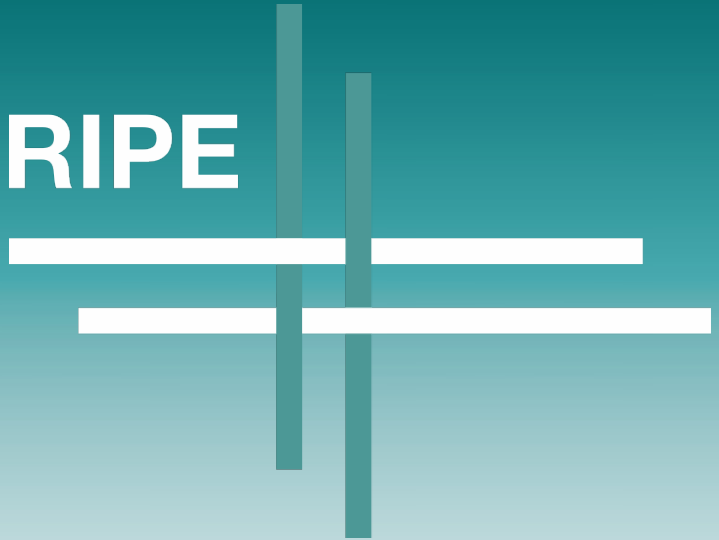


MANRS Training Lab

Open source tooling to provide hands-on labs

Sander Steffann, RIPE78, 2019-05-22

Context

- Developed for MANRS
- But wider applicability kept in mind all the time

- Initial development funded by ISOC (thanks!)
- Released under GPL3 after completion

Design goals

- Lab content goals
  - Allow student to get hands-on experience with different platforms: Cisco, Junos, Mikrotik, etc…
  - Automatic validation of the results
  - Teach student to use IRR

Design goals

- Management goals
  - Allow self-signup by students (optional)
  - Set a time limit for a lab (optional)
  - Allow teacher to extend time limit, pause, restart, export etc.
  - Allow teacher to view what a student is doing and help them

Component choices

- GNS3 for virtual lab
- Django front-end (uWSGI application)
- Web based interface using web sockets
- Redis for live communication channels
- PostgreSQL database for storage

Hardware requirements

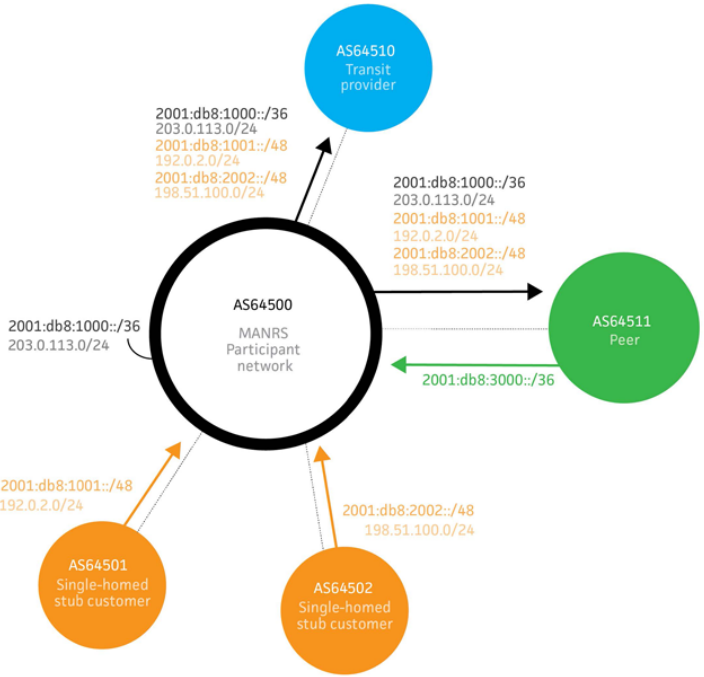
- Heavy hardware preferred
  - Every student gets their own clone
  - Every clone needs a few GB of memory and some CPU cycles
  - Juniper vMX needs a little bit more GB and CPU cores

Workflow

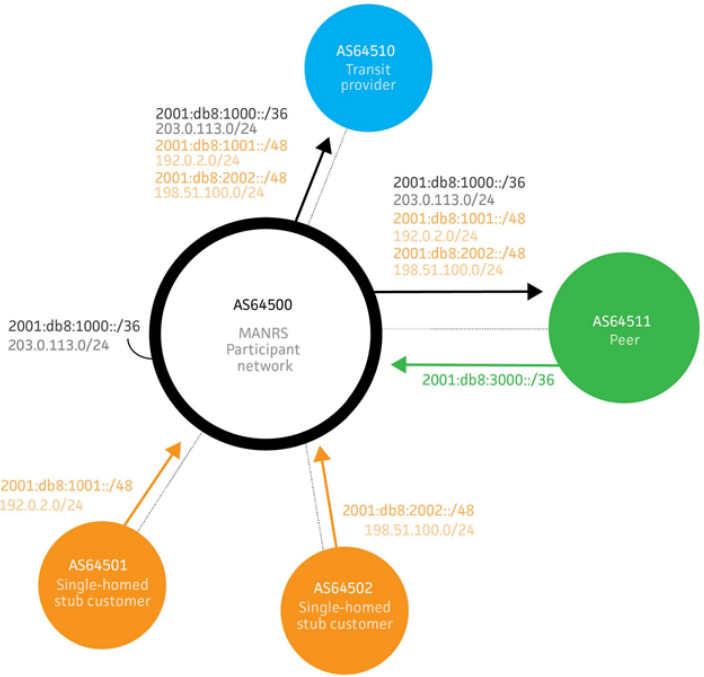
- Build a lab template in GNS3
- Link it to the management system
- Configure description, instructions and goals

