SemanaCap 11 - Tutorial de Looking Glass

Topologia

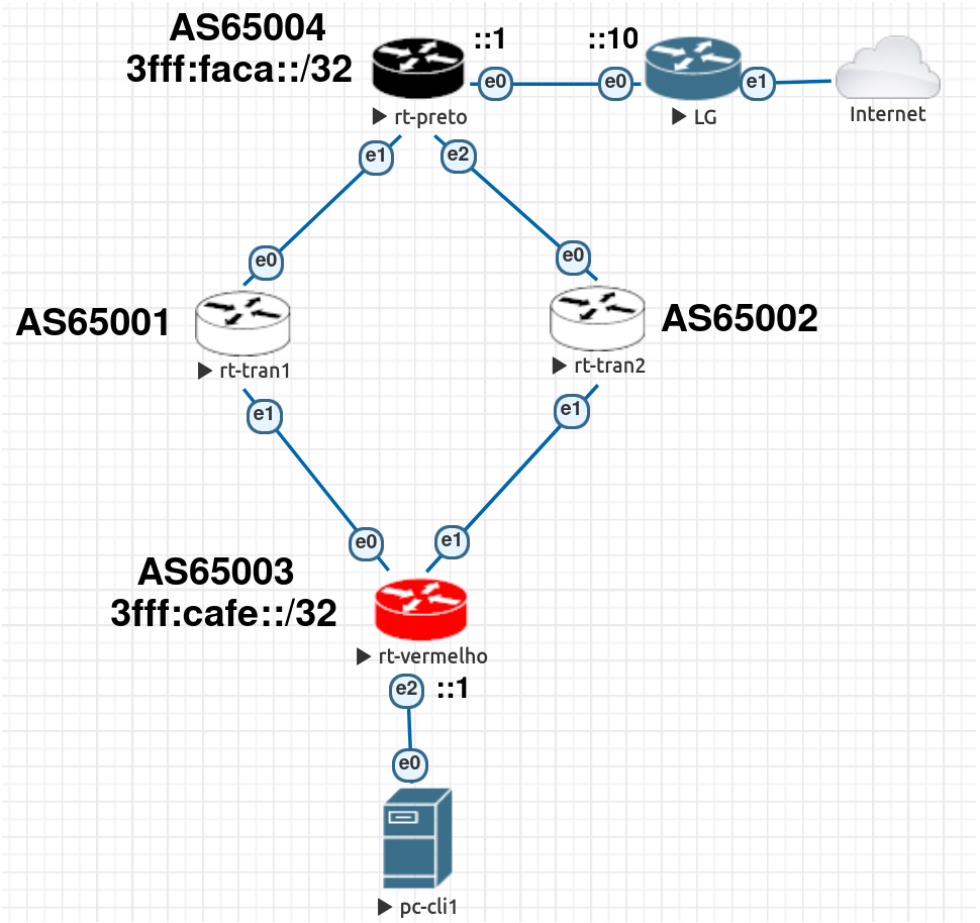

Fig. 1: Topologia Looking Glass

Softwares Utilizados

- **Debian 12 [Bookworm]**
  - https://www.debian.org/releases/bookworm/
- **Hyperglass**
  - https://github.com/thatmattlove/hyperglass
- **Looking Glass by gmazoyer**
  - https://github.com/gmazoyer/looking-glass
- **Docker**
  - https://docs.docker.com/engine/install/debian/

Configurações dos Dispositivos

rt-vermelho

```
frr version 10.4.1
frr defaults traditional
hostname frr-cli
service integrated-vtysh-config
!
ipv6 prefix-list MEU-PREF seq 5 permit 3fff:cafe::/32
!
route-map TRAN1-OUT permit 10
 match ipv6 address prefix-list MEU-PREF
exit
!
route-map TRAN2-OUT permit 10
 match ipv6 address prefix-list MEU-PREF
 set as-path prepend 65003 65003
exit
!
route-map TRAN1-IN permit 10
exit
!
route-map TRAN2-IN permit 10
exit
!
ipv6 route 3fff:cafe::/32 Null0
!
router bgp 65003
 bgp router-id 3.3.3.3
 neighbor 3fff::3 remote-as 65001
 neighbor 3fff::5 remote-as 65002
 !
 address-family ipv6 unicast
  network 3fff:cafe::/32
  neighbor 3fff::3 activate
  neighbor 3fff::3 route-map TRAN1-IN in
  neighbor 3fff::3 route-map TRAN1-OUT out
  neighbor 3fff::5 activate
  neighbor 3fff::5 route-map TRAN2-IN in
  neighbor 3fff::5 route-map TRAN2-OUT out
 exit-address-family
exit
!
```

