校园网络故障案例分析

XIAOYUAN WANGLUO GUZHANG ANLI FENXI

潘伟锵　主编

华南理工大学出版社
SOUTH CHINA UNIVERSITY OF TECHNOLOGY PRESS

校园网络故障案例分析

主　编　潘伟锵
副主编　王　斌　郭　平　沙立新

華南理工大學出版社
SOUTH CHINA UNIVERSITY OF TECHNOLOGY PRESS

图书在版编目（CIP）数据

校园网络故障案例分析 / 潘伟锵主编. —广州：华南理工大学出版社，2015.8

ISBN 978 - 7 - 5623 - 4743 - 9

Ⅰ. ①校… Ⅱ. ①潘… Ⅲ. ① 校园网–故障诊断–案例

Ⅳ. ①TP393.18

中国版本图书馆 CIP 数据核字（2015）第195499号

校园网络故障案例分析

潘伟锵　主编

出 版 人：韩中伟

出版发行：华南理工大学出版社

（广州五山华南理工大学17号楼，邮编510640）

http://www.scutpress.com.cn　　E-mail: scutc13@scut.edu.cn

营销部电话：020-87113487　87111048（传真）

责任编辑：何丽云

印 刷 者：广州星河印刷有限公司

开　　本：787 mm × 960 mm　1/16　印张：10.75　字数：210千

版　　次：2015 年 8 月第 1 版　2015 年 8 月第 1 次印刷

定　　价：68.00 元

序 言

当今社会，网络已经深入到我们工作与生活的每个角落，并且给我们的工作与生活方式带来了巨大的改变。教育这个古老而崭新的行业当然也不能幸免，正被互联网热切地拥抱着。而高校，作为教育链条的顶端，不仅承担着教书育人的职责，更承担着科研的重任，因此，网络对于高校来说显得尤为重要与特殊。

高校校园网是为全体高校师生提供信息服务、网络教学、网络办公和资源共享等数字化服务的。高校校园网的建设，为高校师生提供了简单、便捷的工作与学习环境，为教育教学的改革提供了有效的技术支撑。同时，校园网的建设，极大地缩短学校与外界环境的距离，促进学校与外界社会的学术沟通和交流，为学校的进一步发展提供了坚实的内在条件。特别是近几年来，我国高等教育体制不断改革，教育信息化发展迅猛，网络技术、教育资源、数据挖掘等相关配套设施的大力研发，校园网在高校教育教学工作中的重要性日益突出。加强校园网建设，提供更智能、更互动的网络在线教学模式，将成为未来我国高校教育教学的主流趋势。目前在我国高校中校园网的应用水平与普及程度，早已成为衡量一所高校办学水平的重要标志之一，成为学校的核心竞争力之一。

我国高校校园网建设经历了三个阶段。第一阶段从1994年到2000年，是起步阶段。那时人们的需求并不清晰，网络应用也仅仅是BBS、电子邮件和FTP等，人们争论的焦点更多地集中在校园网主干技术采用ATM还是以太网之上，网络属于初级普及阶段。

从2000年到2010年这10年时间是第二阶段，这是一个大发展阶段。学校基础设施全面普及，以太网一统天下，校园信息化建设全面

展开，从初期单一的应用系统建设到现在的数字化校园平台，目标是实现流程的打通、数据的流通。

从2011年开始进入高校信息化建设的第三阶段，也就是我们经常所说的智慧校园阶段。这一阶段无线网络覆盖校园，用户体验得到改善；更多的物联网(传感器)遍布校园，更多的数据采集和分析；移动应用将为更多的人所使用，从硬件基础设施到各类应用都将得以整合；流程得以梳理整合，数据得以打通和挖掘。

进入智慧校园阶段之后，信息部门的主要工作是整理需求，制定规划，细化应用。部分的应用将通过购买第三方的云端服务来提供，常规的运行维护将通过外包的方式交给专业的第三方服务公司。

大多数高校的信息化经过这20来年的建设，都颇具规模。基础的网络环境都已覆盖校园的每个角落，各类应用系统都已部署应用。在此基础上，保证网络环境、应用系统的平稳运行将是一种常态。高校的用户群体更集中，也很活跃，具有探索精神，从而令网络运行过程中出现的故障更多样，更复杂。

编者常年在信息部门工作，长期从事教育信息化应用与研究工作，基于多年的网络维护经验，把常见的网络故障进行了收集、分类和归纳分析，希望本书成为信息部门的 FAQ，供我们的客服、一线技术人员和最终用户参考。本书由华南理工大学高级工程师潘伟锵任主编、由广东工贸职业技术学院高级实验师王斌、广东交通职业技术学院副教授郭平、淮安市淮安区广播电视台工程师沙立新任副主编。第一章由潘伟锵、王斌、郭平和沙立新共同编写，第二章由潘伟锵和王斌编写，第三章由潘伟锵和郭平编写。在此，感谢相关单位的信息化主管部门及相关人员对本书编写的配合与支持。