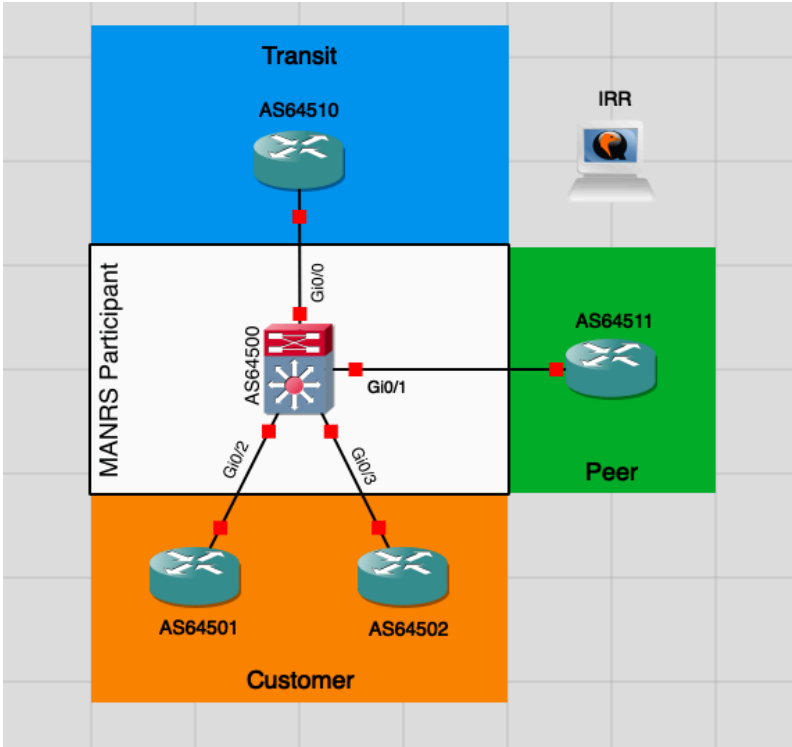
- Each student gets a clone of the template
  - Either created by teacher or by self-signup

