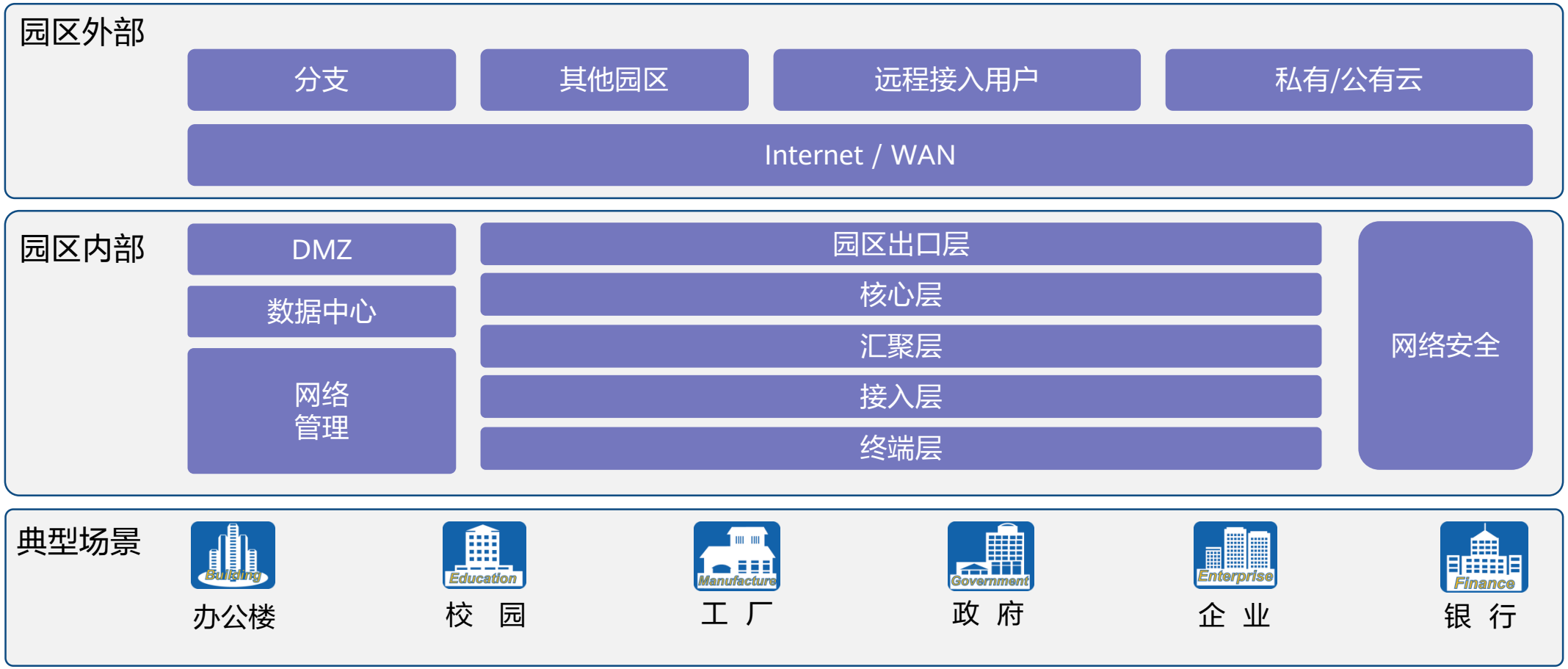
园区网典型组网架构及案例实践

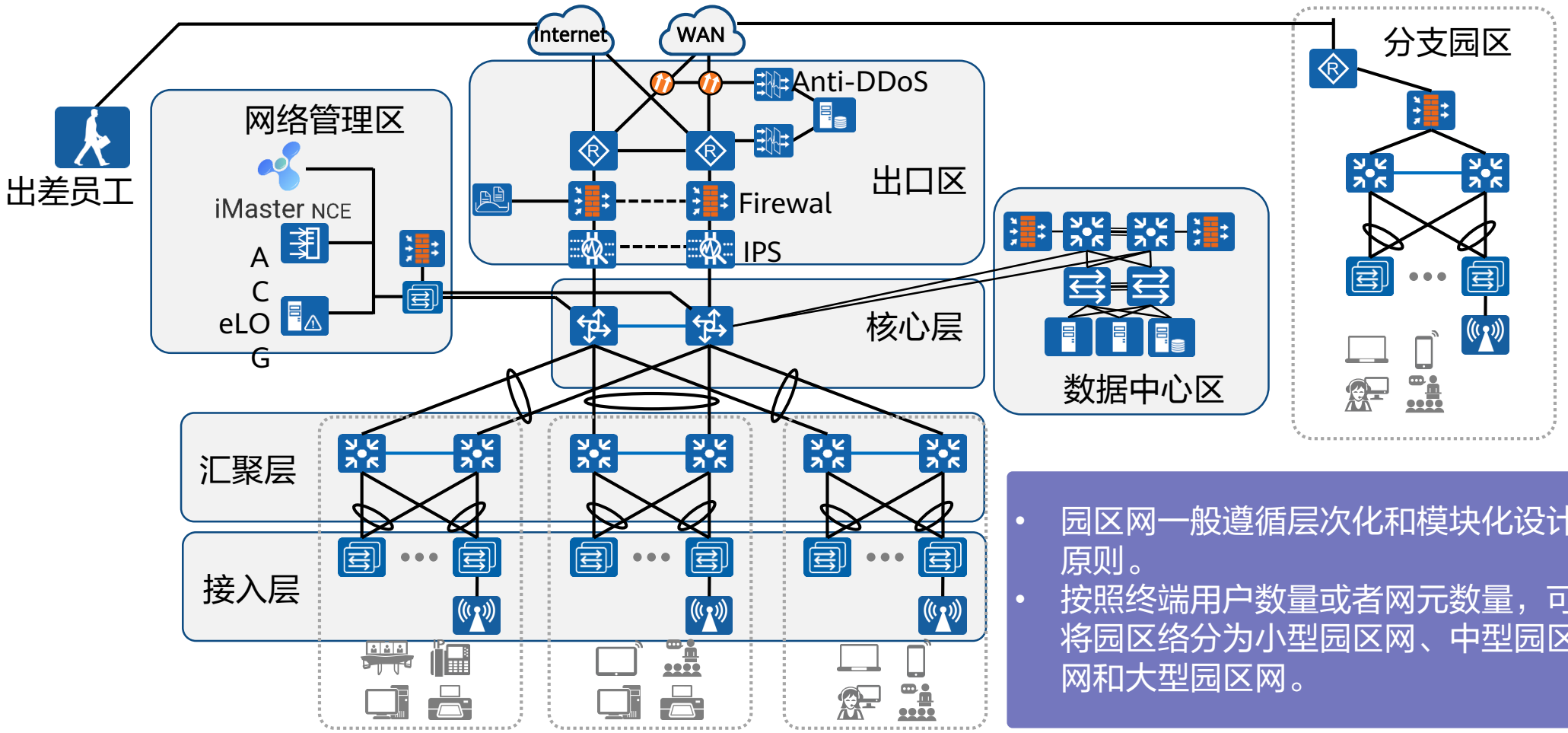
主讲人：施淼淼

目录

什么是园区网

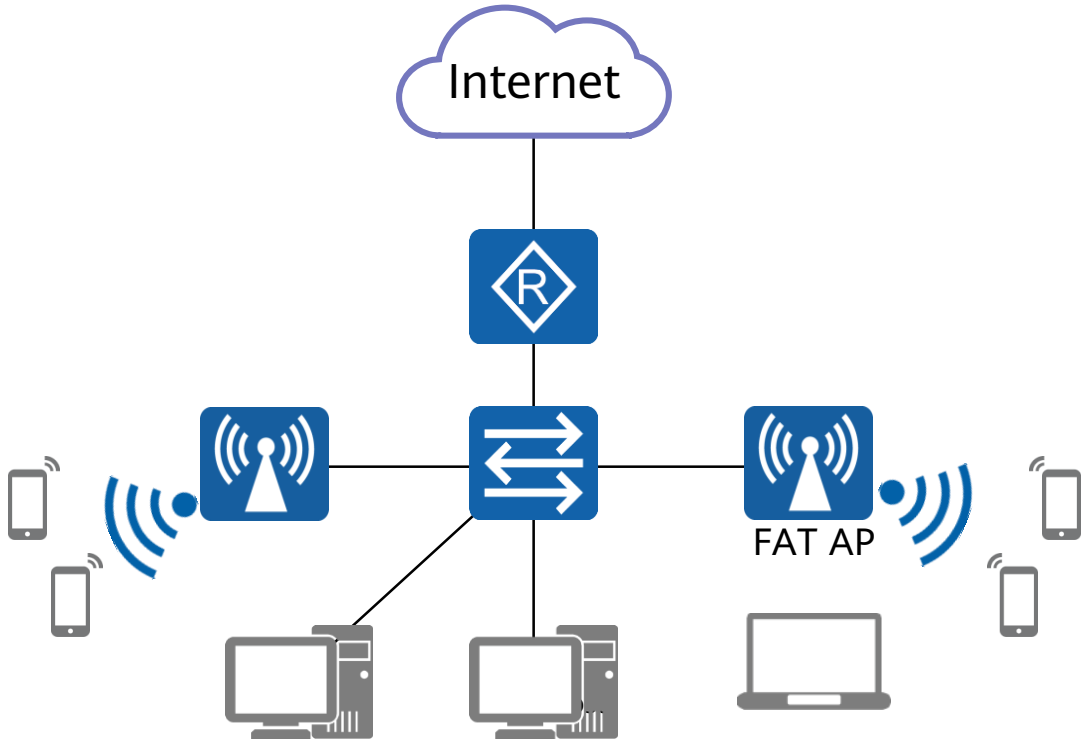


园区网络典型架构



- 园区网一般遵循层次化和模块化设计原则。
- 按照终端用户数量或者网元数量，可将园区络分为小型园区网、中型园区网和大型园区网。

小型园区网络典型架构

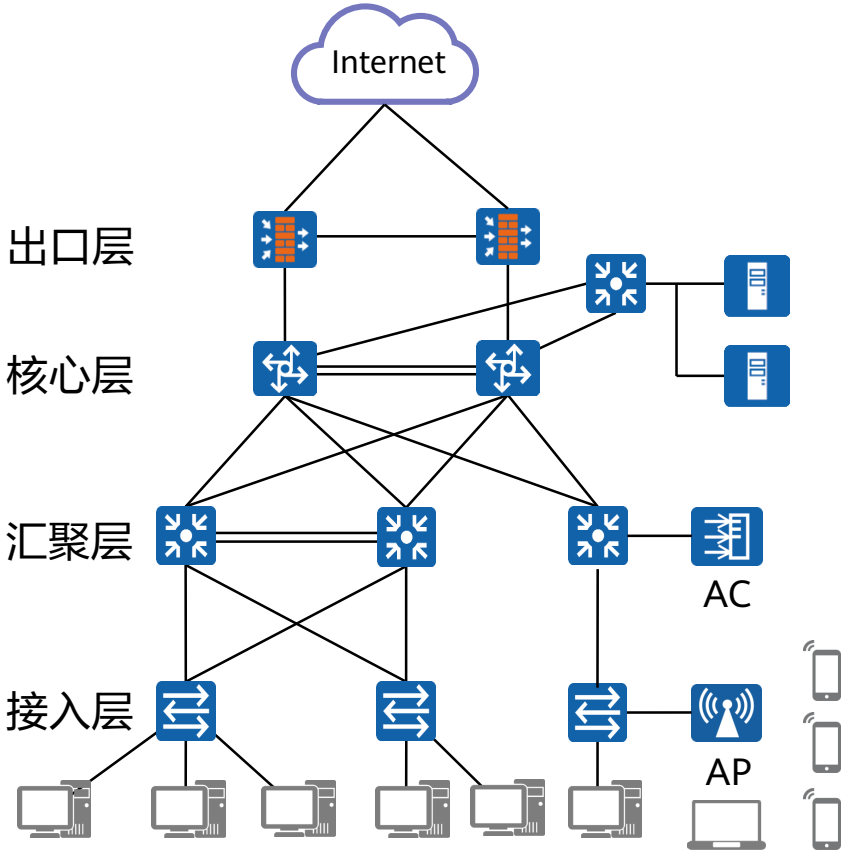


某连锁咖啡店网络拓扑

