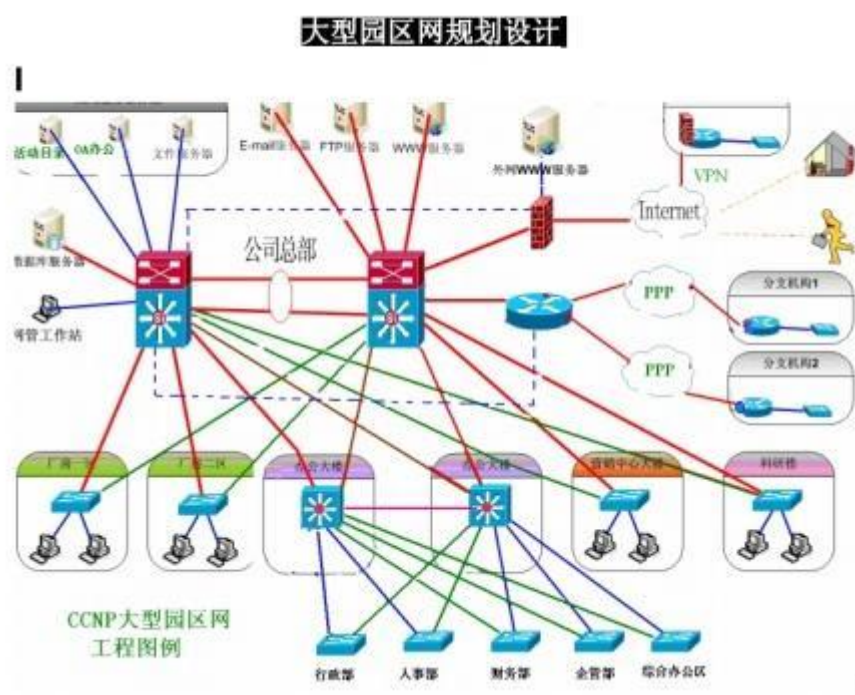


如何规划园区网设计实施时的 IP/VLAN?

IP/VLAN 规划是园区网设计实现的一项重要内容，不合理的规划会直接影响日后的管理维护。所谓 IP / VLAN 规划，就是为接入园区网的所有设备，包括交换机、路由器、防火墙、服务器、客户机、打印服务器等，分配一个惟一的 IP 地址，并为其指定适当的 VLAN。考虑到日后的扩展、维护等问题，园区网的 IP/VLAN 规划不仅应符合网络设计规范，还要有规律、易记忆，能反映园区网的特点。

园区网选用的主干技术、拓扑结构不同，IP/VLAN 规划也会有所区别。本文主要针对在园区网建设中应用比较广泛的网络拓扑就其 IP/VLAN 规划需要考虑的问题进行讨论。

在进行园区网 IP/VLAN 规划前，绘制一幅准确的园区网拓扑图是不可缺少的。准确的网络文档对于日后的升级和分析问题很有帮助。图 1 所示，是一幅典型的园区网拓扑图。



1. 确定园区网一内网 IP 地址的类型

现在园区网建设中 IP 地址规划均采用私有地址进行设计，即由 Internet 地址授权机构（IANA）为园区网一内网分配 RFC1918 中定义的非 Internet 连接的网络地址，留出了三类网络地址，给不连到 Internet 上的专用网使用。园区网一内网可以采用私有 IP 地址的网络地址分配方案；园区网一外网、DMZ 区使用合法互联网 IP 地址。

网络主机比较多即网络人数比较多大型网络可以采用 172 和 10 网段地址，如果是网络较小的可以采用 192.168 网段的地址进行规划。

类	私有地址范围
A	10.0.0.0 到 10.255.255.255
B	172.16.0.0 到 172.31.255.255
C	192.168.0.0 到 192.168.255.255

2. 规划主交换机端口 VLAN 及网络设备 IP

如图 1 所示，网络中的主交换机提供了到各楼宇二级交换机的连接，因此为主交换机的端口指定 VLAN 是规划整个内部网的关键。

特别注意，由于 A 号楼、B 号楼、C 号楼除了有 VLAN1、VLAN2、VLAN3 的用户，都包含部分 VLAN7 用户，所以它们的千兆上联端口也都包含了 VLAN7（举例）。