编　者

2015年6月

专业术语

名称	解　释
空口	Air Interface，指空中接口
LSA	链路状态通告（Link-State Advertisement），LSA被路由器接收用于维护它们的路由选择表
OSPF	开放式最短路径优先(Open Shortest Path First)，是一个内部网关协议，用于在单一自治系统内决策路由
STP	生成树协议(Spanning Tree Protocol)，可应用于环路网络，通过一定的算法实现路径冗余
ARP	地址解析协议(Address Resoloution Protocol)，是获取物理地址的一个TCP/IP协议

目 录

第一章

网络故障分析

1. 校园无线网出现AP无法动态获取IP地址，而PC却能获得地址

故障描述 >>>>>>>>>>>>>

（1）AP无法成功注册到AC上：AC收不到任何有关该AP的报文，该AP无法动态获取地址；

（2）使用PC替换AP设备后，PC可以成功获取地址并正常工作；

（3）通过抓包和调试可以发现AP已经正常发送了DHCP discover报文申请IP地址，但没有收到DHCP offer报文，而通过DHCP server信息发现已经收到了discover报文并且回应了offer报文。

问题原因 >>>>>>>>>>>>>

从DHCP server到AP位置的有线网络的广播报文不通（可通过ARP验证）。

分析和说明 >>>>>>>>>>>>>

（1）PC发出的discover报文中的bootp flags为unicast类型，这样DHCP server回复给其的DHCP offer报文就以单播unicast方式发送。

（2）而AP发送的DHCP discover报文中要求DHCP offer以广播报文发送，此时DHCP服务器的回应报文为广播报文。

总结 >>>>>>>>>>>>>

DHCP协议本身就支持这两种方式的协商，但是由于中间网络的问题，造成了广

播offer报文无法到达AP，导致了AP无法获取地址，最终无法成功注册到AC设备。

2．WLAN用户ping丢包问题如何定位

WLAN网络中，ping操作很多时候都作为验证网络通路状况的一种手段。当ping出现丢包或者伴随着大延时，在应用上就会出现网络不稳定、速度慢等现象。

用于定位的一些命令 >>>>>>>>>>>>

与该特性相关的常用的调试命令如表1所示。

表1　常用调试命令

维护命令	命令说明
reset counters interface	清除所有统计信息（AP用户模式）
display cpu-usage task	显示各任务的CPU利用率（AP隐藏模式）
display interface Ethernet	显示以太网口的统计信息（AP任意模式）
display ar5drv [1|2] radio	显示指定Radio的基本信息（AP隐藏模式）
display ar5drv [1|2] statistics	显示指定Radio的统计信息（AP隐藏模式）
display ar5drv [1|2] queue all	显示指定Radio的队列信息（AP隐藏模式）
display ar5drv [1|2] station all	显示指定Radio的Station列表（AP隐藏模式）
display ar5drv [1|2] station <aid>	显示指定Radio上指定Station的统计信息，aid可以从display ar5drv [1|2] station all查到（AP隐藏模式）

需要特别关注下面几个命令。

1）display ar5drv [1 | 2] statistics

（1）每个Radio有4个普通发送队列和1个紧急发送队列，通常数据报文都走1号队列，因此我们主要关注1号队列。

（2）TxDiscardFrame表示此队列丢弃的报文总数，包括发送失败和队列溢出的报文。

（3）NotEnoughResource表示队列溢出的报文。

（4）TxDiscardFrame/ TxUcastFrameCnt表示丢包率，如果超过3%的时候就

应当警惕了。

（5）RadioResetOnErr意味着Radio芯片复位，会导致丢包。正常情况下不应当出现这个错误。

2）display ar5drv [1 | 2] queue all

（1）这个统计可以看出各个队列的使用情况，FrameCount不为0表示有报文积压。偶尔的几个报文积压不会引起什么问题，但长时间积压上百个报文就应当引起警惕。通常我们主要关注AC1（即1号队列）。

（2）目前AC0-AC3队列的默认长度为324，当FrameCount持续保持300以上时，通常就会引起队列溢出导致丢包，这个也会在display ar5drv [1|2] statistics中的NotEnoughResource同步体现出来。

