计科1306班 陈伟颖 2013011266

基础网络的规划与设计

一、架构分析和设计

1.网络架构分析和布线设置

考虑到本案例中三个校区相距较远，三个校区总体的校园网在分层布线主要采用环形结构；对于每个校区而言，教职工宿舍、学生宿舍、老师办公室以及教室可以搭建树形结构的拓扑，简单划分为两个子网：宿舍区以及教学楼，对于这两个子网采用不同类型的结构。

对教学楼而言，现代网络结构化布线工程中多采用星型结构，主要用于同一楼层，由各个房间的计算机间用集线器或者交换机连接产生的，它具有施工简单，扩展性高，成本低和可管理性好等优点，所以对每栋教学楼而言，每个教室的计算机连接到本层的集线器或交换机，然后每层的集线器或交换机在连接到本楼出口的交换机或路由器，各个楼的交换机或路由器再连接到校园网的通信网中。

对于不同校区的宿舍区而言，采取的是环形结构，并在设备选型和结构设计上考虑整体网络的高性能和高可靠性，选择热路由备份可以有效地提高核心交换的可靠性。

校园网采用星形的网络拓扑结构，骨干网为1000M速率具有良好的可运行性、可管理性，能够满足未来发展和新技术的应用，另外作为整个网络的交换中心，在保证高性能、无阻塞交换的同时，还必须保证稳定可靠的运行。传输介质也要适合建网需要。在楼宇之间采用1000M光纤，保证了骨干网络的稳定可靠，不受外界电磁环境的干扰，覆盖距离大，能够覆盖全部校园。在楼宇内部采用超5类双绞线，其连接状态100m的传递距离能够满足室内布线的长度要求。

2.结构设计

由于该学校网络用途多样，是一个组合型的网络，应该分成基础设施模块、服务器群组、网络管理模块和边界分配模块组成，在本案例中具体为：楼宇接入模块、楼宇分配模块和骨干网。考虑到学生和老师的实际需要，需要设计无线局域网和有线局域网，也需要考虑服务器冗余。

校园网网络整体分为三个层次：核心层、汇聚层、接入层。为实现校区内的高速互联，核心层由1个核心节点组成，包括教学区区域、服务器群；汇聚层设在每栋楼上，每栋楼设置一个汇聚节点，汇聚层为高性能“小核心”型交换机，根据各个楼的配线间的数量不同，可以分别采用1台或是2台汇聚层交换机进行汇聚，为了保证数据传输和交换的效率，现在各个楼内设置三层楼内汇聚层，楼内汇聚层设备不但分担了核心设备的部分压力，同时提高了网络的安全性；接入层为每个楼的接入交换机，是直接与用户相连的设备。

二、编址设计

Internet接入方式主要有拨号上网方式,使用ISDN专线入网,使用ADSL宽带入网,使用DDN专线入网,使用帧中继方式入网,局域网接入。根据需求分析，可以将整体网络分为三种类型的组。

工作组	组数	备注
公共设备组	4组	教学楼＋多媒体教室
教师专用组	1组	每层教学楼，具有VoIP功能
校园无线组	1组	每层教学楼以及宿舍区

IP地址的统一、合理规划以及整个网络向IPv6的演进是关系到整体分层网络稳定、快速收敛的关键，也是某职业技术学院校园网网络设计中的重要一环。IP地址规划的好坏，不仅影响到网络路由协议算法的效率，更影响到网络的性能和稳定以及网络的扩展和管理，也必将直接影响到相关新业务的开拓和网络应用的进一步可持续性发展。

IP地址的分配原则如下：

（1）给三层交换机设备互连的点对点IP地址分配1个C类地址，提供足够的扩展性

（2）考虑到以后的网络扩展规模，二层交换机设备的管理IP地址分配1个C类IP地址；

（3）可以考虑为学校校园网分配若干个C类私有地址段。

服务器集群和办公楼、教学楼教室、以及多媒体教室的IP获取方式为手动分配，其他的均为通过DHCP获取。上网方式均采用NAT方式。根据信息点数可以分配不同网段，对于每个网段而言，IP地址分配都是充足的，而且可拓展性较高，网关分配如下：

地点 / 部门	信息点数	网关
综合教学楼	60	192.168.0.1
普通教学楼1	40	192.168.1.1
普通教学楼2	20	192.168.2.1
综合多媒体教室	120（两个，每个60个信息点）	192.168.3.1
教职工宿舍	1个信息点	192.168.4.1
校园无线	男生宿舍3个信息点，女生宿舍1个信息点，教学楼每层一个信息点、多媒体实验室一个信息点	192.168.5.1
老师办公室	1	192.168.6.1