Example: MANRS Lab

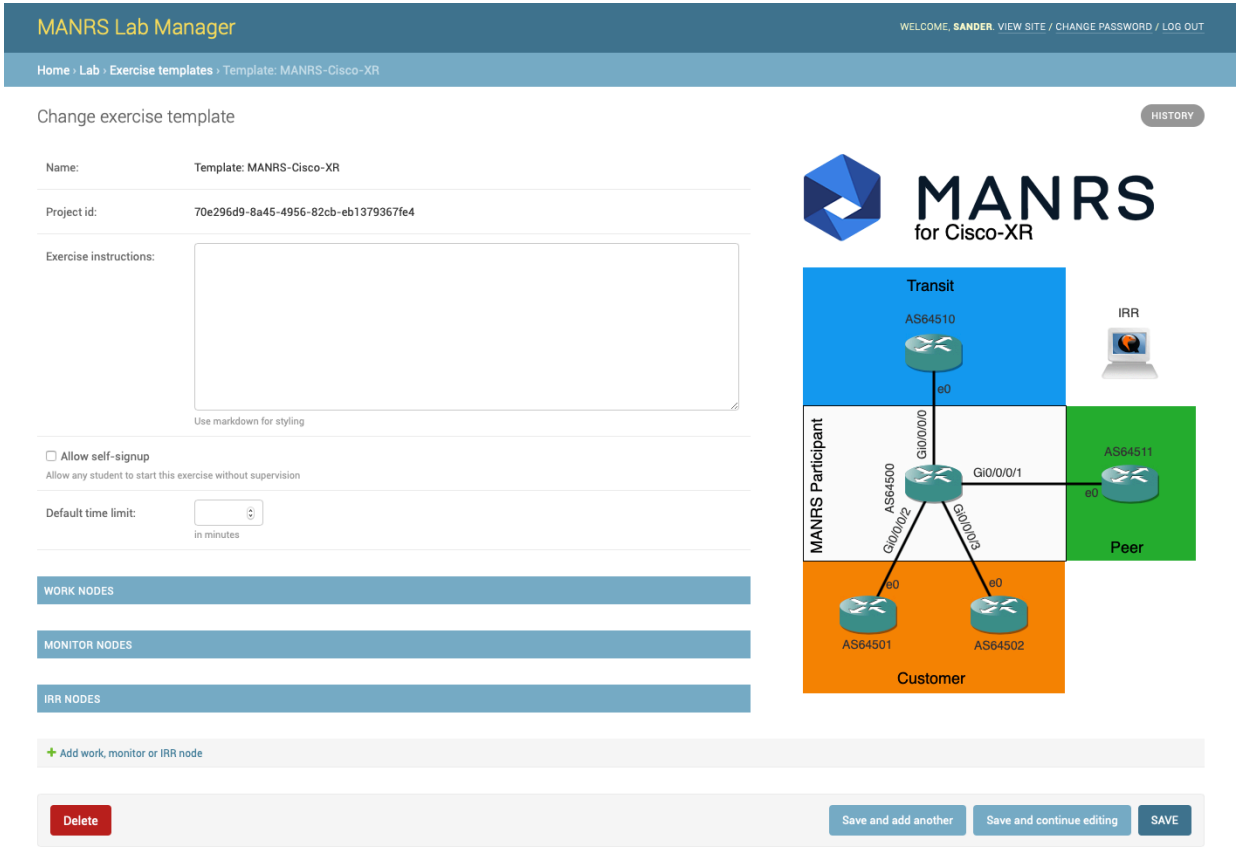


Example: MANRS Lab - GNS3 template

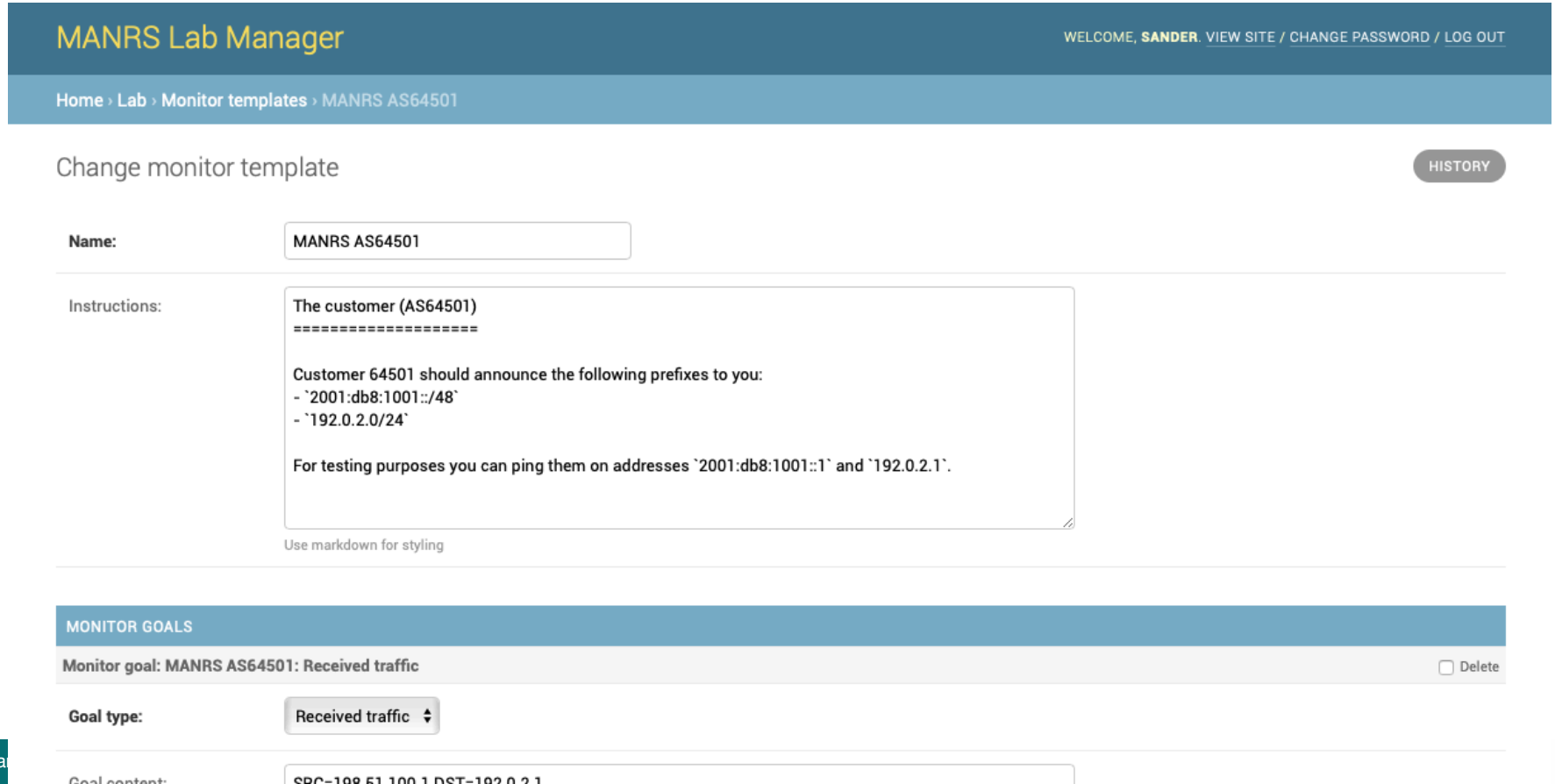




Example: MANRS Lab - Linking to training system



Example: MANRS Lab - Goal definition



MONITOR GOALS

Monitor goal: MANRS AS64501: Received traffic — Delete

Goal type: Received traffic

Goal content:

```
SRC=198.51.100.1 DST=192.0.2.1
SRC=10.0.0.1 DST=192.0.2.1
SRC=2001:0db8:2002:0000:0000:0000:0000:0001 DST=2001:0db8:1001:0000:0000:0000:0000:0001
SRC=2001:0db8:0000:0000:0000:0000:0000:0001 DST=2001:0db8:1001:0000:0000:0000:0000:0001
SRC=2001:0db8:3000:0000:0000:0000:0000:0001 DST=2001:0db8:1001:0000:0000:0000:0000:0001
```