rt-tran1

```
frr version 10.4.1
frr defaults traditional
hostname frr-cli
service integrated-vtysh-config
!
route-map SAIDA permit 10
exit
!
route-map ENTRADA permit 10
exit
!
router bgp 65001
 bgp router-id 1.1.1.1
 neighbor 3fff::6 remote-as 65004
 neighbor 3fff::2 remote-as 65003
 !
 address-family ipv6 unicast
  neighbor 3fff::6 activate
  neighbor 3fff::2 activate
  neighbor 3fff::6 route-map ENTRADA in
  neighbor 3fff::6 route-map SAIDA out
  neighbor 3fff::2 route-map ENTRADA in
  neighbor 3fff::2 route-map SAIDA out
 exit-address-family
exit
!
```

rt-tran2

```
frr version 10.4.1
frr defaults traditional
hostname frr-cli
service integrated-vtysh-config
!
route-map SAIDA permit 10
exit
!
route-map ENTRADA permit 10
exit
!
router bgp 65002
 bgp router-id 2.2.2.2
 neighbor 3fff::4 remote-as 65003
 neighbor 3fff::8 remote-as 65004
```

```
 !
 address-family ipv6 unicast
  neighbor 3fff::4 activate
  neighbor 3fff::8 activate
  neighbor 3fff::4 route-map ENTRADA in
  neighbor 3fff::4 route-map SAIDA out
  neighbor 3fff::8 route-map ENTRADA in
  neighbor 3fff::8 route-map SAIDA out
 exit-address-family
exit
!
```

rt-preto

```
frr version 10.4.1
frr defaults traditional
hostname rt-preto
service integrated-vtysh-config
!
ipv6 prefix-list MEU-PREF seq 5 permit 3fff:faca::/32
!
route-map SAIDA permit 10
 match ipv6 address prefix-list MEU-PREF
exit
!
route-map SAIDA deny 20
exit
!
route-map ENTRADA permit 10
exit
!
route-map SAIDA-LG permit 10
exit
!
route-map ENTRADA-LG deny 10
exit
!
ipv6 route 3fff:faca::/32 Null0
!
router bgp 65004
 bgp router-id 4.4.4.4
 neighbor 3fff::7 remote-as 65001
 neighbor 3fff::9 remote-as 65002
 neighbor 3fff:faca::10 remote-as 65004
 !
 address-family ipv6 unicast
```

```
  network 3fff:faca::/32
  neighbor 3fff::7 activate
  neighbor 3fff::7 route-map ENTRADA in
  neighbor 3fff::7 route-map SAIDA out
  neighbor 3fff::9 activate
  neighbor 3fff::9 route-map ENTRADA in
  neighbor 3fff::9 route-map SAIDA out
  neighbor 3fff:faca::10 activate
  neighbor 3fff:faca::10 route-map ENTRADA-LG in
  neighbor 3fff:faca::10 route-map SAIDA-LG out
 exit-address-family
exit
!
```

rt-lg

```
frr version 10.4.1
frr defaults traditional
hostname rt-preto
service integrated-vtysh-config
!
route-map ENTRADA-IBGP permit 10
exit
!
router bgp 65004
 bgp router-id 4.4.4.5
 neighbor 3fff:faca::1 remote-as 65004
 !
 address-family ipv6 unicast
  neighbor 3fff:faca::1 activate
  neighbor 3fff:faca::1 route-map ENTRADA-IBGP in
exit
!
```

Instalação e configuração do Looking Glass by gmazoyer

Instalar os pacotes necessários

- Instalar as dependências

```
apt install openssh-server git apache2 libapache2-mod-php php php-xml composer php-sqlite3 sqlite3 -y
```

Criação do ambiente de SSH seguro

- Criar usuário

```
useradd -m -s /bin/bash lguser
```

- Criar diretório para as chaves de SSH

```
mkdir -p /var/www/.ssh
```

- Gerar a chave ssh

```
ssh-keygen -t ed25519 -C "lguser@semanacap11.br"
```

- Mudar permissão do diretório .ssh

```
chown -R www-data:www-data /var/www/.ssh
chmod 700 /var/www/.ssh
```

