

用网络通讯分析系统监控广播风暴思科认证 PDF转换可能丢失图片或格式，建议阅读原文

[https://www.100test.com/kao\\_ti2020/644/2021\\_2022\\_\\_E7\\_94\\_A8\\_E7\\_BD\\_91\\_E7\\_BB\\_9C\\_E9\\_c101\\_644084.htm](https://www.100test.com/kao_ti2020/644/2021_2022__E7_94_A8_E7_BD_91_E7_BB_9C_E9_c101_644084.htm) 网络风暴产生的原因

网络不正确的设计和规划。网络设备或者设备的损坏

；HUB做为广播设备本身容易导致；网卡或者交换设备的损坏也可能产生广播风暴。网络环路；路由配置错误，或者在

没有启用STP的交换设备上出现“两端”同时接入错误。其它：

网络病毒本身具有感染后向网内大量扩散传播的特性，也可导致广播风暴。广播风暴的检测 Step1 建立广播数据包

过滤器 点开“过滤器-从过滤器列表”，选择“Broadcast”。

Step2 检测广播风暴的相关参数 用科来网络通讯分析系统进行

捕包（由于已经建立好广播包过滤器，这里所捕获的数据全是广播数据包），然后统计相应的参数。1.统计参数：广播

数据包字节数 广播数据总数 每秒包个数 数据包大小分布 协议类型……（根据自身的网络添加）怎样利用这些参数：我们

这里以100M以太网为例，100M网络每秒的最大数据

为 $12.5M * 1024 = 12800 \text{ Byte/S}$ 。如果网络中广播数据包的每秒数接近或大于此值，网络就存在“广播风暴”了。数据包的总数

、个数以及大小的分布，根根网络的大小而不尽相同，如果发现根网络正常时的值相差较大，也要引起注意。协议类型

主要是统计所占流量最大的协议。这里要注意区分ARP请求

与ARP应答的关系，ARP请求是广播，而ARP应答是单播；如果通过过滤器捕获到ARP协议占用了较大的流量，那网络中

就存在“ARP扫描”，此时我们可以切换到“诊断”视图进行

定位。2.数据包的IPID标识 我们知道，IPID唯一的标识了

数据报或数据报的流；如果网络某一协议所占的流量大，我们可以通过“数据包”视图来查看它的IPID，如果相同，那我们可以判断影响当前网络运行是由网络环路造成的。在当前，网络环路是造成广播风暴的主要原因之一。3.查看网络利用率 怎样利用网络利用率参数 利用率分为位利用率和利用率百分比，我们来看一下网络利用率的计算过程：网络中的实时流量即每秒位数（在“概要视图”中查看）除以网络带宽（100M以太网或1000M以太网）。通常在以太网中，利用率达到50%就已经是非常好的网络了，所以如果广播数据包的利用率达到30%以上，也就是说在100M以太网中广播数据达到30M/S时，那网络中就存在“广播风暴”了。100Test 下载频道开通，各类考试题目直接下载。详细请访问 [www.100test.com](http://www.100test.com)