISATAP隧道方案



应用场景

双栈主机通过IPv4网络接入IPv6网络

解决方案

升级核心层、IPv6边界和数据中心网络，应用隧道接入IPv6用户

主机通过ISATAP隧道接入IPv6核心网络

使用交换机CSS集群技术保证隧道备份，实现主机与网络之间的双ISATAP隧道，保证可靠性。

客户价值：

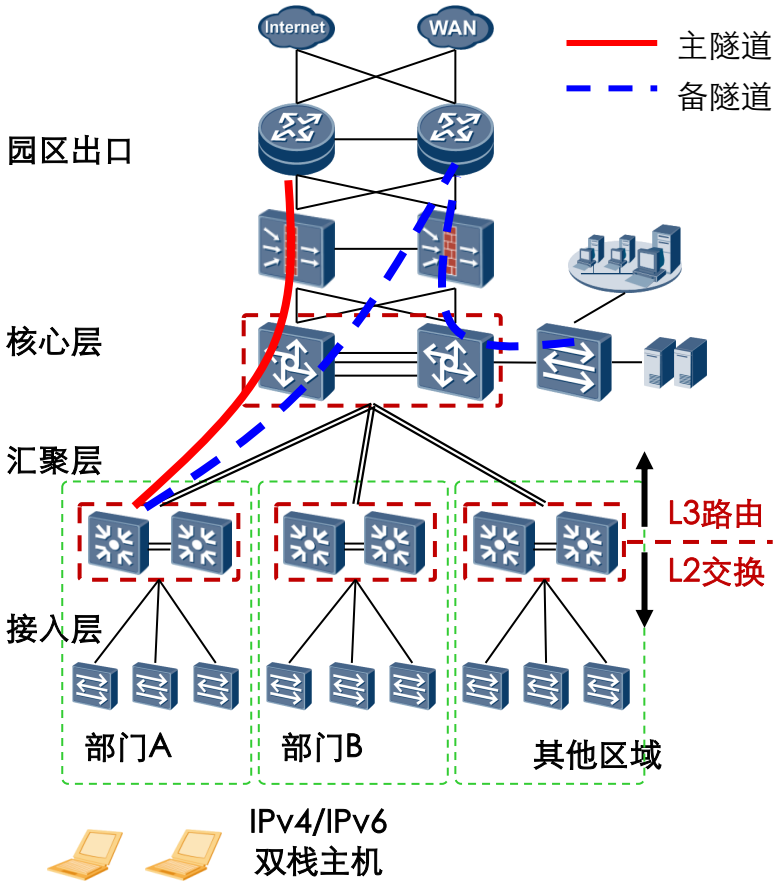
能够利用已有的网络，接入汇聚无须改变，快速引入IPv6服务

不足：

1、核心层接入终端设备，QoS、安全、隧道在核心层进行部署，配置复杂，可能对原有核心业务造成影响，适合小规模部署。

2、ISATAP隧道不支持组播业务。

IPv6 over IPv4手工隧道方案



应用场景

IPv6孤岛通过IPv4网络互连

解决方案

升级园区接入/汇聚设备，园区出口以及IPv6业务区网络。

网络之间通过IPv6 over IPv4手工隧道相连，该隧道可以看作是普通的链路直连。

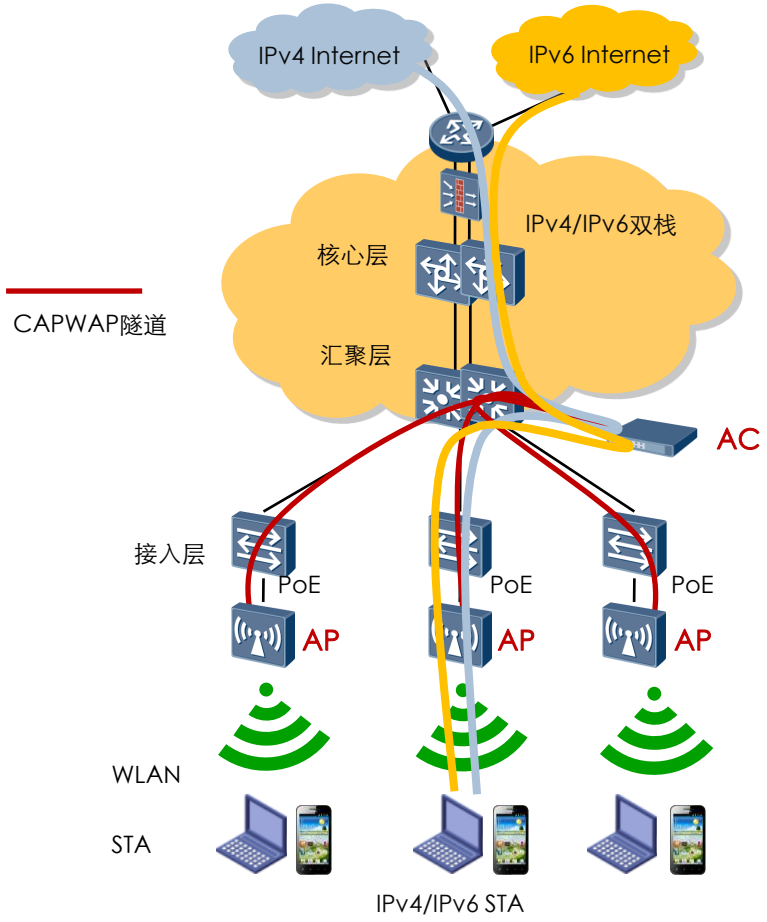
可靠性通过以下技术保证：

- 网络与网络之间的双IPv6 over IPv4手工隧道
- 使用交换机CSS集群技术
- 使用防火墙IPv6 over IPv4手工隧道双机热备技术

客户价值

可以暂不升级核心层设备，园区网需要互通的IPv6网络较少，应用手工隧道配置，易扩展。

WLAN双栈方案——汇聚层AC旁挂



应用场景

双栈WLAN终端接入

解决方案

AC和AP间通过CAPWAP协议建立基于IPv4网络的隧道

AC通过隧道对AP进行动态配置、管理及监控AP为STA提供接入服务，对STA数据进行二层转发

IPv6的数据透传到汇聚层交换机进行处理；

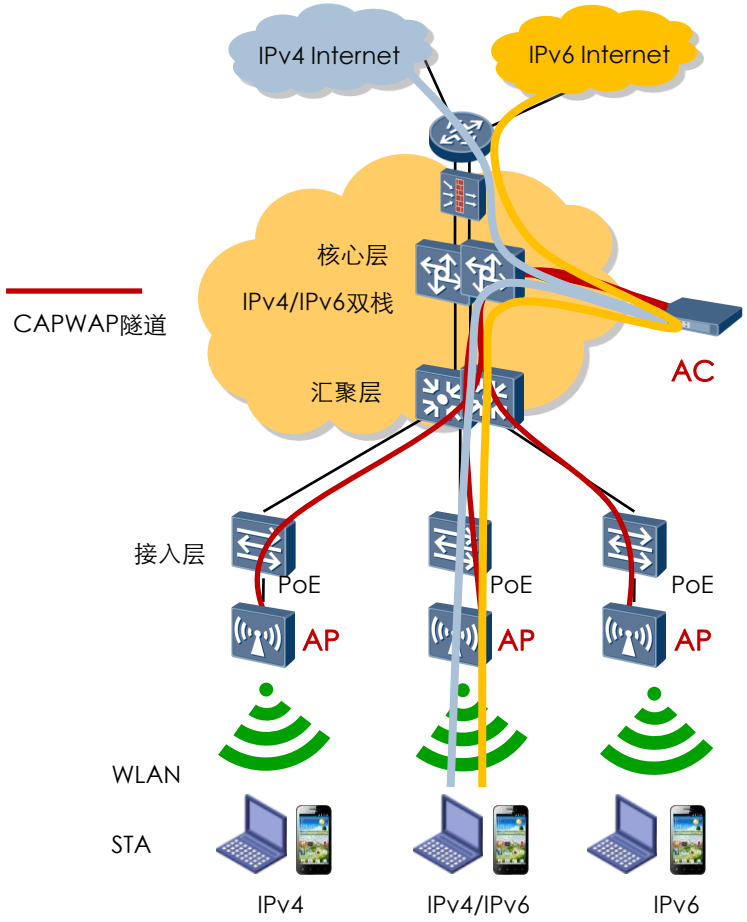
可在汇聚层旁挂独立AC设备或在S9700/S7700框式交换机中部署AC业务插卡

客户价值

便于管理部署；

AC业务插卡与框式交换机融合可减少网络节点数，降低运维成本；

WLAN双栈模式——核心层AC旁挂



应用场景

双栈WLAN终端接入

解决方案

AC和AP间通过CAPWAP协议建立基于IPv4网络的隧道

AC通过隧道对AP进行动态配置、管理及监控AP为STA提供接入服务，对STA数据进行二层转发

IPv6的数据透传到核心层交换机进行处理；

可在核心层旁挂独立AC设备或在S9700框式交换机中部署AC业务插卡

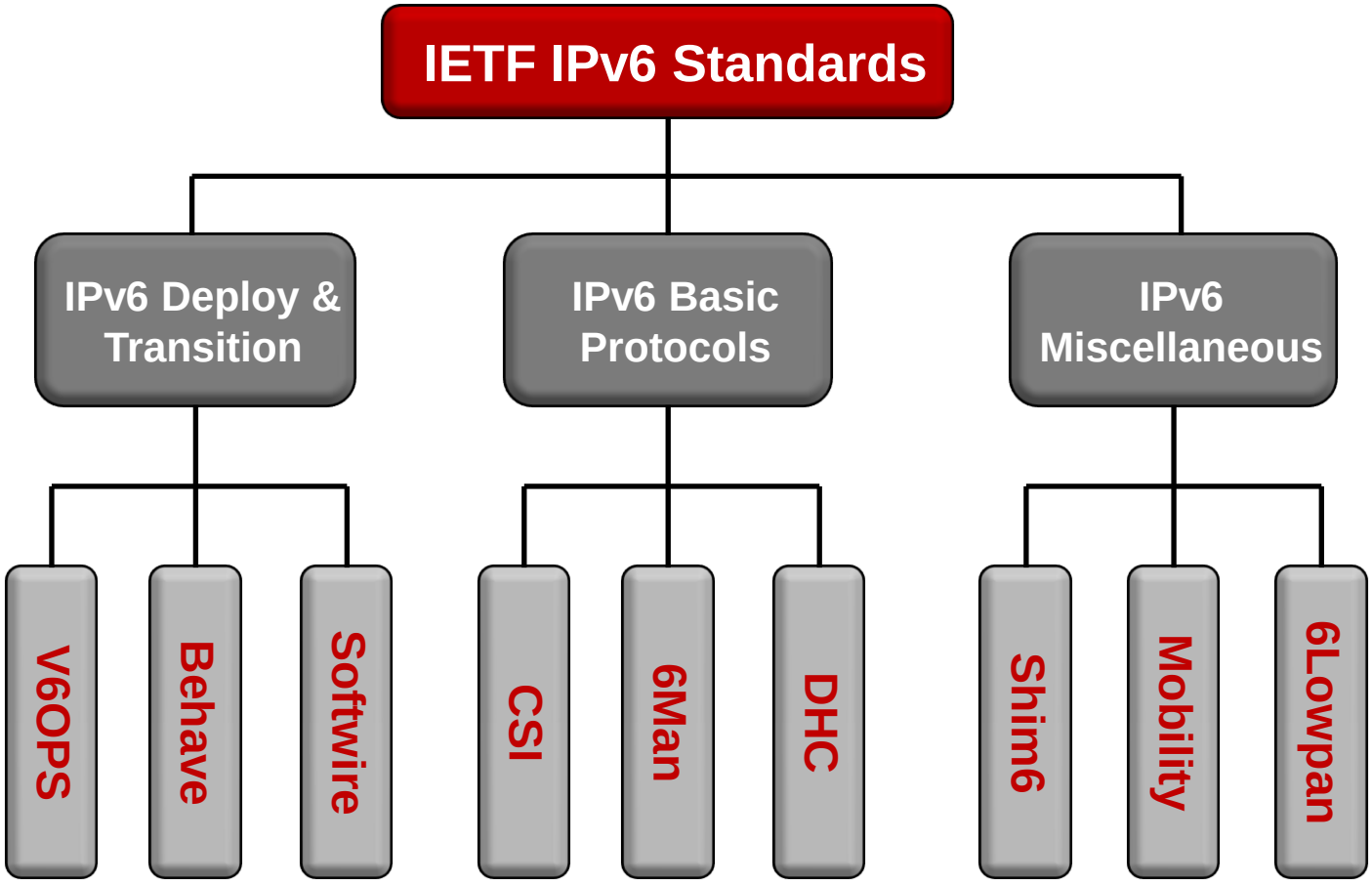
客户价值

便于管理部署；

AC业务插卡与框式交换机融合可减少网络节点数，降低运维成本；

目录

华为公司IPv6方面的技术储备



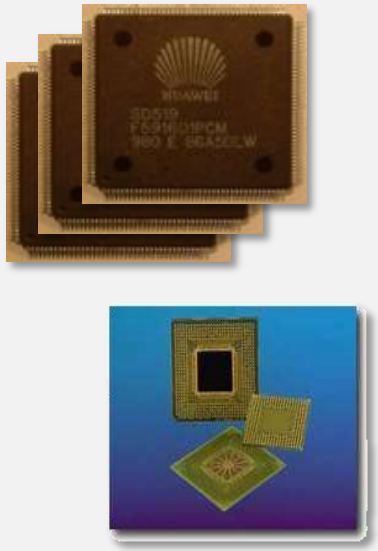
IPv6标准发展的主要贡献力量

华为参与和贡献		IETF IPv6: 16篇RFC, 8篇WG草案	
IETF	华为主导v4tov6transition社区工作。在IETF IAB全会上作为唯一的设备商发表IPv6 过渡材料，冲击IPv6标准的制高点	IPv6过渡技术	3篇 RFC:4952,6036,6264
broadband forum	华为主导v4 to v6 Migration项目，并担任Editor，工作组文稿23篇，个人文稿61篇。	IPv6部署技术	7篇RFC: 5121, 6273, 6279, 6436,6437,6418,6422 8篇WG草案
ITU International Telecommunication Union	华为主导ipv6migration和ipv6na项目，参与其他3个项目,提交文稿33篇全部被接纳。	接入和安全技术	4篇RFC: 5121, 5836, 6440, 6479
中国通信标准化协会 China Communications Standards Association	最近5年50%的IPv6项目由华为牵头，包括：IPv6接入网总体技术要求；DHCPv6标准项目；IPv6过渡的CCSA技术报告等。	地址翻译技术	2篇RFC: 6431, 6156

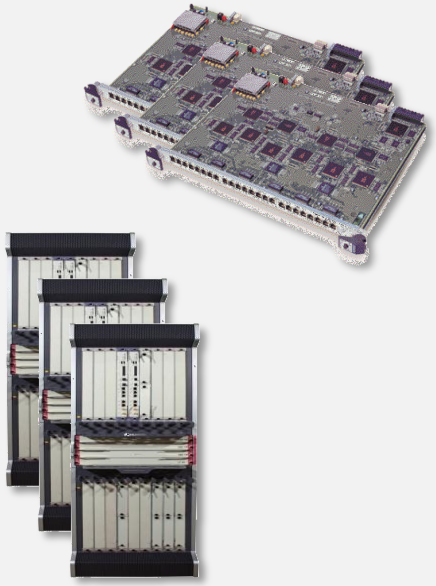
- DS+NAT44(4)、DS-Lite、6rd、Native DS等主流IPv6过渡方案关键技术的**Top3**贡献者
- WG草案数量年增长**3**倍，IPv6领域成长**最快**的IETF标准贡献新势力，遥遥领先国内业界

IPv6创新引擎——自主核心技术

自主知识产权芯片



自主研发设备硬件



独立研发操作系统

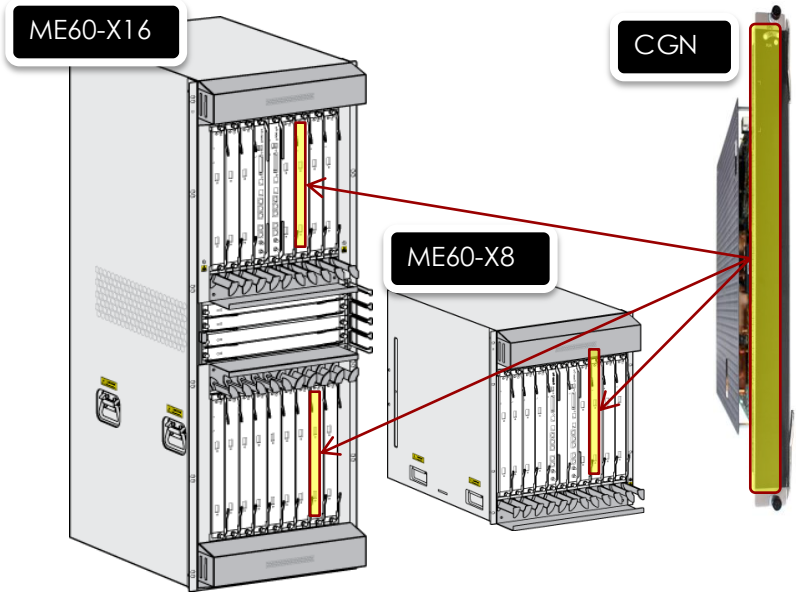
在CNGI项目资助下，华为高端ASIC转发芯片全面支持IPv6功能

部分功能/关键指标处于业界领先水平

大大提升国有品牌T比特核心路由器的竞争力

华为CGN 支持集成部署方式

可选



HW CGN单板简介：

- HW CGN单板可插入Bras/SR ME60/ME60-X/NE40E-X的机框，为哑板；

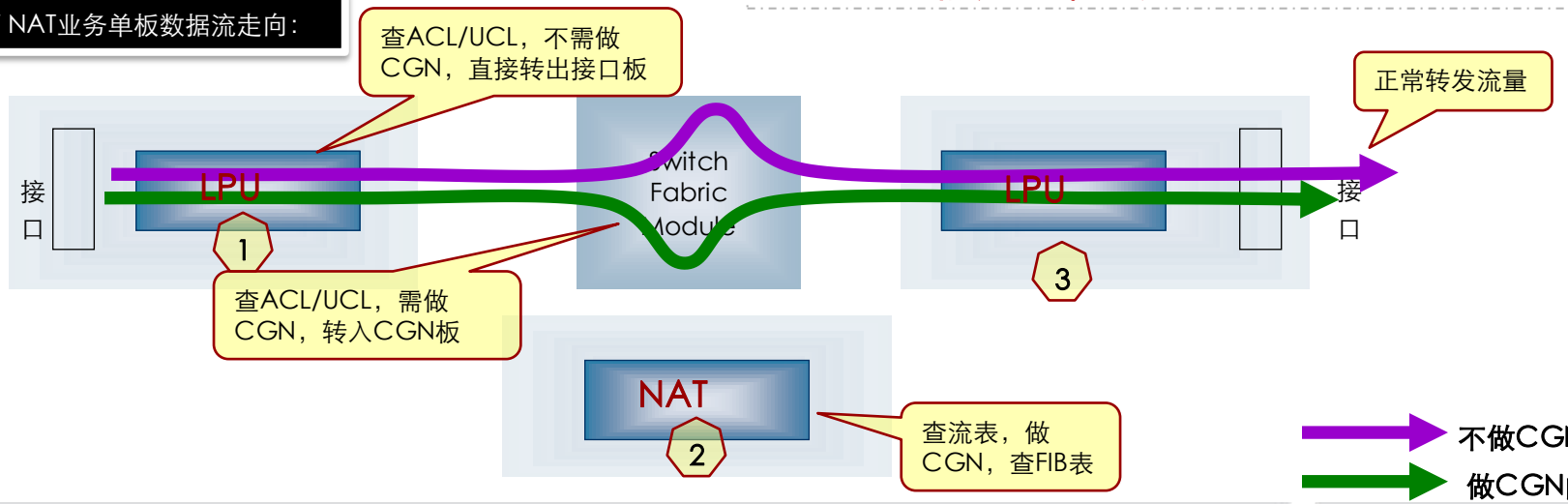
CGN是否会对原有BRAS/SR业务造成影响?

