**方案（1）：大型园区及监控网络配置说明**



‌监控系统划分VLAN的实例‌可以通过以下步骤实现：

‌确定VLAN数量和IP范围‌：

‌VLAN10‌：IP范围为192.168.0.2~192.168.1.254，子网掩码为255.255.255.0，容纳253个设备，专供管理区设备。

‌VLAN20‌：IP范围为192.168.1.2~192.168.1.254，子网掩码为255.255.255.0，容纳254个设备，专供A区摄像头。

‌VLAN30‌：IP范围为192.168.2.2~192.168.2.254，子网掩码为255.255.255.0，覆盖B区。

‌VLAN40‌、‌VLAN40‌、‌VLAN50‌同理划分，分别管理C区、D区、E区‌

‌在核心三层交换机上配置VLAN和IP地址‌：

进入VLANIF10，配置IP地址192.168.0.1作为管理区网关。

进入VLANIF20，配置IP地址192.168.1.1作为覆盖A区的网关。

依次类推，为每个VLAN配置相应的IP地址和网关‌

‌端口配置‌：

将连接下面接入交换机的端口设置为trunk模式，并允许指定的VLAN通过。图上所示5口可以访问vlan10与vlan20并配置trunk模式下接A区交换机，9口可以访问vlan10与vlan30并配置trunk模式下接B区交换机，13口可以访问vlan10与vlan40并配置trunk模式下接C区交换机，17口可以访问vlan10与vlan50并配置trunk模式下接D区交换机，21口可以访问vlan10与vlan60并配置trunk模式下接E区交换机，

