

使用第二层路由跟踪进行排错思科认证 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\\_\\_E4\\_BD\\_BF\\_E7\\_94\\_A8\\_E7\\_AC\\_AC\\_E4\\_c101\\_644538.htm](https://www.100test.com/kao_ti2020/644/2021_2022__E4_BD_BF_E7_94_A8_E7_AC_AC_E4_c101_644538.htm) 通过tracert ip的方式来排除网络故障，相信很多人都非常的熟悉。这是基于IP地址(第三层)路由跟踪，可疑用来排除大部分的网络故障。而使用第二层路由跟踪，其跟第三层路由跟踪非常的相似。其一个本质的区别就在于第二层路由跟踪是基于MAC地址来进行跟踪的，并解决第二层连接的故障。在确定第二层拓扑中数据传输的路径，这个第二层路由跟踪将是一种非常有用的工具。

一、tracert ip的缺陷 tracert ip虽然在排错过程中具有很大的作用，基本上是每个网络管理员必须要掌握的内容。但是在实际应用中其仍然有一定的局限性。如现在用户反映客户端访问文件服务器的速度非常的慢。为了查明原因、排除故障，网络管理员需要先知道客户端与服务器的IP地址。然后通过tracert ip命令，查看客户端与服务器之间的连接是否正常，如是否出现拥塞、数据传输的路径是否合理、有没有出现丢包现象等等。但是如果客户端与服务器之间的网络拓扑比较复杂，那么处理起来仍然会比较麻烦。即使查明了问题发生的原因，也很难查清楚这个问题到底是发生在哪一段。所以tracert ip命令使用的时候有一定的局限性。其比较容易查明问题发生的原因，但是对于问题到底发生在哪个位置，有时候会有点束手无策。特别是在拓扑结构比较复杂的时候，可能只有通过排除法来查明故障点。如此的话，工作量就会比较大。

二、第二层路由跟踪能够精确定位故障点 当遇上上面这种情况时，第二层路由追踪就会非

常的有用。因为通过第二层路由跟踪，可以仅仅使用MAC地址来跟踪网络中的设备连接。如对于直接连接的子网设备，第二层路由追踪命令可以将IP地址作为命令的一部分使用等等。在知道了服务器与客户端的IP地址后，通过查询ARP表，就可以确定它们的MAC地址。然后就可以通过“tracert mac mac地址”命令来定位故障点。

### 三、第二层路由跟踪的前提条件

由于第二层路由跟踪是基于MAC地址的，所以在使用的时候，比tracert ip命令有更多的前提条件。网络管理员必须了解这些内容，以免在排错的时候，做了无用功。其限制条件还是比较多的，具体来说，有如下几条。

- 一是需要主要网络设备所使用的软件版本不同，其会有不同的限制。如思科网络设备中，如果其部署的是CatOS系统，则正在进行排错的设备(如用户终端)必须与sc0或者slo接口处与相同的子网中。而如果交换机使用的是ios软件的时候，则被跟踪的设备必须与交换机上配置的SVI(交换机虚拟接口)处于相同的子网中。这是一个非常严格的限制条件。特别是对于那些平时不怎么接触思科网络设备的用户来说，这一点需要牢牢记住。否则的话，可能得到的结果反而会误导用户排错。
- 二是协议上的限制。如要使用第二层路由跟踪功能，则必须在网络中所有的交换机和接口上运行CDP协议，并且这个CDP协议的工作状态必须是正常的。CDP协议又成为思科发现协议。其主要用来获取相邻设备的协议地址以及发现这些设备的平台。有些时候，网络管理员可能出于安全等考虑，会将这些协议关闭掉。但是如果启用第二层路由跟踪功能，则需要启用这些协议。并且需要确保这些协议工作正常。否则的话，系统返回的信息，会跟实际的情况有所差距，从而影响