- 小型园区网络应用于接入用户数量较少的场景，一般支持几个至几十个用户。网络覆盖范围也仅限于一个地点，网络不分层次结构。网络建设的目的常常就是为了满足内部资源互访。
- 小型园区网络特点：
  - 用户数量较少
  - 仅单个地点
  - 网络无层次性
  - 网络需求简单

终端用户数（个）	<200
网元数量（个）	<25

中型园区网络典型架构

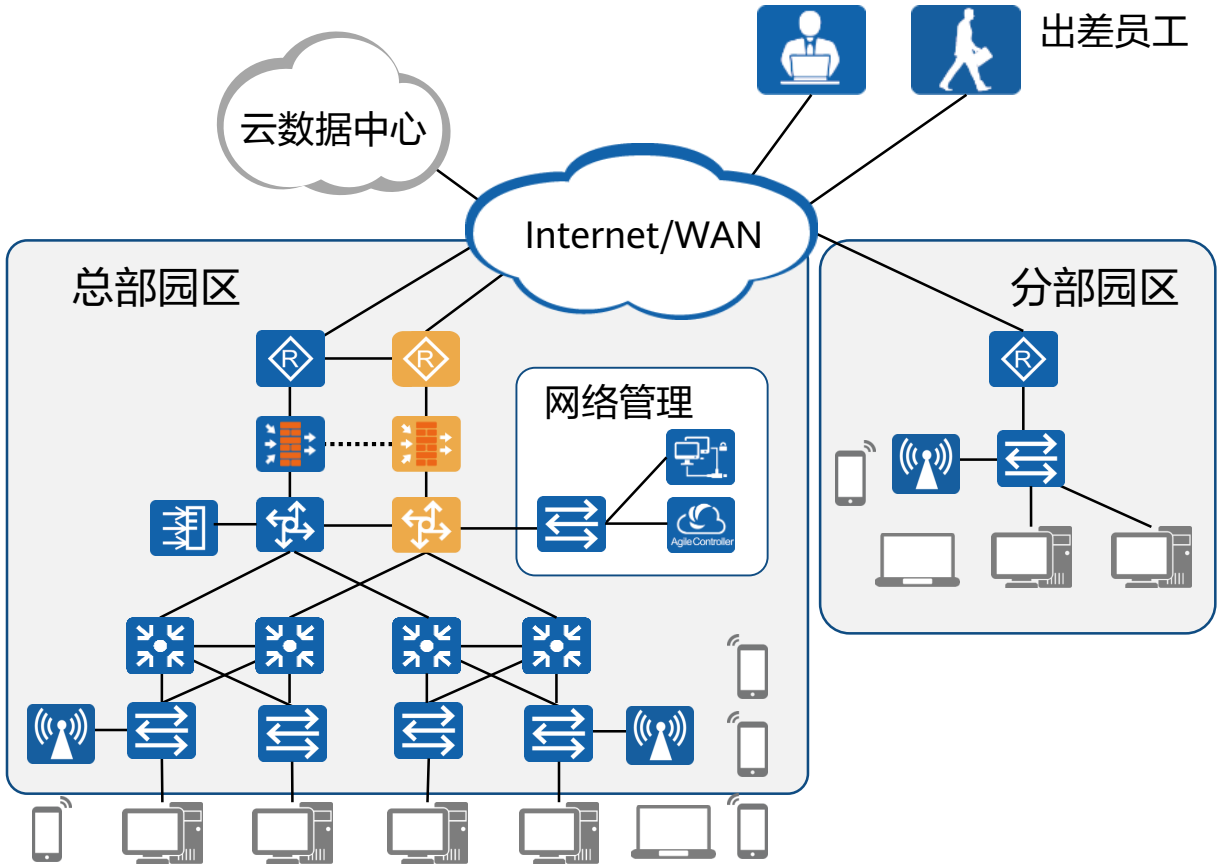


某外贸公司网络拓扑

- 中型园区网络能够支撑几百至上千用户的接入。
- 中型网络引入了按功能进行分区的理念，也就是模块化的设计思路，但功能模块相对较少。一般根据业务需要进行灵活分区。
- 中型园区网络特点：
  - 规模中等
  - 使用场合最多
  - 功能分区
  - 一般采用三层网络结构：核心、汇聚、接入