具体实操：

核心交换机上操作：

1、<Huawei>System-view

[Huawei] vlan batch 10 20 30 40 50 60

解释：一次性批量创建VLAN 10,VLAN 20 vlan30 vlan40 vlan50 vlan60

2. 分配端口到对应VLAN

首先进入系统视图:system-view

先进入端口范围配置管理网络端口：

[Huawei] port-group group-member G0/0/1 to G0/0/4

[Huawei-If-range] port link-type access

[Huawei-If-range] port default vlan 10

[Huawei-If-range] quit

3、设置对应下联交换口

[Huawei]interface G0/0/5

[Huawei-GigabitEthernet0/0/5]port link-type trunk

[Huawei-GigabitEthernet0/0/5] port trunk allow-pass vlan 10 20

[Huawei-GigabitEthernet0/0/5] quit

[Huawei]interface G0/0/9

[Huawei-GigabitEthernet0/0/9]port link-type trunk

[Huawei-GigabitEthernet0/0/9] port trunk allow-pass vlan 10 30

[Huawei-GigabitEthernet0/0/9] quit

[Huawei]interface G0/0/13

[Huawei-GigabitEthernet0/0/13]port link-type trunk

[Huawei-GigabitEthernet0/0/13] port trunk allow-pass vlan 10 40

[Huawei-GigabitEthernet0/0/13] quit

[Huawei]interface G0/0/17

[Huawei-GigabitEthernet0/0/17]port link-type trunk

[Huawei-GigabitEthernet0/0/17] port trunk allow-pass vlan 10 50

[Huawei-GigabitEthernet0/0/17] quit

[Huawei]interface G0/0/21

[Huawei-GigabitEthernet0/0/21]port link-type trunk

[Huawei-GigabitEthernet0/0/21] port trunk allow-pass vlan 10 60

[Huawei-GigabitEthernet0/0/21] quit

4、设置相应VLAN IF网关

[Huawei] interface Vlanif 10

[Huawei-Vlanif10] ip address 192.168.0.1 255.255.255.0

[Huawei-Vlanif10] quit

[Huawei] interface Vlanif 20

[Huawei-Vlanif20] ip address 192.168.1.1 255.255.255.0

[Huawei-Vlanif20] quit

[Huawei] interface Vlanif 30

[Huawei-Vlanif30] ip address 192.168.2.1 255.255.255.0

[Huawei-Vlanif30] quit

[Huawei] interface Vlanif 40

[Huawei-Vlanif40] ip address 192.168.3.1 255.255.255.0

[Huawei-Vlanif40] quit

[Huawei] interface Vlanif 50

[Huawei-Vlanif50] ip address 192.168.4.1 255.255.255.0

[Huawei-Vlanif50] quit

[Huawei] interface Vlanif 60

[Huawei-Vlanif60] ip address 192.168.5.1 255.255.255.0

[Huawei-Vlanif60] quit

5、A区交换机配置

<Huawei>System-view

[Huawei]vlan 20

[Huawei vlan20]quit

[Huawei] port-group group-member Eth0/0/1 to Eth0/0/21

[Huawei-If-range] port link-type access

[Huawei-If-range] port default vlan 20

[Huawei-If-range] quit

[Huawei]interface G0/0/1

[Huawei-GigabitEthernet0/0/1]port link-type trunk

[Huawei-GigabitEthernet0/0/1] port trunk allow-pass vlan 10 20

[Huawei-GigabitEthernet0/0/1] quit

A区摄像头地址配置为：192.168.1.3-254 255.255.255.0 192.168.1.1

6、B区交换机配置

<Huawei>System-view

[Huawei]vlan 30

[Huawei vlan30]quit

[Huawei] port-group group-member Eth0/0/1 to Eth0/0/21

[Huawei-If-range] port link-type access

[Huawei-If-range] port default vlan 30

[Huawei-If-range] quit

[Huawei]interface G0/0/1

[Huawei-GigabitEthernet0/0/1]port link-type trunk

[Huawei-GigabitEthernet0/0/1] port trunk allow-pass vlan 10 30

[Huawei-GigabitEthernet0/0/1] quit

B区摄像头地址配置为：192.168.2.3-254 255.255.255.0 192.168.2.1

7、C区D区E区以上类推即可，改相应的VLAN号即可。‌

**方案（2）：A区与B区互相不能，只与管理区C区相通，C区可以互通AB区**

以下是基于典型园区网架构的交换机配置方案，结合VLAN隔离与ACL策略实现访问控制需求：

‌一、网络架构规划‌

‌VLAN划分‌

A监控区：VLAN 10（网段：10.1.10.0/24）

B监控区：VLAN 20（网段：10.1.20.0/24）

C管理区：VLAN 30（网段：10.1.30.0/24）

核心交换机作为网关，启用三层路由功能。

‌访问规则‌

A区仅允许访问C区（禁止访问B区）

B区仅允许访问C区（禁止访问A区）

C区允许访问A/B区

‌逻辑拓扑‌：

[A区接入交换机]─(Trunk)─┐

 ├─[核心交换机]

[B区接入交换机]─(Trunk)─┘

[C区设备]───(Access VLAN30)─┘

‌二、核心交换机配置（华为/H3C通用）‌

// 1. 创建VLAN并配置网关，A监控区：VLAN 10（网段：10.1.10.0/24），网关10.1.10.1；

B监控区：VLAN 20（网段：10.1.20.0/24），网关10.1.20.1；

C管理区：VLAN 30（网段：10.1.30.0/24），网关10.1.30.1；

vlan batch 10 20 30

interface Vlanif10

 ip address 10.1.10.1 255.255.255.0 #当进入某个vlanif ID号之后重新运行命令将覆盖原来设置重新使新的配置生效。

interface Vlanif20

 ip address 10.1.20.1 255.255.255.0

interface Vlanif30

 ip address 10.1.30.1 255.255.255.0

display interface vlanif 10 // 查看Vlanif10状态及参数

// 2. 配置接入端口（连接C区设备）

[Huawei] port-group group-member G0/0/1 to G0/0/4 #1-4号口为接入管理区设备，如硬盘录像机、管理电脑等。

[Huawei-If-range] port link-type access

[Huawei-If-range] port default vlan 30

[Huawei-If-range] quit

需要添加端口，则重新进入端口视图如需要添加11-15号端口加入VLAN30则操作如下：

[Huawei] port-group group-member G0/0/11 to G0/0/15 #选择端口范围。

[Huawei-If-range] port link-type access

[Huawei-If-range] port default vlan 30

[Huawei-If-range] quit

需要删除端口，则需要根据相应端口类型删除：

查看端口类型命令：display port vlan

按链路类型删除端口与VLAN的绑定‌

Access端口‌

[HUAWEI-GigabitEthernet0/0/1] undo port default vlan // 解除端口与VLAN的绑定 :ml-citation{ref="1,4" data="citationList"}

 Trunk端口‌

[HUAWEI-GigabitEthernet0/0/1] undo port trunk allow-pass vlan 10 // 禁止VLAN 10通过该Trunk端口 :ml-citation{ref="1,6" data="citationList"}