3）display ar5drv [1 | 2] station all

这个统计可以看出指定Radio下连接的所有Station，每个Station分配了一个内部的AID。

4）display ar5drv [1 | 2] station <AID>

一是关注Station的信号强度(RSSI)，二是关注AP向Station发送报文的速率。

问题基本定位分析 >>>>>>>>>>>>

采用“二分法”的思想，分段对丢包问题进行定位。可以按照图1所示流程进行排查。

图1 丢包定位流程图

1）初步判断无线客户端运行状态

通过命令“display wlan client mac-address 0019-d20b-6f4d verbose”可以获知关于客户端的详细信息，其中主要关注RSSI、SNR、Rx Rate、Tx Rate、Up Time几个参数的变化值。

RSSI和SNR反映的是无线客户端在AP处的信号强度，需达到30以上才能保证客户端正常应用。当该值（目前这两个值是一回事）比较低时，需要设法提高用户的信号强度，否则不但其自身表现不好，也会影响到该空口中其他用户的使用表现。

RX Rate记录了AP接收无线客户端的报文速率。如果该值始终保持在低速率（如1、2、11），可能其所处环境丢包比较严重，需要关注空口状况。偶尔的速率变化是正常现象，因为报文的发送是一个动态调整的过程，与信号强度、重传次数、误码率等因素有关。

Tx Rate记录了AP向无线客户端发送报文的速率。如果该值始终较低，同样需要关注空口环境状况。

Up Time记录了无线客户端的在线时间。Up时间如果比较短，则需要考虑该用户是否出现过漫游，因为漫游过程可能会出现零星丢包。通过命令display wlan client roam-track mac-address 0019-d20b-6f4d可以查看客户端的漫游情况。

2）判断无线空口质量

使用命令“display ar5drv [1|2] statistics”判断丢包率，如果低于1%说明空口质量还可以。空口分析是比较复杂的，涉及AP自身问题、AP干扰问题、非WLAN信号干扰问题等。一个信道的空口能力最多22M左右，在多台AP使用相同信道并且互相可见的情况下，当空口转发能力已经饱和时，必然会有AP出现丢包。如果信道充斥大量小包报文时，虽然没有达到22M，但空口的占用率实际已经饱和了，必然会有AP出现丢包。另外，不合理的网络规划带来的隐藏节点问题，无谓的空口冲突等都会降低空口的性能，增加错包概率，导致丢包发生。

可通过软件AirMagNet查看空口环境，分析信道占用率和吞吐量，以及空口报文速率组成和占用比例，如图2所示。

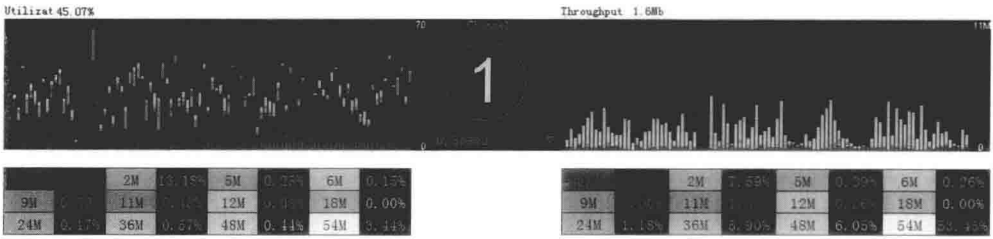

图2 空口环境

导致空口丢包的原因还有几个可能：一是进入AP的报文持续大于空口的发送能力，必然会导致发送队列溢出而丢包；二是AP射频卡芯片出现问题，导致报文发送不出去；三是对空口忙闲的判断出现错误，导致不发送报文，常见的有蓝牙、无绳电话、微波炉等干扰源的影响。

3）判断有线网络问题的测试

采用ping操作，从AC到AP，从AP到AC进行检验，看丢包是否严重。统计AC、AP上下行有线口是否存在明显的错误统计。排查上行链路中报文流量是否饱和，从而淹没ping报文。还可以镜像AP或者AC的端口进行抓包分析，或者抓无线网卡的报文分析，分析ping request和ping reply的交互情况，看是否发生丢包。

