



科来网络应用故障分析表

故障现象	故障详细描述	故障原因分类	故障详细成因	故障分析定位方法	推荐解决方法
网络、应用访问缓慢	1、同一VLAN的内网主机之间访问速度非常缓慢，如互相PING，网上邻居拷贝文件等操作。	网络丢包	网络设备丢包	利用科来网络回溯分析系统采用多段部署的方式，在网络中关键设备的两端进行数据包对比，确定该设备是否丢包，从而准确定位丢包设备。	1、更新存在问题的设备配置。 2、更换存在问题的网络设备。
	2、不同VLAN间的主机，访问速度非常缓慢。		网络拥塞	利用科来网络回溯分析系统监控关键链路（一般是出口链路）的流量占用情况，查看网络利用率是否过高，每秒数据包是否过多，数据包大小分布是否合理、TCP会话是否正常等各项。	1、如果网络拥塞的原因是P2P、病毒、攻击等异常流量引起的，需对这些流量进行控制。 2、如果网络拥塞的原因是网络带宽过小，应考虑增加网络带宽。
	3、内网主机可以打开网页，但速度非常缓慢。		MTU配置不当	通过科来网络回溯分析系统采集关键链路数据，查看传输MTU值，再查看网络中关键设备的MTU配置。	设定合适的MTU值。
	4、内网主机PING外网域名或DNS服务器时，返回时间较大。		网络攻击	通过科来网络回溯分析系统监控关键链路，实时发现网络中的异常网络攻击，根据科来智能诊断，快速判断网络中是否存在异常网络攻击。	根据智能诊断判断的地址进行排查，封堵。
	5、网络中的各种应用出现时断时续的现象。	网络延迟大	负载均衡设备配置不当	利用科来网络回溯分析系统通过多段部署方式，监控流量通过负载均衡后被分配情况，确定是否是由于负载均衡设备把数据包分配到错误的链路引起丢包。	合理配置负载均衡策略
	6、内网主机打开网络中某业务系统时，响应非常缓慢，甚至出现假死状态。		设备延迟	利用科来网络回溯分析系统采用多段部署的方式，在网络中关键设备的两端进行数据包对比传输的TCP数据包时延，分析并定位造成延迟的设备。	1、更新引发延迟设备的配置。 2、更换引发延迟的网络设备。
			传输距离延迟	利用科来网络回溯分析系统监控关键链路，分析TCP连接中三次握手数据包的时间间隔，查看客户端网络延迟、服务端网络延迟，定位延迟位置。	采用多连接或其他传输层协议，避免网络延迟给TCP传输带来的影响。
		应用响应慢	带宽延迟	利用科来网络回溯分析系统监控关键链路，通过分析TCP传输的性能，确定是否存在带宽延迟。通过计算传输的数据量和链路带宽容量，来确定带宽对传输延迟的影响。	增加网络带宽
			TCP连接慢	利用科来网络回溯分析系统捕获应用通讯数据，通过定义应用直接查看三次握手时延，及客户端、服务器端时延，快速判断TCP连接较慢是发生在客户端还是服务器端。	提升网络传输过程中的传输性能。
		相关应用服务响应慢	应用交易处理慢	利用科来网络回溯分析系统捕获应用通讯数据，通过定义应用直接查看客户端请求时间和服务器响应时间，判断服务器是否存在应用交易处理响应慢的现象。	提高服务器自身硬件性能或优化应用软件性能。
			DNS服务器响应慢	利用科来网络回溯分析系统捕获DNS通讯数据，分析DNS请求和响应数据包，查看是否存在DNS服务器响应慢的现象。	优化DNS服务器的软硬件配置。
			数据库服务器响应慢	利用科来网络回溯分析系统捕获数据库通讯数据，分析后台数据库的交易处理请求和响应数据包，查看是否存在数据库交易处理慢的现象。	优化数据库服务器的软硬件配置，优化数据库操作脚本。
网络、应用无法访问	1、内网主机不能与互联网的任意应用进行通信，如网页、邮件、QQ、FTP等都不能使用。	网络不可达	其他相关服务慢	利用科来网络回溯分析系统捕获应用通讯数据，分析其他相关服务的交易处理请求和响应数据包，查看是否存在交易处理慢的现象。	优化相关服务的软硬件配置。
	2、内网主机PING不通DNS服务器，网站域名。		物理链路中断	通过PING定位断点，查看网络设备和物理链路状态，确定是否存在链路中断。	恢复链路的连通性。
	3、内网主机可以上QQ，但打不开网页。		网络设备宕机	通过PING定位断点，查看网络设备和物理链路状态，确定是否存在网络设备宕机。	恢复设备正常运行。
	4、内网主机不能访问网络某个特定的应用服务。		严重丢包	利用科来网络回溯分析系统监控关键链路，查看链路中TCP数据流是否存在大量重传，如果有，则表明网络中存在大量的丢包情况。通过PING目标主机确认是否存在大量丢包。同时通过分段捕获分析数据包定位丢包设备。	1、如果丢包的原因是P2P、病毒、攻击等异常流量引起的，需对这些流量进行控制。 2、如果丢包的原因是某个设备丢包，可考虑对其进行重新配置或更换。
			拒绝服务攻击	利用科来网络回溯分析系统监控关键链路，通过智能报警系统快速判断网络内是否存在拒绝服务攻击，并迅速定位攻击源。	定位攻击源，并对其阻断。
			路由不可达	利用科来网络回溯分析系统监控关键链路，分析捕获到的包中是否存在目的不可达的ICMP数据包。通过tracert命令分析不可达的目标地址路由。	更新路由器的路由配置。
		应用不可达	策略中断	利用科来网络回溯分析系统采用多段部署的方式，在网络中安全设备的两端进行数据包对比，定位中断点，查看是否是由于防火墙等安全设备的访问控制策略阻断了应用通讯。	修正防火墙等设备上的访问控制策略。
			应用宕机	利用科来网络回溯分析系统捕获应用通讯数据，自定义应用并对应用进行监控，出现应用宕机时通过应用警报及时预警。	检查服务器端的应用服务状态。
			应用拒绝服务	利用科来网络回溯分析系统捕获应用通讯数据，根据科来智能警报查看并定位产生攻击的地址。	受到DOS/DDOS等攻击，查找并阻断攻击源。
		应用无响应	策略中断	利用科来网络回溯分析系统捕获应用通讯数据，查看是否存在服务器无法接收到客户端连接请求，或出现连接建立被重置的现象。	修正防火墙等设备上的访问控制策略。
			应用故障	利用科来网络回溯分析系统捕获应用通讯数据，可自定义应用并对应用进行长期监控，可以查看应用请求与响应状态，如果出现服务器未响应请求，则服务端可能出现问题。	检查应用的工作状态，查找应用的BUG，或重启应用，重启服务器。
		相关应用无响应	DNS服务器无响应	利用科来网络回溯分析系统捕获DNS通讯数据，分析相关的DNS请求和响应数据包，查看是否存在DNS服务无法正常解析应用地址情况，导致无法连接应用服务器。	检查DNS服务器软硬件情况，恢复DNS服务。
			数据库服务器无法连接	利用科来网络回溯分析系统捕获数据库通讯数据，分析相关的数据库请求和响应数据包，查看是否存在数据库服务器没有响应，导致无法提供正常交易处理。	检查数据库服务的配置，确保数据库服务正常。
			其他相关服务无法连接	利用科来网络回溯分析系统捕获应用通讯数据，分析其他相关服务器的交易处理情况。	优化相关服务的软硬件及策略的设置，确保服务的正常提供。