物理/链路层配置遵循下面的原则：

1.网络设备互连的物理端口都应该绑定端口的速率和全双工模式；

2.建议所有的Vlan都不要穿透核心层，所有的Vlan都将在汇聚层交换机上终结；

3.本实施方案建议不要启用STP生成树协议，由于所有的Vlan都已在汇聚层交换机终结，在二层上并没有环路存在，故无必要启用；如果开启基于每个Vlan的生成树协议，广播报文将会很多，影响核心交换机性能和网络收敛时间；

4.所有核心层和汇聚层交换机之间的互连端口均设置为Trunk模式，但目前只容许互连Vlan通过，以应付将来有Vlan穿越核心层这种情况；

5. 汇聚层交换机和接入交换机之间的互连端口设置为Trunk模式。

三、性能保障设计

可以采用QoS机制来确定、设置和确保通信流的优先级别。本案例中可以使用区分服务类型的QoS，这种机制的本质是将网络中传输的业务分成多类，在大型的网络中，可以设置一类网络优先度高于其他类，即可以将教师办公室以及教务的优先度设置为高级别，将其他相对而言没有那么重要的教室设备网络、校园网络设置相对较低的级别。

四、管理设计

可以选择SNMP这种管理协议，SNMP运行在TCP/IP协议栈之上，适合用UDP连接。SNMPv3具有数据完整性、数据源端鉴别、数据可用性、报文时效性和限制重播性防护，其安全协议由鉴别、时效性、加密三个模块组成，具有开放和支持第三方的管理结构。

在带内管理和带外管理上，可以采用组合的方式来进行管理，在正常工作的情况下，使用应用的网络传输管理数据流实现对网络的监视和管理；当网络不能正常工作时，可以利用带外的链路获取这些关键节点的信息，实现对设备的监视功能。

由于该学校是三个校区分布，所以在管理结构上，需要采用分布式的结构，每个校区有对等的管理组，虽然在结构上会有点复杂，但对网络监控也能够应对突发事件。网络管理主要需要有，控制通过登录窗口访问外网、监控故障和性能参数、测算网络流量，可以购买相应的管理软件进行管理，以实现全网监控，可以实时监控所有设备的运行状况，并根据网络运行环境变化提供合适的方式对网络参数进行配置修改，保证网络以最优性能正常运行、通过性能任务的配置，可自动获得网络的各种当前性能数据，并支持设置性能的门限，当性能超过门限时，可以以告警的方式通知网管系统。通过统计不同线路、不同资源的利用情况，为优化或扩充网络提供依据、实现服务器与设备的统一管理、自动设置配置文件等功能。

五、安全设计

安全接入和配置是指在物理(控制台)或逻辑(telnet)端口接入网络基础设施设备前必须通过认证和授权限制，从而为网络基础设施提供安全性。限制远程

访问的安全设置方法如下：

访问方式	保证网络设备安全的方法	备注
Console控制接口的访问	设置密码和超时限制	建议超时限制设成5分钟
进入特权exec和设备配置级别的命令行	配置Radius来记录logon/logout时间和操作活动；配置至少一个本地账户作应急之用	
telnet访问	采用ACL限制，指定从特定的IP地址来进行telnet访问；配置Radius安全纪录方案；设置超时限制	
SSH访问	激活SSH访问，从而允许操作员从网络的外部环境进行设备安全登陆	
WEB管理访问	取消Web管理功能	
SNMP访问	常规的SNMP访问是用ACL限制从特定IP地址来进行SNMP访问；记录非授权的SNMP访问并禁止非授权的SNMP企图和攻击	为增加安全,建议更改缺省的SNMP Commutiy子串
设置不同账号	通过设置不同的账号的访问权限，提高安全性	

网络设备拒绝服务攻击的防止主要是防止出现TCP SYN泛滥攻击、Smurf攻击等；网络设备的防TCP SYN的方法主要是配置网络设备TCP SYN临界值，若多于这个临界值，则丢弃多余的TCP SYN数据包；防Smurf攻击主要是配置网络设备不转发ICMP echo请求(directed broadcast)和设置ICMP包临界值，避免成为一个Smurf攻击的转发者、受害者。

访问控制如下：

1.允许从内网访问internet，端口全开放。

2.允许从公网到DMZ（非军事）区的访问请求：WEB服务器只开放80端口，mail服务器只开放25和110端口。

3.禁止从公网到内部区的访问请求，端口全关闭。

4.允许从内网访问DMZ（非军事）区，端口全开放

5.允许从DMZ（非军事）区访问internet，端口全开放

6.禁止从DMZ（非军事）区访问内网，端口全关闭。

此外，需要为该网络设置加密机制和安全认证机制，可以通过相应的管理软件实现该功能。