- 不会；CGN的业务由独立的CGN单板完成，其他单板完成自行处理外，只需引流至CGN单板即可；**所以对Bras业务没有任何影响；**

ACL是否会影响转发性能：

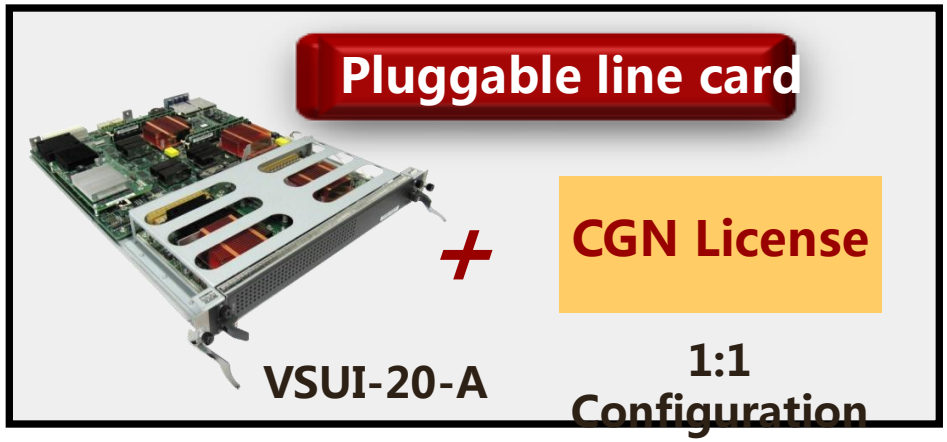
- 不会；HW的ACL都是使用TCAM查找；**可以做到叠加情况下线速转发；**

HW NAT业务单板数据流走向：



华为CGN单板

可选



CGN 单板性能

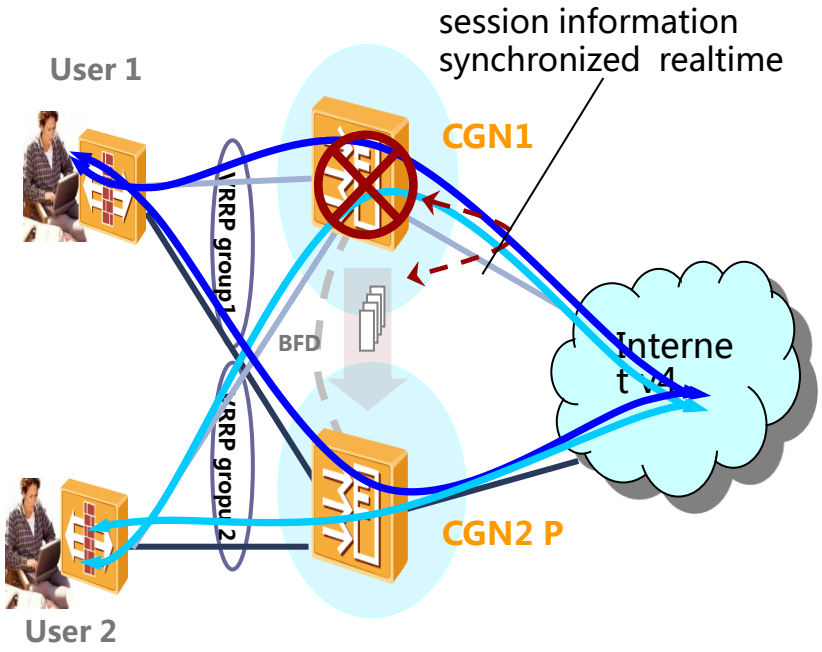
- **Maximum 8 CGN board /equipment**
- **32 hardware thread / CPU**
- **20G processing capabilities/board**
- **12 M flows/board**
- **6M session/board**
- **1M tunnel/board**
- **16K ACL policy/board**
- **400K new flows/s**
- **100us tunnel processing latency and 50us for NAT44**

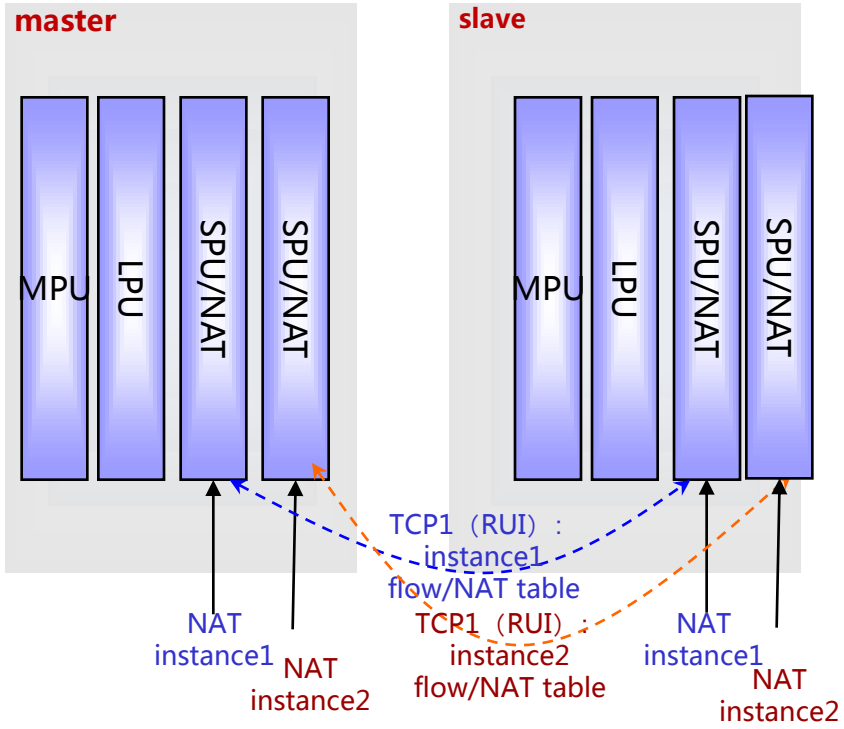
- 集处理和转发性能优势为一体的多核CPU并行处理系统架构
- 基于公平算法的多核CPU负荷分担能力

产品亮点1：业务级CGN热备份

可选

Service-level hot-standby between boards and



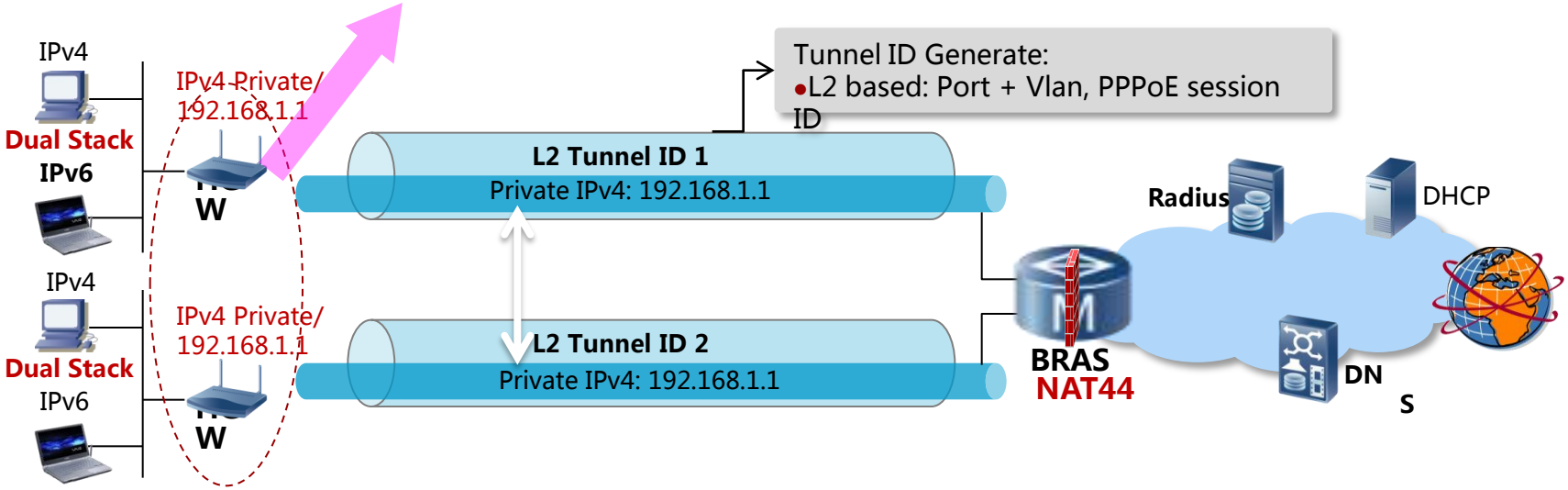


- CGN实例绑定VRRP组，VRRP组绑定接口，通过VRRP组切换实现CGN的热备份；
- 主要亮点：1）实现NAT状态的实时备份；2）实现CGN热备份和负载分担共存；3）通过BFD for VRRP实现50ms的快速保护倒换

产品亮点2：L2 Tunnel-aware CGN 简化业务配置

可选

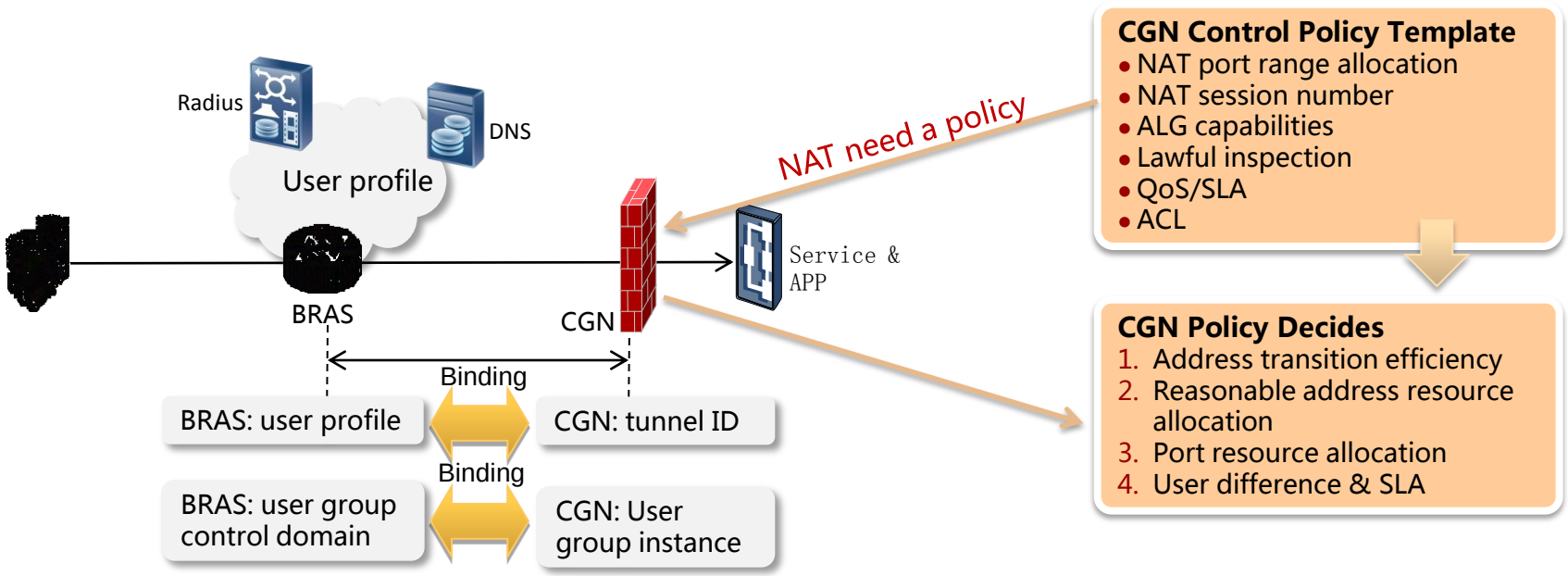
User Identification	IPv4 address	Profile	Parameters
Tunnel ID 1	192.168.1.1	Profile 1	A
Tunnel ID 2	192.168.1.1	Profile 2	B
Tunnel ID 3	192.168.1.1	Profile 3	C



- 与传统NAT不同， L2-aware CGN基于 L2 info + IP + Port 进行私网地址转换；
- 主要亮点：1）基于隧道ID区分用户，所有用户采用相同私网地址，简化用户管理；2）仅1级NAT，业务穿越NAT更容易，同时可减少NAT的抖动和时延。

产品亮点3： 融合CGN&BGN 提供灵活的NAT用户策略管理

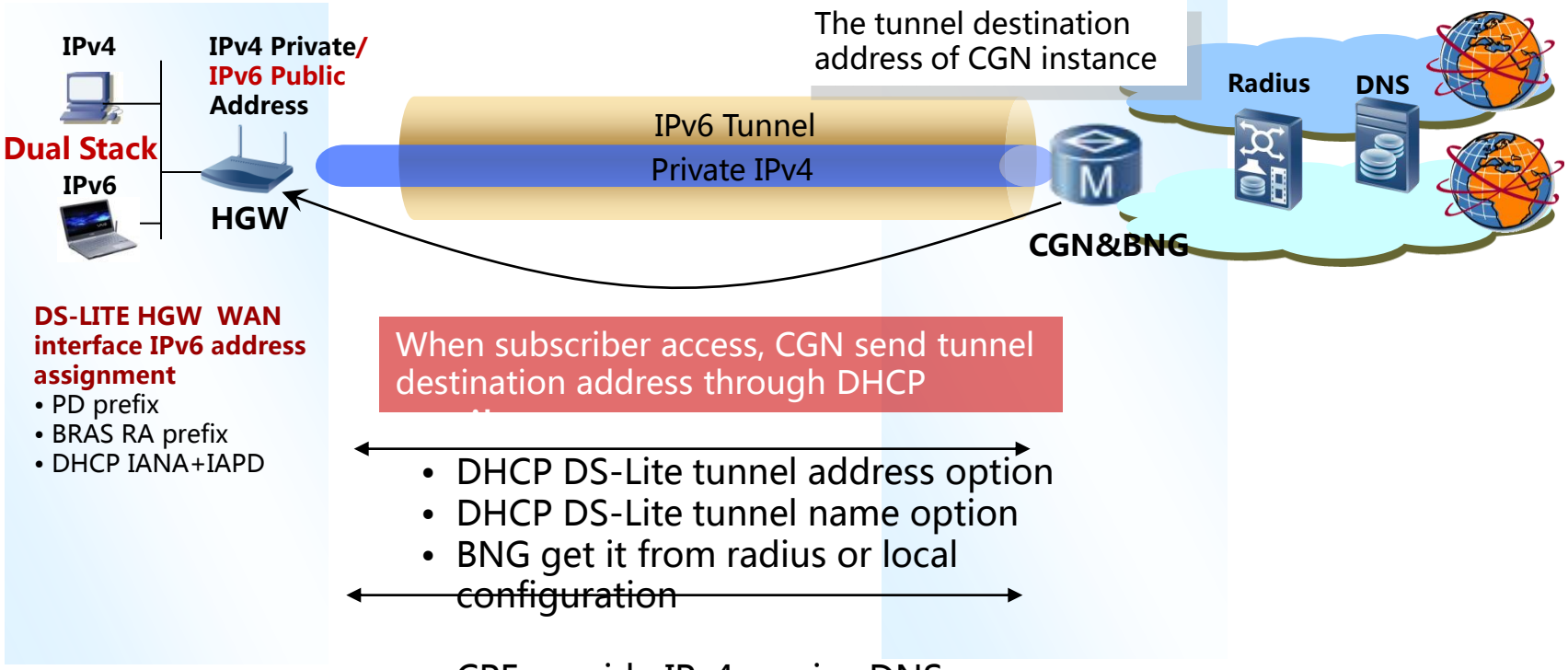
可选



- Radius服务器按照不同的subscriber policy profile下发user profile；通过BARS和CGN的绑定，实现基于user profile的策略控制；
- 主要亮点：1）实现基于用户的统一策略控制；2）融合CGN&BNG减少设备数量，提升网络可靠性，降低成本。

产品亮点4：CGN自动隧道发现简化DS-Lite方案的业务配置

可选



- 对于DS-Lite用户，通过DHCP属性携带隧道的目的IPv6地址和IPv4 DNS，自动建立隧道；
- 主要亮点：简化海量CGN的业务配置，提升运维效率。

产品亮点5： DS-Lite可视化管理

可选

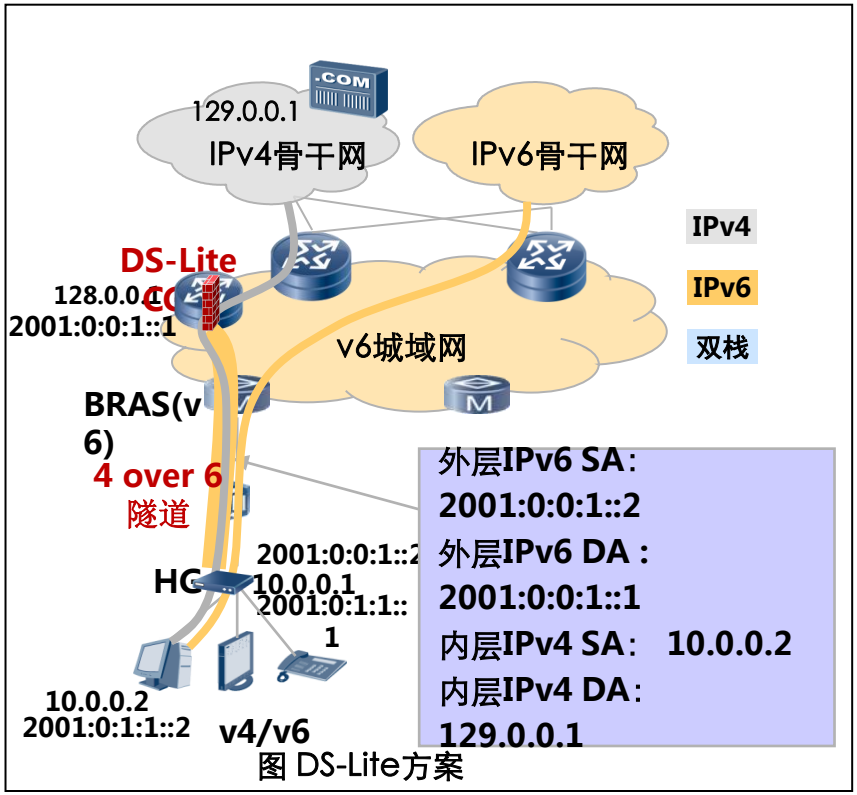


图 DS-Lite方案

网络背景：解决大规模网络中，V4主机穿越V6网络的问题；是4 Over 6隧道技术和NAT的技术结合

业务流程：IPv4报文通过Tunnel通过IPv6网络到达CGN网关， CGN通过4over6隧道收到客户报文后，剥离V6头并将私有IPv4转为公网IPv4报文，并发送到Internet

功能点：

1、开局配置通过批量完成（v4/v6双栈接口配置、CGN设备配置、NAT接口的使能、基于隧道的NAT地址池配置等）

2、4 over 6隧道拓扑显示

3、在隧道拓扑上可以提供接口流量，告警等信息

4、CGN设备NAT关键指标监控和统计

双栈拓扑可视化；

DS-Lite可视化；

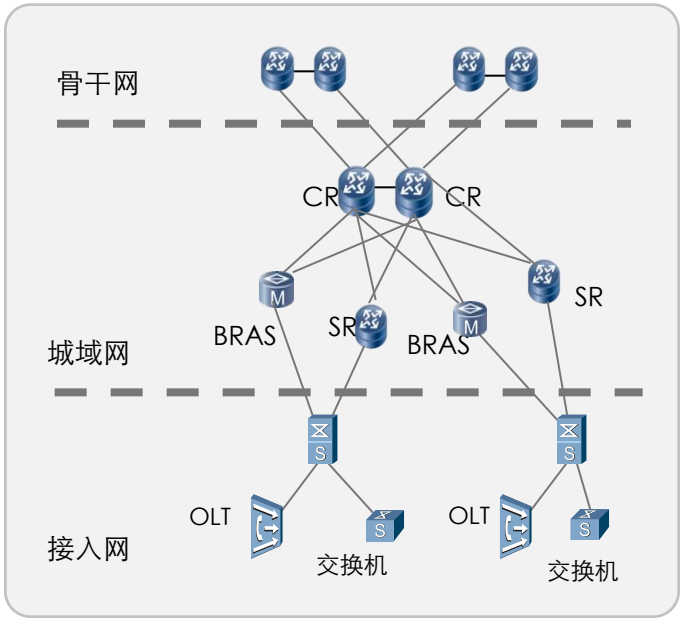
对V6、V4流量分别进行监控，帮助用户及时统计网络中V6与V4的流量，作为V6网络规划的依据

华为可商用部署的端到端IPv6解决方案准备就绪

业务

网络

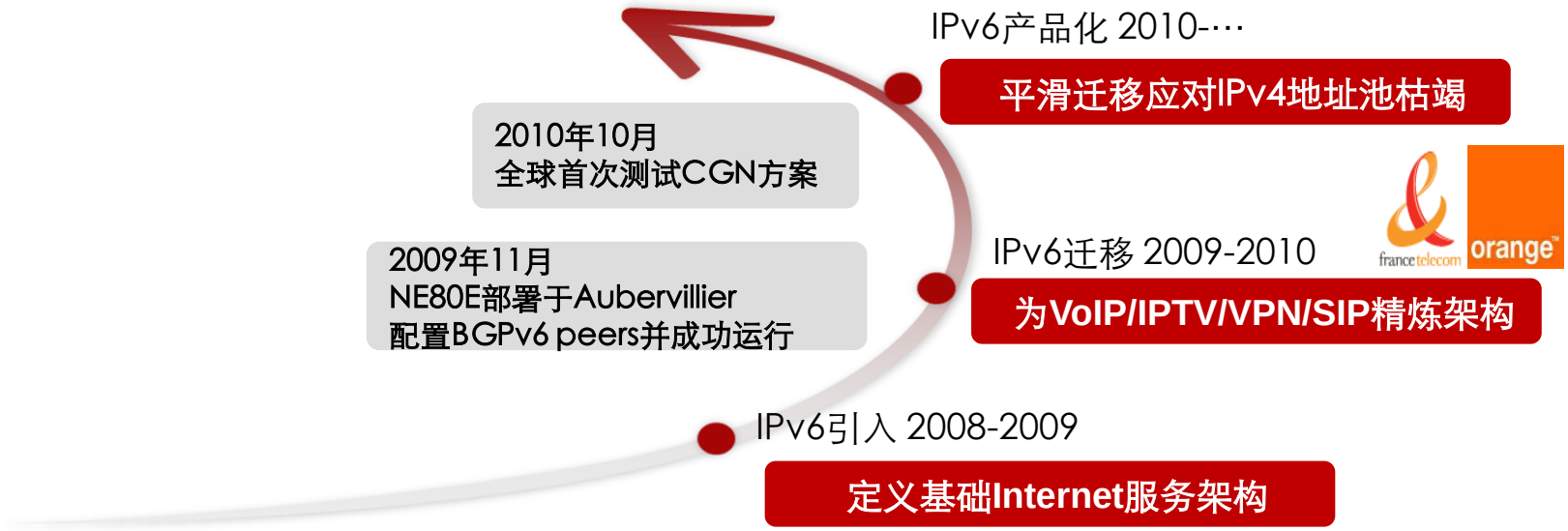
终端



端到端产品/解决方案已完全具备IPv6商用能力

目录

华为IPv6全球商用实践



2010 – 2011，IPv6演进全面启动

完成测试：Telefonica、vodafone、STC、SFR、Bouygues Telecom、JAZZTEL

正在测试：SingTel、true、TM、TELECOM ITALIA、maxis、Globe

新加坡电信IPv6咨询项目背景

新加坡电信IPv6计划

项目背景：

- 新加坡政府出于国家战略的考虑，要求新加坡电信11年底启动IPv6项目；

项目规模：

- 涵盖新电全球范围内八个子网；目前已经启动四个子网项目的咨询；
- 包含新电移动＆固网的全部业务；

对咨询公司的要求：

- 要求是一家综合业务制造商，具备分别针对移动和固网评估的能力；
- **华为是一家综合业务制造商，包含固网、移动、终端、OSS诸多产品线；完全具备新电所要求的综合能力；最终华为中标。**