终端用户数（个）	200~2000
网元数量（个）	25~100

大型园区网络典型架构

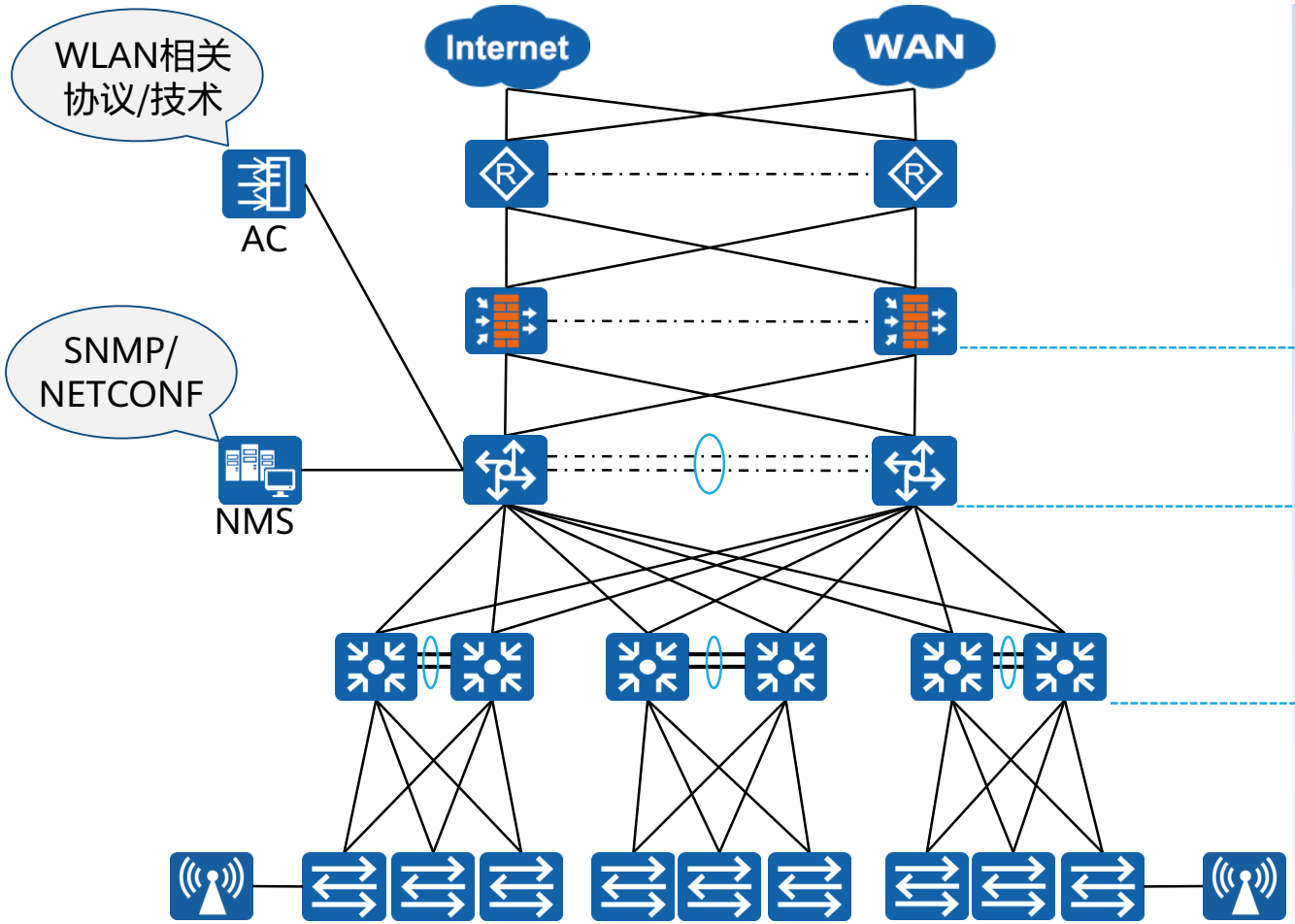


某大型企业网络拓扑

- 大型园区网络可能是覆盖多幢建筑的网络，也可能是通过WAN连接一个城市内的多个园区的网络。一般会提供接入服务，允许出差员工通过VPN等技术接入公司内部网络。
- 大型园区网络特点：
  - 覆盖范围广
  - 用户数量多
  - 网络需求复杂
  - 功能模块全
  - 网络层次丰富

终端用户数（个）	>2000
网元数量（个）	>100

园区网络主要协议/技术



常用协议/技术

NAT、OSPF、静态路由、PPPoE等	出口区
堆叠、OSPF、静态路由、ACL等	核心层
DHCP、堆叠、链路聚合、生成树、OSPF、静态路由等	汇聚层
VLAN、生成树、链路聚合、AAA等	接入层

目录

网络需求

- 某公司（规模为200人左右）因业务发展需要，准备搭建一张全新的园区网络，对网络需求如下：
  - 能够满足公司当前的业务需求
  - 网络拓扑简单，维护方便
  - 提供有线接入供员工办公使用，提供WiFi服务供访客使用
  - 做到简单的网络流量管理
  - 保证一定的安全性

园区网络项目生命周期

1 规划与设计

- 设备选型
- 物理拓扑
- 逻辑拓扑
- 使用技术与协议等

2 部署与实施

- 设备安装
- 单机调测
- 联调测试
- 割接并网等

3 网络运维

- 日常维护
- 软件与配置备份
- 集中式网管监控
- 软件升级等

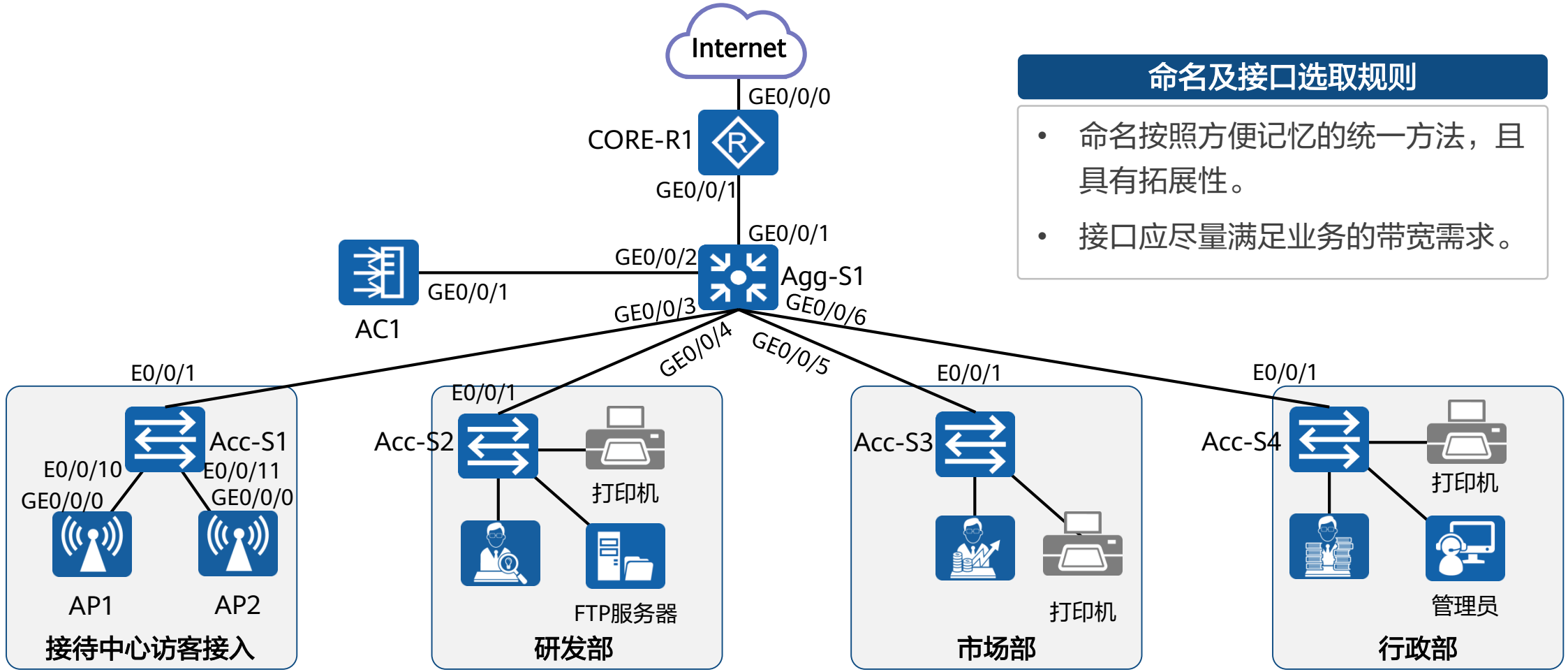
4 网络优化

- 提升网络的安全性
- 软件与配置备份
- 提升网络的用户体验等

小型园区网络设计

1.组网方案设计	2.网络设计	3.安全设计	4.运维管理设计
设备选型	基础业务设计	出口安全设计	基础网络管理
物理拓扑	WLAN设计	内网有线安全	智能运维
	二层环路避免设计	内网无线安全	
	网络可靠性设计		

