

高校校园宿舍网络建设与管理*

商尔从, 何海涛, 古小红, 道 焰
(中山大学网络与教育技术中心, 广州 510275)

摘 要: 总结 1 年多来中山大学校园宿舍网络的建设与管理的实践, 并就一些技术和管理方法进行探讨。

关键词: 宿舍网; 主干网; 网络拓扑结构; DHCP; PROXY; VLAN

中图分类号: TP393.07 **文献标识码:** A

高校校园宿舍网络建设与管理是一个复杂的系统工程。与一般的网络建设管理一样, 它包括三个阶段: 规划、设计阶段; 实施、施工阶段; 运行管理、客户服务阶段。

1 规划、设计阶段——重要的一环, 成败之关键

这个阶段一般包括以下几方面的内容: 网络拓扑的规划、网络技术方案的制订。使用“正式地址”还是“私有地址”; 采用 NAT (NAPT) 技术, 还是代理服务器技术 (包括透明代理服务器技术); 地址分配是否采用 DHCP, 都必须在计划中予以仔细考虑。除此之外, 网络工程施工规划也是需要考虑的。总体网络安全策略也应该在此制订, 至于网络安全策略的细节, 可在网络运行管理阶段中不断加以补充、细化及调整。

1.1 网络拓扑的规划

良好的网络拓扑结构是网络稳定的基础。一般可以采用的网络拓扑结构有: 环型结构、星结构、树型结构等。网络拓扑结构的选择可以根据自身学校的特点 (包括自然地理特点) 选择自己的网络拓扑结构 (图 1):

(1) 规模较小的学校可以采用单一的星型拓扑结构, 这种结构管理方便;

(2) 规模较大的学校可以采用树型的网络拓扑结构, 这种结构管理节点多, 管理难度较大;

(3) 根据自己的历史状况可采取其他的拓扑结构。

1.2 网络技术方案的制订

目前使用的组网技术主要有 ATM、交换以太网, 如果要考虑到历史原因也可以采用其他的技术如 FDDI 等。

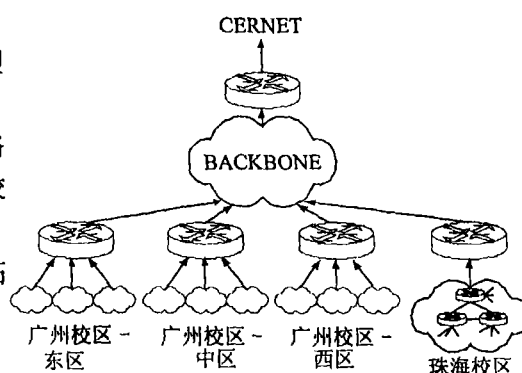


图 1 中山大学校园网拓扑

* 收稿日期: 2000-11-15; E-mail: bug@.zsu.edu.cn

总体上,可以将宿舍网络分为两个大部分:骨干网(核心层和分布层)和楼宇网(接入层)。

骨干网主要是为各区域网络之间提供高速的、无阻塞的信道,在校园网宜选择千兆位交换以太网。这是因为千兆位交换以太网与 ATM、FDDI 技术相比,不但带宽高,而且管理简单。骨干网必须支持 IEEE 802.1Q VLAN,具备第三层交换的功能。

楼宇网是为了给用户提供一个高速的接入方式,在校园网中宜选择 10/100TX 交换以太网,具备第二层交换功能即可。

对于骨干网与楼宇网所使用的主要网络设备的选择方面,可以根据自己学校,以及宿舍使用的特点进行考虑。选择网络设备应该考虑以下几个方面,从中寻求一个自己合适的平衡点:① 自己学校的特点,包括宿舍区与教学区之间的距离;② 需要对宿舍区域网络控制与管理的深度与广度;③ 设备的功能和可管理性及其性能;④ 依赖厂商硬件产品功能,还是采用软件方式实现;⑤ 技术人员的专业技术水平;⑥ 设备的投资。