Monitor goal: MANRS AS64501: IPv4 routes — Delete

Goal type: IPv4 routes

Goal content:

```
BIRD 1.5.0 ready.
10.0.0.0/8        via 203.0.113.252 on eth0 [bgp1 11:48:05] * (100) [AS65001i]
        Type: BGP unicast univ
        BGP.origin: IGP
        BGP.as_path: 64500 64510 65000 65000 65001
        BGP.next_hop: 203.0.113.252
        BGP.local_pref: 100
192.168.0.0/16    via 203.0.113.252 on eth0 [bgp1 11:48:05] * (100) [AS65003i]
        Type: BGP unicast univ
        BGP.origin: IGP
```

Monitor goal: MANRS AS64501: IPv6 routes — Delete

Goal type: IPv6 routes

Goal content:

```
BIRD 1.5.0 ready.
2001:db8:2002::/48 via 2001:db8:1000:fffe::a on eth0 [bgp1 11:44:26] * (100) [AS64502i]
        Type: BGP unicast univ
        BGP.origin: IGP
        BGP.as_path: 64500 64502
```

Example: MANRS Lab - Student's view

MANRS Lab Manager

Dashboard: MANRS-Cisco for Sander Steffann

Logged in as Sander Steffann (sander@steffann.nl)
Home | Admin interface | Change password | Log out

Instructions | AS64500 | AS64501 | AS64502 | AS64510 | AS64511 | IRR | Online

MANRS for Cisco

Welcome to the MANRS for Cisco lab. This lab consists of a transit, a peer, two customers, and your very own Cisco router in the middle. The goal is to implement MANRS on your router so that the other routers cannot send you hijacked routes or traffic with spoofed source addresses. And they will try!

The layout of this lab is based on the MANRS Implementation Guide. The addresses and prefixes used in this lab correspond to those used in that document.

Background information

At the start of the lab all links are configured and BGP sessions exist for both IPv4 and IPv6. There is no filtering in place. That is your task.

Your router (AS64500)

You have full console access to your router. Configure it so it has MANRS.

You should announce the following prefixes from your own router:

- `2001:db8:1000::/36`
- `203.0.113.0/24`

The transit (AS64510)

The transit will send you the most routes. But it isn't behaving completely correct. Some of its routes are your own! Make sure you don't accept them, or someone on the internet might hijack you. There is also traffic coming from the transit with source addresses that don't exist in the routing table. Those should also be blocked.

For testing purposes you can ping the transit on addresses `2001:db8::1` and `10.0.0.1`.

The peer (AS64511)

The peer will do the same as the transit, except that of course it's only allowed to attract traffic for itself. So make sure that you filter what they announce to you, and also make sure they don't use you as a free transit!

The peer should announce the following prefixes to you:

- `2001:db8:3000::/36`

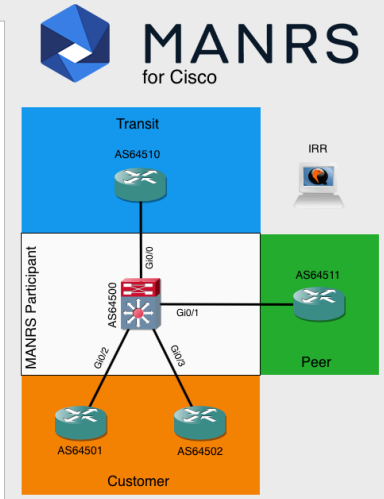
For testing purposes you can ping the peer on address `2001:db8:3000::1`.

The customers (AS64501 and AS64502)