SingTel

咨询/决议期
(2011.6-2011.12)

评估/集成测试期
(2011.12-2012.6)

试商用
(2012.7-2012.12)

全面商用
(2013年后)

新电CTO寄语：

感谢华为积极与新电集团合作，一起走在通向IPv6下一代Internet的旅程上；通过各种互动活动，分享华为的先进经验，确保迁移技术方案的准确性，以及IPv6技能的传递，这是我们所期望的。

华为全面参与中国IPv6商用项目

深圳大运会 IPv6通信网络 | 湖南电信 IPv6城域网络 | 江苏电信 IPv6城域网络 | 上海世博会 IPv6TV应用 | 三大运营商 CNGI骨干网络 | 广东移动 IPv6城域网络 | 江苏移动 省网&城域网 | 北京移动 MDCN网络

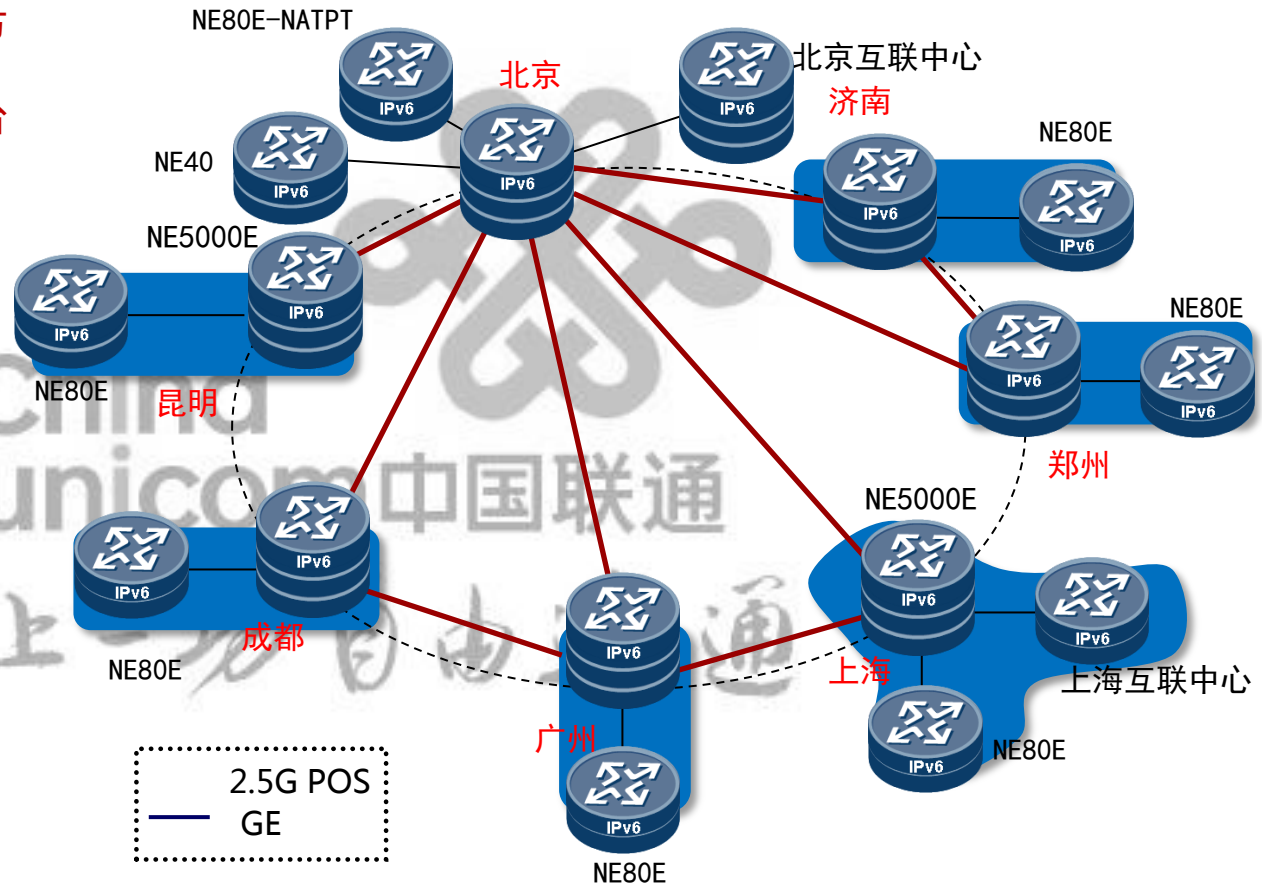
成功打造低成本可复制的长沙模式

IPv6宽带接入认证地址分配 | IPv6专线&VPN业务 | IPv6TV内容&承载 | IPv6校园网接入业务 | IPv6骨干网互联&穿越 | IPv6物联网接入业务 | IPv6手机上网&WAP | 基于IMS的IPv6 SIP业务

IPv4/IPv6双栈升级 | NAT44过渡方案 | DS-Lite过渡方案 | 6PE/6VPE过渡方案 | L2TP过渡方案 | AAA&DNS&BOSS对接 | 用户地址端口溯源方案

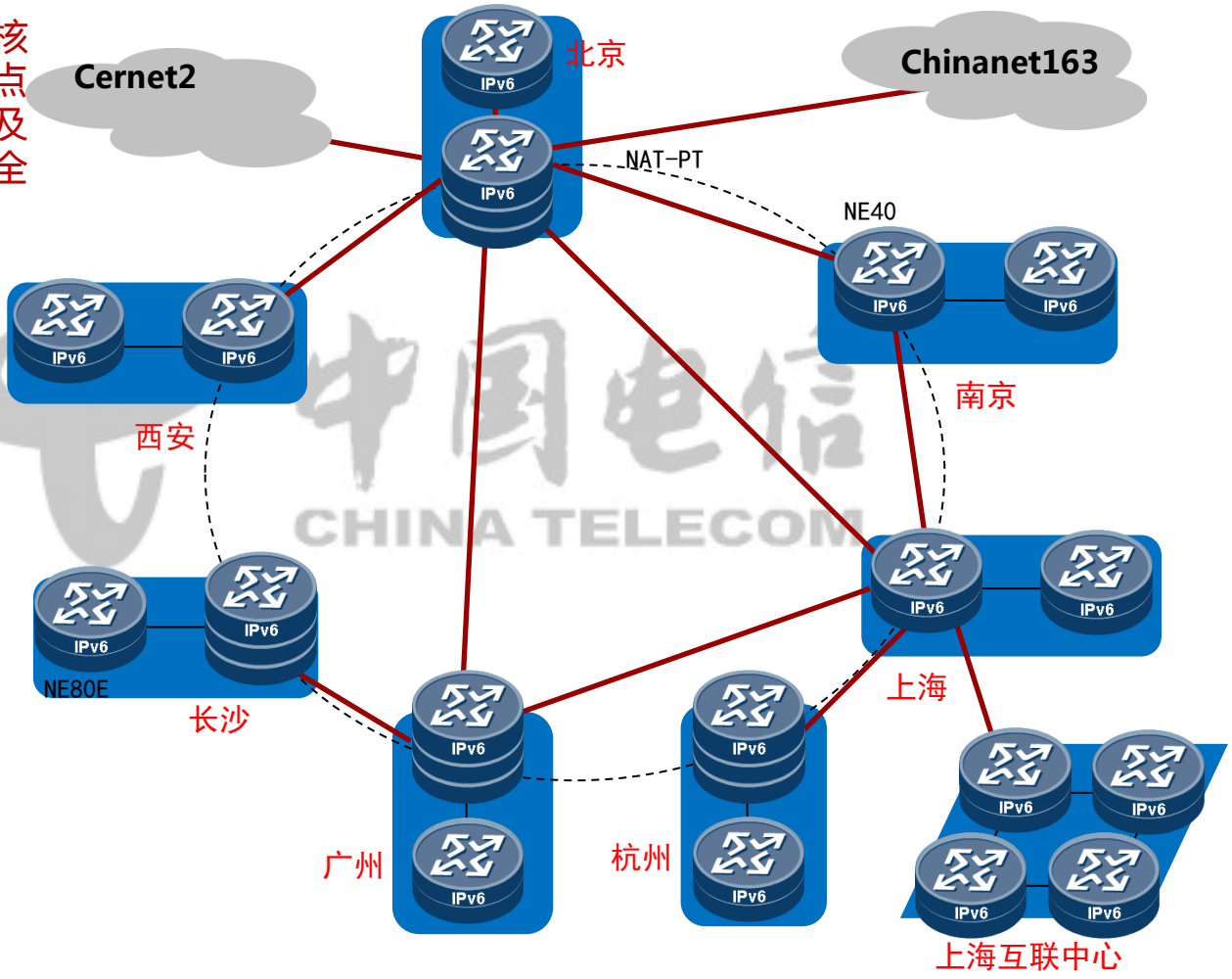
中国联通IPv6主干网

华为承建北京和上海核心节点、全部7个汇聚节点和NATPT网关节点、网管节点，产品包括5台NE5000E、7台NE80E、3台NE40，设备覆盖联通CNGI全网络



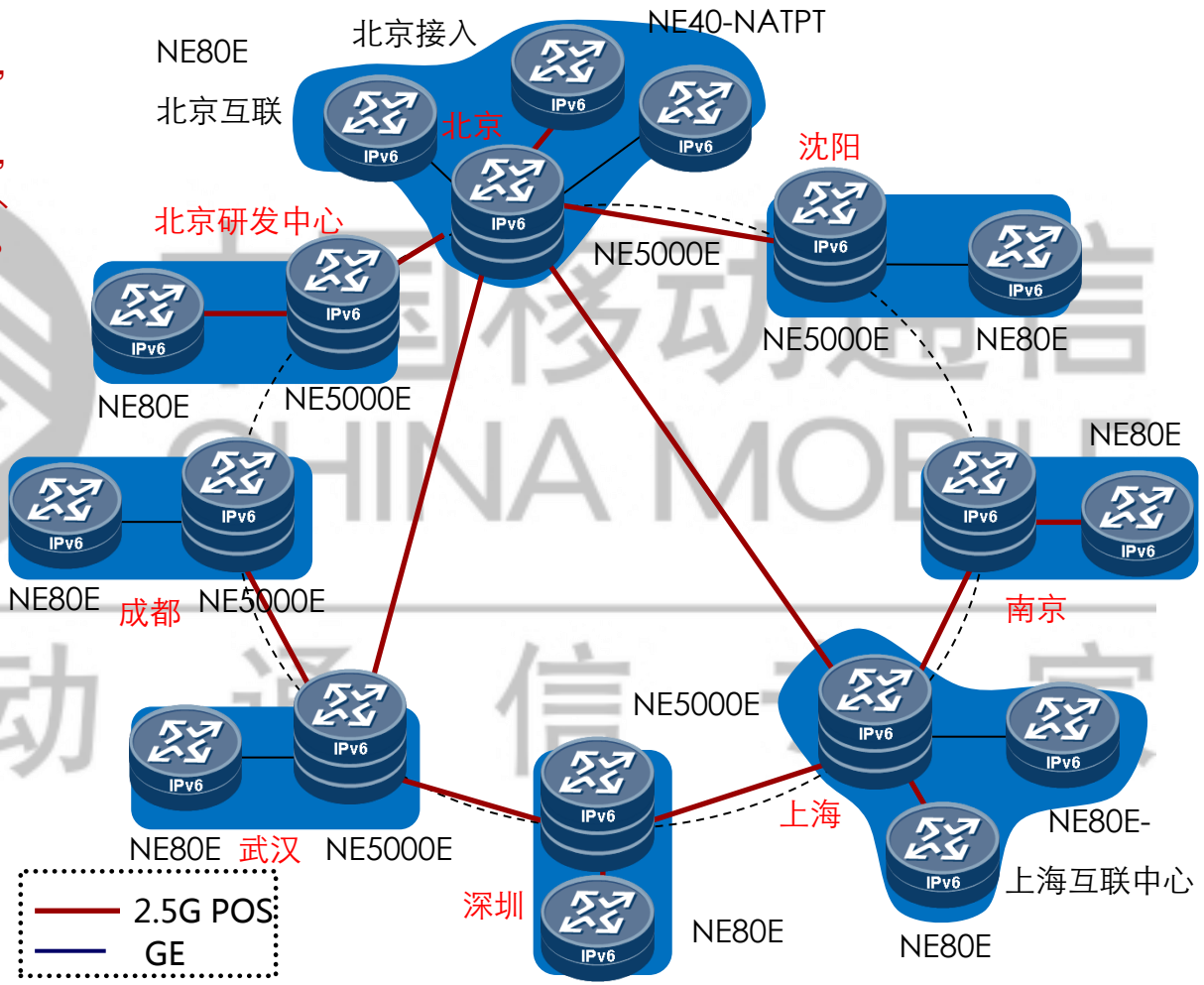
中国电信IPv6主干网

华为公司承建大部分核心节点、全部汇聚节点全部网间路由器，以及上海网络交换中心的全部设备和NATPT网关设备，包括17台NE80E，1台NE40

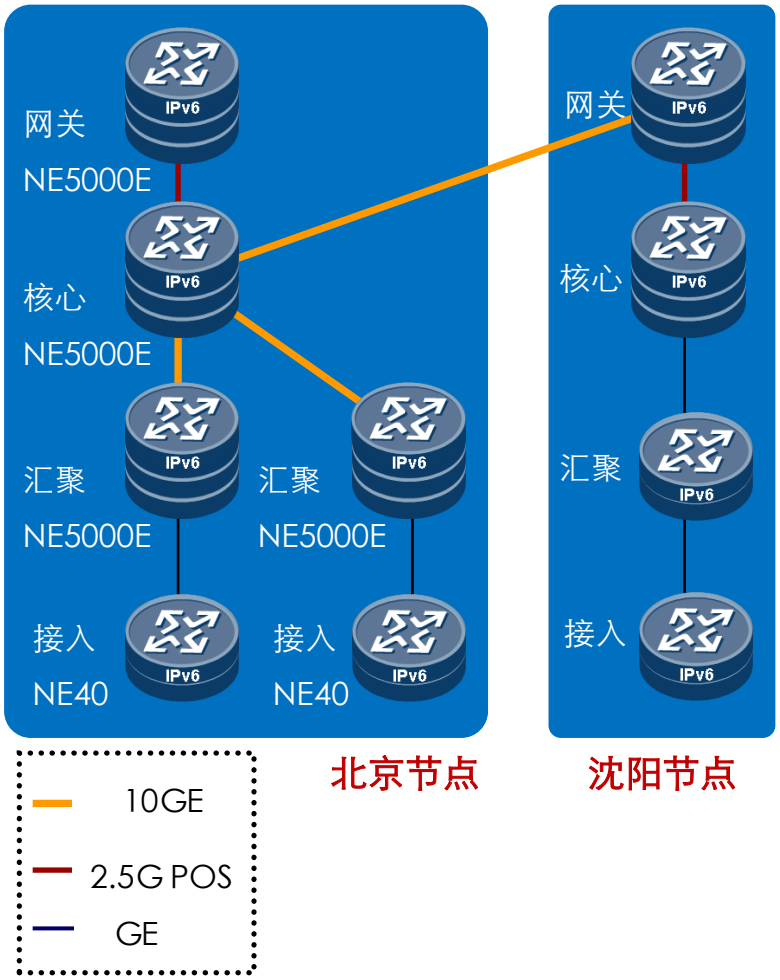


中国移动IPv6主干网

华为承建除南京、深圳以外的6个核心节点，7个接入节点，2个互联中心，1个网关节点，产品包括6台NE5000E、9台NE80E、1台NE40。

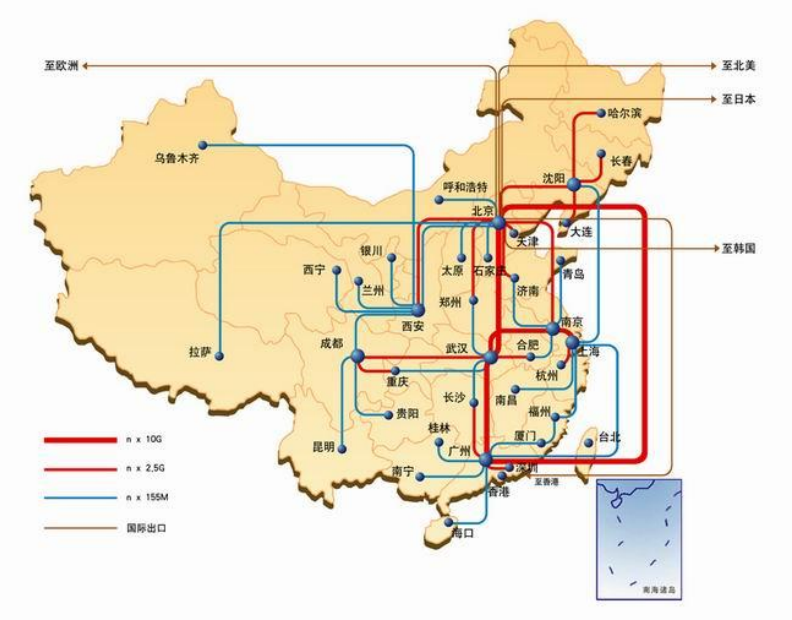


中国铁通IPv6主干网



中国铁通CNGI主干网由北京节点和沈阳节点，共10台设备。华为公司承建北京节点，共6台设备，4台NE5000E和2台NE40。

中国教育和科研骨干网(CERNET)



客户需求

- 扩大网络覆盖和带宽，支持全国211大学高速接入
- 提升网络业务承载能力，支撑面向全国高等教育的普通服务和面向全国高校重点学科建设的科研服务
- 具备向IPv6网络平滑演进能力

解决方案

- 华为承建的核心和接入路由器采用400G平台的NE40E，支持IPv6、IPv4/IPv6双栈和多业务承载，设备支持丰富的IPv4和IPv6协议以及IPv6组播。
- 每槽位可从40G平滑扩容到400G，满足未来3-5年的带宽增长需求。

客户价值

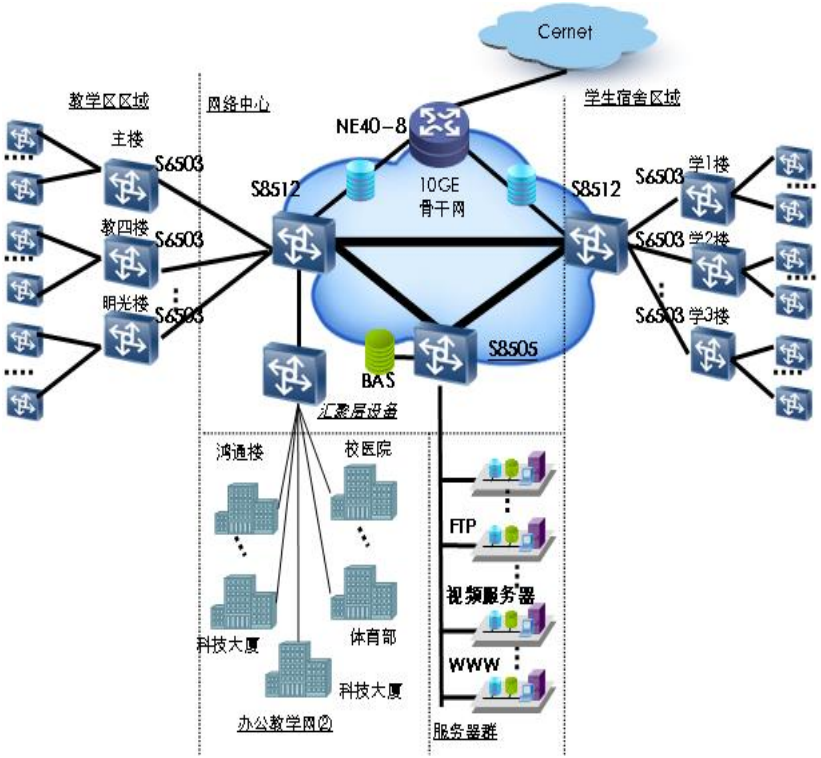
- 多业务承载和IPv4/IPv6双栈，满足科研服务和普通服务的统一承载，并实现向未来网络的平滑演进。
- “IP + 光”具备端到端的100G接入能力，满足全国211大学高速接入的需求。

