# 园区网络故障分析与处理

**摘要：**

本文作者依据其所管理的校园网络自身的问题进行分。目的为了分析园区网络的安全隐患，解决园区网络故障，提出了一种利用协议分析的方法，提高园区网络管理的安全性。该方法利用利用协议分析计算机网络病毒、利用协议分析网络攻击（DoS、DDos）、利用协议分析网络带宽滥用、利用协议分析广播与组播、协议分析网络性能、协议分析 MAC 泛洪攻击等方法来了解网络整体健康状态，并根据分析结果。并采用 NAI 公司 Sniffer pro 软件，利用协议分析技术了解网络整体健康状态、利用协议分析技术统计故障原因、应用程序响应时间分析、协议解码分析等办法来分析和应对网络故障。实践证明，利用协议分析法解决园区网络故障，能迅速准确确定网络故障点，可获得较为满意的网络故障排除效果，使园区网络的安全性、稳定性大大提高。

**正文：**

**大学校园网建立于 1996 年，经历三期的校园网络工程建设，已经逐步的成熟，能够稳定的向内提供各种网络服务。其中，校园网三期工程于 2008 年初启动，目的是进一步的增加学校信息接入点的个数，增加邮件服务，同时替换掉一批陈旧的服务器、交换机，全面提升网络质量、将核心交换区扩容到万兆，同时兼顾对 IPv6 网络的支持。我作为该校园信息中心主管，负责整个校园网络的建设、改造、运维等工作。

## 1. 前言

随着计算机及通信技术的飞跃发展，园区内部管理的网络化及信息化成为一种必然的发展趋势。然而，开放的信息系统必然存在众多潜在的安全隐患，网络病毒、网络攻击对园区网的正常运行有重大的影响。利用协议分析技术已经成为网络管理人员必备手段之一，在园区网故障解决应用中，可以准确定位故障点，从而解决实际网络问题。本人从**学校园区网入手，结合实际的网络分析工具及实践经验，详细论述了园区网络故障分析与排除方法。

## 2. 典型园区网概况

某学校校园网共有信息点将近 3，500 个，办公楼区、本科宿舍区、研究生宿舍区、家庭宿舍区。网络出口光纤接入到路由器再连接到防火墙外网口，防火墙 DMZ 区域连至服务器区域如 WWW 服务器、E-mail 服务器、FTP （FileTransferProtocol）服务器、DHCP 服务器、OA 服务器、VOD 服务器等。防火墙内网口连至 3 层核心交换机， 3 层核心交换机通过光纤线路连至汇聚层 3 层交换机，汇聚层交换机主要负责各个楼的接入层设备与各个机房数据汇聚，汇聚层交换机下行通过千兆多模光纤连接各楼层接入交换机。

**3．网络数据包捕获软件的选择**

捕获与分析网络数据包有硬件和软件两种，硬件的分析仪如 FLUKE、HP WAN/LAN 式协议分析仪等。软件通常用的如 Sniffer pro、Wild Packets Omni Peek、The Ethereal Network Analyzer 等，都能实现监视、分析和网络故障检修，形成事件日志，在出现网络故障时了解其运行情况。笔者提出利用协议分析软件解决网络故障的方法与技术，以 Sniffer pro 为主进行测试。网络数据包捕获软件通过捕获到链路的数据包，可以监视网络的状态、数据流动情况以及网络传输的信息，进行分析解决网络故障。而捕获网络数据包，主要有两种方式：一种是采用镜像方式，也就是把交换机某个端口的流量复制到另外一个端口，然后再把端口接入协议分析系统；另一种是采用基于共享式网络使用集线器（Hub）接入方式，可将网络协议分析软件安装在局域网中任意一台主机上，捕获整个网络中所有的数据通讯，这种方式的缺点是在流量高的情况下，对被监控链路的正常工作带来很大影响，因此一般采用在交换机上配置镜像功能，以实现对网络流量的捕获。捕获数据包的 PC 需要将网卡设置为混杂模式。

**4．网络安全分析**

网络安全分析方法有以下几种：

（1）利用协议分析计算机网络病毒

计算机网络病毒主要是借助网络进行扩散传播，利用主机系统自身的安全性与存在的漏洞对网络或主机进行攻击。如威金病毒利用网络共享开放的 445 端口进行传播，此病毒要先进行网络存活主机与共享进行扫描查找，产生大量的 WINS 查询。利用协议分析技术对网络中异常数据进行分析，可以发现大量的 WINS 请求与正常工作的网络状态有明显区别。利用协议分析技术可分析和定位蠕虫病毒的流量。由于大量感染病毒的计算机不断向网络发送数

据包，而且基于 TCP 协议的 SYN 请求的小数据包没有 SYN 确认，目的地址随机，数量很多，使网络效率非常低，降低网络的性能，并导致正常业务无法正常运行。利用协议分析技术也可以分析和定位 ARP 攻击，通过协议分析捕获网络的 ARP 协议数据，并可发现 ARP 攻击的存在，其特征是网络存在大量的 ARP 广播与发往网关的 ARP 回应。利用协议分析技术还可以分析基于 UDP 与 ICMP 协议的计算机病毒的存在。