4）出现丢包情况下空口报文分析

（1）首先观察出现丢包是否有固定周期，有没有时间上的规律，每次丢包的持续时间是否固定。这个主要关注是不是由于一些特殊的原因而造成的丢包，通常是外界的原因。

（2）出现问题时，使用前面提供的命令收集信息。

（3）单纯的空口抓包分析。建议使用Omni Peek空口抓包，然后进行分析。每一个单播报文的发送都需要ACK的确认。根据抓包情况，按照如下思路分析：

①如果收不到ACK确认（Station没有发送ACK，或者AP没有收到Station发送的ACK），则会进行报文重传；

②从AP到Station以及从Station到AP都遵循这个规律；

③AP设备默认重传次数为5次，Station重传次数不定；

④如果抓包中连续出现多个相同的重传报文而没有ACK报文，说明该报文可能丢失；

⑤根据报文MAC地址，可以确定是AP到Station丢失，还是Station到AP丢失。

丢包定位之全面抓包对比分析 >>>>>>>>>>>>

如果上面的抓包还是不能确认问题，可能还要考虑在多个点同时进行抓包，然后进行对比分析。下面为相关操作的说明。

（1）空口报文要抓取。

（2）可以在AP的上行接口抓包。

（3）可以在无线客户端上使用Ethereal抓无线网卡收发报文。

（4）登录AP，打开debugging ar5 1/2 phy error output verbose命令进行相关分析。

（5）空口报文分析参见“单纯的空口抓包分析”中的描述。

（6）可以通过ICMP报文中的序列号，在多个抓包信息和调试信息中进行对比分析，看看报文到底丢失在什么位置。

（7）对于空口加密报文，由于内部数据无法获知，只能通过猜测匹配。

图3为ping的序列号的位置。

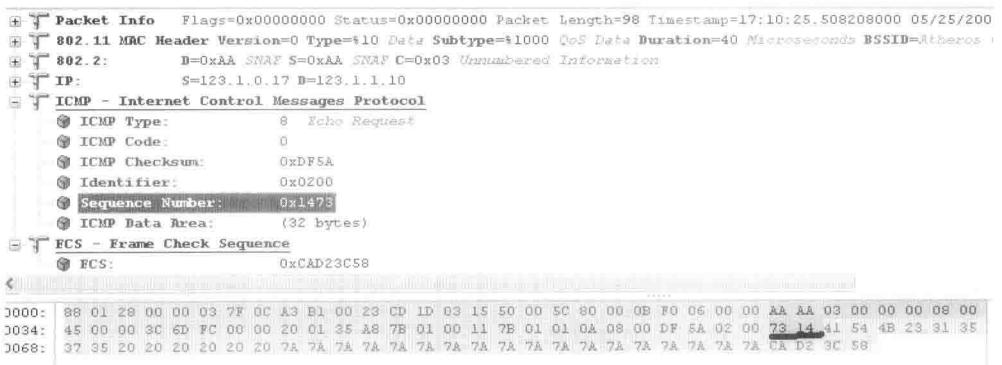

图3 ping的序列号位置

3. 校园无线网络信号覆盖很好，信号可见度高，但干扰严重，用户使用不稳定

无线网络的干扰问题是无线维护工作中最难对付的，而对无线网络干扰的消除工作也是贯穿无线建设工作始末的一项任务。目前，针对无线网络干扰的优化是一项系统工程，从信息采集到信息分析，然后再到优化方案输出，涉及无线侧和数据侧两部分的优化，尤其对于无线校园的覆盖，从覆盖方式到参数调整，都需要进行合理的规划设计。

无线校园作为目前WLAN使用比较集中的热点区域，其反馈的问题也很多，集中在网络使用稳定性和带宽要求两方面。对于带宽的要求，需要根据实际用户数以及客户需求进行AP数量的有计划增加，同时结合用户负载均衡功能以及合理的信号覆盖方案，减少同信道干扰，整体提升网络容量。而对于稳定性的满足，需要综合多方因素进行调整，涉及覆盖方式的调整，信道的合理规划，干扰源的排查，用户使用业务特征的调查和相应针对措施，有线网络或者无线攻击源的排查，用户数的变化，以及无线参数的优化配置。

信号空间可见度高的问题，可以通过修改覆盖方式，如采用功分天线，将天线伸入房间的方式，隔离空间的信号可见度。干扰的排出，一是合理调整信道，包括不同楼层间的信道；二是调整设备功率，降低可见信号干扰程度。

无线校园的业务主要以小包为主，而小包比例的突出会严重降低信道的使用效率，从而降低信道容量，使得用户数据吞吐量整体降低。这种情况下，建议做无线空口限速，然后就是做用户隔离功能，减少不必要的广播报文和一些非法泛洪报文的影响。

空口上的优化也是必要的，可以减弱无线干扰带来的影响。比如调整Beacon发送间隔，提高重传次数以及适时开启RTS/CTS功能，都能够在一定程度上提高网络的稳定性。