中国教育和科研骨干网(CERNET2)

CNGI-CERNET2主干网

在国际上首次提出“建设纯IPv6大型互联网主干网”的技术路线，设计和研制成功大型纯IPv6互联网主干网CNGI-CERNET2。建设纯IPv6大型互联网，体现了加速向下一代互联网过渡的创新技术路线。解决了大规模IPv6主干网拓扑结构和路由设计、地址和域名规划、网络调试测量和网络管理等技术难题，为我国下一代互联网的技术试验和应用示范提供了大规模网络环境，加快了我国下一代互联网的发展进程，在国际学术界产生了重大影响。

北京邮电大学万兆校园网



北京郵電大學
BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

挑战

学生数量增多，业务信息量激增，千兆骨干互联已不能满足高带宽和新业务对带宽的需求

鉴于IPV4向IPV6过渡的长远考虑，需要建设IPV6网络

方案

核心骨干设备之间提升至万兆互联，教学楼、宿舍楼都采用千兆交换机与核心交换机互联，教室、宿舍采用白兆接入

核心交换机替换成双栈交换机，支持访问IPv6网络

价值

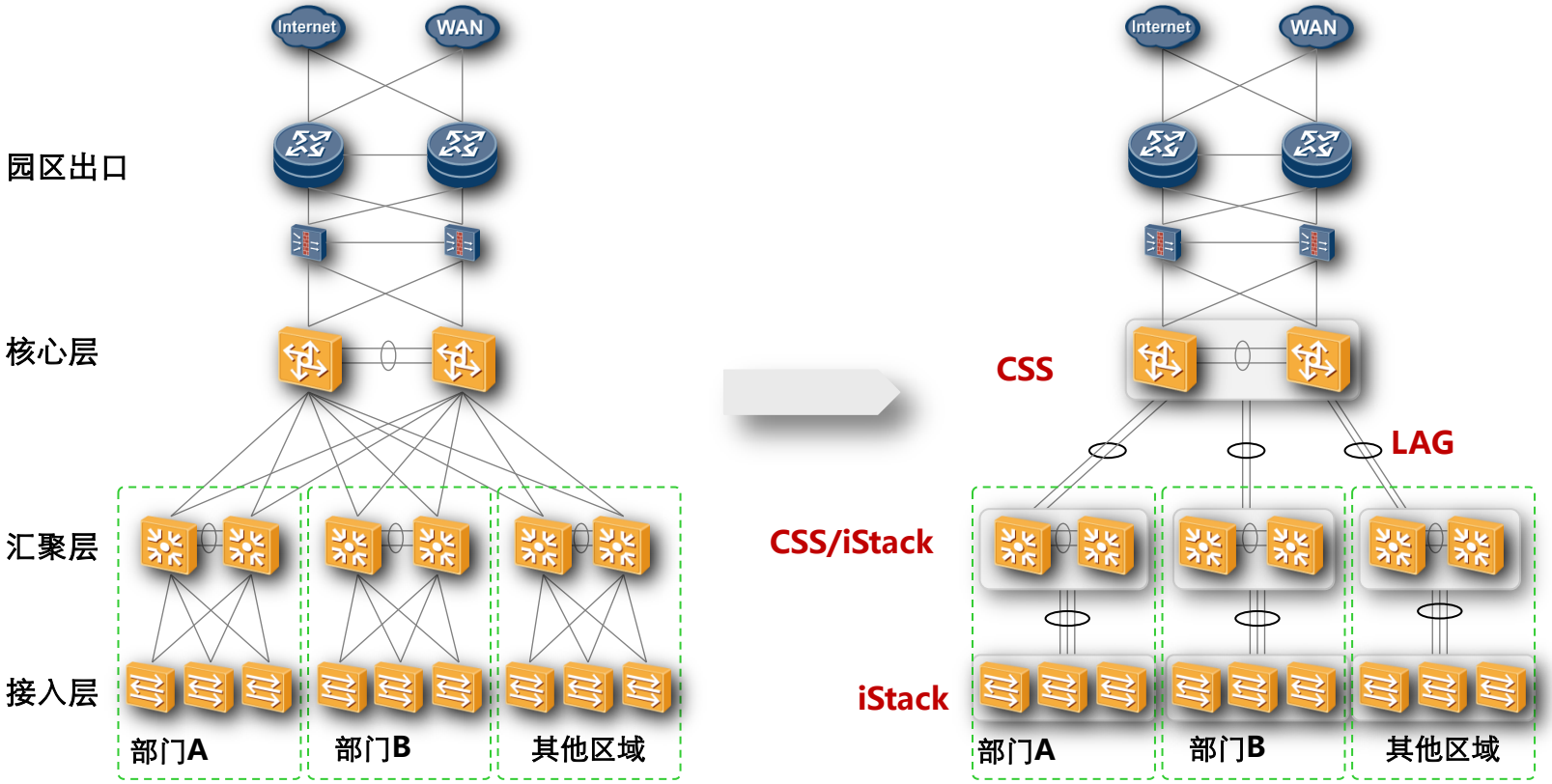
大大提高网络性能和带宽，实现校区内高速互联

师生可以对IPV6网络进行访问，同时可以逐步在IPV6网络中开展IPV6业务

子目录

4 园区网业务解决方案

虚拟园区网—横向虚拟化



简单管理 – 简化网络拓扑；无复杂保护协议STP等

高可靠性 – 快速路由收敛；跨设备链路汇聚

平滑扩容 – 增加新设备，拓扑、链路改动最小

CSS: Cluster Switching System 集群交换机

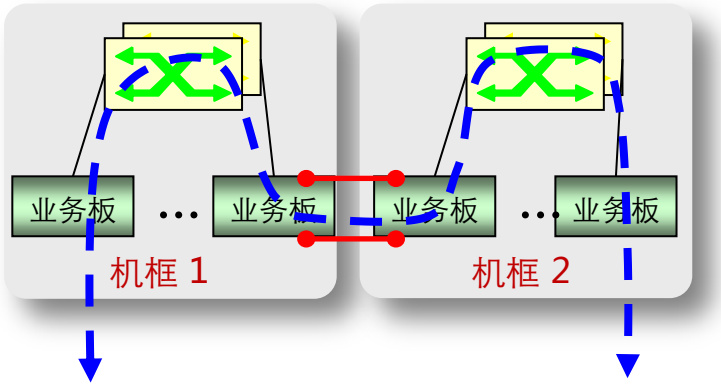
LAG: Link Aggregation Group 链路聚合(集群内)

Stack: 交换机堆叠，应用于盒式产品

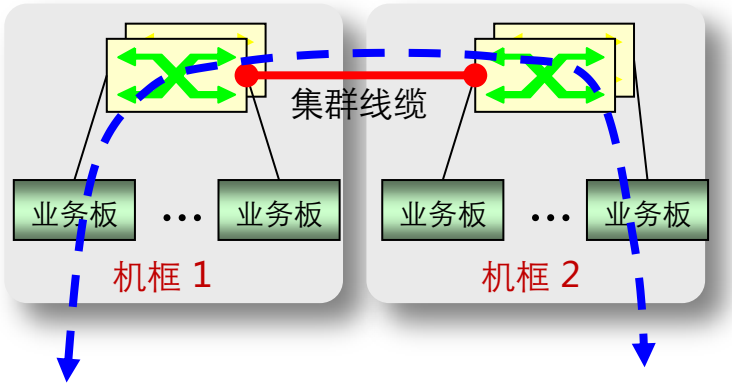
专用集群带宽的横向虚拟化方案

业界集群：160G

华为：256G（未来400G）



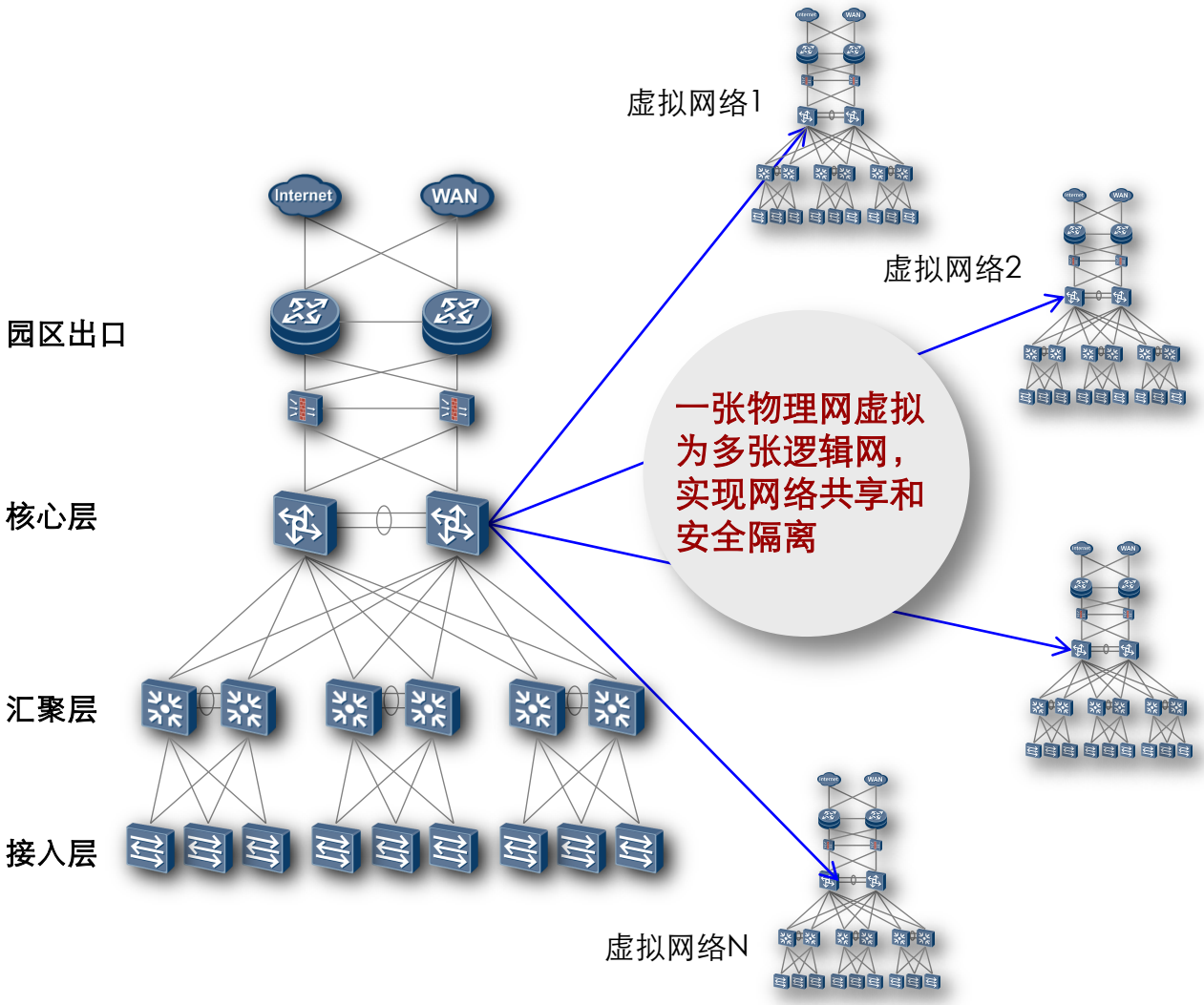
业务板集群



交换网集群

	占用业务槽位	集群带宽	转发效率
华为集群	不占用	高：256G(未来400G)	高：交换网直接互联
业界集群	占用	低：160G	低：需要二次转发

虚拟园区网—纵向虚拟化

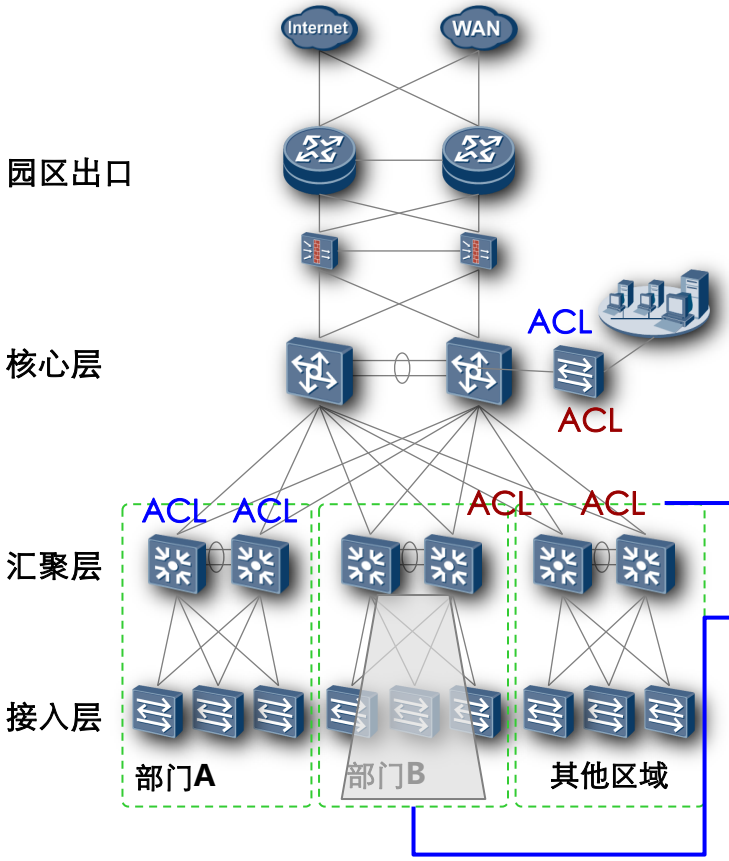


接入控制
保证用户接入身份可靠及安全性

业务逻辑隔离
不同权限业务间相互隔离及互访

资源隔离
不同用户可访问资源的安全隔离

虚拟园区的VLAN隔离和ACL隔离方案



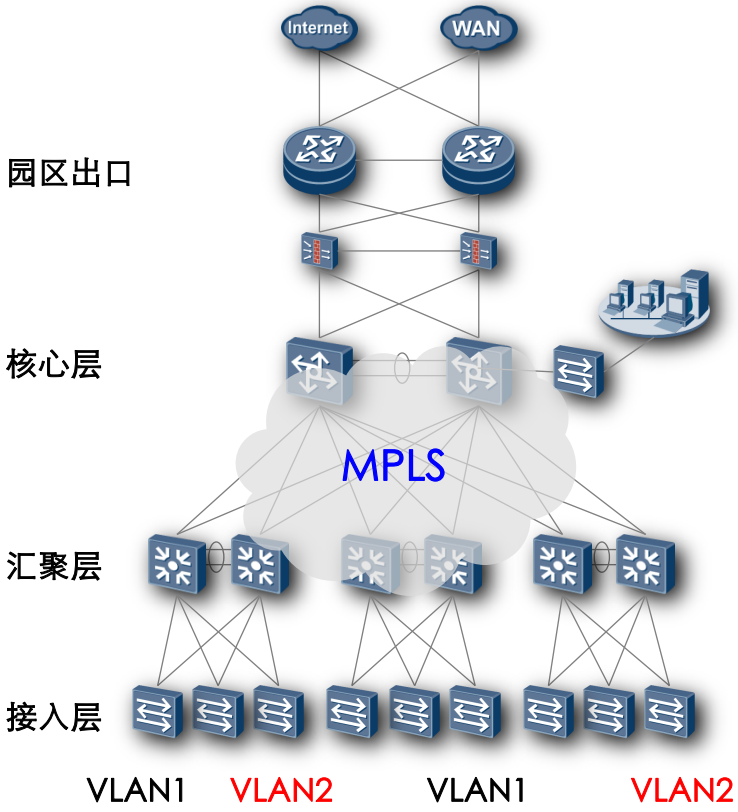
分布式ACL隔离

通过在网络边界和数据区边界部署ACL来限制其它部门的访问。
复杂的策略控制，
同时业务/网络调整时配置需要跟随变动。
适用于小规模园区网

VLAN隔离

广播域大，资源利用率偏低
适合园区网络小范围内部隔离
或者是很小园区网的隔离

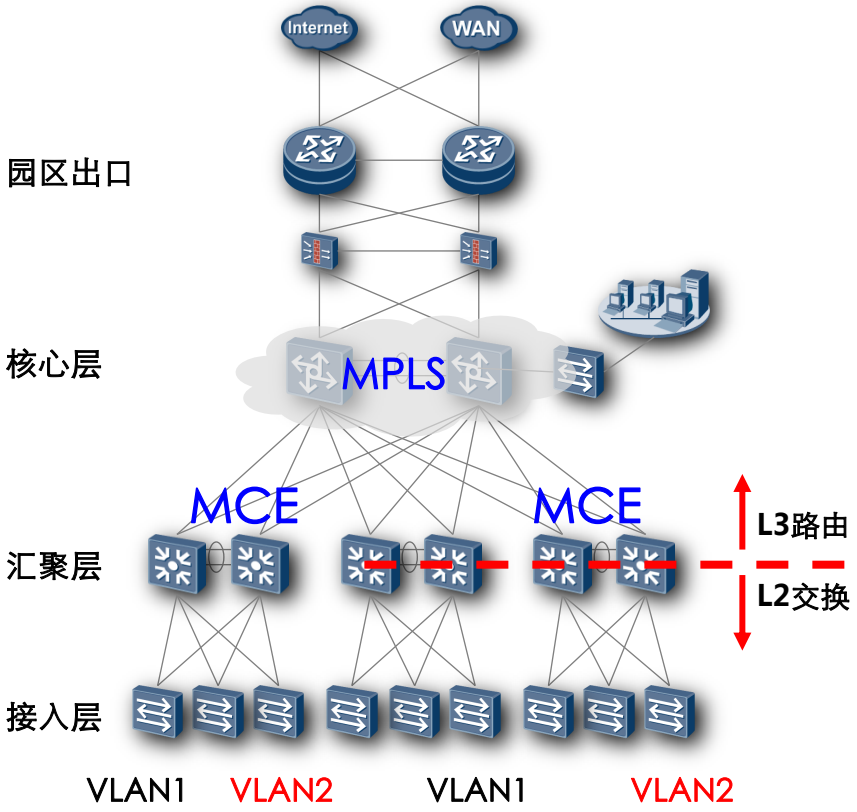
虚拟园区的MPLS VPN+VLAN隔离方案



基于MPLS的隔离

- MPLS部署到汇聚层
- 接入层通过VLAN隔离
- 每个部门/业务区端到端隔离，彼此之间互不影响
- 适用于大型园区网隔离

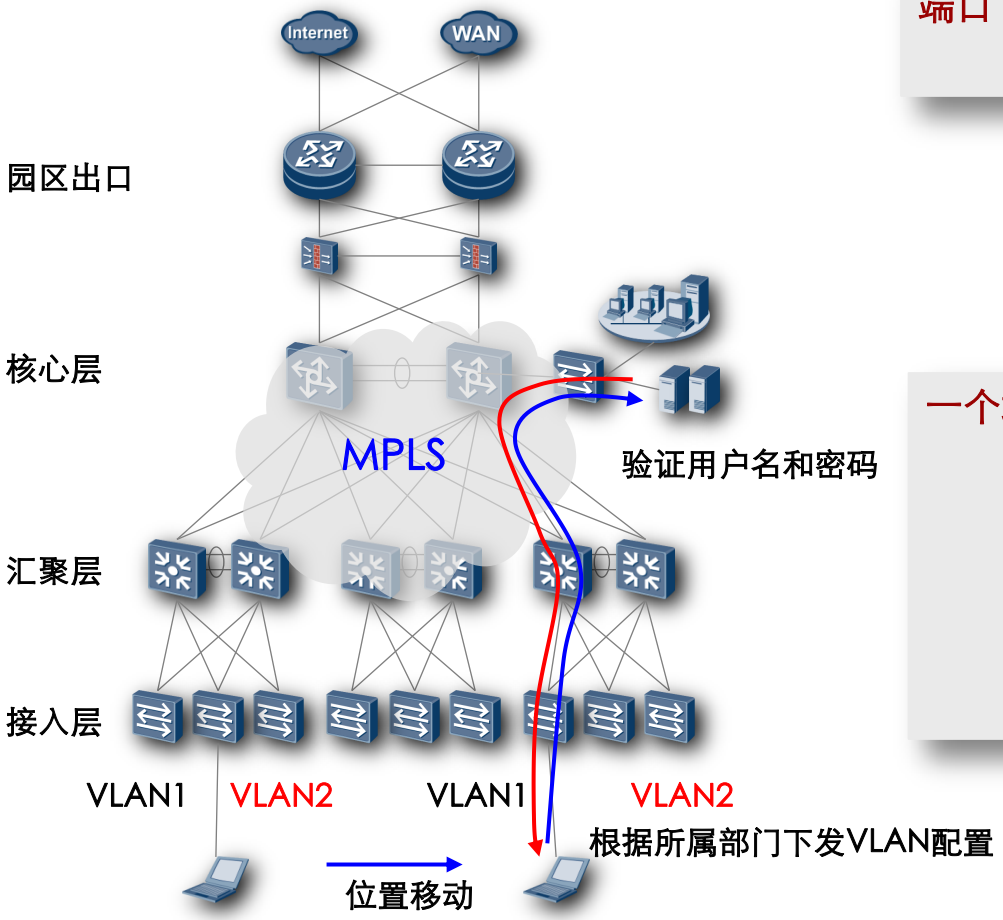
虚拟园区的MPLS VPN+MCE+VLAN隔离方案



基于MPLS的隔离

- 应用于汇聚层不支持MPLS的情况
- MPLS部署到核心层
- 汇聚层通过MCE扩展
- 接入层通过VLAN隔离
- 每个部门/业务区端到端隔离，彼此之间互不影响
- 适用于大型园区网隔离
- 建议：若汇聚层有能力支持MPLS，MCE可以下移到接入层