1.3 IP 网络中地址的选择与分配

IP 网络中网络地址的使用一般有两种方法:采用 RFC 1918 中定义的“私有地址”,或使用“公有地址”。由于目前我们所使用的 IPv4 地址空间已经快被用尽,已经除非学校申请到充足的 IP 地址空间,否则不应该在宿舍区中使用正式的 IP 地址,否则 IP 地址用尽时,就会对正常的教学与科研使用网络造成影响,或面临要更改地址的困境。并且,使用“私有地址”的理由还在于:划分 IP 子网的原则是尽量使地址“聚合”,地址是否“聚合”对网络的稳定性非常重要,若使用正式的 IP 地址则很难做到(图 2)。

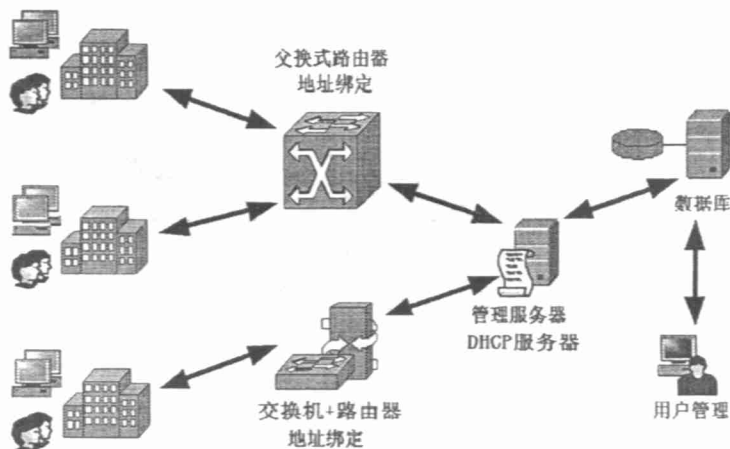


图 2 IP 网络中地址的分配

宿舍用户 IP 地址的获取一般采取两种方式:用户自行选择;或系统自动分配,配合 DHCP 让用户自动获取地址。由于在宿舍网络中,为了安全的需要一般都进行 IP 地址及适配器地址绑定管理策略,因此 DHCP 一般不采用“地址池”分配方式,而采用与适配器地址绑定(固定)分配的方式,让用户从 DHCP 服务器上自动获取地址的好处是:① 当发生网络地址调整、DNS 服务器、网关地址调整时无须提前通知用户更改配置;② 可以自动为用户分配地址的系统,免除了用户登记时录入地址的麻烦。

采用 DHCP 分配获取地址也有其不足之处:DHCP 协议简单,没有任何认证机制,如

果有人在这个网段上配置或假冒一台 DHCP 服务器,就会错误配置 DHCP 客户机,导致用户无法使用网络资源,而且如果网关地址被配置到 DHCP 客户机时,会影响到整个网段的用户可能在一段时间内都无法使用网络资源。

当 IP 网络从 IPv4 向 IPv6 过渡后,也可以考虑采用 IPv6 的正式 IP 地址。

如果使用“私有地址”可以考虑使用 NAT (NAPT) 解决方案,使用 NAT (NAPT) 的好处是:① 使用“私有地址”,可以解决 IP 地址短缺问题;② 可以防止外部地址直接访问宿舍内部网,屏蔽宿舍网的内部结构;③ 无需构建代理服务器。

但是 NAT (NAPT) 也有其不足之处:① 不能进行缓存,减少流量;② 进行地址翻译时, TCP 包中的 TCP/IP 地址信息可能没有被同时翻译;③ 加密 TCP 报头信息的软件和 NAT 协同工作可能会有问题。

1.4 使用代理服务器

宿舍网络无论是否使用“私有网络” IP 地址,都可以配合使用代理服务器。一般地,代理服务器必须具备以下的基本功能:① 能提供全面 TCP、UDP 端口代理;② 可以方便地对 TCP、UDP 端口进行封锁,或只允许某些“安全”的端口通过;③ 在应用软件配置完毕后,代理服务器对于用户来说是透明的;④ 对于没有提供代理服务器接口的应用程序,也应该有办法提供代理。