组网方案设计



命名及接口选取规则

- 命名按照方便记忆的统一方法，且具有拓展性。
- 接口应尽量满足业务的带宽需求。

基础业务设计：VLAN设计

- VLAN编号建议连续分配，以保证VLAN资源合理利用。
- VLAN划分需要区分业务VLAN、 管理VLAN和互联VLAN。
- 最常用的划分方式是基于接口的方式。

业务VLAN设计

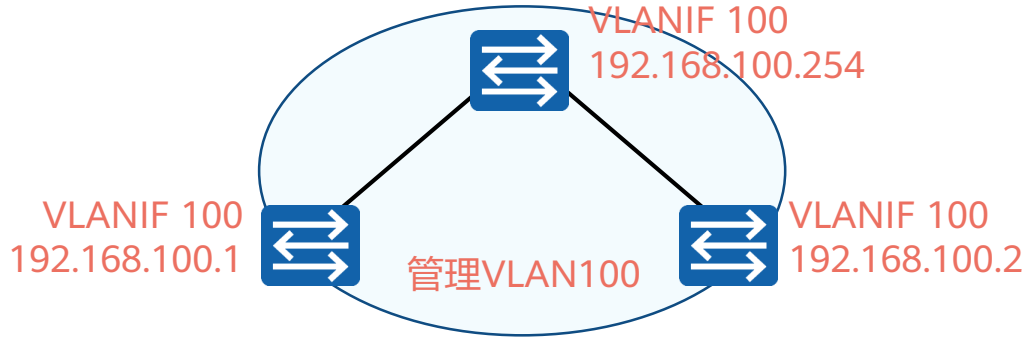
按地理区域划分VLAN

按逻辑区域划分VLAN

按人员结构划分VLAN

按业务类型划分VLAN

管理VLAN设计



通常，二层交换机使用VLANIF接口地址作为管理地址。建议所有属于同一二层网络的交换机使用同一管理VLAN， 管理IP地址处于同一网段。

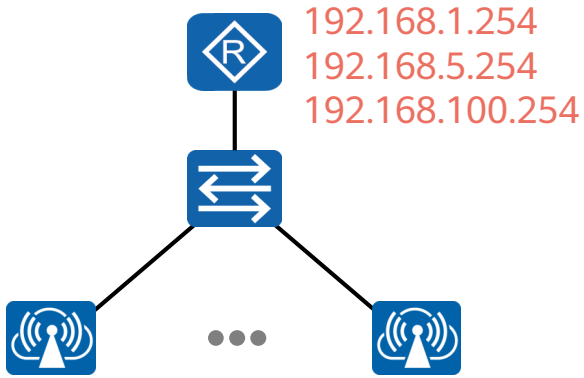
VLAN规划

- 预留二层设备的管理VLAN。
- 根据人员结构划分，分为访客VLAN，研发部VLAN，市场部VLAN，行政部VLAN。
- 考虑到三层交换机需要通过VLANIF与路由连通，所以需要预留互联VLAN。
- AP与AC之间建立CAPWAP隧道所需要的VLAN。

VLAN编号	VLAN描述
1	访客VLAN/WLAN的业务VLAN
2	研发部VLAN
3	市场部VLAN
4	行政部VLAN
100	二层设备的管理VLAN
101	WLAN的管理VLAN
102	Agg-S1与CORE-R1之间的互联VLAN

基础业务设计：IP地址设计

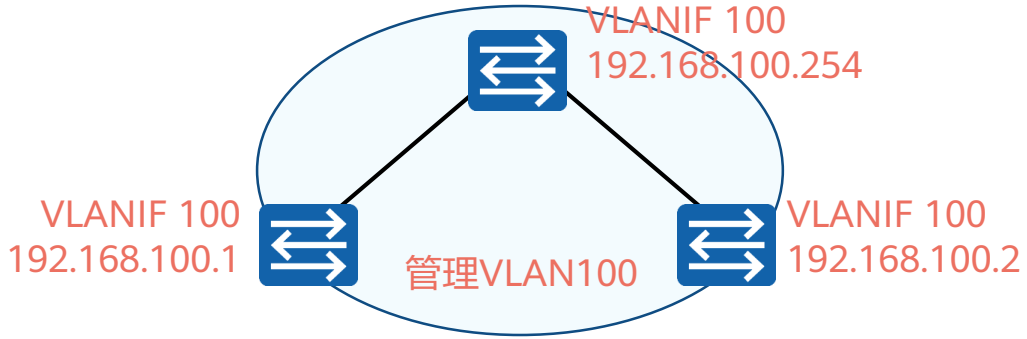
业务IP地址



业务IP地址是服务器、主机以及网关的IP地址。

- 网关IP地址推荐统一使用相同的末位数字，如.254。
- 各业务IP地址范围要清晰区分，每一类业务终端IP地址连续、可聚合。
- 建议使用掩码为24位的IP地址段。

管理IP地址



二层设备使用VLANIF地址作为管理IP地址，建议网关下的所有二层交换机使用同一网段。

网络设备互联IP地址

互联IP地址推荐使用30位掩码的IP地址，核心设备使用主机地址较小的IP地址。

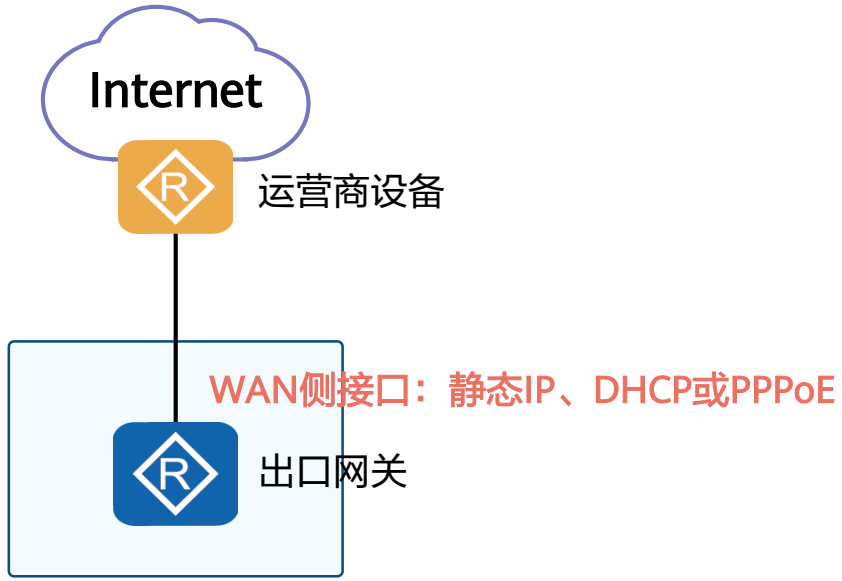
IP地址规划

- 综合考虑接入客户端个数并预留足够的IP地址，为每类业务规划网段及网关地址。
- 为管理IP划分网段。
- 为互联IP划分网段。

IP网段/掩码	网关地址	网段描述
192.168.1.0/24	192.168.1.254	无线接入访客所属网段，网关位于Agg-S1
192.168.2.0/24	192.168.2.254	研发部所属网段，网关位于Agg-S1
192.168.3.0/24	192.168.3.254	市场部所属网段，网关位于Agg-S1
192.168.4.0/24	192.168.4.254	行政部所属网段，网关位于Agg-S1
192.168.100.0/24	192.168.100.254	二层设备的管理网段，网关位于Agg-S1
192.168.101.0/24	N/A	WLAN的管理网段
192.168.102.0/30	N/A	Agg-S1与CORE-R1之间互联网段
1.1.1.1/32	N/A	CORE-R1上的Loopback接口地址，作为管理IP使用