虚拟园区网用户动态接入



端口（用户）固定场景

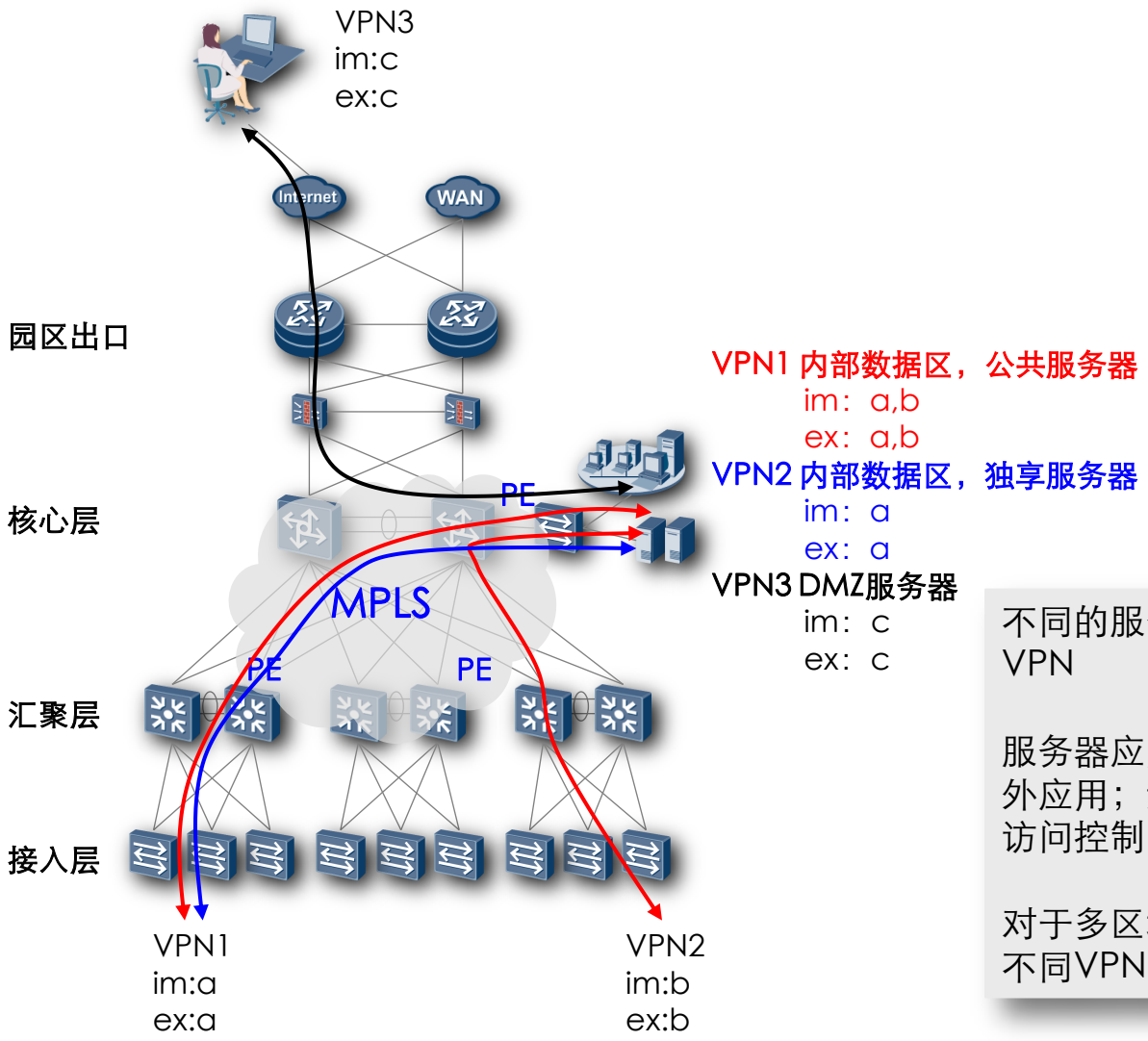
用户VLAN三层接口绑定VRF

一个端口多个VPN共用共用场景

服务器根据认证结果下发VLAN到用户端口，使不同用户进入不同的VPN

VLAN和VRF的邦定关系是固定的，通过动态调整用户VLAN来调整用户的接入VPN

虚拟园区网数据访问方案



VPN1 内部数据区，公共服务器
im：a,b
ex：a,b

VPN2 内部数据区，独享服务器
im：a
ex：a

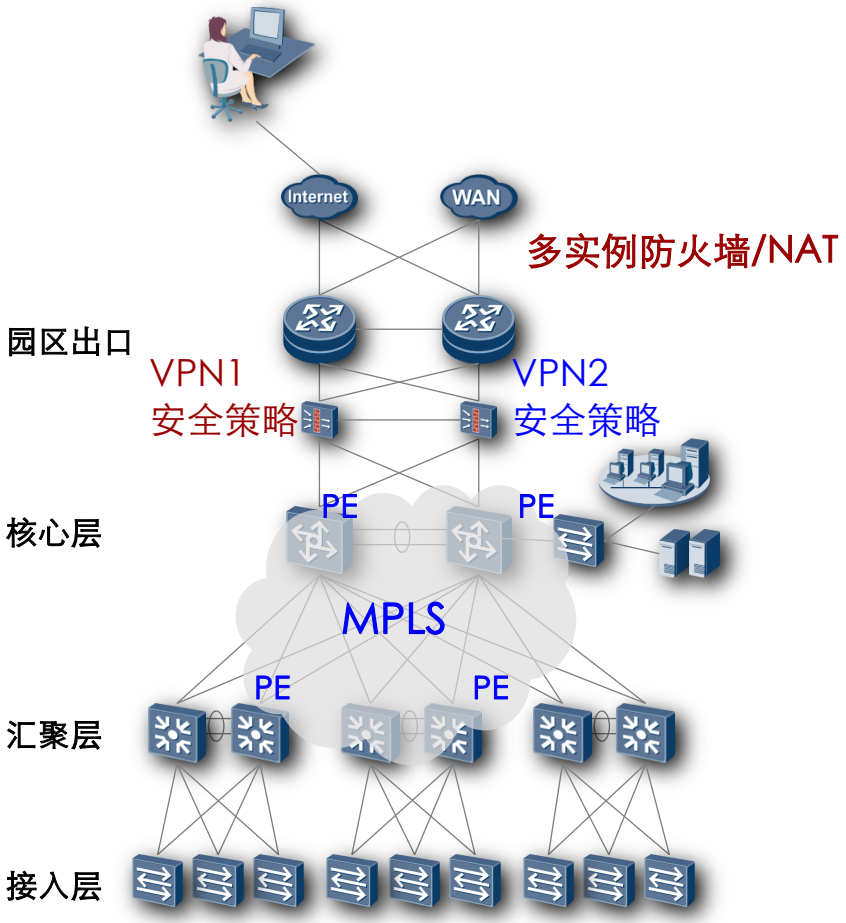
VPN3 DMZ服务器
im：c
ex：c

不同的服务器区通过VLAN接入不同的VPN

服务器应用分三种场景：公共、独享、对外应用；通过MPLS VPN的路由发布实现访问控制

对于多区域访问公共服务器的情况，要求不同VPN的用户IP地址不能重叠

虚拟园区网internet访问



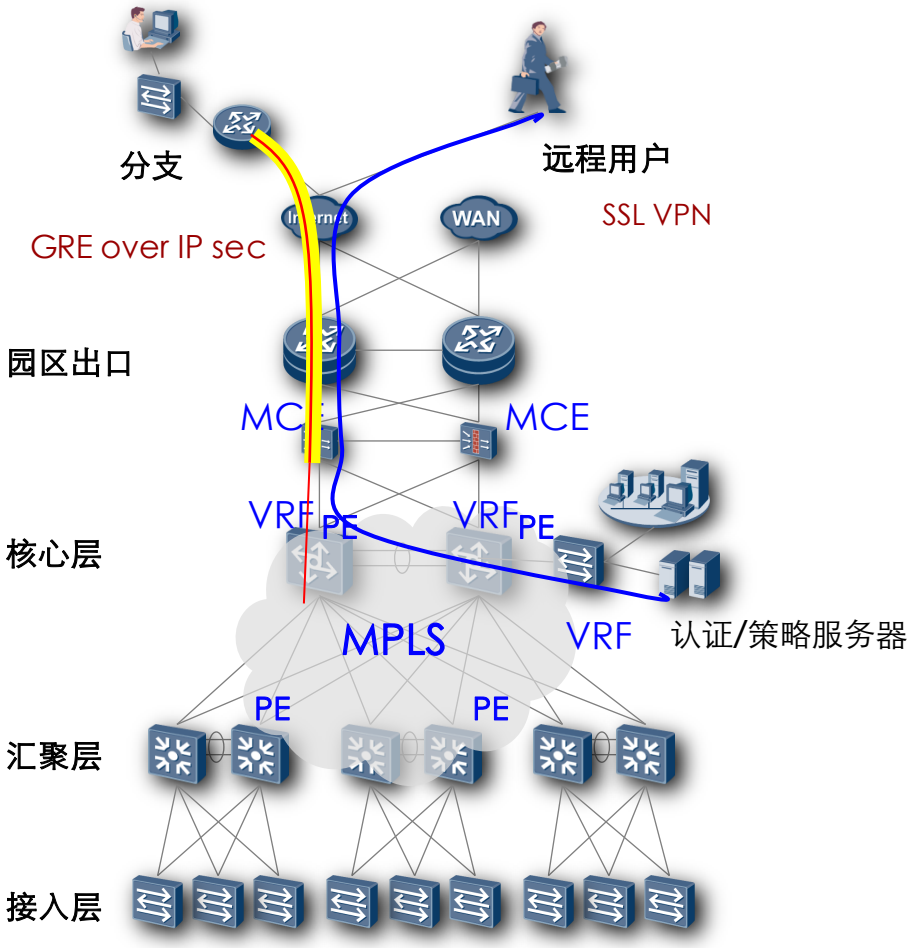
出口安全部署虚拟防火墙，针对不同的业务区部署不同的安全策略，并实现NAT转换

虚拟防火墙通过MCE实现，并与园区MPLS PE设备上需要访问Internet的VRF一一邦定

发布一条默认路由给所有VRF，实现Internet流量的统一出口

经过防火墙/NAT后，所有业务区的流量都变成公网地址，此时可以进行业务互访。

虚拟园区网远程接入



分支接入

在分支和总部园区安全网关之间部署GRE over IP sec隧道，通过将园区网网关GRE隧道的Tunnel口绑定到目标VPN来实现的；

IPSec隧道用户对私网报文加密，确保私网通信的保密性

对于分支也划分多个业务区的情况，通过建立两条GRE over IP sec隧道实现，GRE tunnel口邦定两端的VRF

远程用户接入

用户被SSL VPN终结后，根据对用户的认证结果在网络设备动态配置VLAN，引导用户进入不同的VPN

子目录

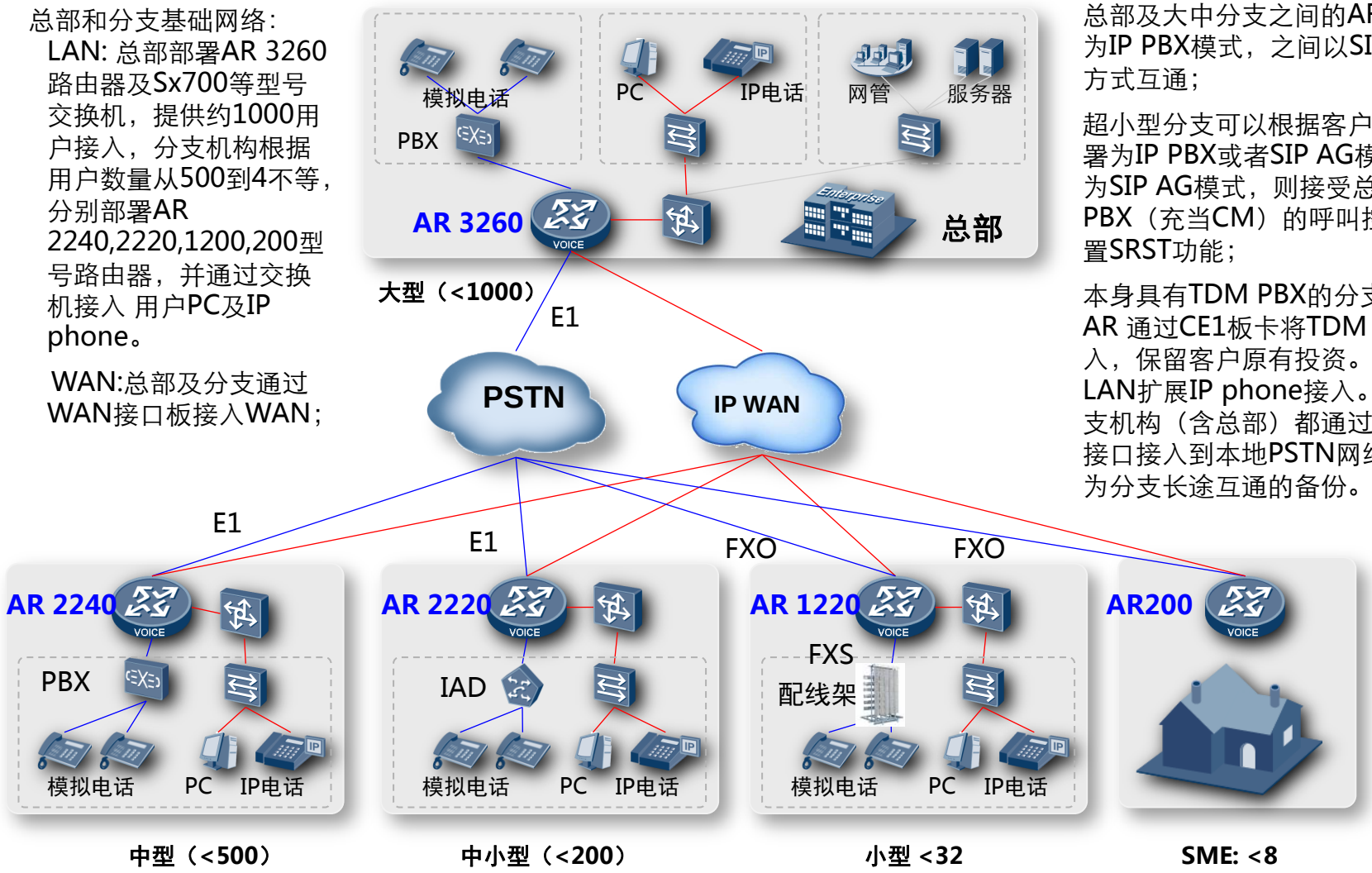
4 园区网业务解决方案

园区语音解决方案

总部和分支基础网络：

LAN: 总部部署AR 3260路由器及Sx700等型号交换机，提供约1000用户接入，分支机构根据用户数量从500到4不等，分别部署AR 2240,2220,1200,200型号路由器，并通过交换机接入 用户PC及IP phone。

WAN:总部及分支通过WAN接口板接入WAN；



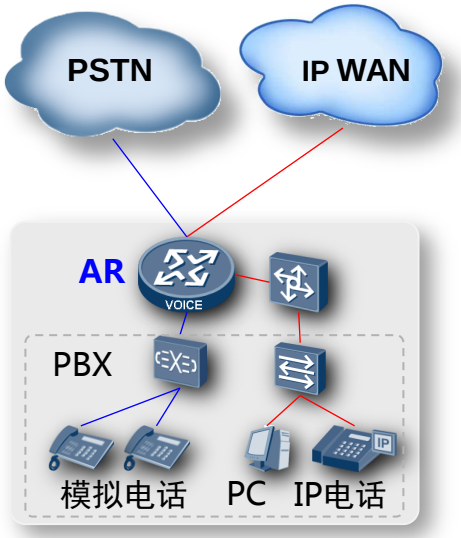
总部和分支之间的VoIP通信服务：

总部及大中分支之间的AR都配置为IP PBX模式，之间以SIP Trunk方式互通；

超小型分支可以根据客户需要部署为IP PBX或者SIP AG模式，若为SIP AG模式，则接受总部IP PBX（充当CM）的呼叫控制，内置SRST功能；

本身具有TDM PBX的分支机构，AR 通过CE1板卡将TDM PBX接入，保留客户原有投资。通过LAN扩展IP phone接入。所以分支机构（含总部）都通过E1/FXO接口接入到本地PSTN网络，并作为分支长途互通的备份。

基础语音方案提供基本业务和补充业务



基本业务
- 基本通话
- 传真业务
- 号码变换
- 智能路由
- CDR功能

补充业务

主叫识别
- 主叫号码显示
- 主叫号码显示限制

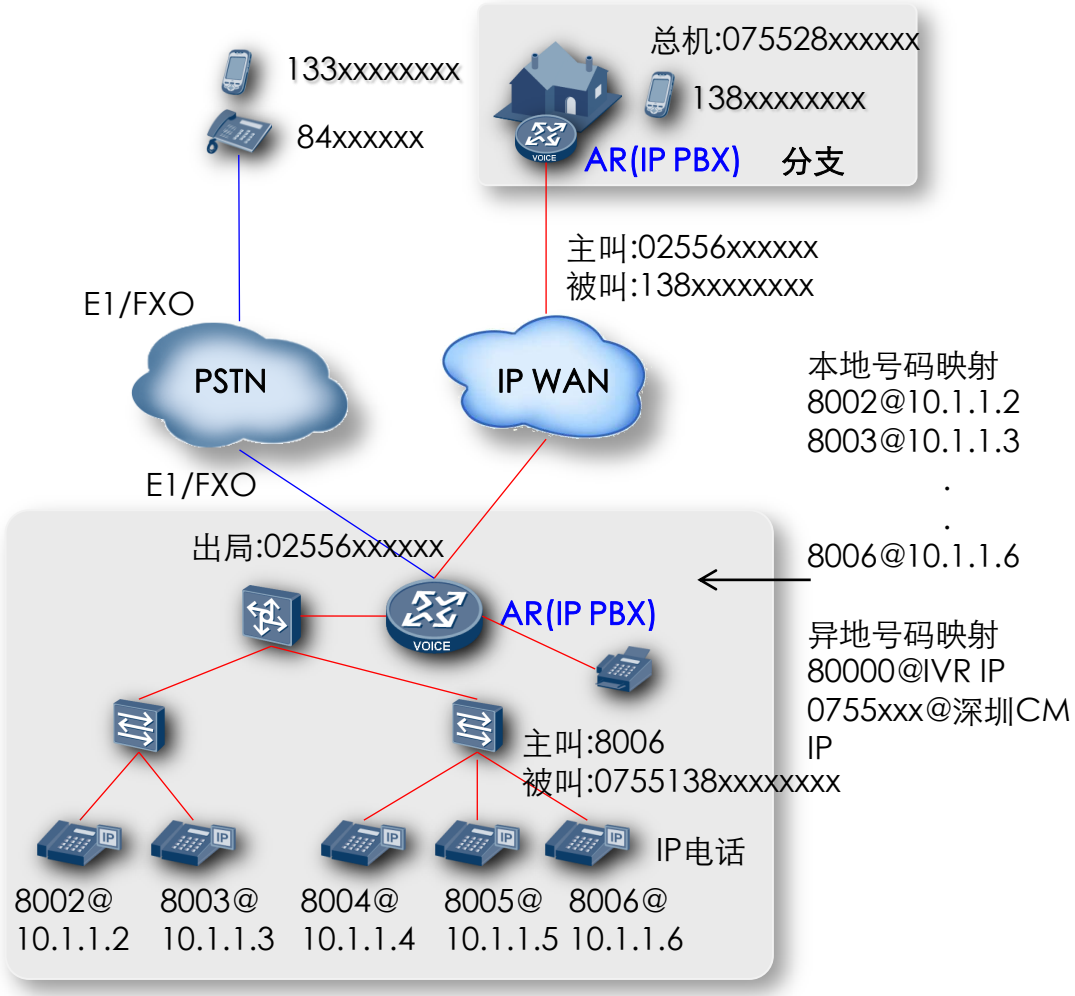
呼叫保持
- 双通话业务
- 呼叫等待
- 呼叫转移
- 三方通话
- 呼叫前转

呼叫控制
- 选择呼叫拒绝
- 选择呼叫接受
- 匿名呼叫拒绝
- 免打扰
- 呼叫拦截

群组业务
- 同振
- 顺振
- 同组代答
- 指定代答
- 一机多号
- IVR排队

个性业务
- 短号呼叫
- 区别振铃
- 缩位拨号
- 闹钟提醒
- 查号业务

IP话机接入方案



在园区出口部署AR 系列路由器作为IP PBX(根据用户容量选择AR 3260/2240/2220/1220/200等型号)