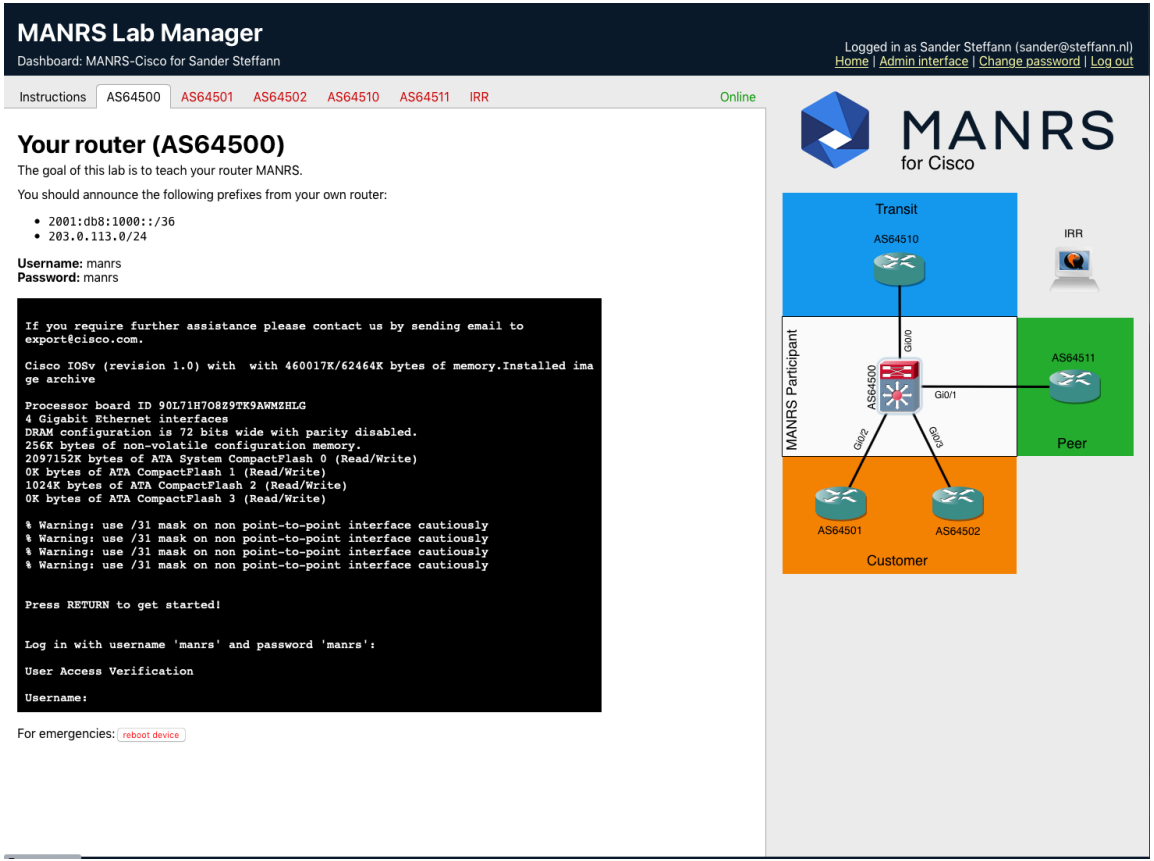
You have two customers in this lab. Both of them have IPv4 and IPv6 address space. AS64501 has address space from your aggregated block, AS64502 has provider independent space. But beware: there is also some hijacking going on! Make sure both of your customers behave and don't interfere with each other or the rest of the internet.

Customer 64501 should announce the following prefixes to you:

- `2001:db8:1001::/48`
- `192.0.2.0/24`



Example: MANRS Lab - Student's view



Example: MANRS Lab - Student's view

MANRS Lab Manager

Dashboard: MANRS-Cisco for Sander Steffann

Logged in as Sander Steffann (sander@steffann.nl)
Home | Admin interface | Change password | Log out

Instructions | AS64500 | AS64501 | AS64502 | AS64510 | AS64511 | IRR | Online

The customer (AS64501)

Customer 64501 should announce the following prefixes to you:

- 2001:db8:1001::/48
- 192.0.2.0/24

For testing purposes you can ping them on addresses 2001:db8:1001::1 and 192.0.2.1.

Looking glass from this router's viewpoint

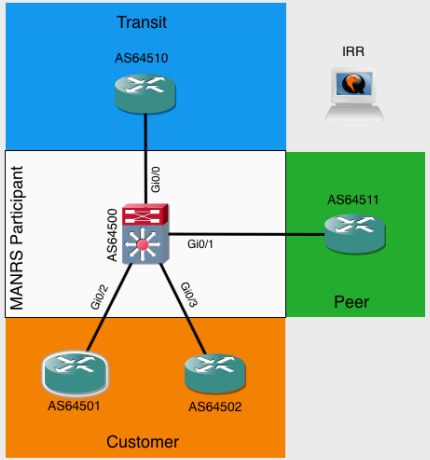
Received traffic (last change at 3:36:18)

Expected	Currently seen
10.0.0.1 to 192.0.2.1	10.0.0.1 to 192.0.2.1
These packets shouldn't be received	192.0.2.3 to 192.0.2.1
These packets shouldn't be received	192.88.99.2 to 192.0.2.1
These packets shouldn't be received	192.88.99.10 to 192.0.2.1
198.51.100.1 to 192.0.2.1	198.51.100.1 to 192.0.2.1
These packets shouldn't be received	198.51.100.3 to 192.0.2.1
2001:db8::1 to 2001:db8:1001::1	2001:db8::1 to 2001:db8:1001::1
These packets shouldn't be received	2001:db8:1000::3 to 2001:db8:1001::1
These packets shouldn't be received	2001:db8:1001::3 to 2001:db8:1001::1
2001:db8:2002::1 to 2001:db8:1001::1	2001:db8:2002::1 to 2001:db8:1001::1
2001:db8:3000::1 to 2001:db8:1001::1	These packets are missing
These packets shouldn't be received	3ffe::2 to 2001:db8:1001::1
These packets shouldn't be received	3ffe::10 to 2001:db8:1001::1