基础业务设计：IP地址分配方式设计

出口网关

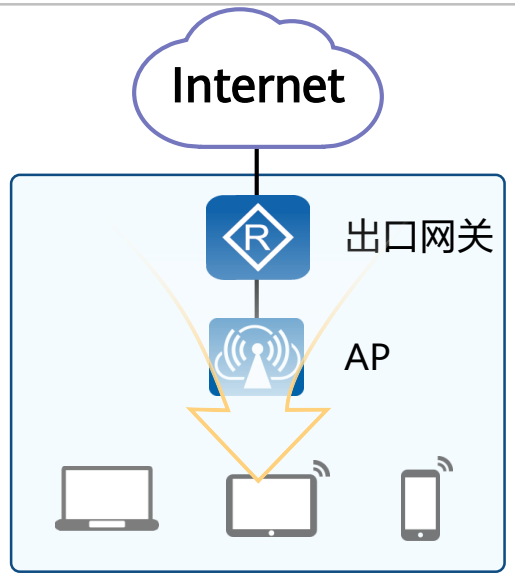


WAN侧接口的IP地址由运营商进行分配，可通过静态IP地址、 DHCP、 或者PPPoE方式分配，需与运营商沟通获取。

服务器、打印机等设备

服务器、特殊终端设备（打卡机、打印服务器、 IP视频监控设备等）建议采用静态IP地址。

终端用户



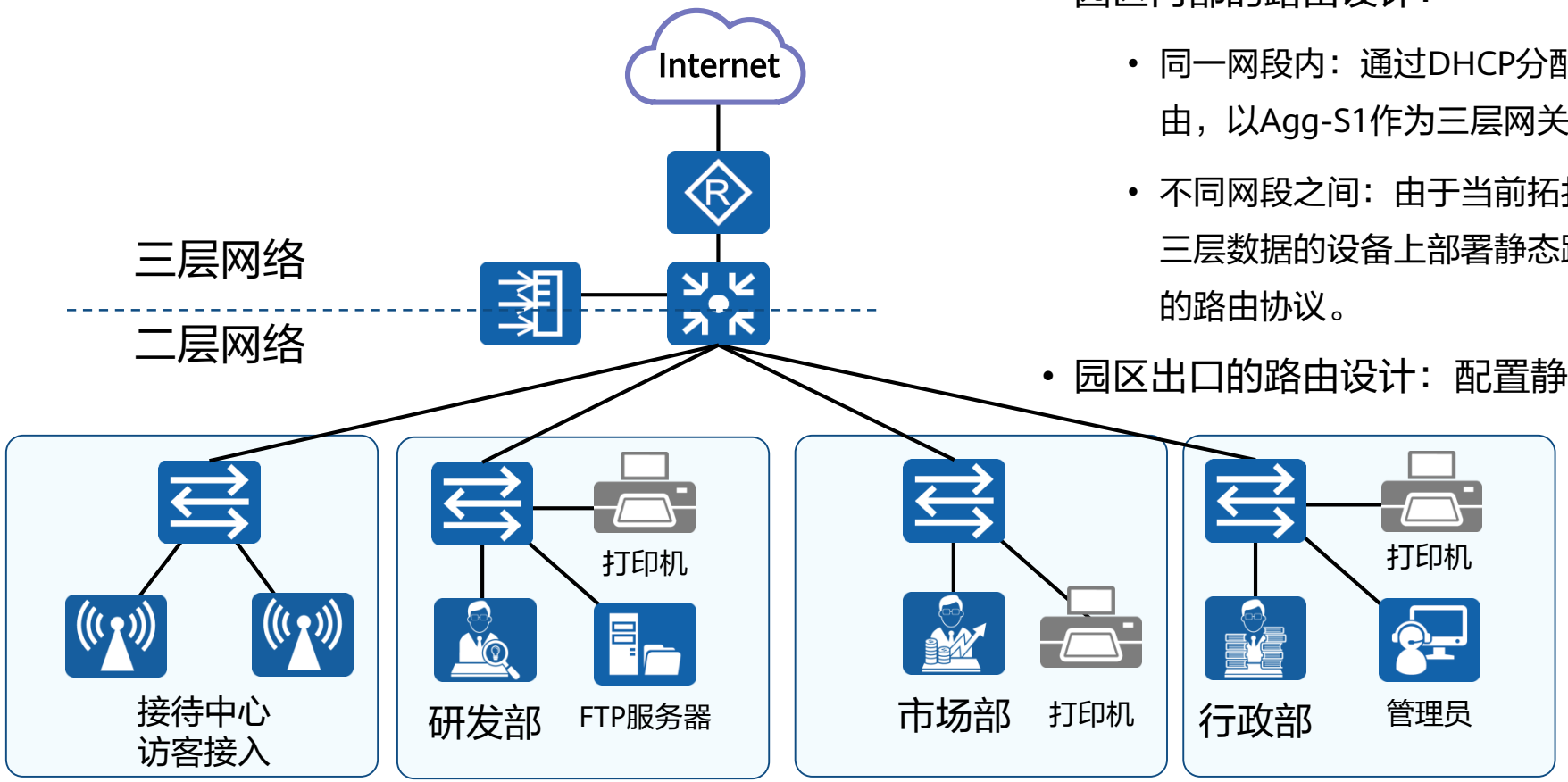
终端用户的IP地址分配，建议采用DHCP方式，由网关设备提供DHCP服务。

IP地址分配方式规划

- 出口网关采用PPPoE方式获取IP地址。
- 所有终端采用DHCP方式获取IP地址，服务器及打印机分配固定的IP地址。
- 所有网络设备上的IP地址采用手工静态方式配置（AP除外）。

IP网段/接口	分配方式	分配方式描述
192.168.1.0/24 192.168.2.0/24 192.168.3.0/24 192.168.4.0/24	DHCP	由网关Agg-S1分配，还应分配给服务器及打印机等固定设备分配固定IP地址。
192.168.100.0/24	静态	设备管理IP，静态配置
192.168.101.0/24	DHCP	AC地址静态配置，AP地址由Agg-S1分配
192.168.102.0/30	静态	互联IP，静态配置
CORE-R1的GE0/0/0	PPPoE	运营商分配的IP地址

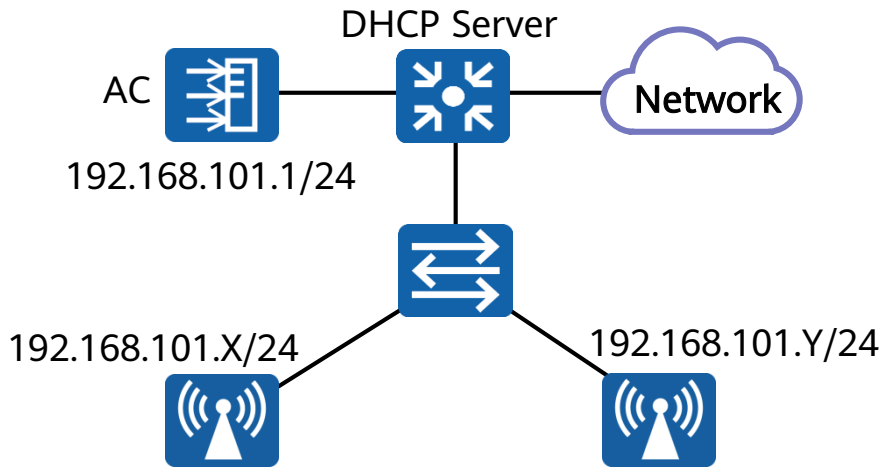
基础业务设计：路由设计



- 园区内部的路由设计：
  - 同一网段内：通过DHCP分配IP地址后默认会生成一条缺省路由，以Agg-S1作为三层网关。
  - 不同网段之间：由于当前拓扑较为简单，通过在所有需要转发三层数据的设备上部署静态路由即可满足需求，无需部署复杂的路由协议。
- 园区出口的路由设计：配置静态默认路由。

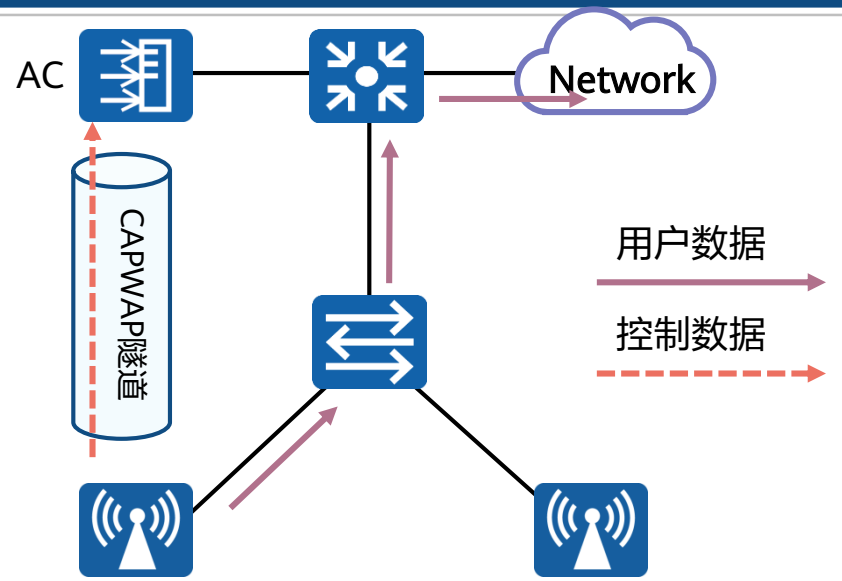
WLAN设计

WLAN组网设计



- 根据AC和AP的IP地址情况，以及数据流量是否流经AC，可将组网划分为：直连二层组网、旁挂二层组网、直连三层组网、旁挂三层组网。
- 本案例采用旁挂二层组网方式