将网络中的主交换机、二级交换机都划到 VLAN11，实现对网络设备安全、有效管理。

3. 规划虚拟局域网 IP 地址

在具有三层交换功能的园区网中，可以按照物理建筑划分虚拟局域网；也可以按职能部门划分虚拟局域网（VLAN），VLAN 成员可以不受地理位置的限制。

VLAN 划分分为两类，根据接入层交换机的端口划分称为静态 VLAN，根据网卡的 MAC 地址划分称为动态 VLAN。当园区网规模较大时，动态 VLAN 实现较为复杂，一般较少采用；应用最多的还是静态 VLAN。为了方便日后的维护管理，VLAN 与 IP 子网之间一般是一一对应的关系。

针对有些部门办公地点分散在几栋楼宇的情况，可以将对应楼宇交换机的指定端口统一划到一个指定 VLAN。这正是使用 VLAN 技术的优势，其成员不受地理位置的限制。

表 3.2 Vlan 划分表

VLAN 号	VLAN 名称	说明
VLAN1	——	管理 VLAN
VLAN2	finance	财务部
VLAN3	Human_resource	人力资源部
VLAN4	After_sale_server	售后服务部
VLAN5	Customer service	客服部
VLAN6	Technique_support	技术支持部
VLAN7	produce	产品部

财务部	192. 168. 2. 0/24	192. 168. 2. 254	254
人力资源部	192. 168. 3. 0/24	192. 168. 3. 254	254
售后服务部	192. 168. 4. 0/24	192. 168. 4. 254	254
客服部	192. 168. 5. 0/24	192. 168. 5. 254	254
技术支持部	192. 168. 6. 0/24	192. 168. 6. 254	254
产品部	192. 168. 7. 0/24	192. 168. 7. 254	254
设备部	192. 168. 8. 0/24	192. 168. 8. 254	254
市场部	192. 168. 9. 0/24	192. 168. 9. 254	254
服务器群 VLAN	192. 168. 10. 0/24	192. 168. 10. 254	254

4. 规划防火墙、路由器、服务器的 IP 地址

WWW/MAIL/DNS 服务器、防火墙的 DMZ 网卡、防火墙的外网卡、路由器以太网口 1、路由器以太网口 2、路由器广域网口 1 应该使用从 ISP 申请到的合法 IP。防火墙的 DMZ 区，如果需要可增加服务器。

5. 规划园区网内网用户的 IP 地址

规划完子网与 VLAN，接下来就要考虑园区网用户 IP 的分配方式。

针对用户比较集中、信息点位置相对固定的情况，建议使用静态 IP。这对于日后的管理、维护、故障排查非常重要，管理员可以根据 IP 地址迅速确定主机所在位置。使用静态 IP，园区网用户与联接交换机的端口处于同一 VLAN。为方便新的用户 IP 地址的分配，应做好现有用户 IP 地址的记录。

当用户变动较大，信息点数量无法准确计算时，建议使用动态 IP。动态 IP 的优势在于方便用户使用，特别适合计算机基础较弱的用户群体。用户只需要将网络属性中的 IP 地

址栏设成自动获取，用户的本机 IP、缺省网关、DNS、WINS 等关键信息，会自动从 DHCP 服务器中得到。

使用 DHCP 服务器可以大大减轻管理员的工作，但也会带来一些新的问题，例如：需要用一台主机提供 DHCP 服务；在上网计算机较多的情况下，如果 DHCP 服务器不稳定，会出现 IP 不能回收、IP 发放不出去等问题。

6. 园区网内网 NAT 实现

当园区网的 IP / VLAN 规划基本完成后，要采用网络地址转换（NAT）技术，即通过 1 个或几个外部 IP 地址来实现园区网—内网用户访问 Internet。目前支持 NAT 的产品非常多，可以是软件，比如 Winrouterpro、Sygate、Wingate、Winproxy 等；也可以是硬件，比如路由器、防火墙，目前园区网中以硬件产品为主。