摘要

伴随着互联网技术的不断发展，各类企业、学校都组建了自己的园区网，人们的工作生活越来越离不开网络，但随之而来的网络安全问题也越来越严重，组建出性能优异且安全稳定的园区网络，已经成为当下网络建设的重要问题。

本项目基于稳定、安全和易于维护的原则，设计一个中大型园区网络，并在GNS 模拟器中进行模拟实现。设计过程中，通过对园区网络的构建与安全防护进行综合分析，采用"模块化，层次化"的思想进行网络规划。首先按照三层网络架构，综合使用 VLAN、MSTP、VRRP、链路聚合等技术，实现内网基本通信；然后使用 ACL、防火墙等技术确保内部网络的安全。项目最终完成了所有网络设备的部署与参数配置，基本实现了网络通信、安全和管理等基本功能。通过测试，所设计的园区网络能够满足不同业务系统的网络需求，同时对于网络信息安全也有一定的保障。

关键字：园区网络；网络规划；网络安全

abstract

With the continuous development of Internet technology, all kinds of enterprises, schools have set up their own park network, people's work and life is more and more inseparable from the network, but the resulting network security problem is becoming more and more serious, formed an excellent performance and safe and stable park network, has become an important problem of the current network construction. Based on the principles of stability, security and easy maintenance, this project designs a network of medium and large industrial parks, and the simulation implements it in a GNS simulator. In the design process, the construction of the park network and the security protection are comprehensively analyzed, and the idea of "modular and hierarchical" is adopted for the network planning. First, according to the three-layer network architecture, VLAN, MSTP, VRRP, link aggregation and other technologies are comprehensively used to realize the basic internal network communication; and then use ACL, firewall and other technologies to ensure the security of the internal network. The project finally completed the deployment and parameter configuration of all network equipment, and basically realized the basic functions of network communication, security and management. Through the test, the designed park network can meet the network needs of different business systems, and also has a certain guarantee for the network information security.

Keywords: Park network; network planning; network security

目录

第 1 章绪论

1.1 研究背景及意义

在飞速发展的信息化社会中，通过网络来获取和交换信息已经成为当今主要的沟通方式之一，即便足不出户，也能做到知晓天下事; 因此，群众对存储在网络中的信息安全意识日益增强。

对于园区网络来说，面对各种恶意扫描，网络攻击，如何保证网络数据安全成为备受关注的问题。就像习总书记说的那样：“没有网络安全，就没有国家安全。”尤其是对于园区网络而言：″保小家才能护大家！″因此，如何组建出性能优异且稳定的网络，已经成为当前时期研发者需要解决的根本问题。

1.2 本项目研究内容

本项目是以某新建园区为研究对象，通过对其进行需求分析来研究如何组建网络稳定、环境安全且扩展性良好的园区网。

在网络建设过程中，严格按照三层网络架构来进行层次划分，根据层次不同选用不同的网络协议。如使用 VLAN 来对网络进行划分，VTP、MSTP 对网络进行统一管理，DHCP 中继实现接入的客户机能够自动接入网络。在网络安全方面，通过对端口信息检测，部署安全策略、防火墙、IPsec-VPN 来对数据进行层层过滤，保护信息安全。

第 2 章关键技术介绍

2.1 路由与交换技术

2.1.1 虚拟局域网技术

虚拟局域网(VirtualLocalAreaNetwork,简称 VLAN)是在物理网络上划分出来的逻辑网络，其划分不受端口的实际物理位置限制，有着和普通物理网络同样的属性。二层的单播、广播、多播帧在一个 VLAN 内转发、扩散，而不会直接进入其他的 VLAN 之中。

按照 IEEE802.1Q 标准，可以将交换机端口设置为 Access 和 Trunk 模式，前者只属于一个 VLAN，用于接入主机或其他网络设备；后者连接多个 VLAN，可以透明传输交换上所有的帧，通过 Trunk 的数据会被打上不同的标签，用于相同 VLAN 之间的数据通信，不同 VLAN 之间想要通信就要借助于三层路由。

2.1.2 链路聚合

为了增强网络的可靠性，引入链路聚合，它是局域网中常用到的一种虚拟化技术手段，能够将网络设备之间的链路形成逻辑意义上的一条链路，通过部署负载均衡策略对通过的数据流量进行分配，如图 2-1 所示：