WLAN数据转发方式设计

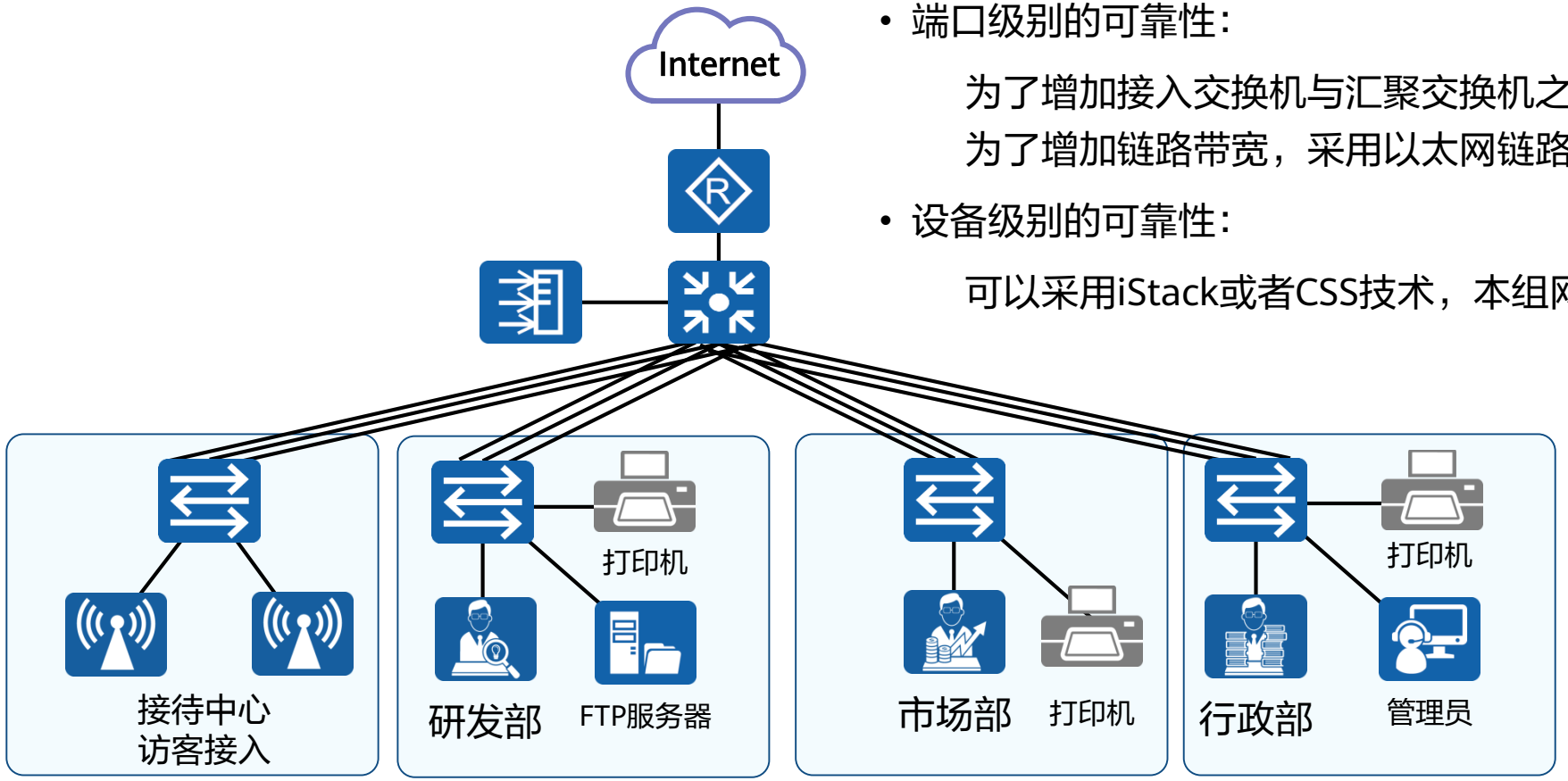


- WLAN中的数据包括控制报文和数据报文
  - 控制报文通过CAPWAP隧道转发
  - 用户数据报文分为隧道转发、直接转发
- 本案例采用直接转发方式

WLAN数据规划

配置项	配置内容
AP管理VLAN	VLAN101
STA业务VLAN	VLAN1
DHCP服务器	Agg-S1作为DHCP服务器为AP和STA分配地址，STA的默认网关为192.168.1.254
AP的IP地址池	192.168.101.2~192.168.101.253/24
STA的IP地址池	192.168.1.1~192.168.1.253/24
AC的源接口IP地址	VLANIF101：192.168.101.1/24
AP组	名称：ap-group1 引用模板：VAP模板WLAN-Guest、域管理模板default
域管理模板	名称：default 国家码：CN
SSID模板	名称：WLAN-Guest SSID名称：WLAN-Guest
安全模板	名称：WLAN-Guest 安全策略：WPA-WPA2+PSK+AES 密码：WLAN@Guest123
VAP模板	名称：WLAN-Guest 转发模式：直接转发 业务VLAN：VLAN1 引用模板：SSID模板WLAN-Guest、安全模板WLAN-Guest