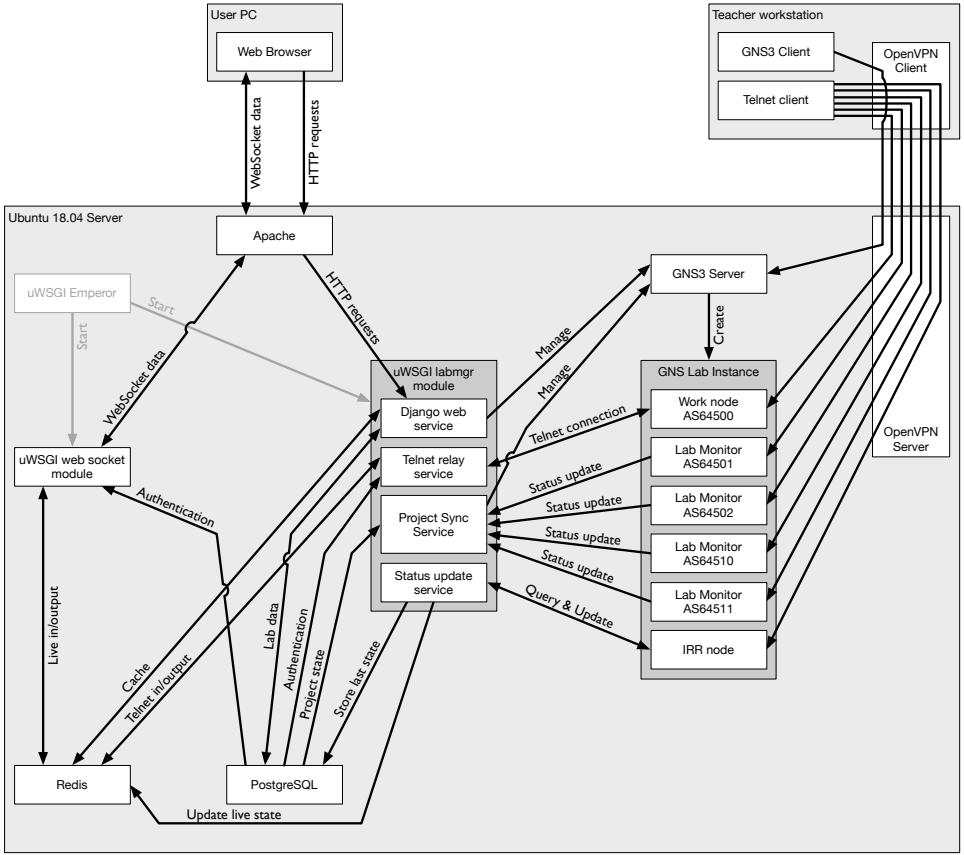
IPv4 routes (last change at 3:38:29)

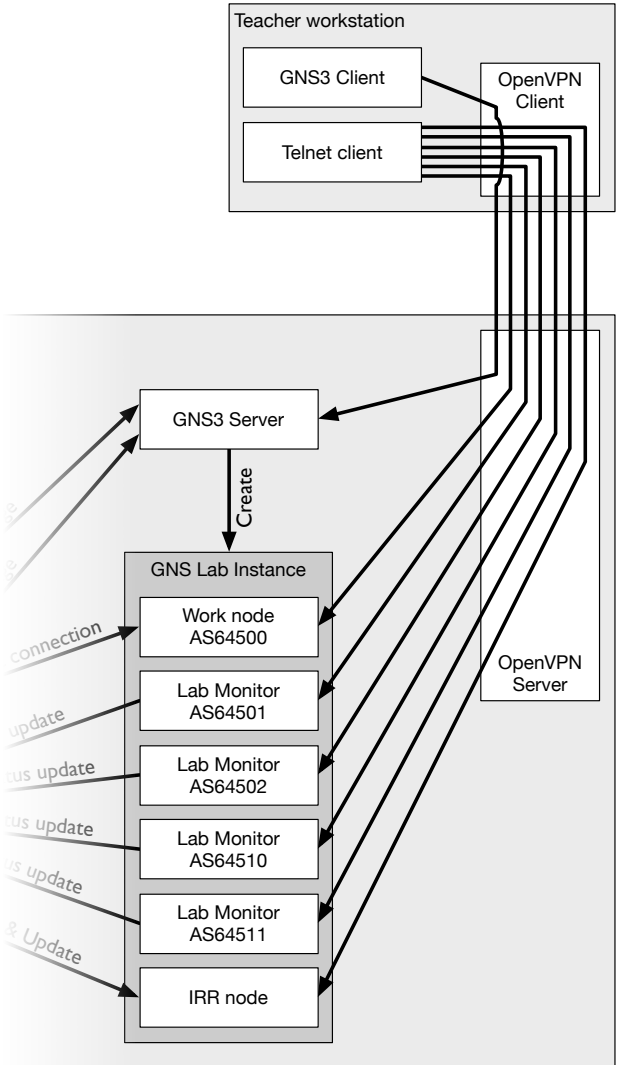
Expected	Currently seen
10.0.0.0/8 AS-Path: 64500 64510 65000 65000 65001	10.0.0.0/8 AS-Path: 64500 64510 65000 65000 65001
172.16.0.0/12	172.16.0.0/12

