Introduction to mini-internet

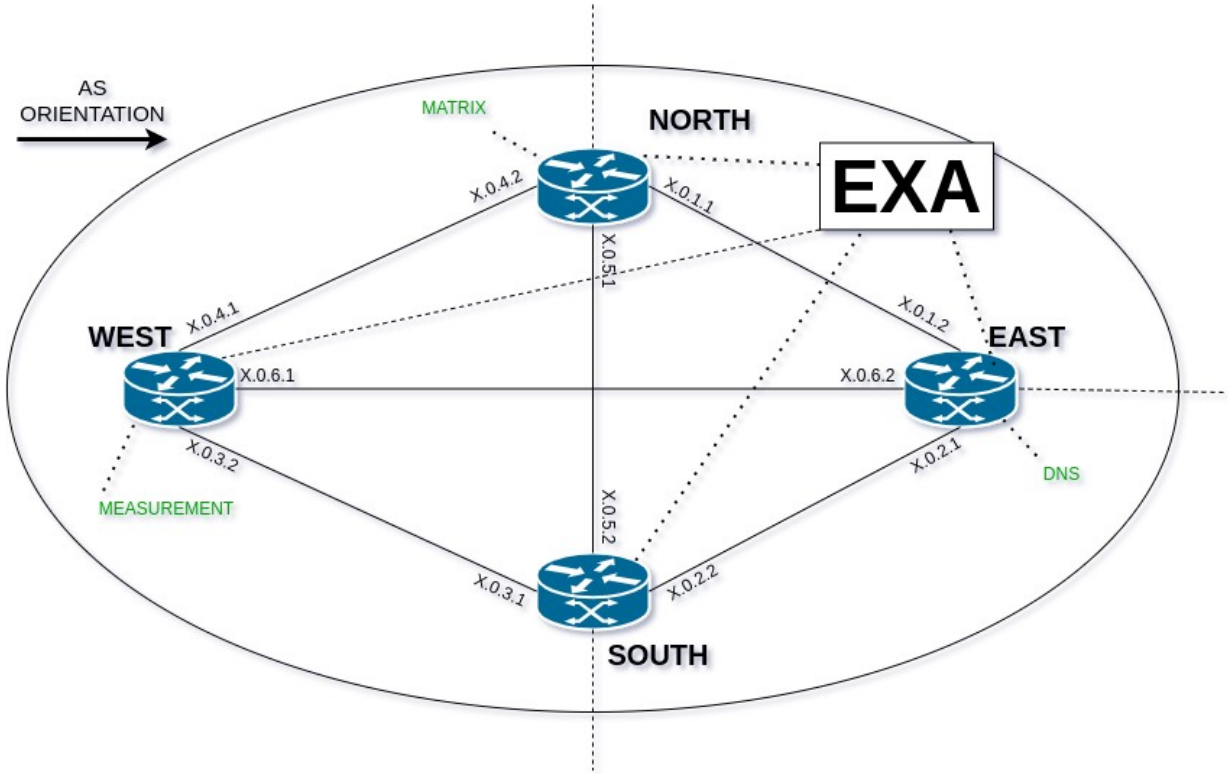
Chris Papastamos

The platform

- Mini-internet is an educational platform that simulates an internet topology and allows student to practice network configuration on it
- Every device (host, switch, router) is simulated using docker containers
- Virtual links connecting the topology is simulated using Open vSwitch links