可靠性设计



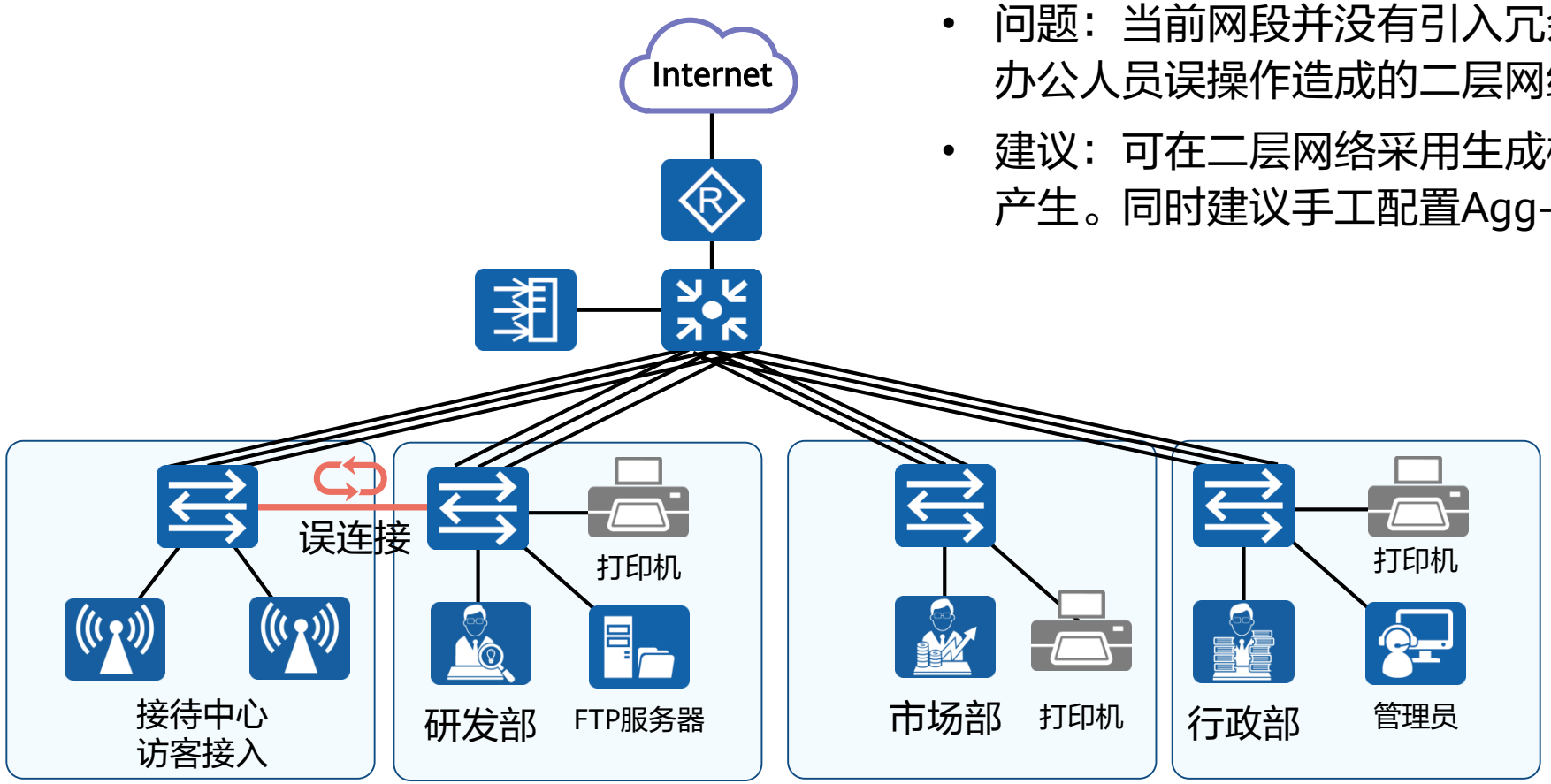
- 端口级别的可靠性：

  为了增加接入交换机与汇聚交换机之间的可靠性，同时为了增加链路带宽，采用以太网链路聚合技术。

- 设备级别的可靠性：

  可以采用iStack或者CSS技术，本组网不涉及。

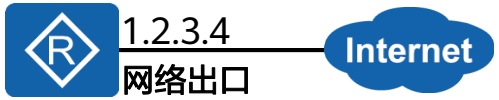
二层环路避免



- 问题：当前网段并没有引入冗余链路，如何防止办公人员误操作造成的二层网络环路呢?
- 建议：可在二层网络采用生成树技术，防止环路产生。同时建议手工配置Agg-S1为根桥。

出口NAT设计

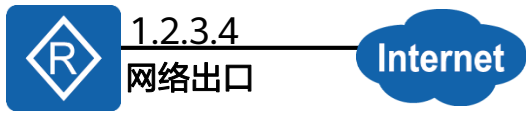
静态NAT



NAT映射表

私网地址	公有地址
192.168.1.1	1.2.3.1
192.168.1.2	1.2.3.2

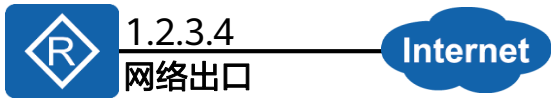
动态NAT



NAT地址池

1.2.3.1	Not Use
1.2.3.2	Not Use
1.3.3.3	Not Use

NAPT与Easy IP



NAT映射表

私网地址：端口	公有地址：端口
192.168.1.10:80	1.2.3.4:10335

NAT Server

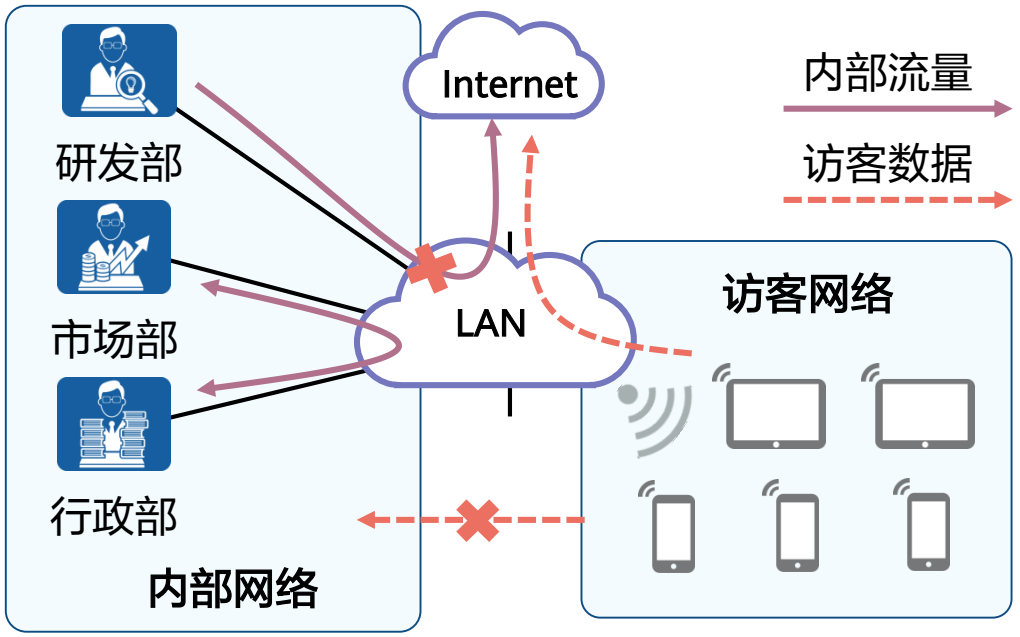
NAT映射表

私网地址：端口	公有地址：端口
192.168.1.1:10321	1.2.3.4:1025
192.168.1.2:17087	1.2.3.4:1026

NAT Server适合内网有服务器需要向外部提供服务的场景。

安全设计

流量管控



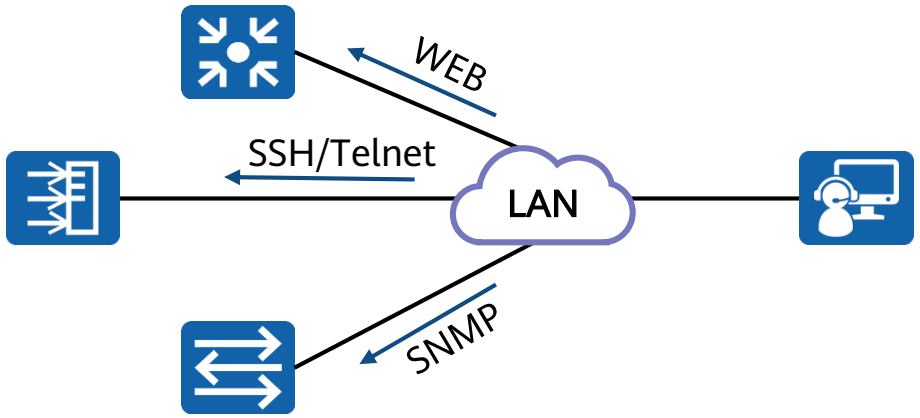
DHCP安全

网络管理安全

- 当使用Telnet或WEB等方式对设备进行网络管理时，可以通过ACL技术，仅允许固定的用户（IP）登录管理。
- 对于集中式网管，SNMPv3增加了身份验证和加密处理，可以大大提高网管的安全性。

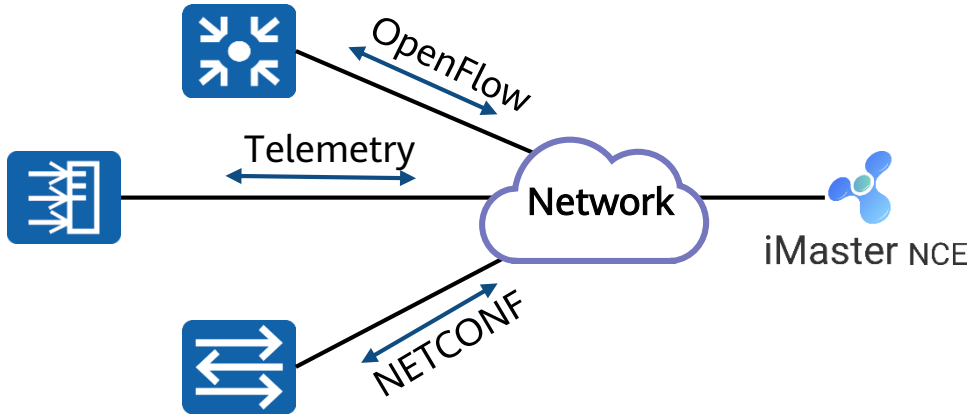
运维管理设计

传统设备管理



- 保证网络管理员与设备IP可达的情况下，可以通过Telnet、WEB以及SSH等方式对设备进行管理。
- 当网络中设备较多时，可部署基于SNMP协议的统一网管软件进行网络的运维与管理。

基于iMaster NCE平台管理



- 除了基于SNMP的传统网管之外，也可采用华为iMaster NCE平台进行网络的管理和运维，实现网络“自动驾驶”。

小型园区网络部署与实施

- 项目的部署与实施需要按照一定流程进行，内容包括：
  - 方案制定
  - 设备安装
  - 网络调试
  - 割接并网
  - 转维培训
  - 项目验收
- 具体流程按照项目实际情况进行确定。

配置方案 (1)