园区内所有IP话机都注册到AR上

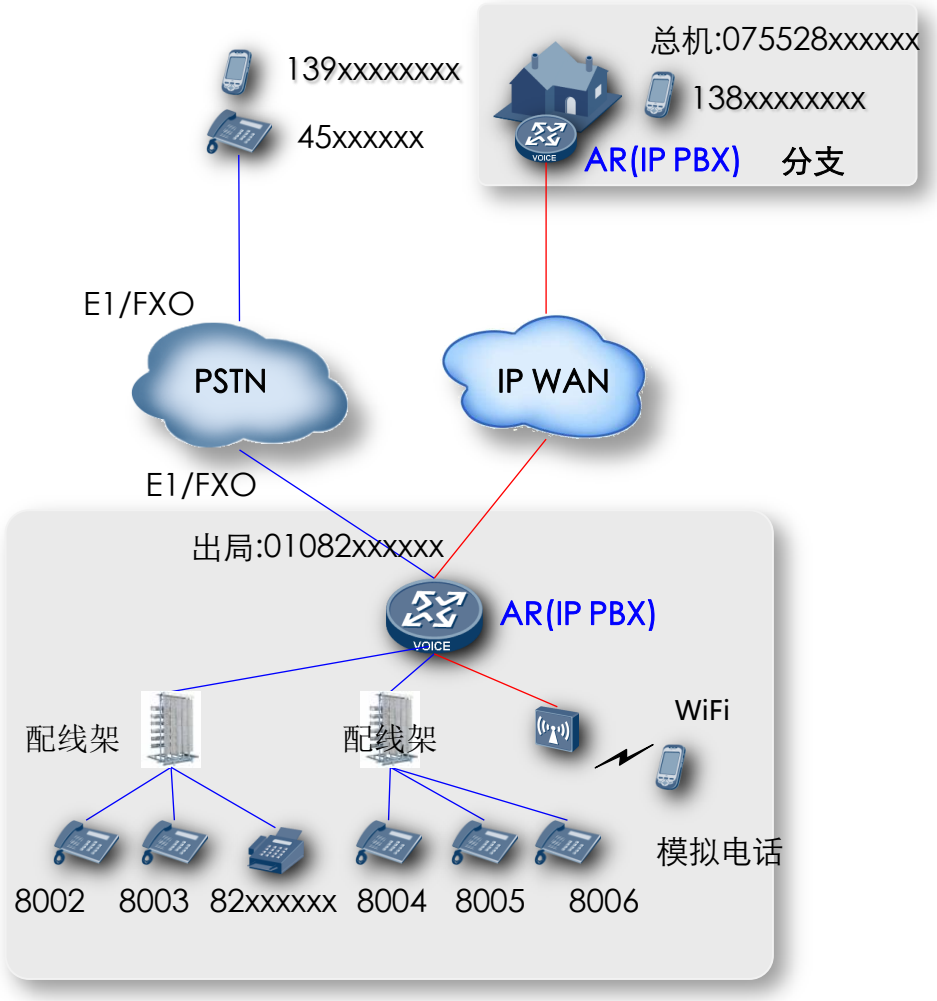
在AR路由器上配置E1或者FXO接口板，连接到本地PSTN网络

由AR 管理出局呼叫路由及园区内部通话路由。

与其它分支园区之间的长途通话通过内部IP网络互通，AR管理内部长途呼叫路由。

房地产、酒店、4S店等连锁型企业，通常在一个城市或全国有大量的分支，每个分支都需要支持4-8路电话，这类企业通常都是追求资本支出风险低，希望能够以尽可能低的代价建立各分支办公环境。而当前的小型PBX或是支持内置PBX的路由器组建的网络还是投入成本较高，AR207V提供集成语音的PBX功能，提供高性价比的连锁企业语音部署方案

模拟话机接入方案



在园区出口部署AR 系列路由器作为IP PBX(根据用户容量选择AR 3260/2240/2220/1220/200等型号)

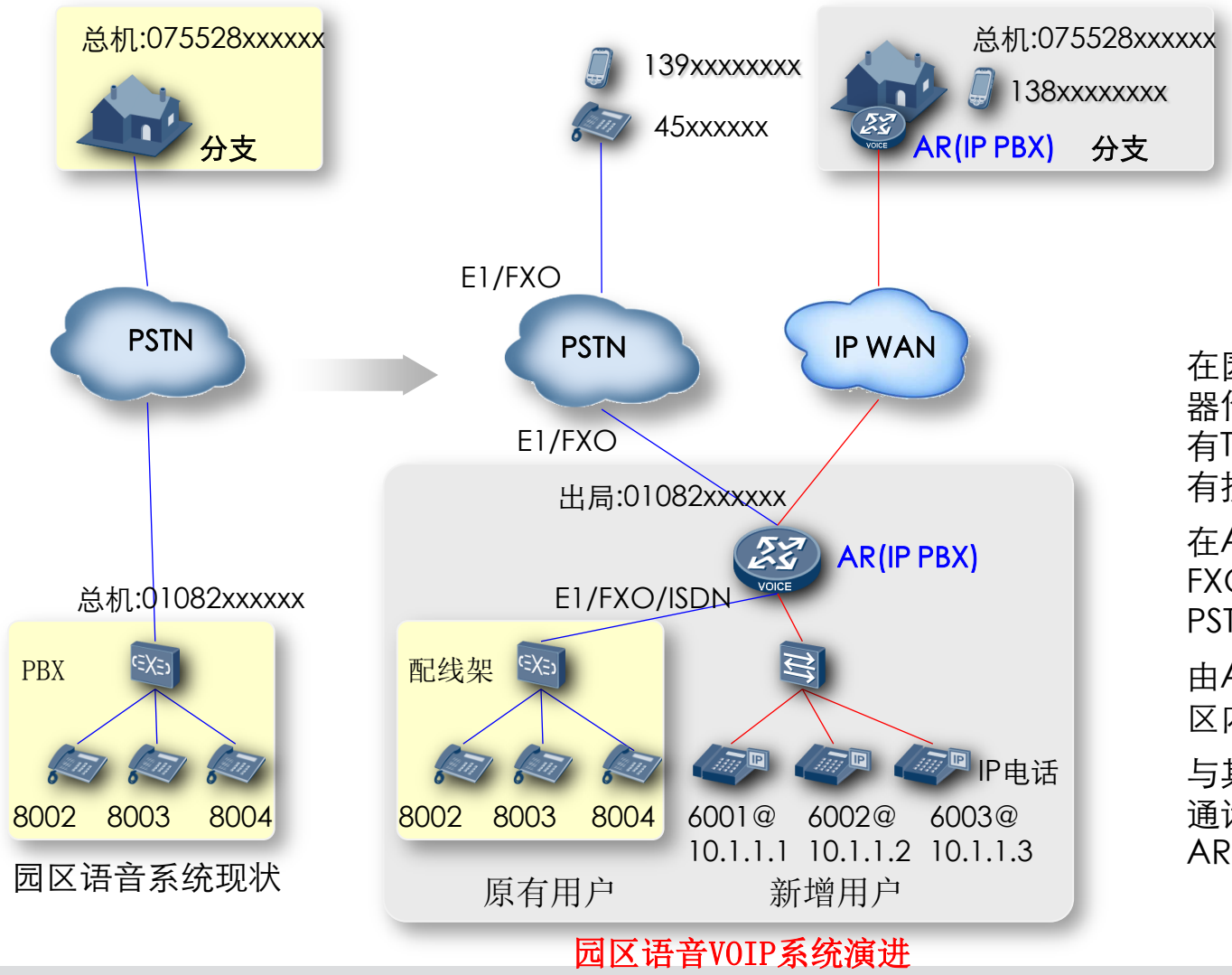
通过FXS板卡接入模拟用户,在AR路由器上配置E1或者FXO接口板，连接到本地PSTN网络

由AR 管理出局呼叫路由及园区内部通话路由。

与其它分支园区之间的长途通话通过内部IP网络互通，AR管理内部长途呼叫路由。

WiFi 终端设备上可安装 软件电话，提供园区内移动语音

TDM PBX接入解决方案



园区语音系统现状

园区语音VOIP系统演进

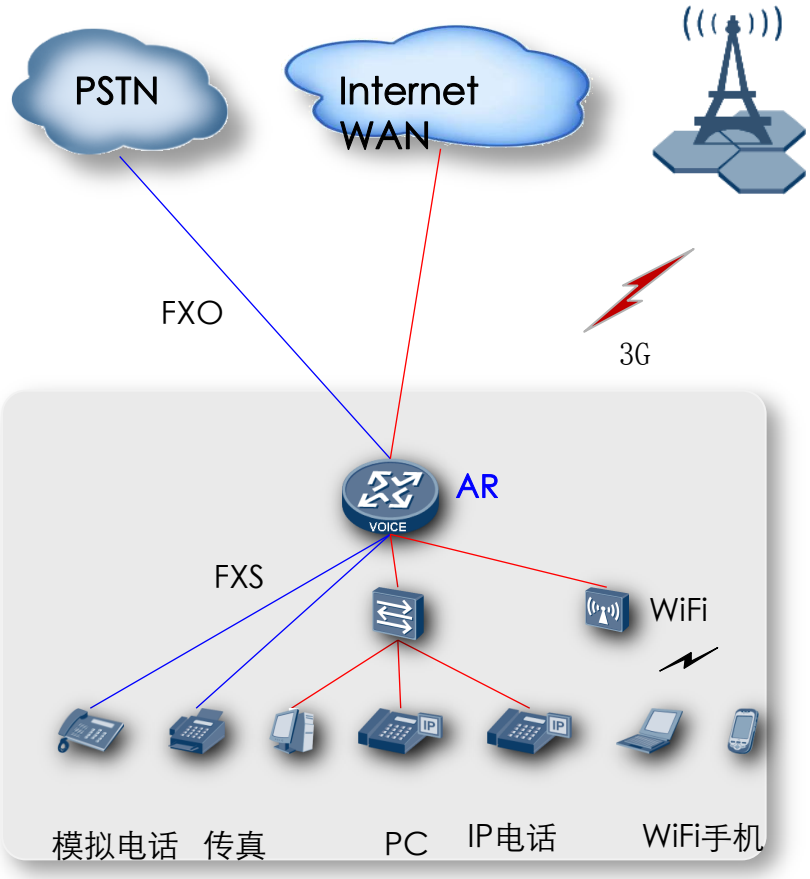
在园区出口部署AR 系列路由器作为IP PBX，通过E1将原有TDM PBX接入到AR,保护原有投资和业务。

在AR路由器上配置E1或者FXO接口板，连接到本地PSTN网络

由AR 管理出局呼叫路由及园区内部通话路由。

与其它分支园区之间的长途通话通过内部IP网络互通，AR管理内部长途呼叫路由。

小型园区ALL in ONE接入方案

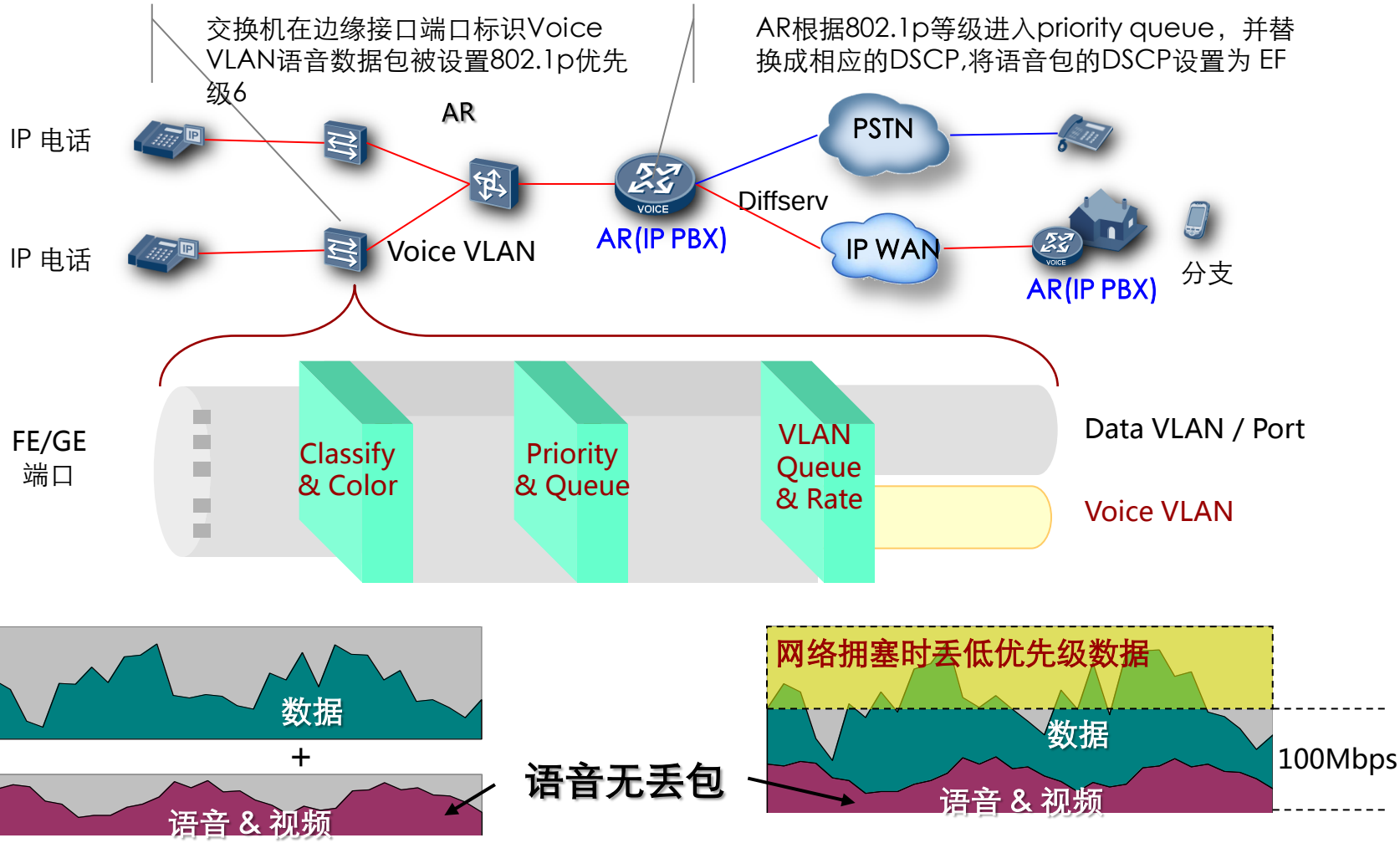


AR集成3G，语音、路由，完成小型园区分支的统一接入。

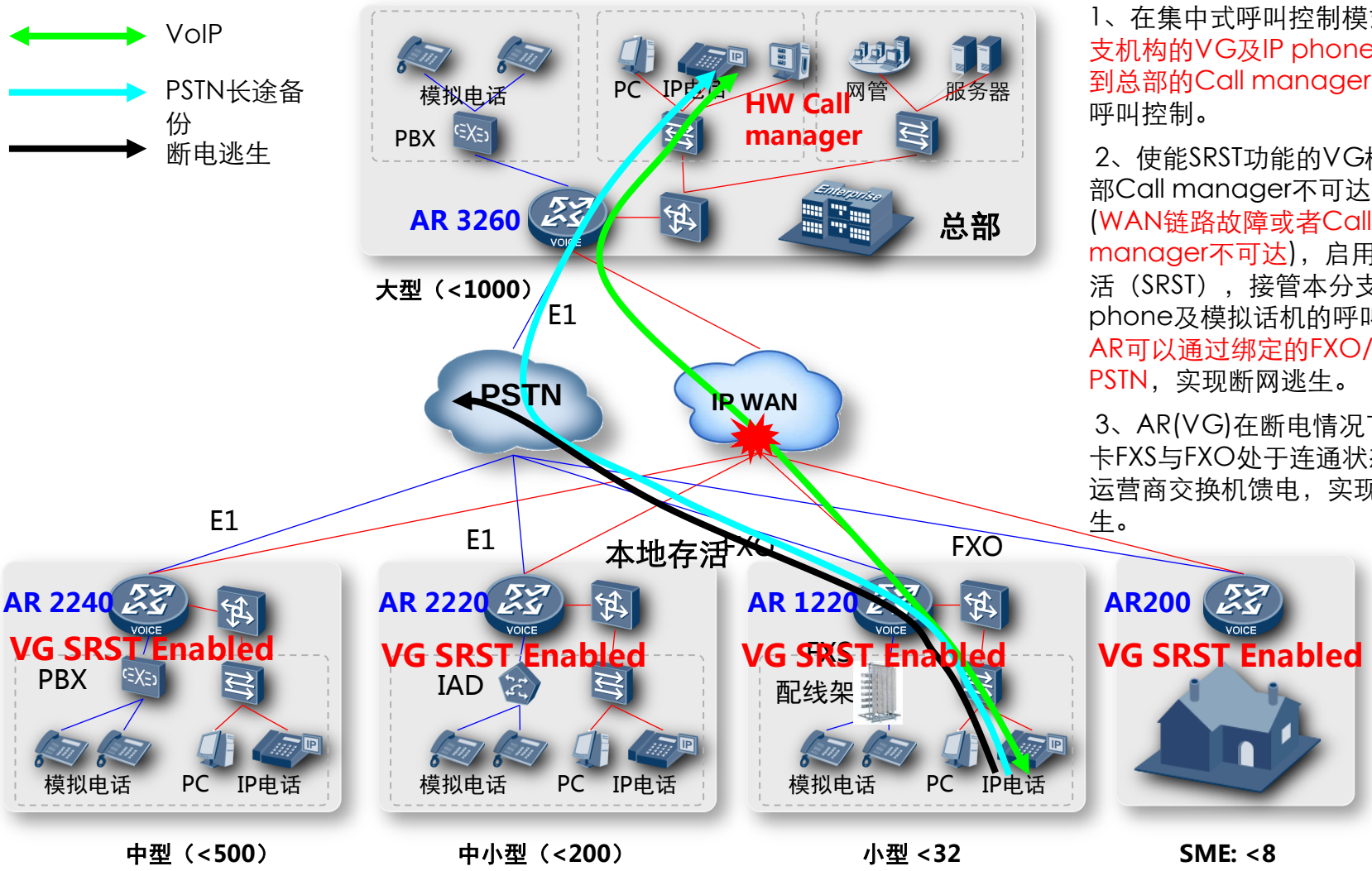
AR200/AR1220连接模拟和IP话机，实现语音功能。

WiFi 终端设备上安装 软件电话，提供移动语音

语音的QoS方案


交换机在边缘接口端口标识Voice VLAN语音数据包被设置802.1p优先级6
AR根据802.1p等级进入priority queue，并替换成相应的DSCP,将语音包的DSCP设置为 EF
IP 电话
IP 电话
AR
Voice VLAN
AR(IP PBX)
Diffserv
PSTN
IP WAN
AR(IP PBX)
分支
FE/GE 端口
Classify & Color
Priority & Queue
VLAN Queue & Rate
Data VLAN / Port
Voice VLAN
数据
+
语音 & 视频
语音无丢包
网络拥塞时丢低优先级数据
数据
语音 & 视频
100Mbps

语音的可靠性方案



1、在集中式呼叫控制模式下，分支机构的VG及IP phone都注册到总部的Call manager，接受呼叫控制。

2、使能SRST功能的VG检测到总部Call manager不可达的情况(WAN链路故障或者Call manager不可达)，启用本地存活（SRST），接管本分支IP phone及模拟话机的呼叫处理，AR可以通过绑定的FXO/E1拨打PSTN，实现断网逃生。

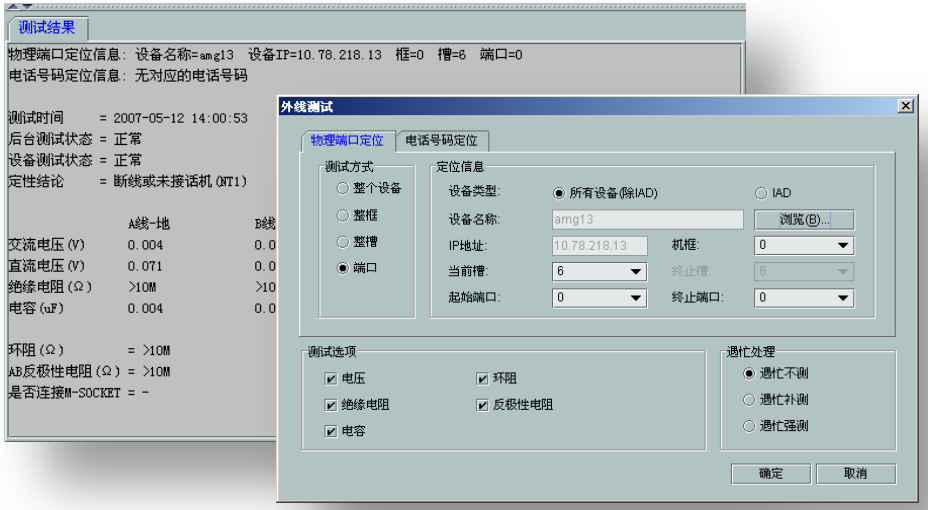
3、AR(VG)在断电情况下，共板卡FXS与FXO处于连通状态，接受运营商交换机馈电，实现断电逃生。

