项目五：项目描述

1.1.1 ARP 攻击预防任务描述

某公司已完成了公司园区网的基本建设，采用 VLAN、生成树、路由等技术构建了稳定的三层园区网络结构，并通过 DHCP 分配客户端网络参数，全公司约有 3000 台计算机通过约 150 台交换机联入校园网，需要稳定地访问校园网和互联网资源。在运行一段时间后发现较多用户计算机经常出现网络中断现象，经检查发现在接入交换机层的客户端计算机修改 IP 和 MAC 地址、计算机病毒感染特别是 ARP 病毒、用户计算机启用了 DHCP 功能等多种影响网络正常运行的现象，为保障校园网络的正常使用和稳定运行，请进行规划并实施。

1.1.2ARP 攻击预防任务目标与目的

1． 任务目标

针对公司园区网接入层的网络安全进行防护的实施，预防当前日益频繁的 ARP 病毒与 ARP 攻击。

2． 任务目的

通过本任务进行交换机的 arp 攻击预防技术配置，以帮助读者深入了解交换机基本配置的基础上，具备利用 arp 攻击预防技术提高网络安全性，预防 ARP 攻击与病毒，并具备灵活运用的能力。

1.1.3 ARP 攻击预防任务需求与分析

1． 任务需求

某公司园区网，办公计算机较多，用户计算机经常出现客户端计算机修改 IP 和 MAC 地址、计算机病毒感染、计算机启用了 DHCP 功能等多种影响网络中断的现象，需要保障公司园区网络的正常使用和稳定运行。

2． 需求分析

需求 1：防止计算机因 ARP 病毒感染而影响网络使用功能，或遭受 ARP 攻击的影响而造成损失。

分析 1：采用防 ARP 检测技术，配置 ARP 检查，对伪造的非法 ARP 报文实施过滤，从而预防 ARP 攻击与 ARP 病毒。

需求 2：防止用户计算机启用 DHCP 服务，造成网络 IP 地址管理、分配混乱。

分析 2：采用 DHCP Snooping 技术，过滤掉非法 DHCP 报文，保证网络主机只能从合法的 DHCP 服务器获取 IP 地址及相关参数。

根据任务需求和需求分析，组建公司办公区的网络结构，如图 4-29 所示。

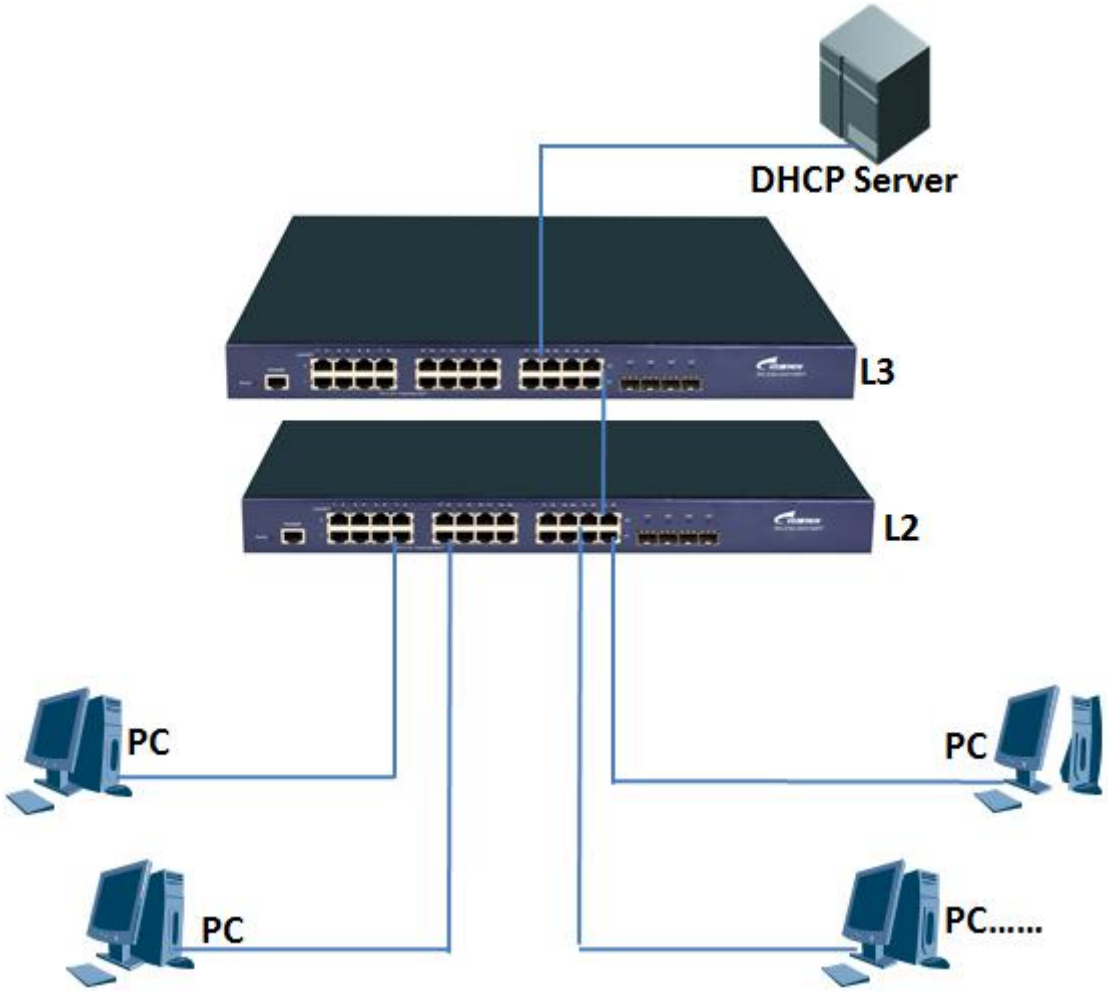

图 4-29 公司网络结构