

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	通过分段捕获的方法，在网络中关键设备的两端，使用科来网络分析系统进行抓包，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。	
			网络拥塞	1、在核心交换机上配置镜像，使用科来网络分析系统抓包。	2、更换存在问题的网络设备。	
			2、分析关键链路（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。	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。		
		MTU配置不当	查看网络中关键设备的MTU配置。	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。		
		2、不同VLAN间的主机，访问速度非常缓慢。	网络延迟大	设备延迟	通过分段捕获的方法，在网络中关键设备的两端，使用科来网络分析系统捕获传输的TCP数据包，分析定位造成延迟的设备。	设定合适的MTU值。
		传输距离延迟		1、在核心交换机上配置镜像，使用科来网络分析系统抓包。	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。	
	2、分析TCP连接中，三次握手数据包的时间间隔，确定链路的延迟情况。					
	3、内网主机可以打开网页，但速度非常缓慢。	带宽延迟	1、在核心交换机上配置镜像，使用科来网络分析系统抓包。	增加网络带宽		
	2、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。					
	5、网络中的各种应用出现时断时续的现象。	网络应用响应慢	TCP连接慢	使用科来网络分析系统在服务器端抓包，捕获客户端的连接请求，查看TCP三次握手的时间间隔，定位服务器是否存在TCP连接慢的现象。	提升网络传输过程中的传输性能。	
			应用交易处理慢	使用科来网络分析系统在服务器端抓包，端捕获客户端的连接请求，查看服务器针对请求的响应时间，定位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。	
	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。	相关应用服务响应慢	DNS服务器响应慢	使用科来网络分析系统在DNS服务器端抓包，分析DNS请求和响应数据包，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	使用科来网络分析系统在数据库服务器端抓包，分析后台数据库的交易处理请求和响应数据包，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。	
其他相关服务慢			使用科来网络分析系统在相关的服务器端抓包，分析其他相关服务的交易处理请求和响应数据包，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。		
网络应用无法访问	1、内网主机不能与互联网的任何应用进行通信，如网页、邮件、QQ、FTP等都不能使用。	网络不可达	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。	
			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。	
			严重丢包	1、在核心交换机上配置镜像，使用科来网络分析系统抓包。	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、分析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。		
				3、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。		
			路由不可达	1、在核心交换机上配置镜像，使用科来网络分析系统抓包。	更新路由器的路由配置。	
	2、分析捕获到的包中是否存在目的不可达的ICMP数据包。					
	策略中断	3、通过tracert命令分析不可达的目标地址路由。				
	2、内网主机PING不通DNS服务器，网站域名。	网络应用不可达	应用宕机	通过分段捕获的方法，在网络中关键设备的两端，使用科来网络分析系统进行抓包，定位中断点，查看是否是由于防火墙等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。	
			应用拒绝服务	使用科来网络分析系统在服务器端抓包，如果都是服务器拒绝客户端的连接请求情况，且进程中没有相应的应用进程，为应用出现宕机。	检查服务器端的应用服务状态。	
			策略中断	使用科来网络分析系统在服务器端抓包，如果应用进程正常，但服务器主动拒绝客户端的连接请求，则为应用拒绝服务。	受到DOS/DDOS等攻击，查找并阻断攻击源。	
	3、内网主机可以上QQ，但打不开网页。	网络应用无响应	策略中断	使用科来网络分析系统在服务器端抓包，如果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，则是有设备进行了通讯阻拦。	修正防火墙等设备上的访问控制策略。	
			应用故障	使用科来网络分析系统在服务器端抓包，如果客户端连接能正常建立，但服务器对交易处理请求无响应，则为应用故障。	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。	
DNS服务器无响应			使用科来网络分析系统在DNS服务器端抓包，分析相关的DNS请求和响应数据包，如果DNS服务器没有响应，则无法正常解析应用地址，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			使用科来网络分析系统在数据库服务器端抓包，分析相关的数据库请求和响应数据包，如果数据库服务器没有响应，则应用无法正常提供数据，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。		
4、内网主机不能访问网络某个特定的应用服务。	相关应用无响应	其他相关服务无法连接	使用科来网络分析系统在其它相关服务器端抓包，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配置，确保服务的正常提供。		