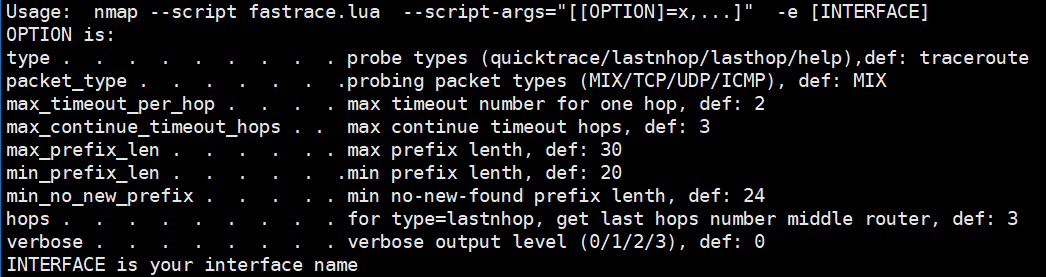
Fastrace 说明文档

1.介绍

Fastrace是一个拓扑测量工具，对于目标和子网，能够执行不同类型的拓扑测量。Fasttrace可以执行的探测类型有normaltrace、treetrace、quicktace、lasthop、lastnhop，其功能参数如下图所示。



* 参数说明：

verbose:输出日志详细程度，0，1，2，3等级，仅对拓扑测量有效

packet\_type:发送探测包类型，仅对拓扑测量有效

type:执行命令类型，末跳探测(last\_hop/lastnhop)/拓扑测量(默认)/quicktrace(快速traceroute)

hops：仅对lastnhop有效，仅探测倒数第hops跳

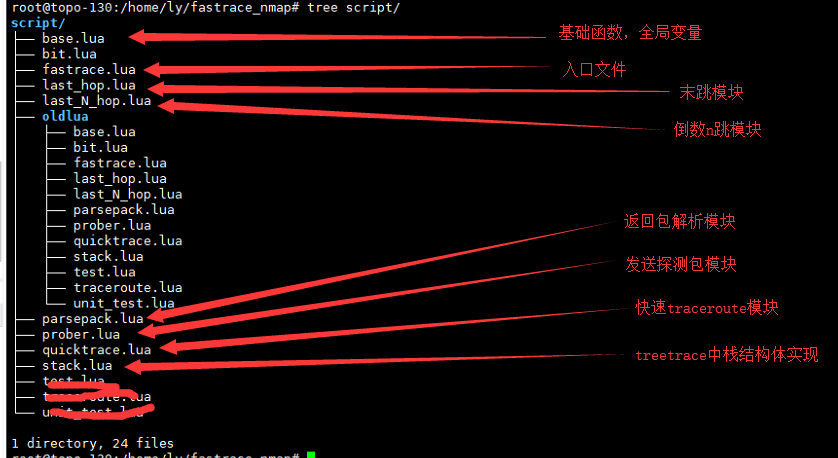
*注：参数如果没有type，默认执行单目标或子网tracroute*

* 工具位置：10.10.11.130:/home/ly/fastrace\_nmap/script

Github: <https://github.com/yiqiaoxihui/fastrace_nmap>

脚本：<https://github.com/yiqiaoxihui/fastrace_nmap/tree/master/script>

* 文件结构



1.1单个目标traceroute

* 命令示例：

nmap --script fastrace.lua --script-args="

