# Goodbye Pork Pie Hat

**Kévin "Chewie" Sztern**

**Jan 14, 2021**

# CONTENTS:

CHAPTER

ONE

# ABOUT THIS PROJECT

## 1.1 *Goodbye Pork Pie Hat*


Welcome to the third and last NET1 project!

*Goodbye Pork Pie Hat* is a jazz piece composed by Charles Mingus as an eulogy to saxophonist Lester Young, and released on his 1959 album "Mingus Ah Um" by Columbia Records. Few jazz songs are as famous as this one, and it naturally became a widely covered jazz standard.

## 1.2 What you have to do

This final project aims to consolidate the knowledge previously acquired in one big project that involves everything you've seen so far (the only exception being DHCP. It's hard to test, so we'll do without for now).

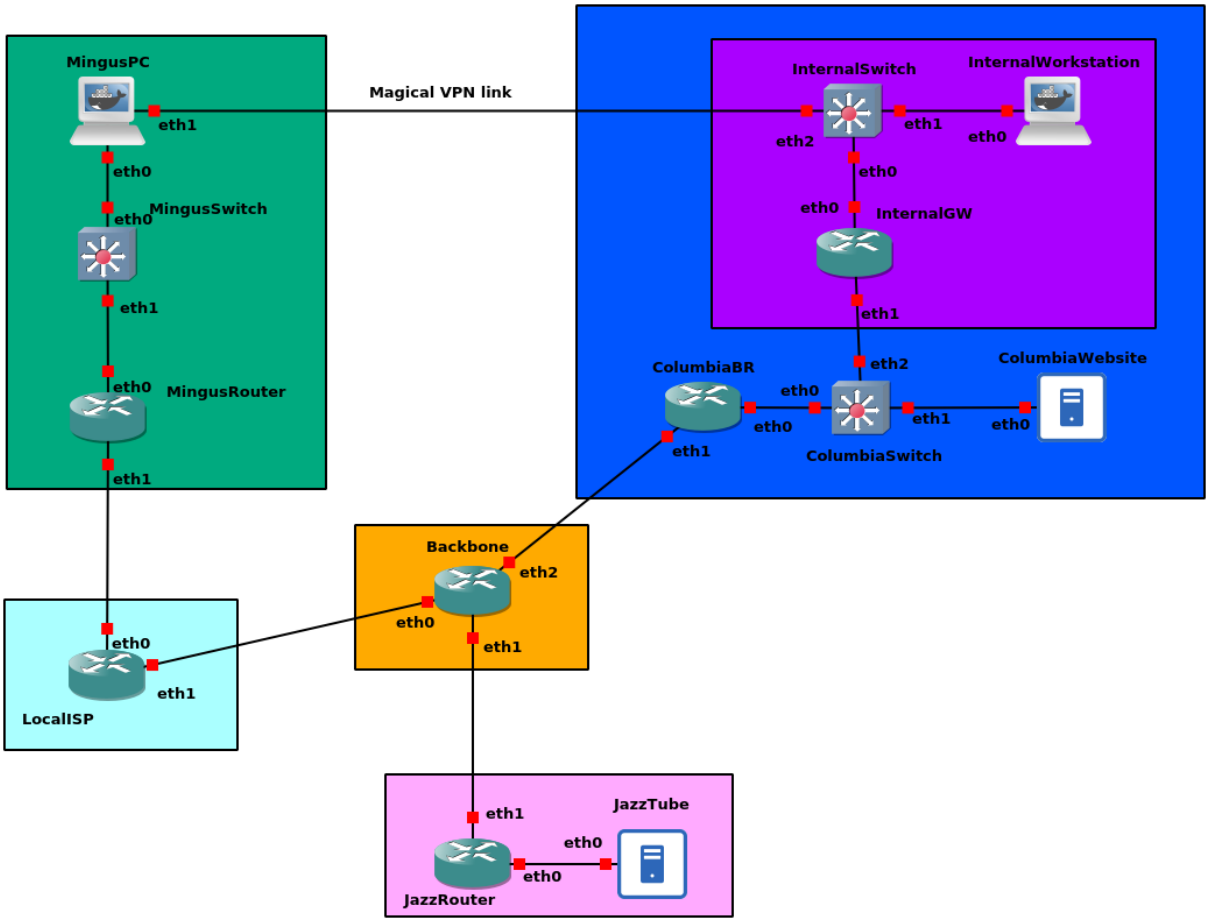
You know the drill, but here's a recap from the previous subjects:

Your goal, in this subject, is to successively play the role of several network administrators, each for its own entity. By locally configuring the network in each area, you will end up with a complex and (relatively) realistic network, putting into practice everything you've learned so far.