管理员的正确排错。通常情况下，在实际排错过程中，利用这个功能之前，笔者都会事先确认CDP协议是否开启并且工作正常。切记，这是一个必须要做的过程。三是交换机规格的限制。现在并不是思科的所有产品都是支持第二层路由跟踪的。对于源和存在问题的设备之间的所有中间交换机，都必须要求支持L2路由跟踪特性。大部分的思科设备现在都支持这个特性。只有那些比较早期的，如2950等产品，需要软件升级之后才能够使用。由于其不怎么引人注目，所以在实际工作中特别容易让人忽视。故笔者在这里特别强调一下。可见，在使用第二层路由跟踪的时候，还是有比较严格的限制的。不过这些限制条件，并不影响其使用价值。在一些复杂的拓扑结构中，网络管理员还是乐意使用这个命令。虽然在前期需要花时间确认这些条件是否满足。

#### 四、第二层路由追踪执行实例简介

假设现在有一个客户端，其MAC地址为AAAA.AAAA.AAAA.0001。还有一个文件服务器，其MAC地址为AAAA.AAAA.AAAA.0002。现在用户反映从客户端访问文件服务器的速度特别的慢。由于企业的网络拓扑比较复杂。从客户端到文件服务器中间要经过五个交换机、两个路由器。在这种情况下，使用tracert ip命令虽然可以查明问题的原因，但是无法精确定位故障点。此时就需要使用基于第二层的路由追踪。通过查询ARP表，可以知道服务器的MAC地址。通常情况下，在执行第二层路由跟踪功能的时候，只要知道目的MAC地址或者交换机的MAC地址，管理员就可以选择网络中的任何交换机。如可以执行命令 `tracert mac AAAA.AAAA.AAAA.0001 AAAA.AAAA.AAAA.0002`命令，来查看这个客户端与服务器之间的连接是否存在问题。有时

候为了缩小范围，也可以将目标MAC地址或者源MAC地址替换掉，如替换为中间交换机的MAC地址。一步步缩小范围，最终就能够精确的定位故障发生的点。显然，通过使用第二层路由追踪得到的结果，可能帮助管理员集中精力对源和目标设备之间的链路进行分析与排错，而管理员不用担心构建的网络图或者复杂的拓扑结构。简而言之，只要知道客户端与服务器以及中间所有交换机的MAC地址，那么只要坐在电脑之前，网络管理员就可以通过不断的执行第二层路由追踪，查询到故障发生的点。点找到之后，再根据原先的网络图纸，找到故障交换机的位置。找到故障计算机后，就可以对其进行排错、维修。要么重新启动、要么升级软件、要么更新等等。这就是后话了。只要能够精确的定位故障点，找到故障的交换机等网络设备，其他一切都简单了。有时候网络排错之所以耗费大量的时间与精力，主要的原因就是找不到问题到底发生在哪里。显然使用第二层路由跟踪功能帮助管理员解决了这个问题。为了尽快找到故障点，这其中还有一个小技巧。其实这就好像是一个差数字的游戏。告诉你数字的范围，如1到100。然后让你猜一个数字。如果猜错的话，就重新给你一个范围。如你猜的是50，如果错的话，那么就会告诉你一个新的范围1到50。在使用第二层路由追踪缩小范围的时候，跟这个猜数字的游戏类似。如果不怎么清楚网络的拓扑图，为了尽快缩小范围，则这当中也会有一些技巧。如尝试命令的时候，可以采用中间值的方式。即如果中间有10个交换机，则可以先在客户端与第5个交换机之间进行测试。采用中间值的方法，可以大幅度减少测试的次数。当中间设备越多，这个方法的效果会越明显。综上所述，第二层

路由跟踪是一个非常有用的排错工具。管理员可以坐在终端前面，确定网络任何两台交换机之间是否存在着故障。在比较复杂的拓扑网络中进行排错的时候，第二层路由跟踪可以帮助管理员精确定位故障点，为解决故障争取宝贵的时间。

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)