- Criar o arquivo de chaves autorizadas no diretório *home* do usuário lguser

```
mkdir /home/lguser/.ssh
touch /home/lguser/.ssh/authorized_keys
```

- Inserir a chave pública gerada no arquivo authorized_keys

```
cat /var/www/.ssh/chave_lg.pub > /home/lguser/.ssh/authorized_keys
```

- Mudar a permissão do arquivo de chaves autorizadas

```
chmod 600 /home/lguser/.ssh/authorized_keys
```

- Criar arquivos de comandos permitidos para o usuário

```
vim /home/lguser/.ssh/lg-restricted.sh
```

- Copiar código

```
#!/bin/bash

case "$SSH_ORIGINAL_COMMAND" in
    ' vtysh -c " show bgp ipv6 unicast '*)
        eval "$SSH_ORIGINAL_COMMAND"
```

```
        ;;
    ' vtysh -c " show bgp ipv6 regexp '*)
        eval "$SSH_ORIGINAL_COMMAND"
        ;;
    ' ping6 '*)
        eval "$SSH_ORIGINAL_COMMAND"
        ;;
    ' traceroute '*)
        eval "$SSH_ORIGINAL_COMMAND"
        ;;
    *)
        echo "Acesso Negado."
        exit 1
        ;;
esac
```

- Mudar a permissão do aquivo lg-restricted.sh

```
chmod 700 /home/lguser/.ssh/lg-restricted.sh
```

- Mudar o dono e permissão do diretório

```
chown -R lguser:lguser /home/lguser/.ssh
chmod 700 /home/lguser/.ssh/
```

- Configurar o arquivo /etc/ssh/sshd_config

```
# Mudar endereço IP do serviço de SSH
ListenAddress ::1
# Quais usuário tem permissão para acessar o serviço de SSH
AllowUsers lguser
# Habilitar autenticação utilizado chaves
PubkeyAuthentication yes
# Desabilitar autenticação via senha
PasswordAuthentication no

# Configurações do usuário lguser
Match User lguser
        PasswordAuthentication no
        AuthorizedKeysFile /home/lguser/.ssh/authorized_keys
        AllowTcpForwarding no
        PermitTunnel no
        ForceCommand /home/lguser/.ssh/lg-restricted.sh
        PermitTTY no
        X11Forwarding no
```

- Adicionar o usuário ao grupo frr e frrvty

```
adduser lguser frr && adduser lguser frrvty
```

- Reiniciar o servidor de SSH

```
systemctl restart ssh
```

- Testar a conexão e segurança dos comandos

```
ssh -i chave_lg lguser@::1 ' vtysh -c " show bgp ipv6 unicast "'

ssh -i chave_lg lguser@::1 ' vtysh -c " show bgp ipv6 unicast 3fff:cafe:: "'

ssh -i chave_lg lguser@::1 ' vtysh -c " show ipv6 route "'

ssh -i chave_lg lguser@::1 ' ls -l / '
```

Instalação do Looking Glass by gmazoyer

- Mudar permissão dos arquivos da pasta html

```
chown -R lguser:lguser /var/www/html/
```

- Mudar para o usuário lguser

```
su - lguser
```

- Remover o arquivo index.html

```
rm /var/www/html/index.html
```

- Clonar o repositório oficial e colocar na pasta www

```
git clone https://github.com/gmazoyer/looking-glass.git /var/www/html
```