At the end of your configuration, you should have reached global connectivity and, save from machines inside a private network, have every machine be reachable from every other machine. Of course, those private machines must be able to reach every public machine with no trouble, thanks to NAT. Do not NAT anything else!

Since creating all the machines is laborious and not very interesting, you will find on the assignment page a base project that you can import in GNS3. In this base project, all the machines are present and correctly plugged, but no configuration is present. All you have to do is go to each machine and configure it as instructed!

The final topology looks like this:




Five entities in this topology, with the last one being a bit more complicated. This topology tells the story of Charles Mingus working from home during the pandemic, and uploading his work to his label so they can release it on JazzTube.

## 1.3 Exporting your project

In order to submit your project, you need to export it in the portable GNS3 format, which is basically a zipfile containing everything.

To do that, you can find the "Export portable project" in the "File" menu from the toolbar.

When asked if you would like to include base images or snapshots, choose "no" for both, the questions are not relevant for docker appliances.

If you're using version 2.2 or above, you can choose the compression method used. I advise you pick the default "Zip compression (deflate)".

Name the file *<login>-porkpiehat.gns3project*, where *<login>* is your login. This is the file you will submit through Moodle. Be careful to input your login **exactly** as found on the intranet, and keep it all lowercase.

Before submitting it, I strongly advise you to try importing it first and testing that everything works correctly, you can never be too sure! I'm not responsible for errors on your part and won't help you if you forgot to test your project before submitting it.

Now, let's go to each area to see its role and how it's supposed to be configured.

CHAPTER

TWO

# THE LOCAL ISP

In this remote part of the world lives a local ISP, diligently providing Internet connectivity to its clients. Of course, this ISP being merely a small local actor, global connectivity is accomplished by a contract with the Backbone, a "meta-ISP" present all over the world. Basically, Backbone is to LocalISP what LocalISP is to Mingus.

Small he may be, LocalISP is nevertheless a registered LIR in his region, and his RIR has given him the *128.66.42.0/24* block. For each new client, the local ISP carves a */31* out of it and attributes one end to the client, keeping the other end for his single router that powers his whole infrastructure (don't do this at home, kids. Also please try to have more than one client if you don't want to starve).

Route wise, the transit relationship it purchased from the Backbone allows it to define a default route towards the backbone. See the Backbone's section for more information on that.

## 2.1 Firewalling

One of the jobs of the ISP is making sure that no private addresses leak out from its customers. To do this, the router is configured to drop all packets containing those addresses. In our case and to save some time, dropping forwarded packets with a source IP in *192.168.0.0/16* will be enough.

**Warning:** Don't forget to save the *iptables* configuration with *iptables-save*! Otherwise, all your precious configuration will be lost on reboot. Remember that *iptables-save* just prints the saved configuration on stdout, you need to redirect it to */etc/sysconfig/iptables* for it to take effect.

## 2.2 Recap

The recap is easy:

| Name | IP Addresses |
|---|---|
| LocalISP | • 128.66.42.69/31 (eth0)<br>• 203.0.113.11/31 (eth1) |

CHAPTER

THREE

# THE BACKBONE

The Backbone is the biggest kid on the block, has datacenters all around the country and can reach every part of it without the help of anyone. The backbone only deals in professional services and doesn't bother with small individual contracts, which is why most regular users of the Internet haven't heard of it.

A proud and eminent LIR in its region, the Backbone was given the *203.0.113.0/24* prefix by the regional authority. Just like LocalISP, the backbone creates */31* pairs out of it to provide connectivity to its clients.

## 3.1 Routes

Note that the role of this service provider is a bit more specialized than you might be used to: its clients are big enough to already have IP addresses of their own, and the service provided is merely a *transit* relationship (as in, the backbone allows traffic to transit through it). The single IP it gives is only necessary to establish a point-to-point link between the routers.

Of course, this means that when purchasing transit from the backbone, clients must inform it of their prefix, so that the backbone may update its routing tables accordingly. Don't forget to add the routes (and to the correct interface)!

## 3.2 Firewalling

In real life, the usual sanity rules would of course be configured, but for the sake of simplicity you don't have to configure anything here. Yay!

## 3.3 Recap

The recap is easy:

| Name | IP Addresses |
|---|---|
| BackBone | • 203.0.113.10/31 (eth0)<br>• 203.0.113.20/31 (eth1)<br>• 203.0.113.30/31 (eth2) |

CHAPTER

FOUR

# JAZZTUBE

JazzTube is the hot new social network where jazz musicians meet and share their songs. It is critical that Adderley can access this site, otherwise he won't be able to share his new album!