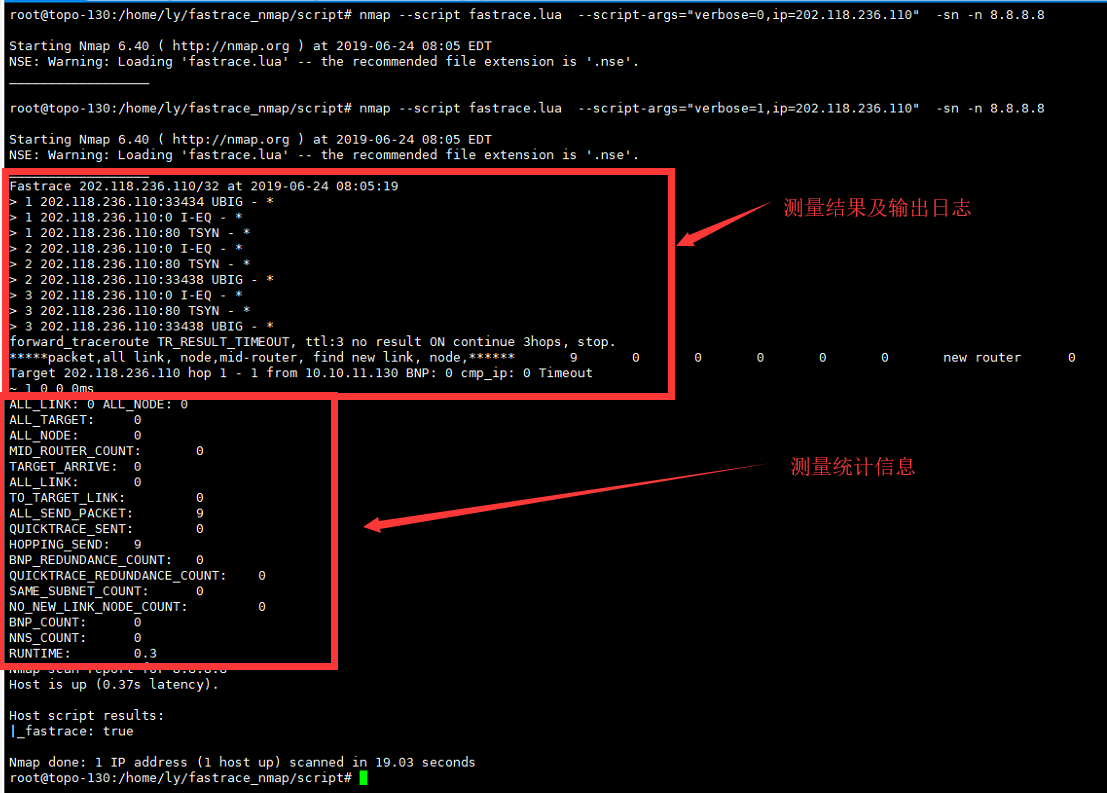
verbose=1, //输出日志等级

ip=36.56.0.0, //traceroute目标

output\_type=file, //输出文件，无此参数默认输出控制台

output\_filename=fi36.56.0.0\_20.min24" //输出文件名

-sn -n 8.8.8.8 //固定，默认让nmap选择外网网卡



1.2子网探测

命令示例：

nmap --script fastrace.lua --script-args="

verbose=1,

ip=36.56.0.0/20, //探测目标网段

max\_prefix\_len=26, //网段划分到这里，必须停止

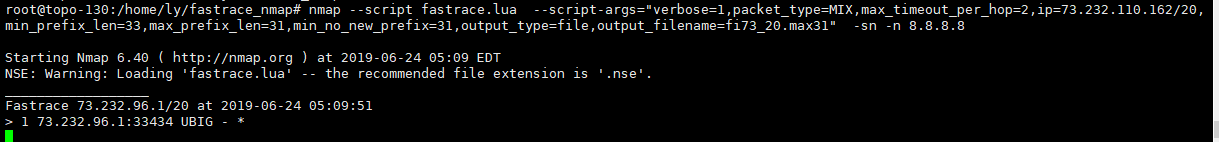
min\_prefix\_len=20, //网段两端目标具有相同末跳，停止前缀