- Instalar o restante dos pacotes

```
composer install
```

Configuração Básica

- Copiar o config.php.example

```
cp config.php.example config.php
```

- Inserir as configurações no arquivo

```
<?php

/*
 * Main configuration file example.
 *
 * DO NOT EDIT NOR RENAME, please copy to 'config.php' and edit the new file!
```

```
 */

// People to contact
// Set both to null to not display any contact information
$config['contact']['name'] = 'Looking Glass User';
$config['contact']['mail'] = 'lguser@semanacap10.br';

// Frontpage configuration

// Title of the page
$config['frontpage']['title'] = 'Looking Glass SemanaCap';
// Logo to display (remove it to not display any logo)
$config['frontpage']['image'] = 'logo.png';
// Disclaimer to inform people using the looking glass
// Set it to null to not display a disclaimer
$config['frontpage']['disclaimer'] = 'LG da SemanaCap Edição 10!';


// Routers definitions
// Authentication based on SSH with key
// The hostname or the IP address
$config['routers']['router1']['host'] = '[::1]';
// The user to use to connect to the router
$config['routers']['router1']['user'] = 'lguser';
// The public key of the given user
$config['routers']['router1']['private_key'] = '/var/www/.ssh/chave_lg';
// The passphrase of the key (optional if the key has no passphrase)
$config['routers']['router1']['pass'] = 'lg123';
// The authentication mechanism to use (ssh-key for SSH based on keys)
$config['routers']['router1']['auth'] = 'ssh-key';
// The router type (can be cisco, ios, juniper or junos)
$config['routers']['router1']['type'] = 'frr';
$config['routers']['router1']['disable_ipv4'] = true;
// The router source interface to be used
$config['routers']['router1']['source-interface-id'] = '3fff:faca::10';
// The router description to be displayed in the router list
$config['routers']['router1']['desc'] = 'LG do Roteador de Borda Preto';

$config['antispam']['enabled'] = false;
//$config['antispam']['database_file'] = '/var/www/db/lg_antispam.db';

$config['misc']['allow_private_asn'] = true;

// End of config.php
```

- Desativar comandos

```
$config['doc']['bgp']['command'] = null;
$config['doc']['as-path-regex']['command'] = null;
$config['doc']['as']['command'] = null;
$config['doc']['ping']['command'] = null;
$config['doc']['traceroute']['command'] = null;
```

- Colocar comando personalizado

```
$config['doc']['bgp']['command'] = 'show bgp ipv6 unicast';
$config['doc']['bgp']['description'] = 'Mostra as rotas recebidas via BGP';
$config['doc']['bgp']['parameter'] = 'Aqui você mostra como usar o <strong>comando</strong>';
```

Ativar o AntiSpam

- Criar o arquivo que será utilizado pelo sqlite

```
mkdir /var/www/anti-spam/
touch /var/www/anti-spam/lg.sqlite
```

- Setar as permissões

```
chown -R www-data:www-data /var/www/anti-spam/
chmod -R 700 /var/www/anti-spam
```

- Adicionar configuração no arquivo config.php

```
$config['antispam']['enabled'] = true;
$config['antispam']['database_file'] = '/var/www/anti-spam/lg.sqlite';
```

- Verificar informações no DB

```
# Entrar no banco de dados
sqlite3 /var/www/anti-spam/lg.sqlite

# Listar tabelas
.tables

#Exibir informações da tabela users
SELECT * FROM users;

# Apagar todos os registros da tabela users
DELETE FROM users;
```

Instalação e configuração do Hyperglass

Criação do ambiente de SSH seguro

- Instalar servidor de SSH

```
apt install openssh-server -y
```

- Criar usuário

```
useradd -m -s /bin/bash lguser
```

- Adicionar o usuário ao grupo frr e frrvty

```
adduser lguser frr && adduser lguser frrvty
```

- Criar diretório para a chaves de SSH

```
mkdir -p /etc/hyperglass/.ssh
```

- Gerar a chave ssh

```
ssh-keygen -t ed25519 -C "lguser@semanacap11.br"
```

- Mudar permissão do diretório

```
chmod 700 /etc/hyperglass/.ssh/
```

- Criar o arquivo de chaves autorizadas

```
mkdir /home/lguser/.ssh
touch /home/lguser/.ssh/authorized_keys
```

- Inserir a chave publica no arquivo

```
cat /etc/hyperglass/.ssh/chave_hyperglass.pub > /home/lguser/.ssh/authorized_keys
```

- Mudar a permissão do arquivo de chaves autorizadas

```
chmod 600 /home/lguser/.ssh/authorized_keys
```

- Mudar o dono e permissão do diretório

```
chown -R lguser:lguser /home/lguser/.ssh
chmod 700 /home/lguser/.ssh/
```

- Criar pasta para os commandos

```
mkdir /opt/comandos-lguser
```

- Criar link para os commandos

```
ln -s /usr/bin/vtysh /opt/comandos-lguser/vtysh
```

```
ln -s /usr/bin/ping /opt/comandos-lguser/ping
ln -s /usr/bin/traceroute /opt/comandos-lguser/traceroute
```