Hybrid端口‌

[HUAWEI-GigabitEthernet0/0/1] undo port hybrid vlan 10 // 取消VLAN 10的标签/无标签配置

// 3. 配置Trunk端口（5号口连接A区接入交换机）

interface GigabitEthernet0/0/5

 port link-type trunk

 port trunk allow-pass vlan 10 30

// . 配置Trunk端口（9号口连接B区接入交换机）

interface GigabitEthernet0/0/9

 port link-type trunk

 port trunk allow-pass vlan 20 30

// 4. 配置ACL实现访问控制，规则名为abc，规则号为3000

acl name abc 3000

 rule 5 deny ip source 10.1.10.0 0.0.0.255 destination 10.1.20.0 0.0.0.255 // 禁止A→B

 rule 10 deny ip source 10.1.20.0 0.0.0.255 destination 10.1.10.0 0.0.0.255 // 禁止B→A

 rule 15 permit ip source 10.1.10.0 0.0.0.255 destination 10.1.30.0 0.0.0.255 // 允许A→C

 rule 20 permit ip source 10.1.20.0 0.0.0.255 destination 10.1.30.0 0.0.0.255 // 允许B→C

 rule 25 permit ip source 10.1.30.0 0.0.0.255 destination any // 允许C→A/B

// 5. 应用ACL到VLAN接口

interface Vlanif10

 traffic-filter inbound acl name abc // A区入方向过滤

interface Vlanif20

 traffic-filter inbound acl name abc // B区入方向过滤

interface Vlanif30

 traffic-filter inbound acl name abc // C区入方向过滤

Ctrl+Z进入用户视图，save 按y保存配置。

undo traffic-filter inbound acl name abc

‌三、A/B区接入交换机配置‌

// A区接入交换机（连接核心的端口配Trunk）

<Huawei>System-view

[Huawei]vlan 10

[Huawei vlan10]quit

[Huawei] port-group group-member Eth0/0/1 to Eth0/0/21

[Huawei-If-range] port link-type access

[Huawei-If-range] port default vlan 10

[Huawei-If-range] quit

[Huawei]interface G0/0/1

[Huawei-GigabitEthernet0/0/1]port link-type trunk

[Huawei-GigabitEthernet0/0/1] port trunk allow-pass vlan 10 30

[Huawei-GigabitEthernet0/0/1] quit

Ctrl+Z进入用户视图，save 按y保存配置。

// B区接入交换机（配置同理，VLAN改为20）

<Huawei>System-view

[Huawei]vlan 20

[Huawei vlan20]quit

[Huawei] port-group group-member Eth0/0/1 to Eth0/0/21

[Huawei-If-range] port link-type access

[Huawei-If-range] port default vlan 20

[Huawei-If-range] quit

[Huawei]interface G0/0/1

[Huawei-GigabitEthernet0/0/1]port link-type trunk

[Huawei-GigabitEthernet0/0/1] port trunk allow-pass vlan 20 30

[Huawei-GigabitEthernet0/0/1] quit

‌四、关键技术验证‌

‌VLAN隔离‌：A/B区属于不同VLAN，二层天然隔离79。

‌三层控制‌：ACL在核心网关过滤跨网段流量：

禁止规则：deny A↔B（规则5、10）

放行规则：permit A→C、B→C、C→any（规则15、20、25）811。

‌策略优先级‌：ACL规则按序号匹配（小序号优先），deny规则置于permit前避免误放行812。

‌测试命令‌：

A区设备 ping B区IP → ‌不通‌

C区设备 ping A/B区IP → ‌通‌

‌五、扩展建议‌

‌安全增强‌：在核心交换机启用dhcp snooping防私接设备36，开启stp root-protection防环路9。

‌高可用设计‌：若为双核心架构，需同步配置VRRP网关冗余及ACL策略1

**（3）1000路监控IP规划，选VLAN的分析必要性。**

 为什么不能用一个网段？

想象一下，1000户人家共用同一套门牌号系统，快递员送件时将如何应对？同样，IP冲突、故障排查难、广播风暴等问题将频繁出现。

4步搞定1000路监控IP规划

核心工具：一台三层交换机，划分5个VLAN（虚拟局域网）。

VLAN10 IP范围：192.168.0.1~192.168.0.254，子网掩码：255.255.255.0，容纳254个设备，专供A区摄像头。

VLAN20 IP范围：192.168.1.1~192.168.1.254，子网掩码：255.255.255.0，覆盖B区，独立管理不干扰。

VLAN30、VLAN40、VLAN50同理划分，分别管理C区、D区、E区。总容量：5\*254=1270个IP，完美适配1000路监控！

 为什么不建议改子网掩码？

有人提出：“直接改子网掩码为255.255.252.0，一个网段就能塞下1000个IP！”看似省事，实则隐患重重：全员大杂烩、广播风暴、DHCP陷阱等问题将层出不穷。

运维效率翻倍的3个技巧

IP分段命名：按区域标记（如A区-001~254），台账清晰易查。

定期IP扫描：用工具批量Ping检测，故障设备无处遁形。

预留扩展空间：每个VLAN预留少量IP，应对临时新增需求。

总结

大型监控与园区项目，IP规划是命脉！250点位是红线：超量必分VLAN！6个网段稳如磐石：给录像机一个网段，这样交换机设置好，都能访问各网段，而前端摄像机只能访问本网段设备。