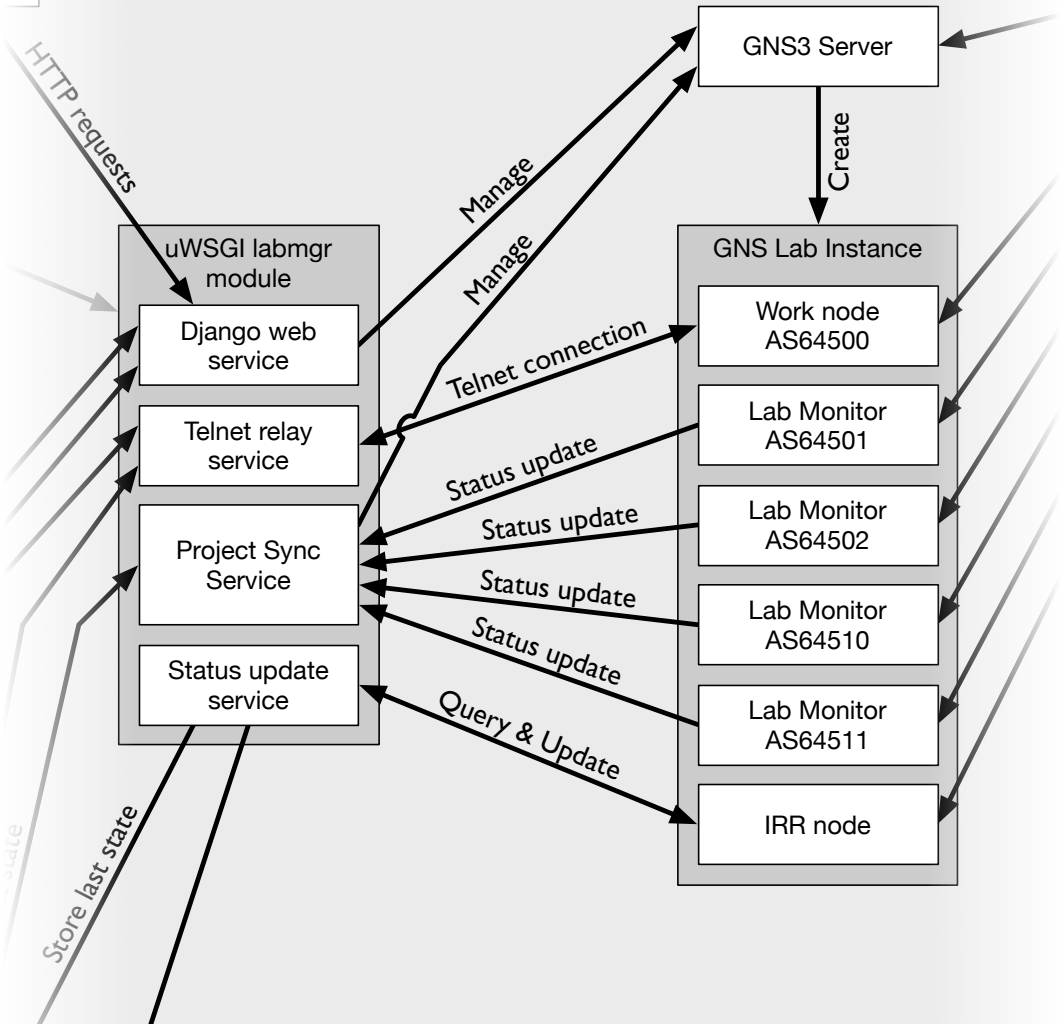
MANRS for Cisco

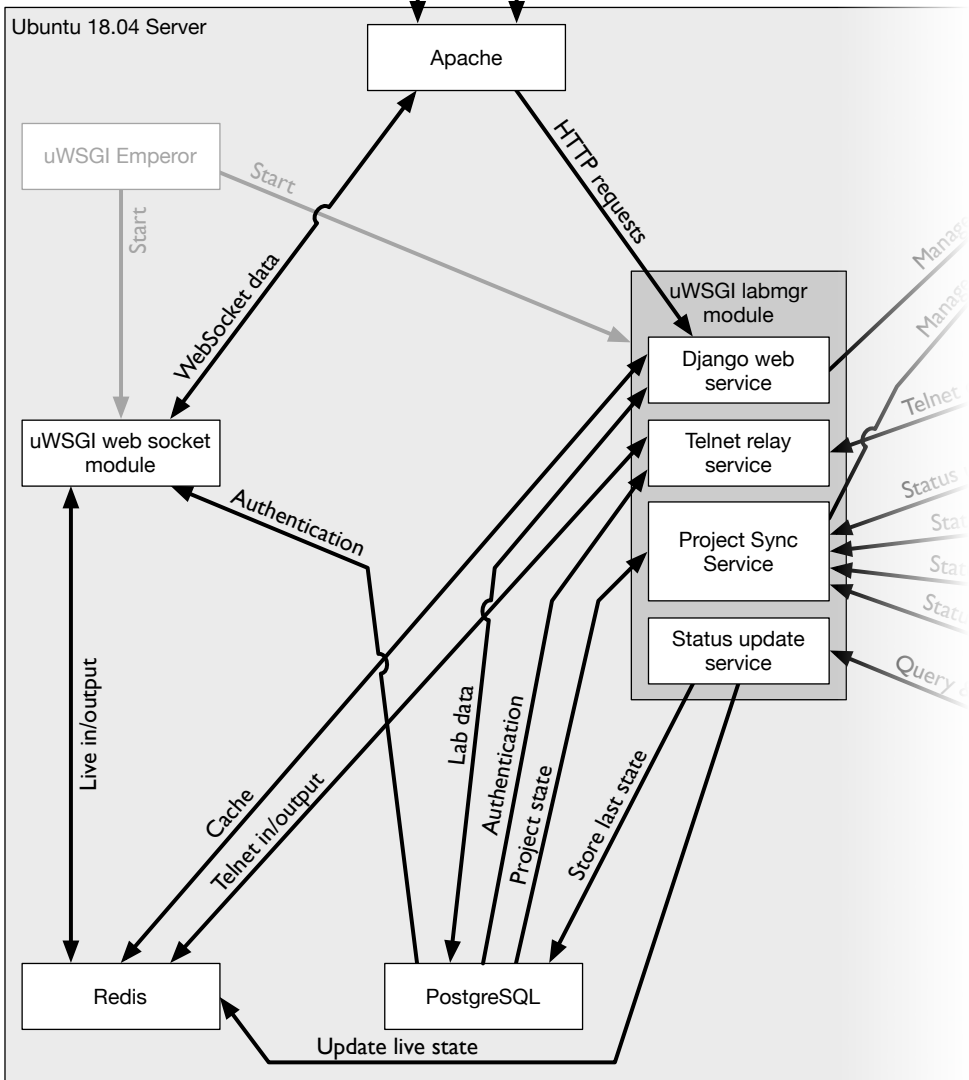


Software architecture

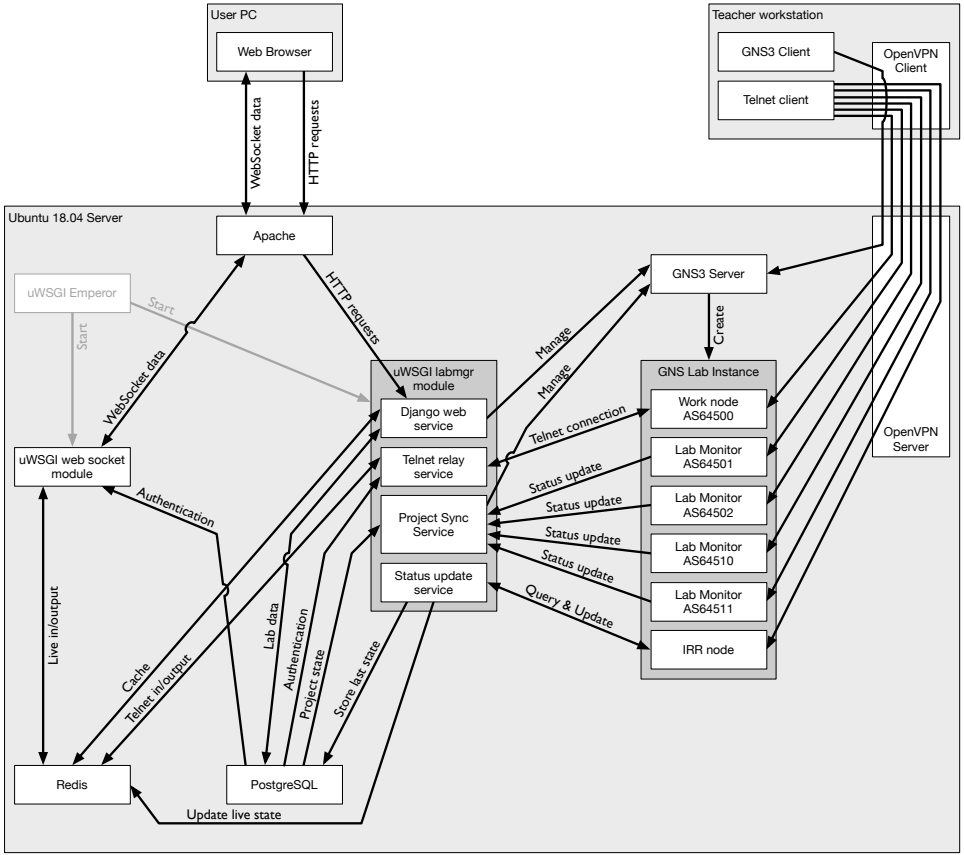



Teacher workstation
GNS3 Client
Telnet client
OpenVPN Client
GNS3 Server
Create
GNS Lab Instance
Work node AS64500
Lab Monitor AS64501
Lab Monitor AS64502
Lab Monitor AS64510
Lab Monitor AS64511
IRR node
OpenVPN Server
connection
update
us update
us update
s update
Update


GNS3 Server
Create
HTTP requests
uWSGI labmgr module
Django web service
Telnet relay service
Project Sync Service
Status update service
Manage
Manage
Telnet connection
Status update
Status update
Status update
Status update
Query & Update
GNS Lab Instance
Work node AS64500
Lab Monitor AS64501
Lab Monitor AS64502
Lab Monitor AS64510
Lab Monitor AS64511
IRR node
Store last state


Ubuntu 18.04 Server
Apache
uWSGI Emperor
Start
Start
HTTP requests
WebSocket data
uWSGI labmgr module
Django web service
Telnet relay service
Project Sync Service
Status update service
uWSGI web socket module
Authentication
Live in/output
Cache
Telnet in/output
Lab data
Authentication
Project state
Store last state
Redis
PostgreSQL
Update live state

Software architecture



Future developments

- Add other types of router for the student
  - Juniper cRPD, Alcatel/Nokia etc…
- Add RPKI validation to the lab
- Optimise performance of the IRR node under load

Questions?