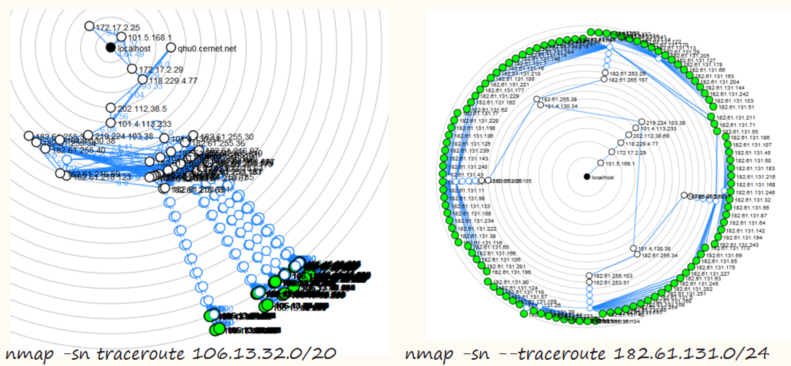
网络拓扑探究

我们使用 Zenmap，一个用于 nmap 的跨平台图形用户界面应用程序，来了解我们 AS 的结构和拓扑。 为了对我们的网络进行相对较快的扫描，我们使用了 nmap 的 traceroute 技术来了解跳距和网络结构。 下面显示了两个示例扫描。

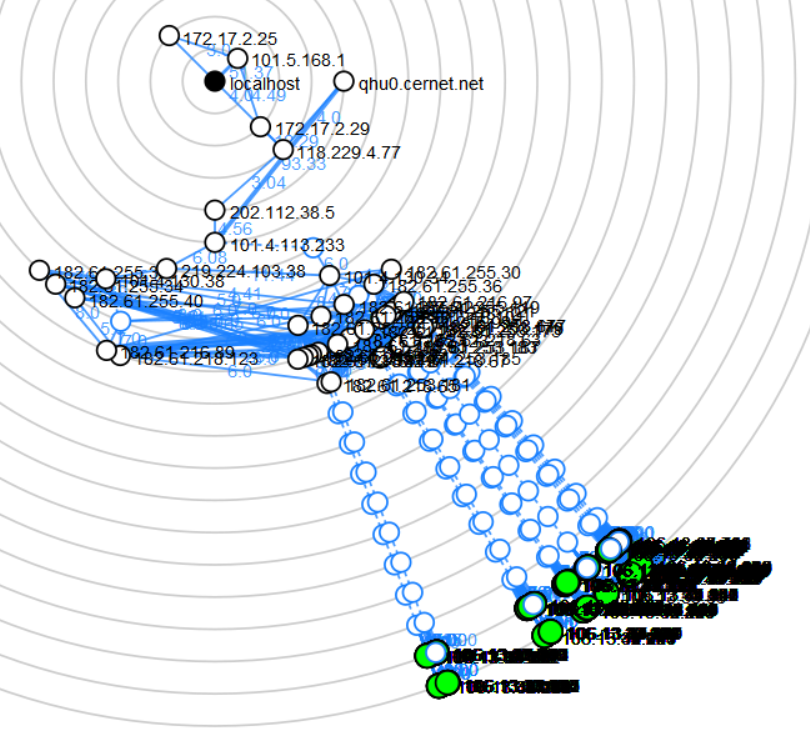
如何看图:

1. 白色圆圈表示网络路径中的中间主机未被端口扫描。
2. 绿色圆圈代表开放端口少于 3 个的端口。(但是其实没有扫端口)
3. 网络距离显示为同心灰色环。 每增加一个环就意味着距离中心主机多一个网络跃点
4. 如果跃点没有 RTT（缺少 traceroute 条目），则连接以蓝色虚线显示，建立连接的未知主机以蓝色轮廓显示。

