Department of Informatics

BGP AND DNS

Network Security

Diego Sempreboni

INTRODUCTION

In this lab, you are going to have some hands-on experience with both BGP and DNS. You will see how IP packets make it from one point in the Internet to another, you will connect to a real Internet router serving millions of people, you will make different types of DNS queries and understand real examples of DNS attacks, and you will be able to graphically visualise the Internet and some of its AS.

HOW DO YOU GET FROM HERE TO THERE?

In this question, you will attempt to identify how routes are constructed across the Internet. The standard tool to look at the route from your machine to some other machine is traceroute.

First of all, yourself with traceroute. For that you can run:

```
man traceroute
```

Try traceroute on an internal and an external site. e.g.:

```
traceroute google.com
```

Explain what you see. Also count the number of hops between you and the other computer.

A different way is to see the list of ASes you need to pass through. You can look at the BGP tables from any number of so-called “looking glass” routers on the Internet. You can find a list here:

https://www.bgp4.net/doku.php?id=tools:ipv4_route_servers

Pick a server and telnet to it. For example:

```
telnet route-server.ip.tiscali.net
```

(you will get prompted to log in as public user with public password, just do it)

Then at the prompt given by the looking glass router, you can type in a Cisco command. e.g.:

```
show route <ip_address>
```

You can use any ip address you like - e.g. you can get the ip address for google.com from when you used traceroute and try it.

You really are at the command prompt of a real, live, router on the Internet! Type in

```
show ?
```

to see this.

Try some of the other commands.

WHO OWNS SOME INTERESTING PART OF THE INTERNET?

As discussed in the class, the Internet is made of a number of autonomous systems. It is sometimes interesting (as well as important) to figure out who owns some part of the Internet. One tool to use for this is the whois database. You can have a look at the WHOIS primer here: http://whois.icann.org/en/primer

RIPE NCC maintains the database within Europe. Have a look at its FAQ:

https://www.ripe.net/data-tools/db/faq

Figure out your machine's IP address (what command would you use, from previous practicals?). Then look up who owns that IP address, by looking up on the RIPE database: https://apps.db.ripe.net/search/query.html
Did your query return anything??

You may also issue a whois command from your linux command prompt:

```
whois <IP-addr>
```

Any more clues now after seeing the output of whois as to why you could not find your IP address?? **(do not continue until you know - you can check with your TA to be sure)**

If you are behind a router (and indeed you are in the labs), then your computer will not know about the public IP address as the router does a network address translation. You could ask some website what your public IP address is using `curl` or `wget` (two Linux tools to get HTTP resources) and extract the information you need from it. You can do for instance:

```
curl https://ipinfo.io/ip
```

This is basically the same as opening a browser and putting https://ipinfo.io/ip in the URL field - try it!

The external IP address is what identifies you on the Internet. If you have a broadband service at home, you have probably just one external IP address, generally assigned by the service provider. However, universities and companies might have bought a series of external IP addresses to handle the network infrastructure. It might be that the external IP address of the classmate close to you is different than yours. Check this!

Now, try again to search for that external IP address in the RIPE database and using the whois command as above to see if you can get from there who this external IP address belongs to. Does it make sense? **(check with your TA you got it)**

WHO SI CALLED WHAT?

As seen in the lectures, DNS names map from human readable and more memorable names to IP addresses which are routable. Read about DNS here:
https://danielmiessler.com/study/dns/

You can fetch DNS information using the program dig. Have a look at how to use dig here:

https://www.madboa.com/geek/dig/

Now, use dig to demonstrate that KCL has outsourced its e-mail operations to outlook.com

(do not continue without being sure you have demonstrated it - check with your TA)

DNS is critical to Internet security. One of the most sophisticated attacks on DNS was discovered by Dan Kaminsky. [optional] You can read about this
here: http://unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html
and about Dan Kaminsky on Wikipedia.

A GRAPHICAL VIEW OF THE INTERNET

Go to http://bgp.he.net and explore! Enter your machine's IP address, and check out more information about KCL's AS number (what is it?), its upstream connectivity, etc.