检测非业务应用路由(针对windows)Cisco认证考试 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/557/2021_2022__E6_A3_80_E6_B5_8B_E9_9D_9E_E4_c101_557852.htm 检测非业务应用路由(针对windows)：一些大型企业和单位由于网络规模大，IP地址分配不是全面覆盖，部分员工没有合法IP地址，不可以上互联网。导致员工私接路由器上网的问题屡禁不止，这种非法接入路由的行为危害有多大，我就不多说了（环路隐患、占用带宽、工作效率低下等），这给网络管理员带来了很大问题！经初步实践，下述两种方法对检测非业务应用路由有所帮助（工具：科来网络分析系统）：方法1：TTL值排除法（要求对网络拓扑十分了解）原理:Windows操作系统定义，pc机的应用服务生成的数据包的初始TTL值为128，根据路由的原理，数据包每被路由一次，TTL值就要减1，所以，以私接路由器IP地址为源地址生成的数据包的TTL值最大为127；因此根据实际的网络拓扑和捕获的数据包的TTL值可以判断是否使用了私接路由器！1）.在总工程节点下的端点视图下，对流量和网络连接数大的节点作记录，然后分别定位到相应的节点作具体分析！2).定位到相应的节点后，在数据包视图下，查看相应的源地址是本机的数据包的TTL值。3）.由于Windows操作系统定义，pc机的应用服务生成的数据包的初始TTL值为128，根据路由的原理，数据包每被路由一次，TTL值就要减1，所以，以私接路由器IP地址为源地址生成的数据包的TTL值最大为127；因此根据实际的网络拓扑和捕获的数据包的TTL值可以判断是否使用了私接路由器！ 100Test 下载频道开通，各类考试题目直接下载。详细请访问