min\_no\_new\_prefix=26, //未发现新边，节点时停止的前缀

output\_type=file, //将测量结果写入文件

output\_filename=fi36.56.0.0\_20.min24" //写入文件名称

-sn -n 8.8.8.8



* **关键技术：**

1. 将目标网段划分成更小网段，对子网段进行正向反向探测，直到覆盖该网段内的全部目标（max\_prefix\_len=31）
2. NNS:参考路径为超时终止，目标也在最大跳超时，终止探测。原始程序存在问题：终止探测时未更换不同探测包，一次超时就终止，导致本能发现的目标未能发现。本程序已改进，NNS时，更换全部类型探测包探测，但是只要使用NNS终止正向探测，还是会有目标未能发现。
3. 反向探测停止:反向探测遇到相同路由器接口，停止探测，实验发现，目标平均最大跳数为15，反向探测停止时跳数为12，1到11跳均不用探测。

* **测试参数指标**

1. max\_prefix\_len.测试时设为31，即对目标网段全部目标测量，对于/20网段内全部4096个目标探测发现，发现路由器接口平均为200个，而发现目标数目平均为2000个，目标数目远大于中间路由器数目。因此，max\_prefix\_len只有设置为最大31，才能发现全部目标，否则，总有目标未发现。max\_prefix\_len每增加1，测量目标扩大2倍，发现目标数目大约也扩大二倍。
2. min\_prefix\_len:目标与参考路径末跳相同时停止探测的前缀，小于max\_prefix\_len时有效。未测试该参数变化对测量结果的影响。事实上，只要未覆盖测量网段内全部目标，总有目标未发现。
3. min\_no\_new\_prefix\_len:本次正向反向探测未发现新边和新节点时停止探测。未测试该参数变化对测量结果的影响。事实上，只要未覆盖测量网段内全部目标，总有目标未发现。

* 结果处理脚本

见2.2

1.3quicktrace

一次发ttl=1到30的包

命令示例

nmap --script fastrace.lua --script-args="