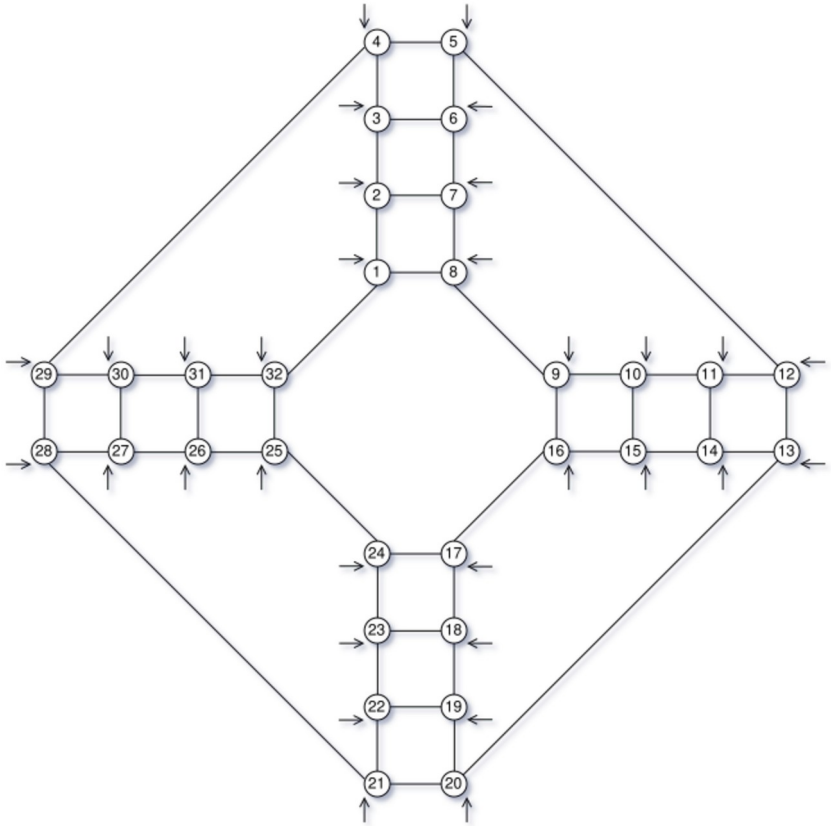
AS Topology - internal

- Each AS contains 4 routers placed in a diamond configuration and they are connected in a full-mesh style.
- 3 out of the 4 routers (NORTH, SOUTH and EAST) have external connections to the neighboring ASes.
- As seen on the top-left corner, the orientation of this demonstration AS follows the arrow displayed



AS Topology - external

- All Ases are connected according to the figure on the right. Every student will be assigned an AS and a Target AS.
- Your objective is to hijack the target AS, calculate which ASes you will affect with your hijack.
- While you attack a fellow student of yours, someone will target your AS! You have to detect the hijack and mitigate it accordingly.



Connecting to the Proxy

- Each AS has a proxy container where one can login with the AS password.
- To connect to the proxy, ssh to the server IP: 147.52.203.13 as user root
- For each AS the port number is equal to: 2000+[AS#]

```
chris@chris-PC-Ubuntu:~$ ssh root@147.52.203.13 -p 2001
root@147.52.203.13's password:
+-------------------------------------------------+
|                                                 |
|          HY436 - Software Defined Networks      |
|         Assignment 4 | BGP Hijack Simulation    |
|                                                 |
|          For any inquiries contact the TAs      |
|         Chris Papastamos: csd4569@csd.uoc.gr    |
|         Manos Lakiotakis: manoslak@csd.uoc.gr   |
|                                                 |
|   From here, you can access your virtual devices|
|   with the goto.sh script. For instance:        |
|                                                 |
|   ./goto.sh EAST router                         |
|                                                 |
+-------------------------------------------------+
root@g1-proxy ~>
```

Connecting to the Proxy

./goto.sh script:

Using this script you can access all the devices in your topology. Pressing the TAB key will bring suggestions from the available devices.

```
root@g1-proxy ~> ./goto.sh
EAST   NORTH  SOUTH  WEST
root@g1-proxy ~> ./goto.sh EAST
host    router
root@g1-proxy ~> ./goto.sh EAST router
```

./save_configs.sh script:

This script will save the configurations of each router in the proxy container. You will need to copy them to your device in order to turn them in with your report

```
root@g1-proxy ~> ./save_configs.sh
Warning: Permanently added '158.1.10.1' (ECDSA) to the list of known hosts.
Connection to 158.1.10.1 closed.
Warning: Permanently added '158.1.11.1' (ECDSA) to the list of known hosts.
Connection to 158.1.11.1 closed.
Warning: Permanently added '158.1.12.1' (ECDSA) to the list of known hosts.
Connection to 158.1.12.1 closed.
Warning: Permanently added '158.1.13.1' (ECDSA) to the list of known hosts.
Connection to 158.1.13.1 closed.
  adding: configs_10-12-2023_18-21-31/EAST.txt (deflated 68%)
  adding: configs_10-12-2023_18-21-31/NORTH.txt (deflated 69%)
  adding: configs_10-12-2023_18-21-31/SOUTH.txt (deflated 68%)
  adding: configs_10-12-2023_18-21-31/WEST.txt (deflated 69%)
Download zip file:
    scp -P 2001 root@duvel.ethz.ch:configs_10-12-2023_18-21-31.zip .
Overwrite the config folder in the current directory:
    scp -r -P 2001 root@duvel.ethz.ch:configs_10-12-2023_18-21-31 config
root@g1-proxy ~> ls
configs_10-12-2023_18-21-31      exabgp_output  restart_ospfd.sh    save_configs.sh
configs_10-12-2023_18-21-31.zip  goto.sh        restore_configs.sh
root@g1-proxy ~>
```