1. 网络设备之间物理线路连接，配置链路聚合，同时添加接口描述，详细内容如下：

设备	接口	配置内容
Acc-S1	Eth-trunk 1	mode:LACP-static Trunkport :GE0/0/1、GE0/0/2、GE0/0/3 description:to Agg-S1's eth-trunk 1
	E0/0/10	Description:to AP1
	E0/0/11	Description:to AP2
Acc-S2	Eth-trunk 1	mode:LACP-static Trunkport :GE0/0/1、GE0/0/2、GE0/0/3 description:to Agg-S1's eth-trunk 2
Acc-S3	Eth-trunk 1	mode:LACP-static Trunkport :GE0/0/1、GE0/0/2、GE0/0/3 description:to Agg-S1's eth-trunk 3
Acc-S4	Eth-trunk 1	mode:LACP-static Trunkport :GE0/0/1、GE0/0/2、GE0/0/3 description:to Agg-S1's eth-trunk 4
AC1	GE0/0/1	Description:to Agg-S1’s GE0/0/2
CORE-R1	GE0/0/1	Description:to Agg-S1’s GE0/0/1

设备	接口	配置内容
Agg-S1	Eth-trunk 1	mode:LACP-static Trunkport :GE0/0/3、GE0/0/7、GE0/0/8 description:to Acc-S1's eth-trunk 1
	Eth-trunk 2	mode:LACP-static Trunkport :GE0/0/4、GE0/0/9、GE0/0/10 description:to Acc-S2's eth-trunk 1
	Eth-trunk 3	mode:LACP-static Trunkport :GE0/0/5、GE0/0/11、GE0/0/12 description:to Acc-S3's eth-trunk 1
	Eth-trunk 4	mode:LACP-static Trunkport :GE0/0/6、GE0/0/13、GE0/0/14 description:to Acc-S4's eth-trunk 1
	GE0/0/1	Description:to CORE-R1’s GE0/0/1
	GE0/0/2	Description:to AC1’s GE0/0/1

配置方案 (2)

2. 基础业务-VLAN配置，采用基于端口的划分方式，详细内容如下:

设备	接口	类型	配置内容
Acc-S1	Eth-trunk 1	Trunk	PVID:100 Allow-pass VLAN 1、100、101
	E0/0/10		PVID:101 Allow-pass VLAN 1、101
	E0/0/11		
Acc-S2	Eth-trunk 1	Trunk	PVID:100 Allow pass VLAN 2、100
	其他接口	Access	Default VLAN 2
Acc-S3	Eth-trunk 1	Trunk	PVID:100 Allow pass VLAN 3、100
	其他接口	Access	Default VLAN 3
Acc-S4	Eth-trunk 1	Trunk	PVID:100 Allow pass VLAN 4 、100
	其他接口	Access	Default VLAN 4

设备	接口	类型	配置内容
Agg-S1	Eth-trunk 1	Trunk	PVID:100 Allow-pass VLAN 1、100、101
	Eth-trunk 2	Trunk	PVID:100 Allow pass VLAN 2、100
	Eth-trunk 3	Trunk	PVID:100 Allow pass VLAN 3、100
	Eth-trunk 4	Trunk	PVID:100 Allow pass VLAN 4 、100
	GE0/0/2	Access	Default VLAN 101
	GE0/0/1	Access	Default VLAN 102
AC1	GE0/0/1	Access	Default VLAN 101

配置方案 (3)

3. 基础业务-IP地址配置，终端与AP采用DHCP方式，设备采用静态配置，详细内容如下：

设备	接口	地址/掩码
Agg-S1	VLANif1	192.168.1.254/24
	VLANif2	192.168.2.254/24
	VLANif3	192.168.3.254/24
	VLANif4	192.168.4.254/24
	VLANif100	192.168.100.254/24
	VLANif101	192.168.101.254/24
	VLANif102	192.168.102.2/30
CORE-R1	GE0/0/1	192.168.102.1/30
	GE0/0/0	PPPoE自动获取
	Loopback0	1.1.1.1/32

设备	接口	地址/掩码
Acc-S1	VLANif100	192.168.100.1/24
Acc-S2	VLANif100	192.168.100.2/24
Acc-S3	VLANif100	192.168.100.3/24
Acc-S4	VLANif100	192.168.100.4/24
AC1	VLANif101	192.168.1.101/24

配置方案 (4)

4. 基础业务-IP地址分配方式配置，关于DHCP的详细内容如下：

网段	其他参数	备注
192.168.1.0/24	Gateway:192.168.1.254 DNS:192.168.1.254	Agg-S1为DHCP Server
192.168.2.0/24	Gateway:192.168.2.254 DNS:192.168.2.254	Agg-S1为DHCP Server 给打印机（1）以及FTP分配固定IP地址
192.168.3.0/24	Gateway:192.168.3.254 DNS:192.168.3.254	Agg-S1为DHCP Server 给打印机（2）分配固定IP地址
192.168.3.0/24	Gateway:192.168.4.254 DNS:192.168.4.254	Agg-S1为DHCP Server 给打印机（3）及网络管理员分配固定IP地址
192.168.101.0/24	N/A	Agg-S1为DHCP Server 不分配AC所占用的地址（192.168.101.1）

配置方案 (5)

5. 基础业务-路由配置，由于网络规模较小且网元数量较少，采用静态路由方式，详细内容如下：

设备	路由配置	备注
Acc-S1	0.0.0.0 0 192.168.100.254	为了让网络管理员可以跨网段访问二层交换机。
Acc-S2		
Acc-S3		
Acc-S4		
AC1	0.0.0.0 0 192.168.101.254	为了让管理员可以跨网段访问AC1。
Agg-S1	0.0.0.0 0 192.168.102.1	访问Internet的流量所匹配的路由。
CORE-R1	192.168.0.0 20 192.168.102.2	核心路由器访问内网，该路由为聚合后的路由。
	默认路由	指向外网接口。

配置方案 (6)

6. 网络管理配置，采用Telnet远程管理，认证方式为AAA，详细内容如下：

设备	管理方式	认证方式	备注
Acc-S1	Telnet	本地AAA	用户名和密码应该足够复杂且不一致，同时需要做好记录工作。
Acc-S2			
Acc-S3			
Acc-S4			
Agg-S1			
CORE-R1			
AC1			
AP1&AP2	AC集中控制和管理	N/A	N/A

7. 网络出口配置

设备	接口	接入方式	NAT方式	备注
CORE-R1	GE0/0/0	PPPoE	Easy IP	用户名：PPPoEUser123 密码：Huawei@123

配置方案 (7)

8. WLAN配置，按照WLAN规划内容进行配置即可。

9. 安全相关配置，详细内容如下:

模块	相关技术	配置内容
流量监控	Traffic-Policy 、NAT、ACL	1.配置高级ACL，阻止源为192.168.1.0/24，目的为内网业务网段的流量，放通其他流量。配置Traffic-filter引用此ACL，并在接口上应用。 2.配置基本ACL，仅放通源为192.168.1.0/24的流量，并引用到网络出接口的NAT功能上。
网络管理安全	AAA、ACL	配置基本ACL，仅放通源为管理员的IP地址，反掩码为0，并引用到所有被管理设备的VTY接口下。
DHCP安全	DHCP Snooping	在所有接入交换机上开启DHCP Snooping功能，同时配置上行接口为Trusted接口。

小型园区网络调试

1.联通性测试

- 基础链路对接测试
- 二层互通测试
- 三层互通测试

2.高可靠性能力调试

- 防环功能测试
- 路径切换测试
- 双机热备测试

3.业务性能测试

- 业务流量测试
- 访问控制测试

小型园区网络运维

- 项目上线运行之后，就进入到了运维阶段，常见的运维手段包括：
  - 设备环境检查
  - 设备基本信息检查
  - 设备运行状态检查
  - 业务检查
  - 告警处理
- 当网络达到一定规模，可以采用网络管理软件进行管理和运维，提升效率。

小型园区网络优化

- 通过网络优化，能够整体提升网络的可靠性、健壮性，更好的支撑企业业务的发展。常见的优化方案包括但不限于：
  - 设备性能优化，如升级硬件设备、更新设备软件版本等。
  - 网络基础优化，如网络架构优化、路由协议调整等。
  - 业务质量优化，如针对语音、视频业务的优先转发等。
- 应从网络需求出发，结合实际情况制定适合的优化方案。

本章总结

- 本章介绍了园区网络的概念、类型以及常见技术等。
- 了解园区网络生命周期：
  - 规划与设计
  - 部署与实施
  - 网络运维
  - 网络优化
- 结合之前课程内容，着重介绍了园区网络的规划设计与部署实施，完成一张小型园区网络的搭建。