语音业务监控，实时排障

语音质量监控方案，主动管理你的语音网络

通过UDP Jitter报文模拟语音报文检测语音质量，支持定时检测、阈值告警等。

语音质量一目了然：时延、抖动、丢包，快速发现语音质量问题。



一键式内外线测试，快速故障定位

模拟用户环路、模拟用户板等各项性能和指标（如线间电容、电阻、振铃、馈电、拨号音等）测试，由此判断是否出现断线、短路等故障，为用户语音线路维护提供参考。

批量放号，简化运维

批量号码发放，全面提升语音放号效率

号码资源查询、统计管理。

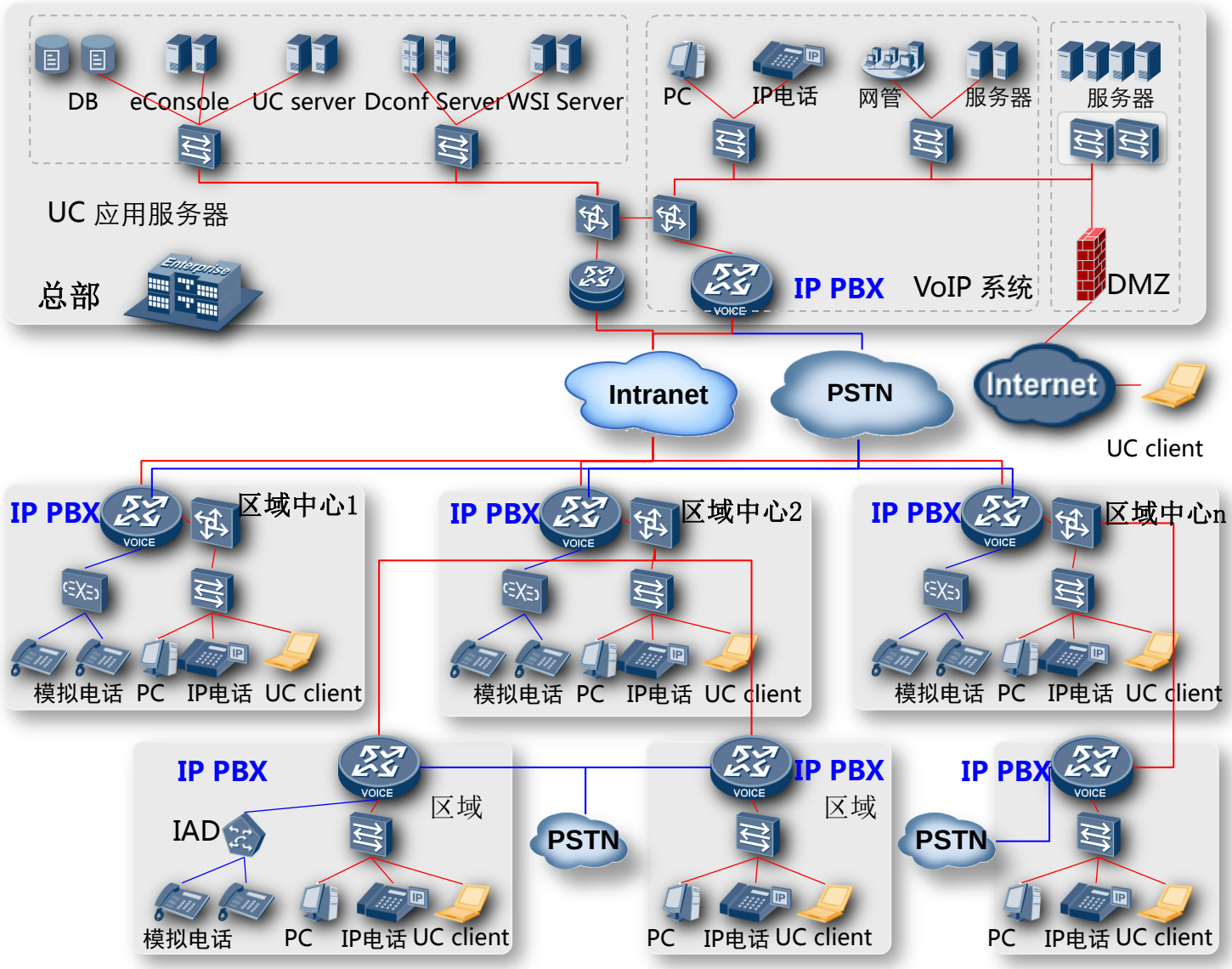
为SIP用户、POTS用户分配号码。

序列号码批量管理，全面提升语音放号效率。

零星无规律号码批量配置：采用Excel导入等各种方式。

Page 410

园区网语音及UC通信架构



总部：部署大容量 IP PBX及UC系统，会议服务器，用于总部用户接入，统一通信服务和会议业务，对外通过E1/SIP Trunk与本地运营商互通，并且为各区域中心的IP PBX及下级IP PBX提供呼叫路由。

各大区域中心：部署IP PBX为区域中心用户提供VoIP业务，对外通过E1/SIP Trunk与本地运营商互通。本区域中心的IP PBX为该区域下各个代表处间语音互通提供二级呼叫路由。

海外各办事处：部署IP PBX，负责办事处语音接入，并通过FXO/E1实现本地PSTN落地

统一消息系统：语音留言和传真信箱服务

留言

语音邮件:

- 支持无条件、无应答、遇忙留言

传真邮件:

- 一人一号传真邮箱
- 统一接入码传真邮箱

提醒

- 留言灯(MWI)
- 短信提醒
- Email提醒
- 电话语音提醒

获取

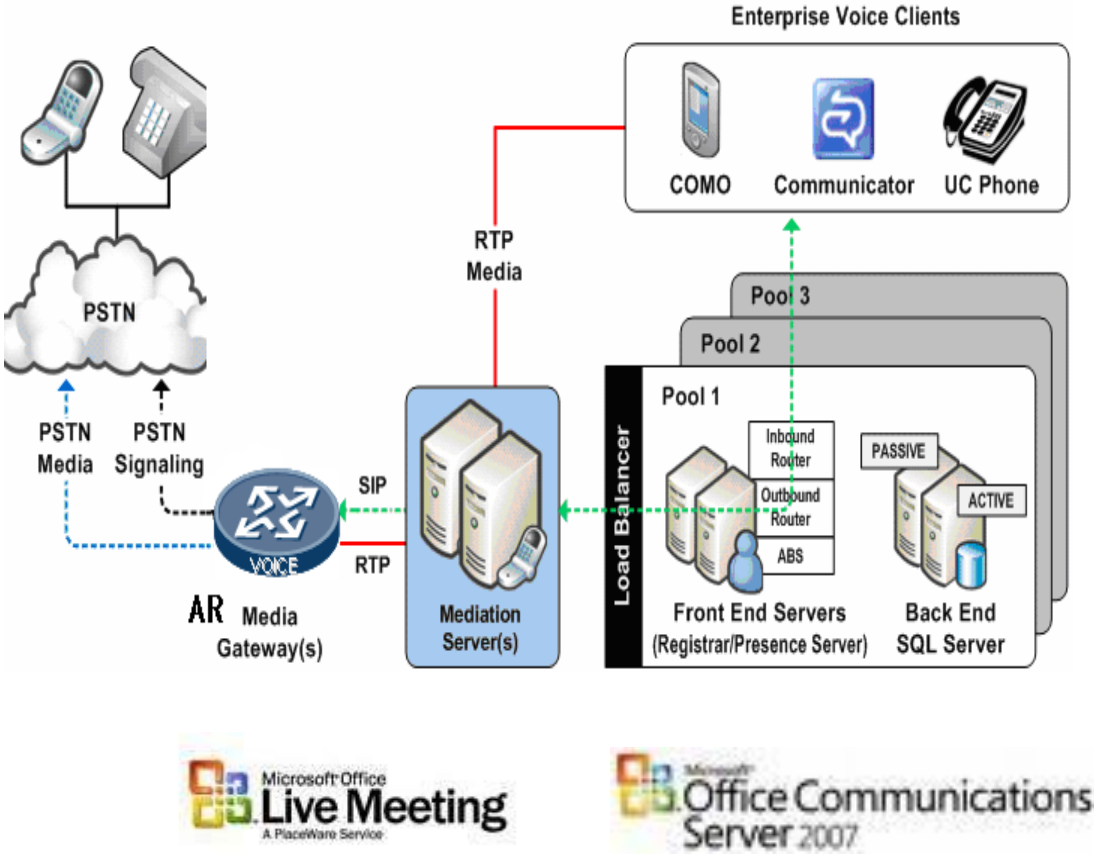
语音邮件:

- 支持话提取
- 支持Email接收

传真邮件:

- 支持传真机提取
- 支持Email接收

统一通信:微软系统集成AR



AR通过SIP trunking over TLS 和微软OCS、Exchange服务相连。为用户提供:一个号码能与多个终端进行绑定、语音通话、视频通话、视频会议、状态呈现、统一消息、协同

子目录

4 园区网业务解决方案

园区视频监控解决方案概述

存储系统

频图像的保存 – 如IP SAN设备

前端系统

视频信号的采集 – 如模拟摄像机、IP摄像机、视频编码器

承载网络

频图像的传输 – 如交换机、WLAN、PON设备

管理平台

监控系统的管理 – 包括硬件服务器及管理软件等

监控中心

频图像的显示 – 如大屏幕、控制台等

园区视频监控系统是园区安全防范系统的重要组成部分，它是一种防范能力较强的综合系统，主要应用在两个方面：

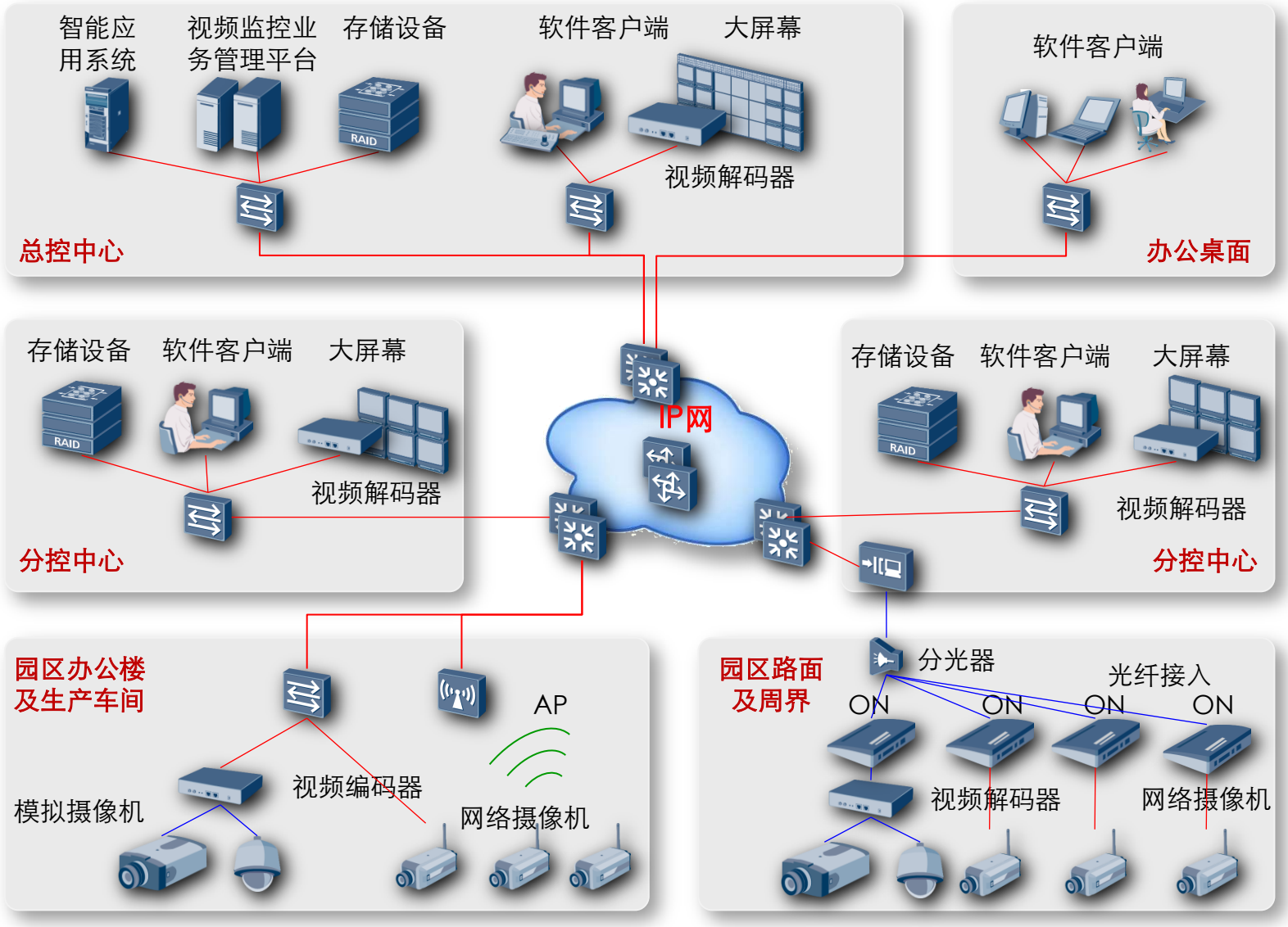
1、安防：视频监控作为一种技防手段，为园区的内部安防工作提供重要保障。

2、辅助管理：在某些行业，为加强管理，将视频监控作为辅助管理手段，如制造型企业对于生产线的可视化管理，学校进行远程监考等。

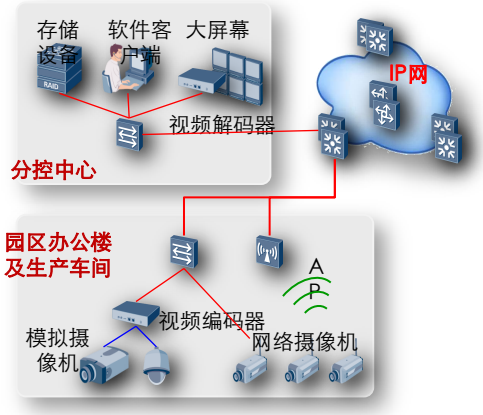
包含五大部件：前端系统、存储、承载网络、监控中心及管理平台

我们重点关注承载网络部分的方案设计

园区视频监控解决方案拓扑图



园区视频监控解决方案功能



图像监控
- 单画面
- 多画面
- PTZ控制
- 画面轮循
- 电视墙

存储回放
- 图像存储
- 本地抓拍
- 图像检索
- 智能标记

个性功能
- 图像抓拍
- 图像识别
- 电子地图
- 行为识别

报警联动
- 报警输入
- 控制输出
- 移动侦测
- 信息存储
- 呼叫前转

管理功能
- 用户管理
- 权限管理
- 设备管理
- 日志管理

视频监控承载网络设计原则

视频监控承载网络在整个视频监控系统中很简单，可以参考园区网的原则分为核心、汇聚和接入层。

每路视频图像在高清编码格式（1080P）下至少需要6-8M的带宽，且是连续的大带宽传输，对于带宽和实时性有一定的要求，因此对于视频监控承载网络建设总的原则是采用单独的接入交换机和汇聚交换机来承载视频监控业务，通过园区的核心交换机实现互通。

前端设备接入网络设计原则：

1、对于室内部署的视频监控前端设备主要采用交换机接入，根据前端设备数量和点位分布情况配置接入交换机，可采用S2700/3700。在无法布线的环境下可以采用WLAN方式接入。

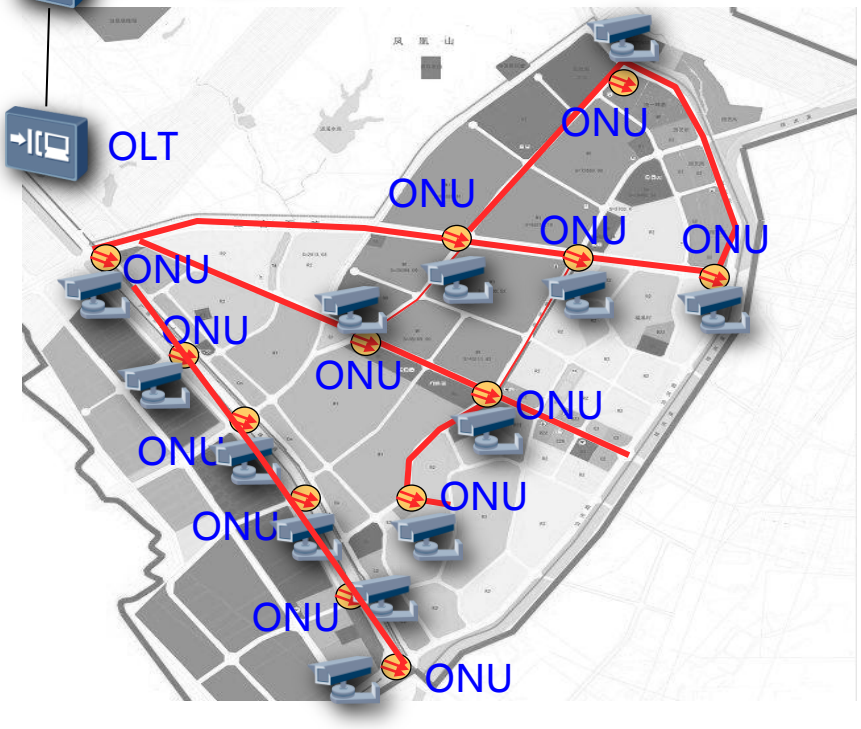
2、对于室外部署的视频监控前端设备可灵活采用交换机、PON和WLAN设备接入。需要根据视频监控前端设备的实际部署情况进行室外接入网络的设计。

存储和管理平台设备接入网络设计原则：

存储设备和管理平台所使用的服务器一般会集中部署在监控中心机房，且都是千兆网口，建议采用S5700做接入。

园区路面与周界监控网络xPON接入方案

监控中心



场景：

园区路面与周界的监控点采用xPON方案接入，沿园区主干道铺设光纤，在需要部署视频监控点的地方，用ONU接入IP摄像机或视频编码器。

方案特点：

高效接入网络：园区路面与周界的监控点分布广，并且呈不规则分布，采用PON的多级分光以高效的光纤资源利用率实现接入网络的广覆盖。

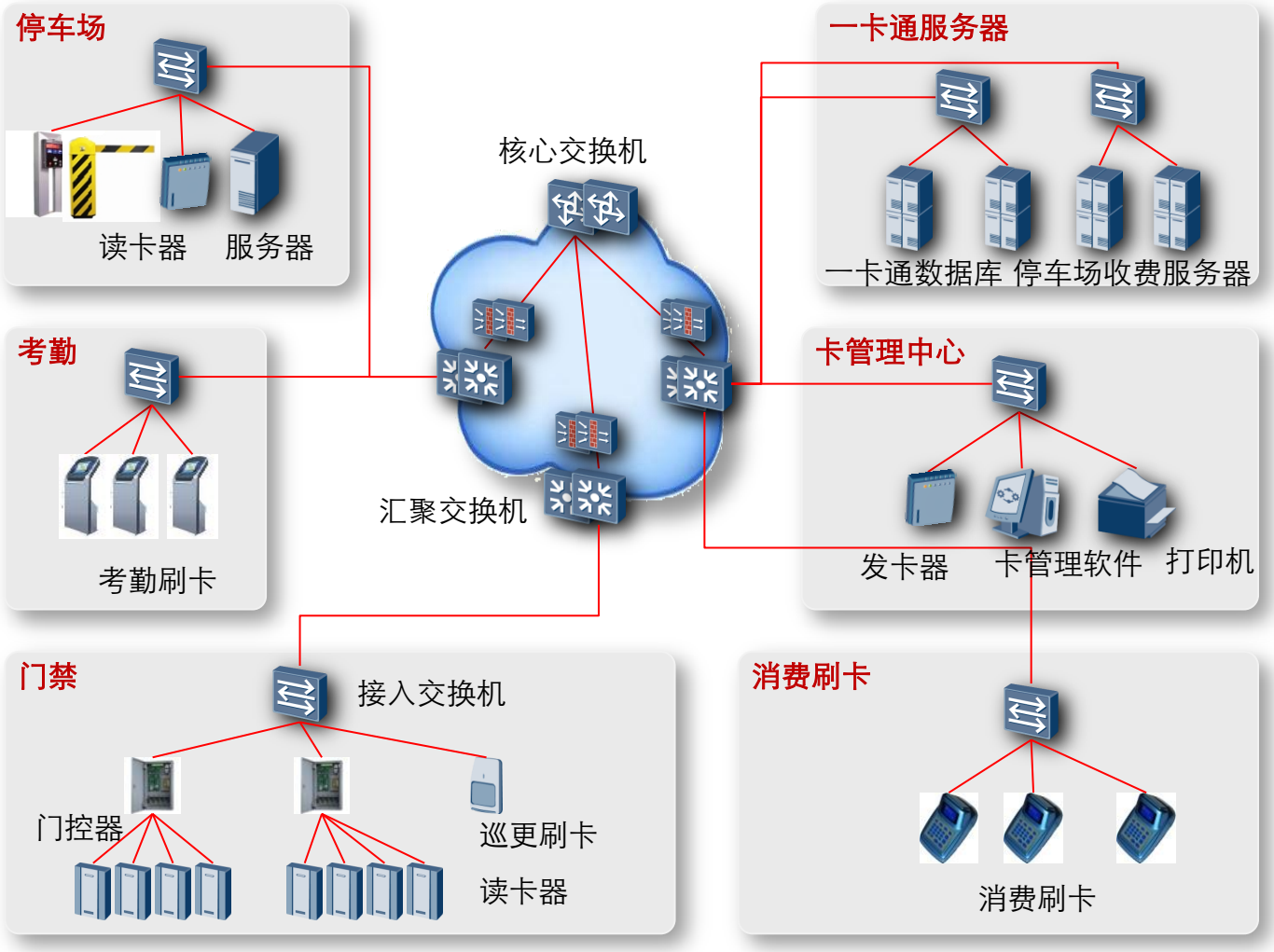
高可靠性：无源分光无器件无需供电和维护，不易受外界环境干扰，故障率低。

扩容方便：在视频监控点需要新增的时候方便扩容，无需重新部署光纤。

子目录

4 园区网业务解决方案

一卡通系统方案(门禁 停车场 消费巡更 考勤等)