“私有地址”与代理服务器方案的优点是可以解决地址短缺的问题,如① 通过在代理服务器上进行带宽分配、控制每个客户机的链接数,缓解网络被过度滥用的问题。网络被过度滥用表现在:使用太多的进(线)程、连接下载;下载大的游戏或电影;发放垃圾邮件等;② 利用代理服务器的缓存、网络资源重定向等功能可以节省带宽及缓解校园网出口的压力;③ 利用代理服务器对学生在网络上的行为可以起到一定的监管和约束作用。

使用“私有地址”与代理服务器方案也有其不足之处,如① 需要维护一台或多台的代理服务器,增加了工作量;② 代理服务器设置不当,会变为宿舍网的“瓶颈”;③ 由于代理服务器常被学生视作“限制”的工具或手段,会引起部分学生的不满,代理服务器常会成为学生“黑客”攻击的目标。

1.5 使用代理服务器集群 (Proxy Cluster)

代理服务器集群是一种实现冗余的设计方式,多台代理服务器组成代理服务器集群,客户机与代理服务器之间,通过域名轮询机制及代理自动配置,可以实现代理服务器间的容错及负载平衡。当用户规模扩大时,可增加代理服务器以满足需求。

1.6 中山大学目前的宿舍代理服务器系统

广州、珠海校区各有一组代理服务器集群,代理类型有 HTTP 和基于 Socks 的代理,提供 HTTP, HTTPS, FTP, POP3, IMAP4, OICQ, PCICQ 等协议的代理。

代理服务器统计(广州校区数据),每天使用人数:1 000 ~ 1 500;每天请求次数:500 万次左右;每天流量:30 ~ 40 GB;缓存命中率:10% ~ 30% (不少于 4 GB)。

1.7 网络工程施工规划

网络工程施工规划主要包括:户外光缆工程规划、户内布线工程规划(机柜、配线架、跳线、网线)、网络设备安装计划、施工中的规范与约定、文档中使用的标记法、线标规范等。

2 实施——规划实现的过程

在实施中对规划的正确性、完善性进行验证,必要时对规划和计划进行调整。

网络工程管理,包括:投标,评标,工程进度、质量跟踪,工程验收与竣工报告等部分。需要提出的是:一方面,加强工程实施中的监管和工程结束时的验收工作,及时发现问题和要求施工方修正;另一方面,充分重视施工文档,对施工方竣工报告的内容必须提出统一的要求(如布线的竣工报告中应包括建筑物的立面图、平面图,图中应注明走线的方向和房间号等)。

评标时应应对投标公司的资质状况、业绩状况、施工方案水平、服务承诺、价格等方面进行认真审查;签约时应特别注意提出对工程验收及服务承诺的要求;而在工程施工阶段,指派专人及学生网管员跟进,不但可及时检查保证工程的质量,更可为将来的维护管理带来经验和便利。工程完成后,应由中心及公司有关人员组成验收小组,共同对工程进行验收。验收范围应包括:①检查图纸、测试报告及有关说明是否齐全;②标签是否清晰明确;③布线是否规范;④进行联通测试;⑤培训有关人员;⑥写好验收报告,双方签字;⑦应将所有资料整理后归档,便于以后查找及维护时调用。

需要指出的是:一般来说,每个学校有十余栋学生宿舍楼,宿舍楼的布线工程会由若干公司完成。每个公司使用的布线系统、施工的方法都有所不同,为了方便以后的维护工作,应该制定“施工规范”(如配线架在机柜的位置,标签的制作及粘贴等),要求各家公司遵守。

总之,网络工程管理是高校宿舍网络建设与管理这一系统工程中非常重要的一环,尤其对运行管理、客户服务阶段有举足轻重的重要意义。

3 管理——长期艰苦的工作

网络的日常管理与维护,是一项长期而艰巨的工作,它是对规划合理性、工程质量的一种验证和考验,如何制订学生用户管理策略是其中重要的一环。

网络运行管理主要有两大部分:学生宿舍网络管理策略的制订和学生用户管理策略的制订,前这主要是从技术方面着眼,而后者则是从与学生用户之间的关系来考虑。

3.1 学生宿舍网络管理策略

网络管理策略制订往往要考虑以下几个因素:①需要控制与管理的深度与广度;②需要管理的层次越深、幅度越大,需要的资源也越多;③策略的可操作性与可被接受性。可以从两个角度进行考虑:从网络管理者的角度、从用户的角度。如果制订的策略必须是管理者容易操作,用户容易接受的;④设备的功能和可管理性;⑤技术人员的专业技术水平。