Connecting to a router

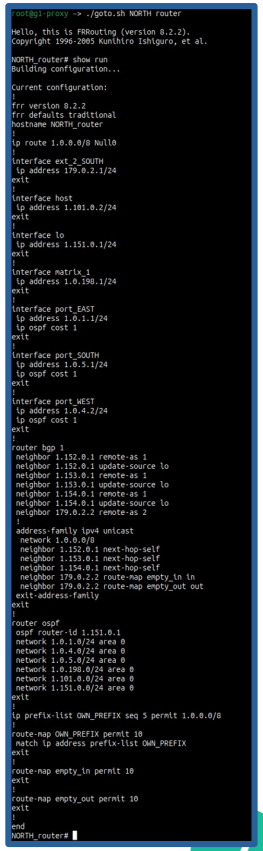
Using the ./goto.sh script you can connect to a router of your AS.

```
root@g1-proxy ~> ./goto.sh NORTH router

Hello, this is FRRouting (version 8.2.2).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

NORTH_router#
```

In the command line of the router you can execute the command “show run”. This command displays the current running configuration. The screenshot on the right displays the output of the command (It is a little bit long to fit in a slide).



Advertising a prefix

```
Hello, this is FRRouting (version 8.2.2).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

EAST_router# conf t
EAST_router(config)# ip route 2.0.0.0/8 Null0
EAST_router(config)# router bgp 1
EAST_router(config-router)# network 2.0.0.0/8
EAST_router(config-router)# exit
EAST_router(config)# exit
```

On the top screenshot we can see an example where the EAST router of AS1 is configured to advertise the prefix 2.0.0.0/8.

You can verify the advertisement by looking at the output of the show run command and verifying that the commands you just ran exists in the running configuration.

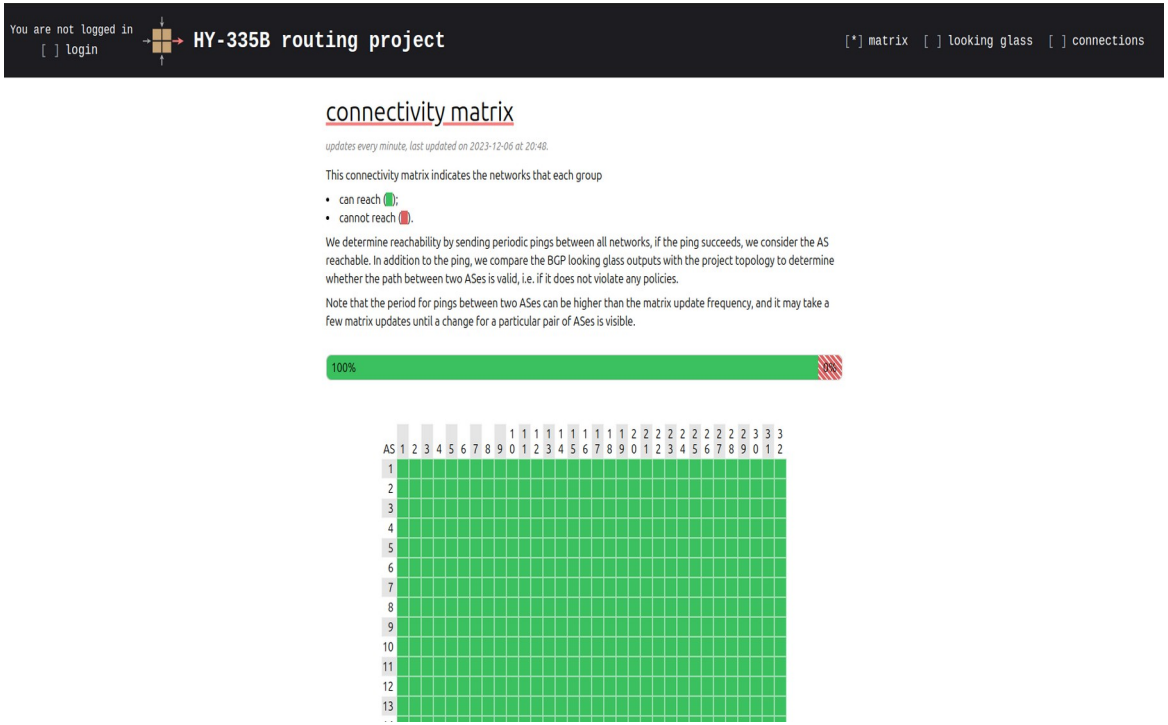
```
router bgp 1
 neighbor 1.0.197.6 remote-as 1
 neighbor 1.151.0.1 remote-as 1
 neighbor 1.151.0.1 update-source lo
 neighbor 1.153.0.1 remote-as 1
 neighbor 1.153.0.1 update-source lo
 neighbor 1.154.0.1 remote-as 1
 neighbor 1.154.0.1 update-source lo
 neighbor 179.0.1.2 remote-as 8
 !
 address-family ipv4 unicast
  network 1.0.0.0/8
  network 2.0.0.0/8
  neighbor 1.0.197.6 route-reflector-client
  neighbor 1.0.197.6 route-map LOCAL_PREF_IN_EXA in
  neighbor 1.0.197.6 route-map LOCAL_PREF_OUT_EXA out
  neighbor 1.151.0.1 next-hop-self
  neighbor 1.153.0.1 next-hop-self
  neighbor 1.154.0.1 next-hop-self
  neighbor 179.0.1.2 route-map empty_in in
  neighbor 179.0.1.2 route-map empty_out out
 exit-address-family
exit
```

```
ip route 1.0.0.0/8 Null0
ip route 2.0.0.0/8 Null0
```