4. 高校网络访问速度慢的探究和分析

故障现象描述 >>>>>>>>>>>>

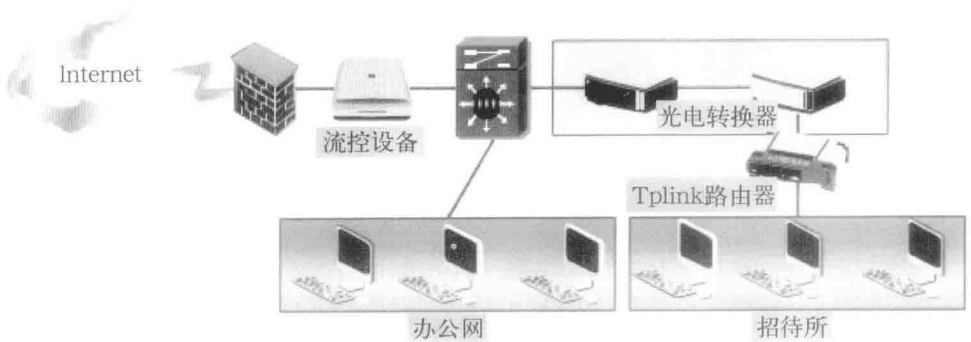

图4 用户基本网络拓扑

用户为一招待所，基本网络拓扑如图4所示，整个网络环境主要是通过核心交换机连接一个流控设备，然后流控设备再连接到防火墙，通过防火墙上网。招待所的网络通过连接一台Tplink 路由器进行了地址转换，将所有从招待所出去的主机地址都映射为一个地址：192.168.30.253。

整个学院的网络主要分为办公网和家用网两部分，故障出现在招待所网络，而办公网没出现故障。招待所内的主机要上网，打开网页的速度非常慢，特别是像sina这样的图片很多的网站，甚至是访问本学院对外的web服务器也很慢。但是一旦把招待所网络全部断掉，用一台机器直接连接在招待所的路由上访问，打开速度却非常正常，而且在出现故障时，我们通过ping 测试发现ping 网站的延时只有几十毫秒，也没有严重的丢包现象。

分析目标 >>>>>>>>>>>>

确认Internet访问速度慢是由于网络原因引起的，还是其他原因引起的，我们可以实地捕获招待所计算机对互联网访问的数据流进行分析，通过访问的整个过程来分析判断访问速度慢的原因是由于网络时延、丢包，还是其他原因引起的。

分析设备部署 >>>>>>>>>>>>

我们在招待所交换机上、学院核心交换机上部署分析设备，镜像网络流量，对访问互联网的流量进行捕获并进行分析，如图5所示。

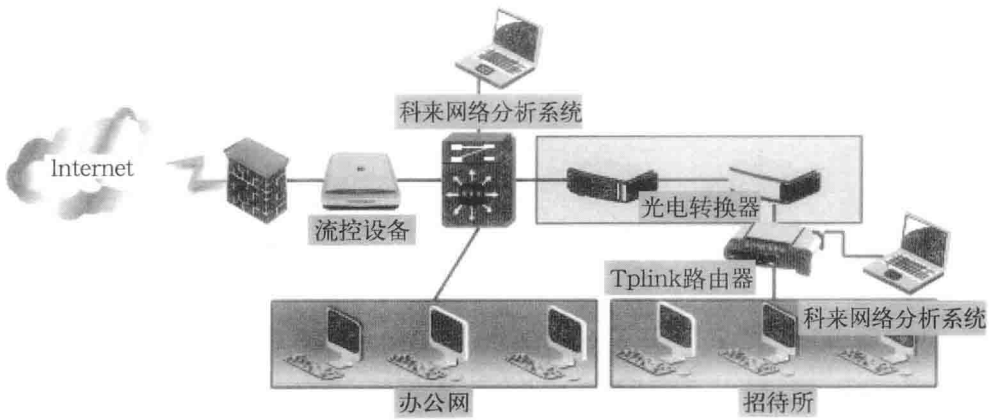

图5　分析设备部署

分析情况 >>>>>>>>>>

1）在招待所捕获的对外访问的数据分析

首先在招待所捕获一个我们对外web服务器访问的数据流，然后对该数据流进行详细解码分析，如图6所示。

图6 TCP会话数据包

TCP会话分析中，我们得到该数据流的如下信息：

数据流持续时间：1分17秒，也就是这个访问整个持续的时间。总字节数：57KB。

从上面的数据上我们可以看到，整个访问的总字节数只有57KB，但整个时间用了1分多钟，确实是非常的慢。

2）解码分析详细的会话过程

（1）三次握手时间。

通过解码分析详细的访问过程，我们发现这个数据流的三次握手时间很短，只有不到1毫秒，说明网络的时延很短。

（2）服务器响应。

通过分析服务器响应的数据包，服务器对get请求的响应为145毫秒，响应速度正常。

（3）数据传输时间。