- Mudar PATH to usuário

```
echo "export PATH=/opt/comandos-lguser" >| /home/lguser/.profile
```

- Mudar permissões do serviço de SSH

```
# Mudar endereço IP do serviço de SSH
ListenAddress 3fff:faca:1::1
# Quais usuário tem permissão para acessar o serviço de SSH e suas redes de origem
AllowUsers lguser@3fff:faca:1::100
# Habilitar autenticação utilizado chaves
PubkeyAuthentication yes
# Desabilitar autenticação via senha
PasswordAuthentication no

# Configurações do usuário lguser
Match User lguser Address 3fff:faca:1::100
   PasswordAuthentication no
   AuthorizedKeysFile /home/lguser/.ssh/authorized_keys
   ForceCommand /bin/rbash -l
   AllowTcpForwarding no
   PermitTunnel no
   X11Forwarding no
```

- Reiniciar o servidor de SSH
- Regra de ip6tables

```
ip6tables -A INPUT -p tcp -s 3fff:faca:1::100 --dport 22 -j ACCEPT
ip6tables -A INPUT -p tcp -s ::1 --dport 22 -j ACCEPT
ip6tables -A INPUT -p tcp --dport 22 -j DROP
```

Instalação do Docker

- Adicionar a chave do respositório

```
apt update

apt install ca-certificates curl

install -m 0755 -d /etc/apt/keyrings
curl -fsSL https://download.docker.com/linux/debian/gpg -o /etc/apt/keyrings/
docker.asc
chmod a+r /etc/apt/keyrings/docker.asc
```

- Adicionar o repositório oficial

```
echo \
"deb [arch=$(dpkg --print-architecture) signed-by=/etc/apt/keyrings/docker.asc]
https://download.docker.com/linux/debian \
$(. /etc/os-release && echo "$VERSION_CODENAME") stable" | \
tee /etc/apt/sources.list.d/docker.list > /dev/null

apt update
```

- Instalar o Docker

```
apt install docker-ce docker-ce-cli containerd.io docker-buildx-plugin docker-
compose-plugin -y
```

- Testar o docker

```
docker run hello-world
```

Comandos úteis do docker

- Listar containers em funcionamento

```
docker ps
```

- Listar as redes do docker

```
docker network ls
```

- Ver logs de um container

```
# Use a opção -f para acompanhar em tempo real
docker logs <nome-do-container>
```

- Parar todos os container

```
docker stop $(docker ps -a -q)
```

- Apagar todos os containers (use com cuidado)

```
docker rm $(docker ps -a -q)
```

- Docker CLI Cheatsheet
  - https://docs.docker.com/get-started/docker_cheatsheet.pdf

Instalação do HyperGlass

- Instalar o hyperglass

```
mkdir /etc/hyperglass
cd /opt
git clone https://github.com/thatmattlove/hyperglass.git --depth=1
cd /opt/hyperglass
```

- Criar serviço no systemd

```
cp /opt/hyperglass/.samples/hyperglass-docker.service /etc/hyperglass/
hyperglass.service
ln -s /etc/hyperglass/hyperglass.service /etc/systemd/system/hyperglass.service
systemctl daemon-reload
systemctl enable hyperglass
```

- Criar arquivo de env

```
touch /etc/hyperglass/hyperglass.env
```

- Copiar arquivo de sample

```
cp .samples/sample_devices.yaml /etc/hyperglass/devices.yaml
```

- Criar interface

```
docker network create \
    --driver=bridge \
    --ipv6 \
    --subnet 3fff:faca:1::/64 \
    --gateway=3fff:faca:1::1 \
    -o com.docker.network.bridge.trusted_host_interfaces="ens3" hyperglass
```