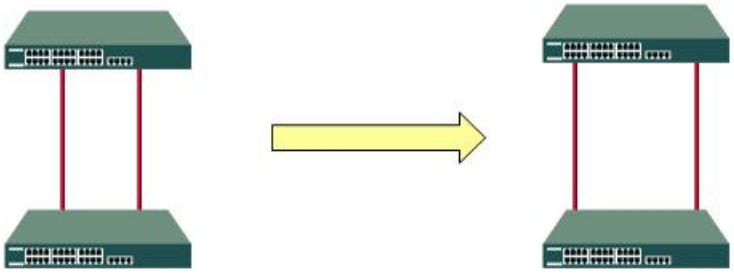

图 2-1

对于接入各楼层的物理设备来说,可以使用堆叠的方式来实现设备的虚拟化，增强网络的稳定性，如图 2-2 所示：

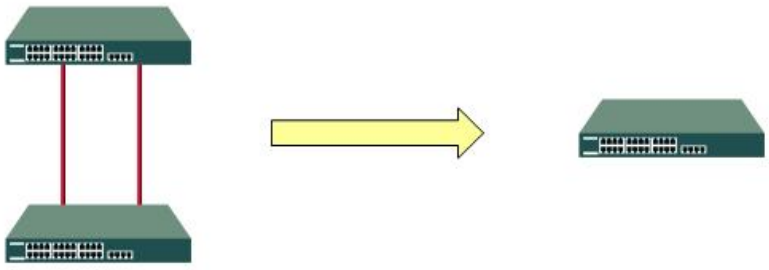

图 2-2

2.1.3 多生成树技术

多生成树技术(MultipleSpanningTreeAlgorithmandProtocol,简称 MSTP)具有 RSTP 的快速收敛机制，是基于实例(Instance)进行生成树计算，能够把 VLAN 映射到实例中，从而实现基于 VLAN 的数据分流；同时一个 VLAN 只能映射到一个实例中，一个或多个 VLAN 可以映射到同一个实例中，从而实现基于 VLAN 的负载均衡。

每个实例独立进行 STP 计算时，不同实例的根网桥可以不同，同一个端口在不同的实例中端口角色和状态也可以不同。如图 2-3 所示：

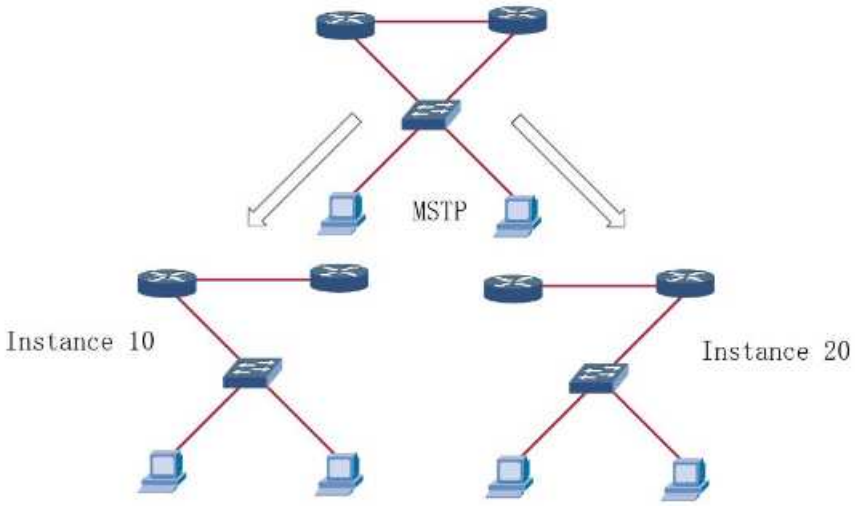

图 2-3

2.1.4OSPF

OSPF(开放最短路径优先)是 IETE 开发的基于链路状态的自治系统内部路由协议，它能够传播对端设备不具有的路由信息，实现网络迅速收敛，避免网络资源浪费；其工作过程主要经历四个阶段：寻找邻居->建立邻居管理->链路状态路由->计算路由。

OSPF 工作过程如图 2-4 所示，其工作原理如下：

(1)通过发送 Hello 包与邻居建立邻居关系；

(2)运行 ospf 的路由器通过 LSA 同步到 LSDB;

(3)每台路由器通过查看自己的路由表，为不同的流量选择最适合的路线。

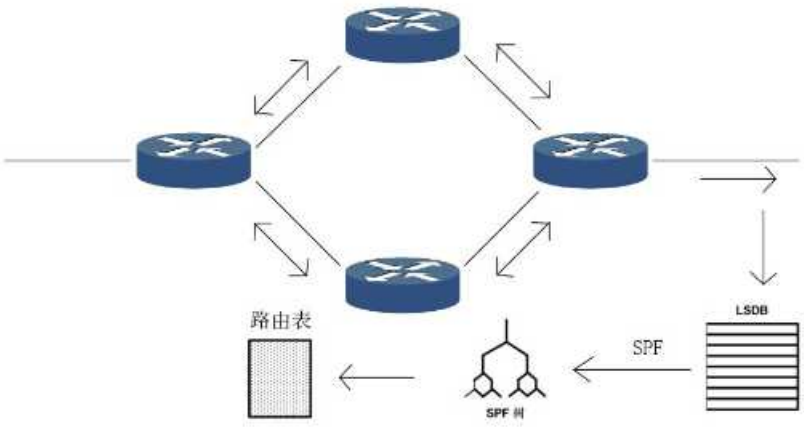

图 2-4

2.1.5DHCP 中继

为了增强网络的健壮性，在核心层部署 DHCP 中继协议，解决 DHCP 客户端不能跨网段获取 IP 地址的问题，这样做的优势是，可以在多个不同网络上的 DHCP 客户端使用相同的 DHCP 服务器，既节省成本，又方便对内部网络进行集中管控和维护。如图 2-5 所示：