（2）利用协议分析网络攻击———DoS&DDoS

DoS& DDoS 网络攻击是网络中最有威胁的攻击方式，很难通过技术手段进行防范。对网络中的关键服务设备的特定协议或端口实施的 WWW 服务受到此攻击后，将无法提供正常用户的访问。此种攻击是对网络可用性的攻击，目前有效的解决方案是利用 IPS 技术加以防范，但找到攻击的源头最好的办法是利用协议分析技术捕获流量进行分析后定位，分析的方法与病毒的分析方法类似。

（3）利用协议分析网络带宽滥用

网络带宽滥用主要以 P2P 下载软件的随意使用最为常见，网络带宽滥用可能导致网络的访问性能下降，正常的网络业务无法进行。多数 P2P 软件有固定的协议和端口，可以在防火墙上进行访问控制，但也有一些软件的协议和端口是不固定或其下载是通过 HTTP 协议完成的，在防火墙上很难控制。但它们都有一个共同的特点，就是内部的一个主机与外部建立大量连接，且下载流量很大。利用协议分析技术对内部 IP 协议分别统计流量即可发现占用网络带宽的主机。

（4）利用协议分析广播与组播

网络中大量广播与组播可以导致网络性能急剧下降，甚至无法进行正常通信。其特征非常明显，如广播的目的物理地址为 0xFFFFFFFFFFFF，多播有特定的 MAC 与 IP 地址范围。另外由于链路故障造成的网络环路广播，其特征为目的地址不是广播地址，可能是特定的地址，但有大量重复的数据包在网络中存在，利用协议分析技术可以很容易定位。

（5）协议分析网络性能

还有很多网络问题表现为网络性能很低，网络延迟很大， TTL 返回时间很长。造成网络性能下降的原因很多，如线路损耗、网络设备故障或配置不当等。利用协议分析技术分析

网络中不同地址及协议的响应时间可以有效定位故障原因。

（6）协议分析 MAC 泛洪攻击

此类攻击的特点是在大量网络中不存在源 MAC 地址的数据包发往交换机，耗尽交换机的 MAC 地址表，使交换机对单播目的数据帧进行泛洪。因为单播的数据帧也会发往所有端口，所以利用协议分析技术很容易发现攻击的存在。网络中的安全问题还有很多，都可以借助协议分析技术加以定位和解决。为使网络故障的定位和解决更加有效，就要利用协议分析技术对网络正常工作时的状态进行统计，建立基准，通过协议捕获流量与基准对比分析即可确定是否存在安全问题。

**5．网络安全问题的解决措施**

我们经常使用 NAI 公司的网络协议分析软件 Sniffer pro 来分析和解决问题。把安装有 Sniffer pro 软件的主机连接到关键交换机某一快速端口，以此端口为镜像目的端口，以网络主干所连接的交换机端口作为镜像源端口，对网络中的流量进行捕获，以便于协议分析。

（1）利用协议分析技术了解网络整体健康状态

利用协议分析软件的 Dashboard 可查看网络的利用率、每秒数据包数量和错误数据包的数量，同时可定义一个上限值（阀值）。当协议分析软件统计发现某一项参数超过上限值时，可进行报警、记录并发出通知。一般交换网络的利用率上限在 80%左右，如果超过此上限，则需查找问题所在。

（2）利用协议分析技术统计故障原因

利用协议分析软件的 HostTable 和 Matrix 可以发现特定地址的主机网络带宽滥用行为和节点间实时的连接情况，网络带宽滥用表现为单一内部地址的大量入站与出站数据包和传输速度。也可以发现某一协议的数据量统计。如 HTTP 协议、DNS 协议等，如果发现有大量的 ARP 协议数据，则可进一步利用 DECODE 功能进行分析。

（3）应用程序响应时间

利用协议分析软件的 ART 功能可以有效发现网络性能类故障、计算机病毒和网络攻击的存在。

（4）协议解码分析

利用协议分析软件的解码 DECODE 功能也可以更深层次地了解网络故障，如计算机病毒、广播量和网络攻击的存在。协议分析技术可以解决的问题还有很多，如：利用 History Samples 可创建统计记录与图表，建立基准以供参考。利用 Protocol Distribution 可了解网络协议分布使用统计表，以供分析故障原因等。

**6．小结**

网络故障的原因很多，单纯的维护网络中的关键设备，如：防火墙、路由器、核心交换机、汇聚交换机、接入交换机等，很难找到理想的网络安全解决方案。但是有一点可以确定，几乎全部的安全问题的源头存在或发起于主机，且 80%的安全问题源自内部网络，如病毒、攻击等。通过主机对网络的准入控制及监控和审计可多角度、深层次、大范围扼制网络安全问题的发生。通过客户端安装软件对网络的访问进行验证、审计与监控将是未来网络安全技术手段的发展趋势。