- Editar o compose.yaml

```
services:
    redis:
        image: "redis:alpine"
        networks:
            - hyperglass

    hyperglass:
        depends_on:
            - redis
        environment:
            - HYPERGLASS_APP_PATH=/etc/hyperglass
            - HYPERGLASS_HOST=${HYPERGLASS_HOST-::}
            - HYPERGLASS_PORT=${HYPERGLASS_PORT-8001}
            - HYPERGLASS_DEBUG=${HYPERGLASS_DEBUG-false}
            - HYPERGLASS_DEV_MODE=${HYPERGLASS_DEV_MODE-false}
            - HYPERGLASS_REDIS_HOST=${HYPERGLASS_REDIS_HOST-redis}
            - HYPEGLASS_DISABLE_UI=${HYPEGLASS_DISABLE_UI-false}
            - HYPERGLASS_CONTAINER=${HYPERGLASS_CONTAINER-true}
            - HYPERGLASS_ORIGINAL_APP_PATH=${HYPERGLASS_APP_PATH}
        build: .
        ports:
```

```
            - "${HYPERGLASS_PORT-8001}:${HYPERGLASS_PORT-8001}"
        volumes:
            - ${HYPERGLASS_APP_PATH-/etc/hyperglass}:/etc/hyperglass
        networks:
            hyperglass:
                ipv6_address: 3fff:faca:1::100
        secrets:
            - chave_ssh

networks:
       hyperglass:
               external: true

secrets:
  chave_ssh:
    file: /etc/hyperglass/.ssh/chave_hyperglass
```

- Iniciar o hyperglass

```
systemctl start hyperglass
```

Configuração de dispositivos

- Arquivo devices.yaml

```
devices:
  - name: Roteador Preto
    address: 3fff:faca:1::1
    credential:
      username: lguser
      key: /run/secrets/chave_ssh
    platform: frr
    attrs:
      source4: 127.0.0.1
      source6: 3fff:faca:1::1
    directives:
      - builtins: false
      - show-bgp-route-frr
      - show-bgp-regexp-frr
      - ping
      - traceroute
```

- Arquivo directives.yaml

```
show-bgp-route-frr:
  name: BGP Route (FRR IPv6)
  rules:
    - condition: '.*'
```

```
      action: permit
      command: 'vtysh -c "show bgp ipv6 unicast {target}"'
  field:
      description: "Prefixo"

show-bgp-regexp-frr:
  name: BGP Regexp (FRR IPv6)
  rules:
    - condition: '.*'
      action: permit
      command: 'vtysh -c "show bgp ipv6 regexp {target}"'
  field:
      description: "AS Regex"

ping:
  name: Ping( IPv6)
  rules:
    - condition: '^((([0-9a-fA-F]{1,4}:){7,7}[0-9a-fA-F]{1,4})|(([0-9a-fA-F]{1,4}:)
{1,7}:)|(:(:[0-9a-fA-F]{1,4}){1,7})|(([0-9a-fA-F]{1,4}:){1,6}:[0-9a-fA-F]{1,4})|
(([0-9a-fA-F]{1,4}:){1,5}(:[0-9a-fA-F]{1,4}){1,2})|(([0-9a-fA-F]{1,4}:){1,4}(:[0-9a-
fA-F]{1,4}){1,3})|(([0-9a-fA-F]{1,4}:){1,3}(:[0-9a-fA-F]{1,4}){1,4})|(([0-9a-fA-F]
{1,4}:){1,2}(:[0-9a-fA-F]{1,4}){1,5})|([0-9a-fA-F]{1,4}:((:[0-9a-fA-F]{1,4}){1,6})))/?
(12[0-8]|1[0-1][0-9]|[1-9][0-9]|[0-9])$'
      action: permit
      command: 'ping -6 -c4 {target}'
  field:
      description: "Endereço IPv6"

traceroute:
  name: Traceroute ( IPv6)
  rules:
    - condition: '.*'
      action: permit
      command: 'traceroute {target}'
  field:
      description: "Endereço IPv6"
```

Referências

- Lista de Looking Glass BPF
  - https://wiki.brasilpeeringforum.org/w/Looking_Glass
- Como Ter Seu Proprio Looking Glass
  - https://wiki.brasilpeeringforum.org/w/Como_Ter_Seu_Proprio_Looking_Glass
- Desvendando o Looking Glass (Semana de Infraestrutura 2023)
  - https://ftp.registro.br/pub/gter/gter52/07-Looking-Glass-Provedores.pdf
- Hyperglass
  - https://github.com/thatmattlove/hyperglass
- Looking Glass by gmazoyer
  - https://github.com/gmazoyer/looking-glass
- Instalação Docker (Debian)
  - https://docs.docker.com/desktop/setup/install/linux/debian/