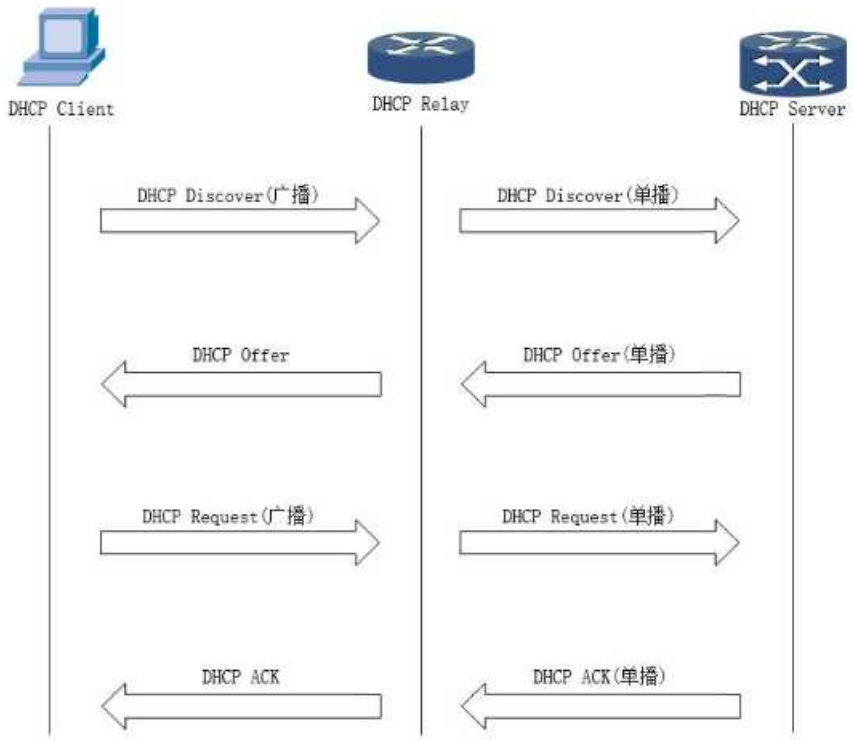

图 2-5

1.1.6VRRP

虚拟路由冗余协议(VirtualRouterRedundancyProtocol),是一种网关冗余协议，通过交互报文，把多台“路由器”虚拟为一台逻辑的“路由器”，主机把这台虚拟路由器设置为网关或者下一跳。由一台物理路由器承担网关的作用，一旦这台物理路由器失效，则由备份路由器自动承担网关的作用。如图 2-6 所示：

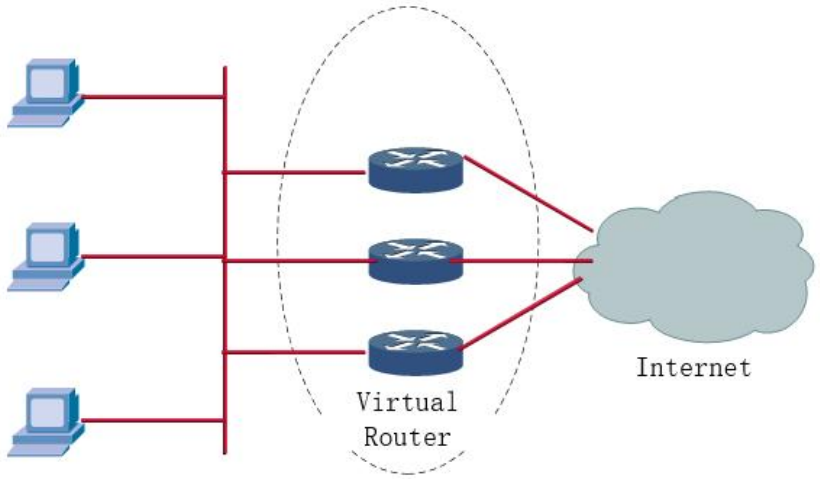

图 2-6

其工作原理是：

(1)VRRP 组(VRID)由多个路由器组成，属于同一 VRRP 组的 VRRP 路由器相互交换报文；

(2)虚拟路由器：有一个 master 和若干个 backup 组成，主机将虚拟路由器设置为网关；

(3)虚拟 IP：虚拟路由器的 IP 地址；

(4)虚拟 MAC：虚拟路由器拥有的虚拟 MAC，虚拟路由器使用虚拟 mac 回应对虚拟 IP 的 ARP 请求；

(5)MASTER 路由器：master 路由器就是在 VRRP 组实际转发数据包的路由器；

(6)BACKUP 路由器：backup 路由器就是在 VRRP 组中处于监听状态的路由器，一旦 MASTER 路由器出现故障，

backup 就开始接替工作。

2.1.7NAT

网络地址转换(NetworkAddressTranslationNAT)主要用来解决 IPv4 地址短缺问题，它能够把私有的内网地址(IP 地址)转换成合法的公网地址，能够有效解决公网 IP 地址不足的问题。