In networking terms, JazzTube is a *content provider*, an entity important enough to be recognizable on the network, but whose goal is to provide a service to the end user. Think of Youtube and Netflix for real-life comparisons.

Don't be fooled by there only being one server visible: JazzTube is kind of a big deal, and negotiates its transit directly through the BackBone. Of course, it has its own prefix, and that prefix is *128.66.51.0/24*.

## 4.1 Recap

The recap should have no surprise:

| Name | IP Addresses |
|---|---|
| JazzRouter | • 128.66.51.1/24 (eth0)<br>• 203.0.113.21/31 (eth1) |
| JazzTube | • 128.66.51.99/24 (eth0) |

CHAPTER

# FIVE

# CHARLES MINGUS

Since the beginning of the epidemic, Charles Mingus has been reasonably practicing social distancing, and instead of going to Columbia's studio, composed his work at home. He is a client of "the Local ISP", and was given a single IP that he uses on his box (represented as two separate appliances here, the switch and the router).

## 5.1 SNAT

In prevision of new computers at his home, Adderley uses a private IP range inside his local network, *192.168.0.0/24*, and has configured his router for SNAT.

**Warning:** One can never say it enough: don't forget *iptables-save*, and redirecting it to the proper file!

## 5.2 The magical VPN link

This regular Internet connection works great to browse every website out there (the whole two of them!), but Charles sometimes need to access his work computer at Columbia. Unfortunately, this computer is on a private network inside the company, not reachable from outside.

To circumvent this, the nice sysadmins at Columbia configured a VPN for this kind of use cases, and installed the appropriate software on Adderley's home PC. Charles doesn't really understand how this works, and neither should you. Just think of this as a magical link that directly connects his PC to the internal switch, bypassing everything else. As such, it's just like if *MingusPC* was also part of the internal local network (*10.0.0.0/24*). Please don't ask how this works. It's magic, OK?

**Warning:** Be careful with your default route! Only packets destined to the internal network should go through this interface. Other packets addressed to the Internet (including Columbia's public facing servers) should go through the regular route.

## 5.3 Recap

To recap:

| Name | IP Addresses |
|---|---|
| MingusPC | • 192.168.0.2/24 (eth0)<br>• 10.0.0.3/24 (eth1) |
| MingusRouter | • 192.168.0.1/24 (eth0)<br>• 128.66.42.68/31 (eth1) |

CHAPTER

SIX

# COLUMBIA RECORDS

The label producing Charles Mingus' album, complete with studios and workstations for the musicians! Not that they're used much though, with all the pandemic and whatnot.

A client of the backbone, Columbia has configured the IP given to it on its border router, *ColumbiaBR*. Being a big business, Columba negotiated directly with the regional authority to get their own public prefix, *198.51.100.0/24*. They asked their provider to route all packets addressed to this network to their border router.

The Columbia website makes use of this public address space, and runs on a publicly accessible network, just behind the border router (again, don't do this at home).

## 6.1 The internal network

There is still a tricky bit, though. The workstations and such are not publicly accessible, and instead run on a private network, *10.0.0.0/24*, that gets NATted out by *InternalGW*. The switch on this internal switch has been magically configured to run a state of the art VPN solution with military grade encryption sponsored by Raid Shadow Legends and Squarespace. This VPN is already configured, you don't need to do anything. Consider remote VPN clients as just another machine connected to the switch.

Note that from a technical perspective, the internal network is entirely self contained, and cannot be accessed from the public parts of Columbia. From the point of view of *ColumbiaBR* and *ColumbiaWebsite*, this whole internal network is just a single machine with only one IP address.

**Warning:** Usual warning about not forgetting *iptables-save* and redirecting it properly here.

## 6.2 Recap

To recap:

| Name | IP Addresses |
| --- | --- |
| ColumbiaBR | • 198.51.100.1/24 (eth0)<br>• 203.0.113.31/31 (eth1) |
| ColumbiaWebsite | • 198.51.100.2/24 (eth0) |
| InternalGW | • 10.0.0.1/24 (eth0)<br>• 198.51.100.3/24 (eth1) |
| InternalWorkStation | • 10.0.0.2/24 (eth0) |

CHAPTER

SEVEN

# CONCLUSION

This project marks the end of the NET1 course. If you've followed so far and managed to complete the project, congratulations! Your networking abilities are now nothing to be ashamed of, and might even net you the admiration of future colleagues!

I truly hope that this course brought you all the skills I wished to transmit. Courses are always a work in progress, so don't hesitate to give me your feedback on ways to improve this course for the next year!

May the jazz be with you.