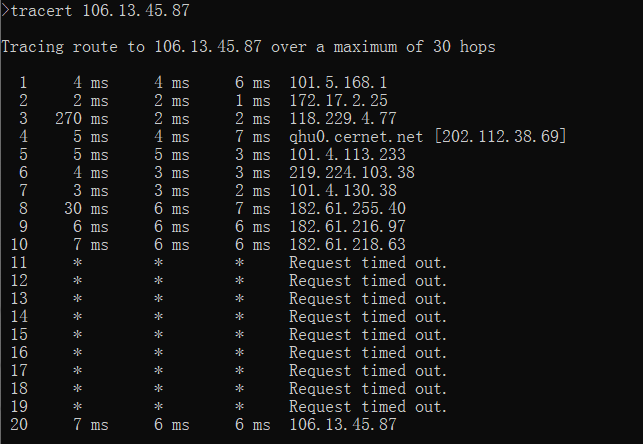
命令描述

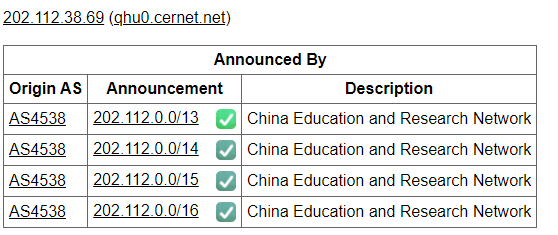
* -sn：禁用端口扫描
* -T4 -T<0-5>：设置timing template(时序模板)（越高越快），提高质量和性能
* -A：启用操作系统检测、版本检测、脚本扫描和跟踪路由
* -v 增加详细程度

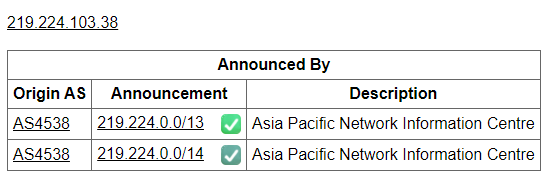
我们以上面左图做分析

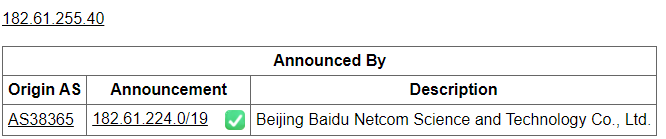


因为我们使用了nmap的traceroute功能，所以我们可以和tracert（Windows系统）进行对比，看看是否可以得到类似的结果

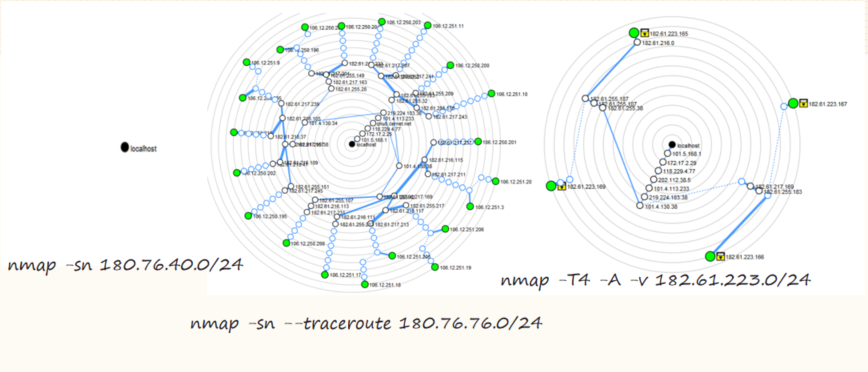
、

\* 代表图表上的白色圆圈。 并且使用 bgp.he.net，我们可以看到我们必须穿过哪个 AS 才能到达我们的目的地





可以看到，最初是从CERNET AS开始，然后穿过亚太网络信息中心，最后到达北京百度网通科技有限公司，这就是我们要分析的AS。这里有几个使用 zenmap 创建的图表。



我们还可以看到，所有图的前几跳都是相同的，这意味着每次都有一致的路径。我们可以看到一些图形不包含任何可以使用 nmap 找到的可见主机（绿色圆圈）。 可能设置了防火墙以防止数据包到达某些主机。由于 zenmap 基于 nmap，它包含了更多上图中未使用的功能。 例如，它可用于显示主机有多少开放端口、主机是什么类型的设备以及是否设置了防火墙。