一卡通系统是园区运行基础之一，需要建立数据备份机制，保障数据

安全卡业务（门禁、停车场、消费、巡更、考勤）系统构成一个相对独立的子系统（子网）

接入交换机供卡业务终端的接入，设备层汇聚。

卡业务的发卡数据、消费记录、考勤记录的数据集中在服务器机房的后台数据库系统（服务器）中

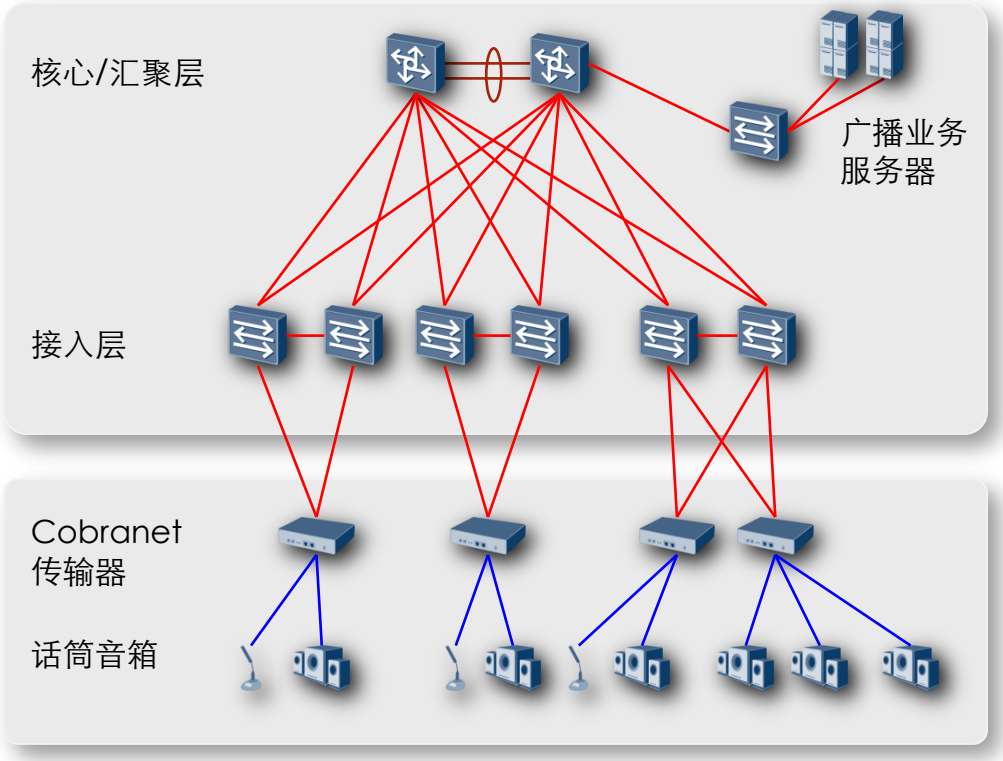
整个卡业务子网用防火墙保证网络的安全性、隔离性和受控互访性

子目录

4 园区网业务解决方案

广播承载网络概述

广播系统的应用



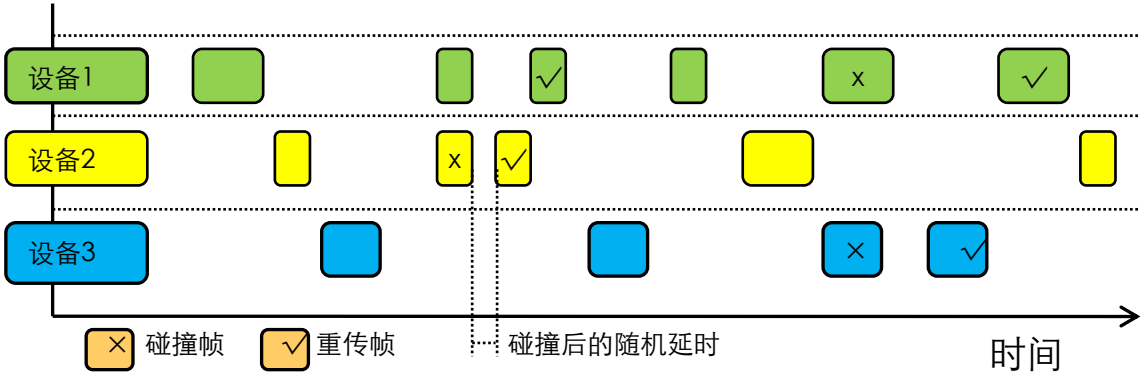
广播系统在机场、铁路、地铁站台、演艺场、会议中心、学校、大学、主题公园、议会、法庭、公司会议室、培训机构、运动场馆等场所应用广泛。

Cobranet等技术的出现，使得广播音频通过以太网承载，简化部署，增强可靠性,数据和音频承载互不影响，较传统的音频模拟传输有较大优势

广播网推荐独立组网，物理隔离，层次化架构，冗余链路，避免成环

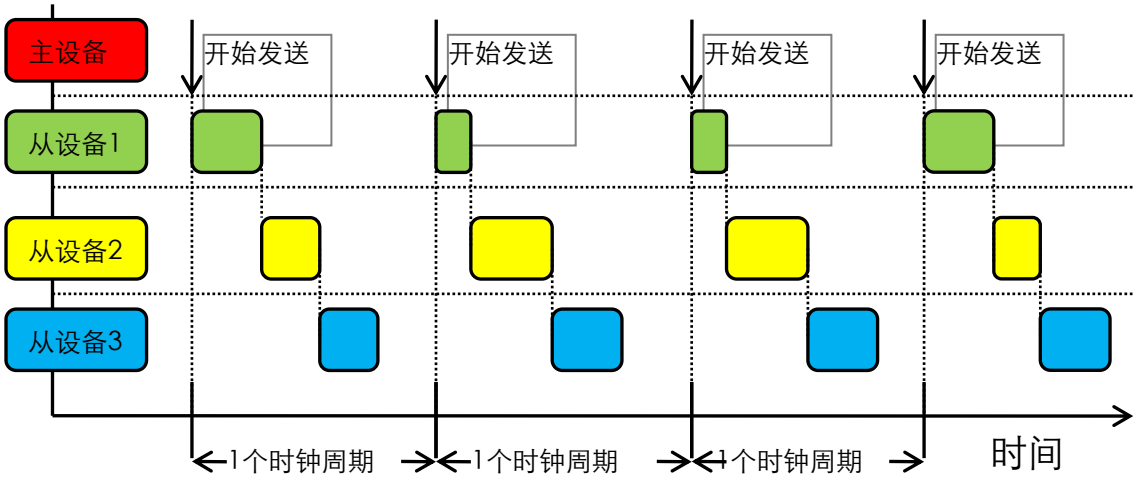
方案特点
音频单元、音频控制器间通过以太网CobraNet报文传输，设备布放更加灵活,CD级的高音质,支持网管控制

Cobranet和普通以太网的数据转发差异



普通以太网

发送前检测线路忙状态，空闲则发，发送后检测是否碰撞，碰撞后随机延时后再重发



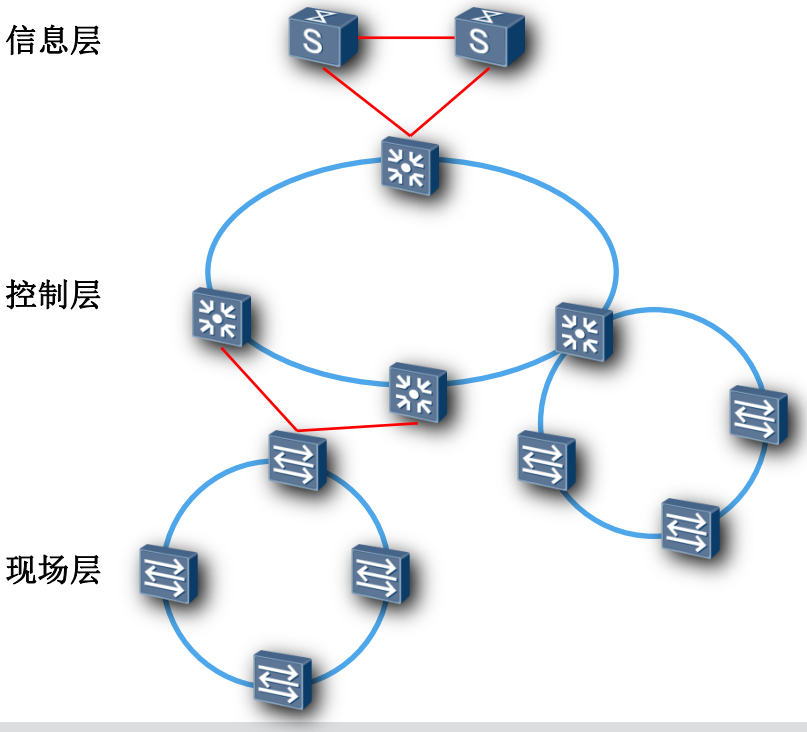
Cobranet

由网络中选出的主设备统一协调发送顺序，各个从设备听从号令依次发送

子目录

4 园区网业务解决方案

工业以太网解决方案



工业以太网在园区生产信息化系统的应用

园区网存在生产信息化系统。两化（工业化、信息化）深度融合，促进企业对生产信息化系统进行改造。生产信息化系统主要包括：生产自动化控制系统、生产管理系统、生产环境安全数据监测系统、生产环境视频监控系统等。

由于以太网的标准化、开放性和成本低等优势，工业以太网技术正在快速地进入生产信息化系统应用场合，工业以太网成为生产信息化的基础网络，帮助用户获得更加开放集成的生产信息化整体解决方案。

工业以太网涉及的产品主要是工业交换机、工业路由器、工业WLAN等，应用最多的是工业交换机。

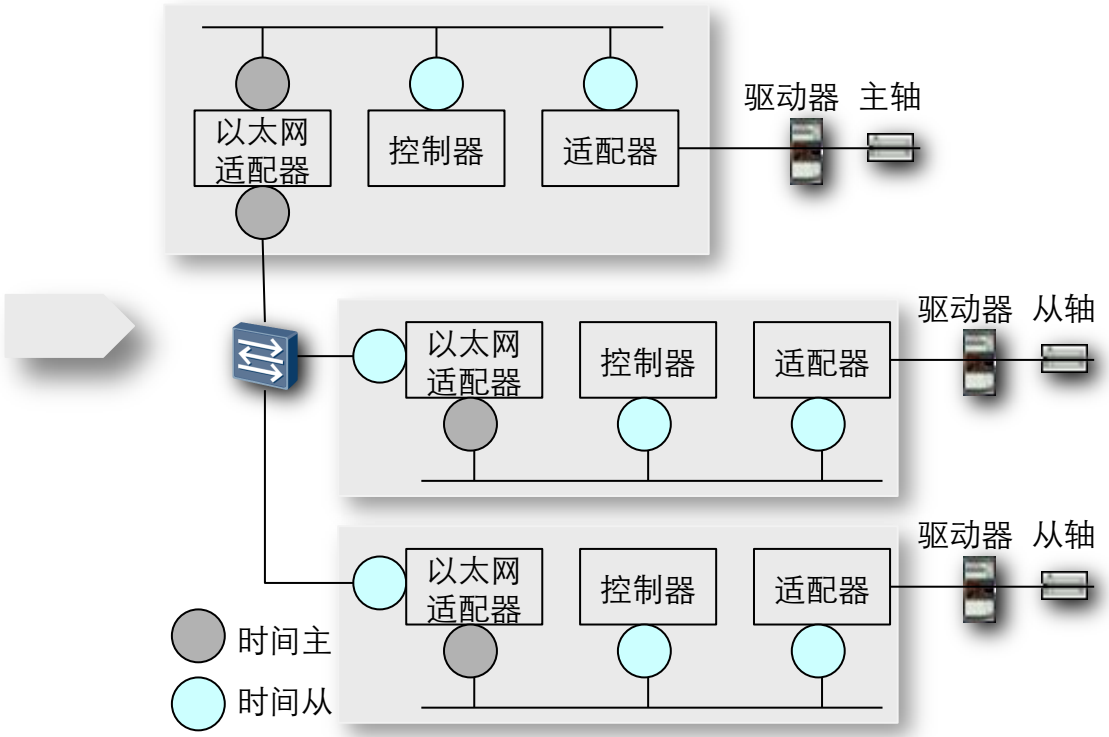
方案特点：

在工业交换机的组网方案中一般可分为信息层，控制层和现场层，越往下层越接近工业现场，对环境适应能力和实时性要求越高，在组网方案重点关注：

环网架构提高拓扑可靠性，提供极短的网络故障恢复时间（采用私有环网协议）。

高精度网络对时协议（IEEE1588v2）

1588v2协议在工业自动化控制系统的应用



现代化的工业生产自动化控制系统要求高速、高精度和灵活性，要求不同生产线之间时间精确同步。

右图的基本控制模型在工业自动化行业应用广泛， 在分布式控制系统中使用了IEEE1588v2协议，通过运动控制器、驱动器相连，并通过主轴和从轴之间的时间同步来达到精确控制不同运动单元的操作部件。

目录

Page 428

香港交易所 CCTV 网络

- **项目背景**
  - 香港交易所是世界排名第四的股票交易中心。此次项目中，香港交易所需要建立一个数据中心的CCTV（闭路电视）网络。考虑到股票交易的特殊性，项目对网络设备的稳定性有着非常严格的要求。

- **解决方案**
  - 华为提供端到端的CCTV网络设备，包括核心交换机S9300，汇聚交换机S5700和PoE接入交换机S3700;
  - 核心层，部署S9300交换机，采用关键部件冗余设计和CSS堆叠设计；汇聚层，部署S5700交换机采用了双归链路设计；接入层，部署S3700 PoE交换机，接入摄像头并为其供电，同时也为将来的网络扩展保留20%的端口。

- **客户收益**
  - 与honeywell公司（监控设备制造商）的监控设备良好的互通性；
  - 高可靠性和稳定性，确保业务永续;
  - 弹性网络架构，能有效地支撑未来的业务扩展;
  - 高安全性，可满足CCTV业务的安全要求;
  - 华为公司为客户提供专业的POC测试以验证方案的可行性，帮助客户降低风险。

中国农业银行北京办公中心融合园区网

- **项目背景**
  - 中国农业银行是中国4大银行之一，全球第14大银行。国内拥有24064个网点，1171家海外代理行。
  - 农业银行北京办公中心规模很大，包括公主坟、金玉和东单等办公点，需要支持数千人同时办公。
  - 北京办公中心业务复杂，对网络安全性、可靠性要求很高。
- **解决方案**
  - 采用57台S9300为中国农业银行北京办公中心构建高质量的园区网络。
  - 核心层，采用关键部件冗余设计和CSS堆叠设计；汇聚层，采用了双归链路设计，保证了网络的高可靠性。
  - 部署BFD，E-OAM等故障检测技术，实现端到端50ms业务倒换
- **客户收益**
  - 保护现网投资，和现网接入层设备良好对接。
  - 网络性能和防攻击能力得到大幅提升。
  - 高可靠性和高稳定性，确保业务永续。
  - 实现了多业务承载，简化了网络结构和业务部署。

中国农业银行
AGRICULTURAL BANK OF CHINA

中国东方航空昆明新机场项目

- **项目背景**
  - 随着云南“桥头堡”计划，昆明新机场为中国东方航空云南分公司发展获得了一个新的历史发展机遇。新机场的网络设计要求无线网络信号需要完全覆盖整个工作区域，用来提高移动办公的灵活性；同时，要求考虑互联网和广域网的负载均衡和高安全性。

- **解决方案**
  - 部署S9300系列交换机，并采用SPU板，作为核心交换设备。
  - 在核心层和汇聚层使用的CSS堆叠技术，用来加强网络管理。
  - 在网络边缘部署防火墙，IPS和SSL VPN。
  - 使用NAC解决方案，用来提高网络的安全性。

- **客户收益**
  - 任何时间任何地点都可以高速地访问局域网和无线局域网，提高了工作效率。
  - 冗余设计，提高了网络的可靠性并有效防止服务中断。

中國東方航空
CHINA EASTERN

Sochi冬季奥林匹克运动会信息网

- **项目背景**
  - Megafon是世界上最大的运营商之一，负责本届运动会交付ICT解决方案，对本届奥委会负责。此次，华为公司与Megafon合作，为本届盛会端到端交付一个信息网络。项目要求网络具有容量大，时延小，高可靠，良好的扩展性和快速业务开通能力。
- **解决方案**
  - 每个园区和分支的核心层和汇聚层部署 S9300，配置12 x 10GE线速转发单板
  - 在园区和分支的接入层部署400多台S5700/3700/2700系列交换机。
  - 核心、汇聚、接入三层环状组网，环两端接入不同汇聚点。
- **客户收益**
  - 交换机高性能配置保证整网大容量且无阻塞转发。
  - 环形组网有效解决单点故障。
  - 可平滑升级成为3G IP骨干网，有效保护了现有投资

法国政府网络（SIEA）

- **项目背景**
  - 法国政府的公共管理项目，需要覆盖100多个城镇，每年为90,000左右市民提供服务。该项目覆盖区域大并且交付周期较短，需要华为公司提供低成本的方案并且高效的交付。
- **解决方案**
  - 采用交换机长距离覆盖设计，骨干环10G，接入环1G。
  - 按照华为万兆园区方案，在接入层部署S5300/S5700，核心层部署S9300。
  - 配置高密度10GE光端口，保证长距离无阻塞转发。
- **客户收益**
  - 与Cisco和Nortel网络设备的完美对接互通。
  - 10GE光端口保证了业务当前及长期发展需要，符合客户的长远成本利益。
  - 短时间，高质量交付，充分满足客户高效的需求。

巴西Ceara洲电子政务项目

- **项目背景**
  - 为满足电子政府要求，Ceara（塞阿拉）洲根据IT建设部门ETICE的规划，为下辖的15个城市/县、各部委和委员会统一建设新一代电子政务网络，提供语音、数据和视频业务。
  - 由于现网接入设备众多，运维困难，华为设备需要与现网的手机等通信终端兼容。
- **解决方案**
  - 采用华为万兆园区方案，在接入层部署S5300/S5700，汇聚层部署S9300。
  - 提供了一个集成的园区网方案，兼容原有网络终端，充分利旧。
- **客户收益**
  - 华为PoE交换机是与第三方的IP电话兼容，保护客户投资。
  - 华为交换机大容量，高密度，绿色环保，降低客户运维成本。
  - 视频，语音和数据业务在以太承载网上可靠传输，确保了政府的高效率。

南非Stellenbosch 大学网络

- **项目背景**
  - Stellenbosch大学被确认为在南非的四个顶尖的研究型大学之一。它成立于1866年，拥有约150年的历史。大学坐落在斯泰伦博斯中心地带。随着学校的发展，当前的网络不能满足学校日益增长的带宽要求，需要对现有网络进行升级改造。
- **解决方案**
  - 部署S9312核心交换机，替换旧的设备。
  - 配置40*10GE接口卡，以实现高的接口转发能力。
  - 使用CSS堆叠技术来扩大核心交换机容量，同时增强了网络的可靠性。
- **客户收益**
  - 在单机柜中取得最高的端口密度。
  - 增强网络质量监控和简化运维工作。
  - 节省电信机房空间，采用高度的设备成本降低30%用电量。

UNIVERSITEIT STELLENBOSCH UNIVERSITY

葡萄牙ZON NDD&L2-MEF网络

- **项目背景**
  - ZON是葡萄牙最大的有线电视和电信运营商，拥有超过160万签约用户和300多万家庭用户。同时，ZON也拥有该国最大的基于光纤的网络。
    ZON需要建立二层MEF的网络，具有高可靠性，高可扩展性，低成本和快速恢复能力。整个网络可以为业务提供强大的QoS能力。
- **解决方案**
  - 华为整合DWDM产品和交换机产品建设该网络：在汇聚节点部署S9312，在主节点部署S9306和接入节点部署S5300 。
  - 华为S9300和S5300系列交换机可以提供丰富的QoS特性，能满足客户的服务质量的要求。
  - 部署U2000网管来管理DWDM产品和交换机产品。
  - 设备：S9300系列：50+ ，S5300系列：500+。
- **客户收益**
  - 华为公司提供的DWDM产品和交换机产品可以由华为U2000网管进行管理，为客户节省成本。
  - 华为专有的特性SEP（智能以太网协议）具有50ms的快速恢复能力，用来提高以太网环路网络的可靠性。
  - S9300与S5300具有丰富的QoS特性，可以满足客户很高的QoS要求。

中钢南非有限公司骨干网

- **项目背景**
  - 中钢南非有限公司成立于1996年11月，设计铬铁年产量为12万吨，销往日本，欧洲，中国，韩国，台湾等国家和地区。目前根据业务发展需要，把铬铁产量已计划提高到年产36万吨。与此同时，需要对目前网络进行改造，以满足不断增长的业务带宽要求。

- **解决方案**
  - 部署 S9300系列产品建立核心网络。
  - 部署 S5300系列产品作为接入交换机，方便接入和扩展。
  - 部署端到端的网络管理软件eSight。

- **客户收益**
  - 在单机柜中取得最高的端口密度。
  - 增强网络质量监控和简化运维工作。
  - 节省电信机房空间，采用高度的设备成本降低30%用电量。

Huawei Enterprise A Better Way