常用的网络安全策略有:①划分 VLAN,将广播域划分到适当的范围,防止“广播风暴”的发生;②对 IP 地址及适配器地址进行登记管理,以及在路由器上实行 IP 地址及适配器地址绑定;③在路由器上进行包过滤,防止学生“黑客”对校园内别人的计算机进行攻击;④保证服务器安全,除了要保证操作系统的安全还要保证应用服务的安全。需要指出的是:以上所述的主要是保证校园网的安全性。作为管理人员,还必须要制定外网(校园网外)的安全策略,防止从校园网内部发起的对外网的安全侵犯,中山大学宿舍网

使用“私有地址”,使得无法与外网直接相联,在根本上防止了类似事件的发生。

3.2 学生用户管理策略

我们对学生用户的管理策略可以概括为:制定条例、宣传教育、参与自治。

3.2.1 制订条例 管理条例的制订,应该要以现有的法律及法规为依据。目前国家、教育网、广东省教育和科研计算机网都分别制订了计算机网络有关的法律、法规,主要有:《中华人民共和国计算机信息网络国际联网管理暂行规定》、《中国教育和科研计算机网暂行管理办法》、《广东省教育和科研计算机网暂行管理办法》。另外我校在建网之初也制订了《中山大学校园网管理暂行办法》,随着网络不断发展,我们根据学校自身的特点对有关规定进行了补充修改,如学生宿舍大规模联网后,我们对管理办法加以了适当的扩充和细化,目前已经先后出台了三个“办法”及“规定”:《中山大学学生宿舍区联网管理暂行办法》、《学生宿舍上网违规处罚暂行规定》、《学生区联网流量管理办法(暂行)》。

3.2.2 宣传教育 制订了规章制度,我们通过各种形式广为宣传:将有关的管理制度放在网上显著的位置,便于学生查阅;在BBS上开辟栏目,及时张贴。在学生办理入网手续时就向他们发送有关计算机安全的手册,让学生了解应遵守的计算机安全法规、可能出现的安全问题及如何进行防范。采取让学生用户签署认可书的办法,让他们重视有关法规的重要性,同时也为以后在必要时采取处罚行动提供了一个依据。对一些典型的违规行为在网上通报,起警示和教育作用。

3.2.3 参与自治 采取学生自己管自己的策略,让学生兼职网管员参与宿舍网络的建设和管理,主要采取以下几个方面的措施:

(1)制订了《中山大学学生兼职网管员管理暂行规定》,明确了学生网管员的责权利,着重从培养学生能力出发,吸引一批优秀学生参加。

(2)作好组织工作。对学生网管员小组进行培训,定期开会交流,提高网络学生网管员的业务水平和思想水平,可以第一时间了解到学生宿舍网络中出现的新问题,并提出解决办法。实践证明,学生网管员小组能分担相当部分的宿舍网络的维护工作,他们熟悉情况,能迅速及时地为同学服务,方便了学生,出现问题时能协助中心作好解释疏导工作,起到了“上传下达、相互沟通、协调”的作用。但聘请学生网管员也存在某些问题,如因权限和技术水平问题,学生网管员有时不能解决故障;还有经费等问题,这些都需要我们今后不断解决。另外,我们在《学生宿舍上网违规处罚暂行规定》中明确执行连坐原则,使学生之间互相约束,以确保网络的正常运行。

Construction and Management of the Dormitory Network in Campus

SHANG Er-cong^{*}, HE Hai-tao, GU Xiao-hong, DAO Yan

Abstract: In the paper, the practice of the construction and management of the dormitory network in Zhongshan University since 1999, and some technology and management methods are introduced.

Keywords: dormitory network; backbone; topology; DHCP; PROXY; VLAN

^{*} Network and Education Technology Center, Zhongshan University, Guangzhou 510275, China