Platform’s Website

You can access the platform’s website in the by visiting hy436.duckdns.org:8000 on your web browser. The website consists of 3 main indexes:

- **Matrix**
- **Looking Glass**
- **Connections**

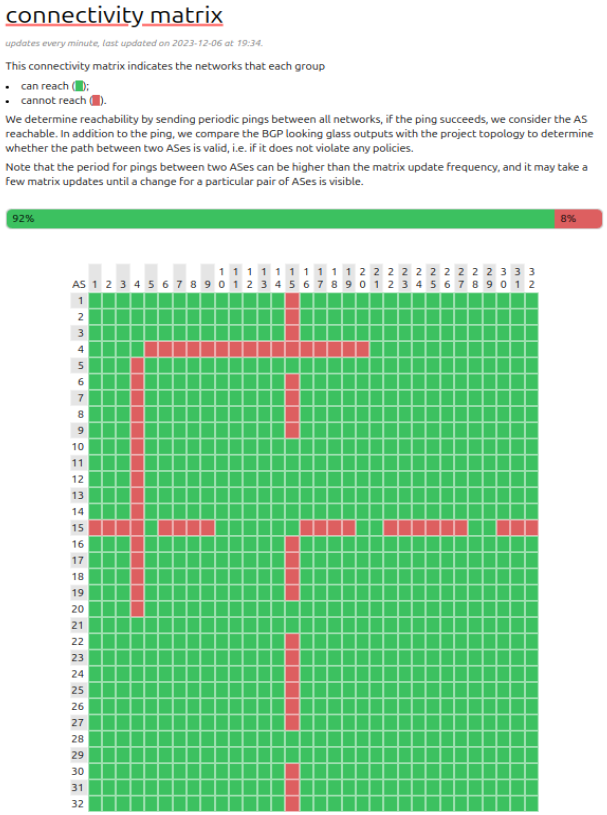


Connectivity Matrix

The connectivity matrix displays the status of the connectivity between any two ASes using a green square for connected and red for not connected.

Using the connectivity matrix you can quickly distinguish BNZ hijacks and their target.

The matrix has a response time of approximately 20 minutes so be patient with it.



Looking Glass

The BGP Looking Glass is a tool that can be used to take a peek on the accepted routes of any router of any AS.

Using the filter fields on the top, you can select the desired router .

The output of the Looking Glass contains the selected path for each advertised prefix.