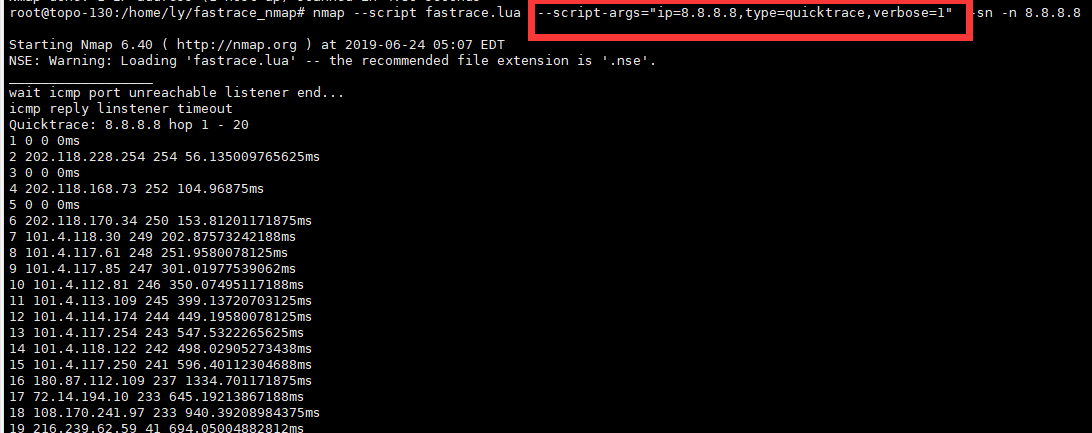
ip\_file=ip/ip112\_20,

output\_type=file,

type=quicktrace,

verbose=1,

output\_filename=quicktrace/fi112\_20.quicktrace" -sn -n 8.8.8.8



1.4lastlhop

对目标列表进行末跳探测

type= last\_hop

命令示例：

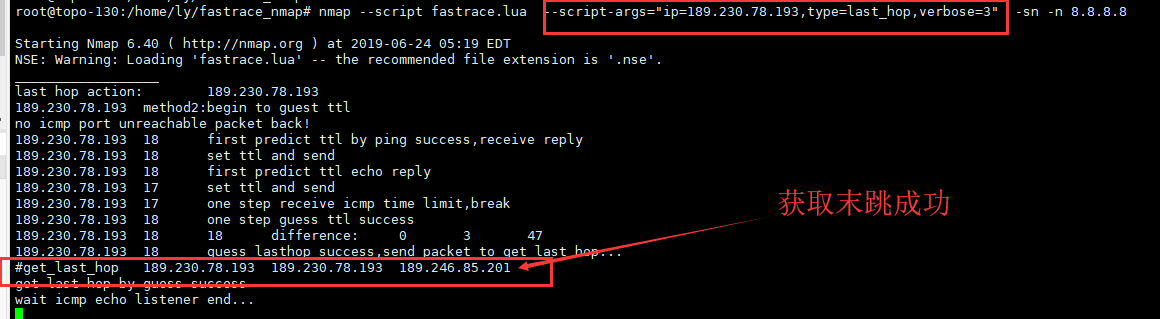
nmap --script fastrace.lua --script-args="

ip\_file=ip/ip112\_20,

type= lastl\_hop,

verbose=1

" -sn -n 8.8.8.8



* 结果处理脚本

见2.3

1.5lastnhop

获取倒数n跳

type= lastnhop

hops= hops

命令示例

nmap --script fastrace.lua --script-args="

ip\_file=ip/ip112\_20,

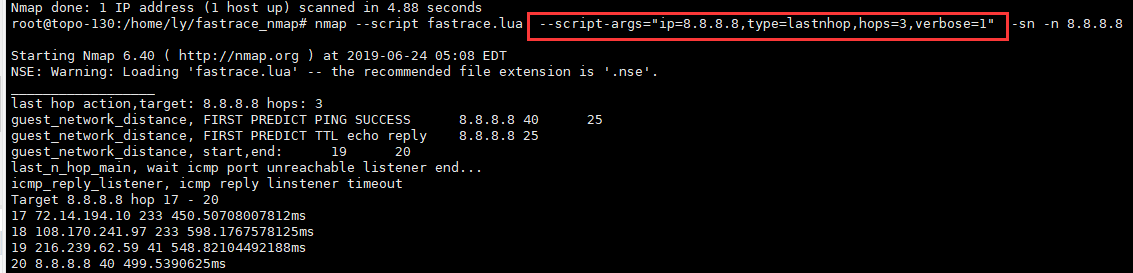
output\_type=file,

type= lastnhop,

hops=3,

verbose=1,

" -sn -n 8.8.8.8



2.其他脚本

位置：10.10.11.130：/home/ly/fastrace\_nmap/python\_script

Github:<https://github.com/yiqiaoxihui/fastrace_nmap/tree/master/python_script>

2.1 [scamper\_json\_get\_link\_node.py](https://github.com/yiqiaoxihui/fastrace_nmap/blob/master/scamper_json_get_link_node.py)

从scamper json格式数据统计边节点信息

脚本位置：

例如：python [scamper\_json\_get\_link\_node.py](https://github.com/yiqiaoxihui/fastrace_nmap/blob/master/scamper_json_get_link_node.py) 输入文件

2.2[get\_link\_node\_from\_fastrace.py](https://github.com/yiqiaoxihui/fastrace_nmap/blob/master/get_link_node_from_fastrace.py)

从fastrace子网探测输出文件中统计节点，边信息

例如：python [get\_link\_node\_from\_fastrace.py](https://github.com/yiqiaoxihui/fastrace_nmap/blob/master/get_link_node_from_fastrace.py) 输入文件

2.3 extract\_lasthop\_result.py

末跳输出结果处理脚本，统计末跳获取量，写入文件

例如：python extract\_lasthop\_result.py /home/ly/nmap\_script/realtest/ip.10w.combine 1

参数 1：输入文件 /home/ly/nmap\_script/realtest/ip.10w.combine为末跳初始原始数据文件

参数2：1表示统计末跳IP写入文件，文件名在输入文件名后加”.lh”