You can use this functionality to detect BGP Hijacks.

looking glass

> *Looking Glass servers (LG servers) are servers on the Internet running one of a variety of publicly available Looking Glass software implementations. They are commonly deployed by autonomous systems (AS) to offer access to their routing infrastructure in order to facilitate debugging network issues. A Looking Glass server is accessed remotely for the purpose of viewing routing information. Essentially, the server acts as a limited, read-only portal to routers of whatever organization is running the LG server.*
>
> Looking Glass Server
> wikipedia.org

AS 1 **Router** NORTH

```
2023-12-06T18:34:28
BGP table version is 58, local router ID is 1.151.0.1, vrf id 0
Default local pref 100, local AS 1
Status codes:  s suppressed, d damped, h history, * valid, > best, = multipath,
               i internal, r RIB-failure, S Stale, R Removed
Nexthop codes: @NNN nexthop's vrf id, < announce-nh-self
Origin codes:  i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

   Network          Next Hop            Metric LocPrf Weight Path
* i1.0.0.0/8       1.154.0.1                0    100      0 i
* i                1.153.0.1                0    100      0 i
* i                1.152.0.1                0    100      0 i
*>                 0.0.0.0                  0         32768 i
*> 2.0.0.0/8       179.0.2.2                0              0 2 i
*> 3.0.0.0/8       179.0.2.2                               0 2 3 i
*> 4.0.0.0/8       179.0.2.2                               0 2 3 4 i
* i5.0.0.0/8       1.152.0.1                     100       0 8 7 6 5 i
*>                 179.0.2.2                               0 2 3 4 5 i
* i6.0.0.0/8       1.152.0.1                     100       0 8 7 6 i
*>                 179.0.2.2                               0 2 3 6 i
* i7.0.0.0/8       1.152.0.1                     100       0 8 7 i
*>                 179.0.2.2                               0 2 7 i
*>i8.0.0.0/8       1.152.0.1                0    100       0 8 i
*>i9.0.0.0/8       1.152.0.1                     100       0 8 9 i
*>i10.0.0.0/8      1.152.0.1                     100       0 8 9 10 i
* i11.0.0.0/8      1.152.0.1                     100       0 8 9 10 15 14 11 i
*>                 179.0.2.2                               0 2 3 4 5 12 11 i
* i12.0.0.0/8      1.152.0.1                     100       0 8 7 6 5 12 i
*>                 179.0.2.2                               0 2 3 4 5 12 i
* i13.0.0.0/8      1.152.0.1                     100       0 8 9 10 15 14 13 i
*>                 179.0.2.2                               0 2 3 4 5 12 13 i
*>i14.0.0.0/8      1.152.0.1                     100       0 8 9 10 15 14 i
*>i15.0.0.0/8      1.152.0.1                     100       0 8 9 16 i
*>i16.0.0.0/8      1.152.0.1                     100       0 8 9 16 i
* i17.0.0.0/8      1.153.0.1                     100       0 32 25 24 17 i
*>i                1.152.0.1                     100       0 8 9 16 17 i
* i18.0.0.0/8      1.153.0.1                     100       0 32 25 24 17 18 i
*>i                1.152.0.1                     100       0 8 9 16 17 18 i
* i19.0.0.0/8      1.153.0.1                     100       0 32 25 24 17 18 19 i
*>i                1.152.0.1                     100       0 8 9 16 17 18 19 i
* i20.0.0.0/8      1.153.0.1                     100       0 32 25 26 27 28 21 20 i
* i                1.152.0.1                     100       0 8 9 10 15 14 13 20 i
*>                 179.0.2.2                               0 2 3 4 5 12 13 20 i
* i21.0.0.0/8      1.153.0.1                     100       0 32 25 26 27 28 21 i
*>                 179.0.2.2                               0 2 3 4 29 28 21 i
*>i22.0.0.0/8      1.153.0.1                     100       0 32 25 24 23 22 i
*>i23.0.0.0/8      1.153.0.1                     100       0 32 25 24 23 i
*>i24.0.0.0/8      1.153.0.1                     100       0 32 25 24 i
*>i25.0.0.0/8      1.153.0.1                     100       0 32 25 i
*>i26.0.0.0/8      1.153.0.1                     100       0 32 25 26 i
*>i27.0.0.0/8      1.153.0.1                     100       0 32 25 26 27 i
* i28.0.0.0/8      1.153.0.1                     100       0 32 25 26 27 28 i
*>                 179.0.2.2                               0 2 3 4 29 28 i
* i29.0.0.0/8      1.153.0.1                     100       0 32 31 30 29 i
*>                 179.0.2.2                               0 2 3 4 29 i
*>i30.0.0.0/8      1.153.0.1                     100       0 32 31 30 i
*>i31.0.0.0/8      1.153.0.1                     100       0 32 31 i
*>i32.0.0.0/8      1.153.0.1                0    100       0 32 i

Displayed  32 routes and 49 total paths
```

Connections

The Connections page displays the external connections of your AS with its neighbors.

In this index you can find information about the external links of your AS to further understand the topology.

Using the filter fields on the top, you can filter the results by source or destination AS .